ID: 1405276
Cookbook: browseurl.jbs
Time: 09:11:05
Date: 08/03/2024
Version: 40.0.0 Tourmaline

Table of Contents

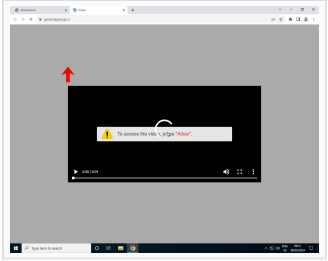
Windows Analysis Report

http://gossnabgroup.ru

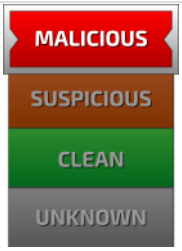
Overview

General Information

Sample URL:	http://gossnabgroup.ru
Analysis ID:	1405276
Infos:	



Detection

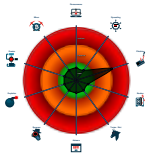


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dom…
- Phishing site detected (based on OC…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5084 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 5932 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=2344 --field-trial-handle=2284,i,3100902536086182891,1735761918452591964,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6428 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://gossnabgroup.ru MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

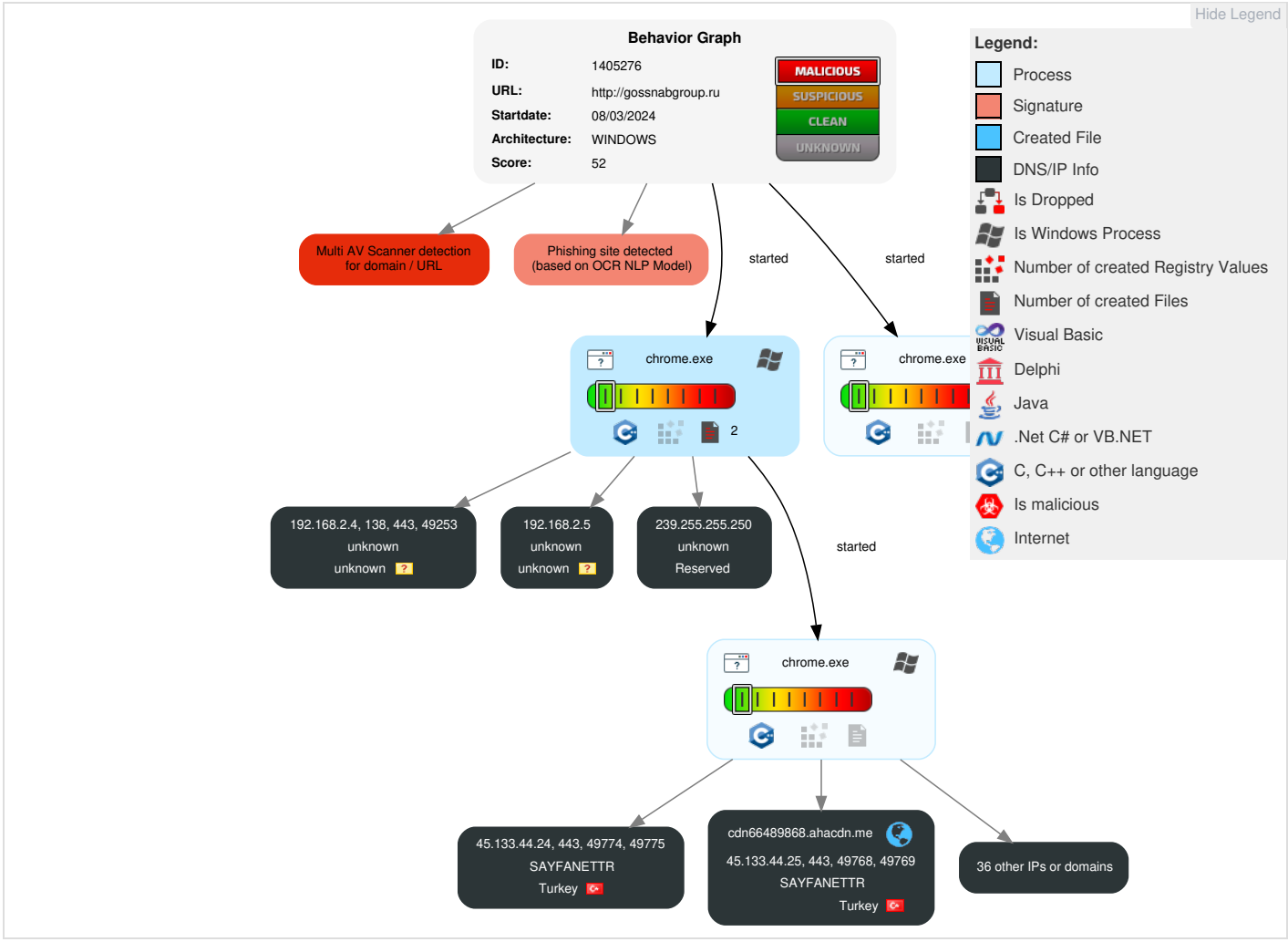
Phishing

Phishing site detected (based on OCR NLP Model)

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	3 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	4 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

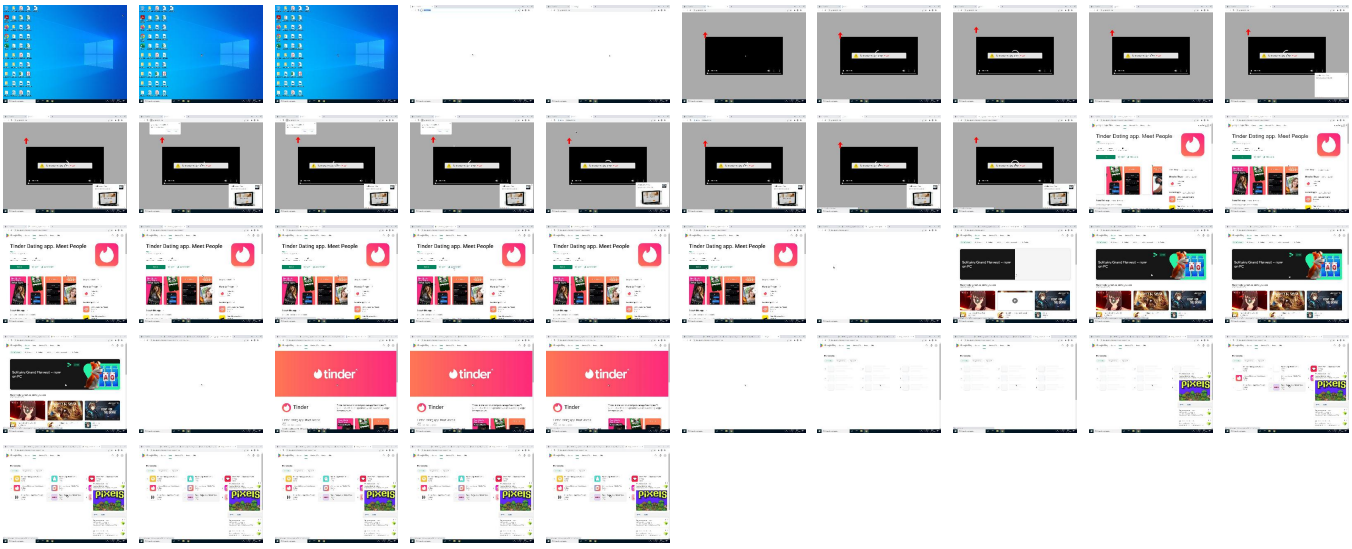
Behavior Graph

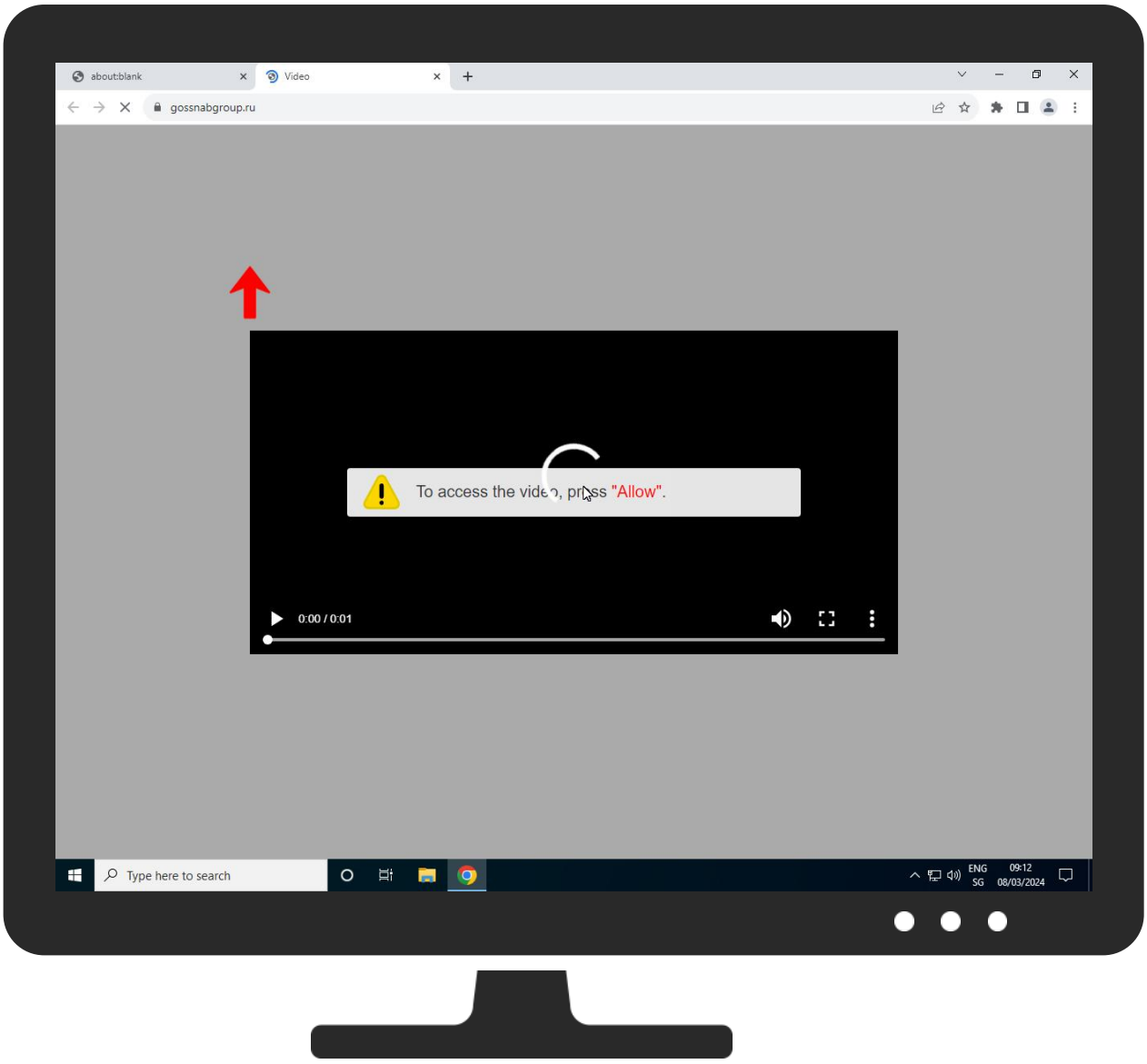


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://gossnabgroup.ru	0%	Virustotal		Browse
http://gossnabgroup.ru	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
storage.multstorage.com	0%	Virustotal		Browse
fp2e7a.wpc.phicdn.net	0%	Virustotal		Browse
fp.metricswpsh.com	2%	Virustotal		Browse
cdn.gdns.revopush.com	2%	Virustotal		Browse
winrenew-cash.life	12%	Virustotal		Browse
notification.tubecup.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
nereserv.com	1%	Virustotal		Browse
js.nextpsh.top	10%	Virustotal		Browse
gossnabgroup.ru	0%	Virustotal		Browse
ntvpforever.com	1%	Virustotal		Browse
subscribers.production.wpu.sh	0%	Virustotal		Browse
us.superfasti.co	0%	Virustotal		Browse
js.wpshsdk.com	2%	Virustotal		Browse
sw.wpushorg.com	0%	Virustotal		Browse
js.capndr.com	0%	Virustotal		Browse
js.wpadmngr.com	0%	Virustotal		Browse
img.cdn.house	0%	Virustotal		Browse
cdn.stgcdn.com	0%	Virustotal		Browse
e32350d110.84bfe218ba.com	2%	Virustotal		Browse

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/tools/feedback/	0%	URL Reputation	safe	
http://https://biz-qa.gcp.wazestg.com	0%	Avira URL Cloud	safe	
http://https://gweb-nextregistration.appspot.com	0%	Avira URL Cloud	safe	
about:blank	0%	Avira URL Cloud	safe	
http://https://www.gstatic.c..?/recaptcha/releases/QquE1_MNjnFHgZF4HPsEcf_2/recaptcha__.	0%	Avira URL Cloud	safe	
http://https://www.editionsatplay.com	0%	Avira URL Cloud	safe	
http://https://cdn.stgcdn.com/files/6b7c183bc5faf7a9ba96b9f945eeaf83.jpg	0%	Avira URL Cloud	safe	
http://https://img.cdn.house/i/1/u5KMKIF1XZfyyXSH2MpUbH2gGje5Q5HBBLuJA3hGbrFW1WEPRUiVcPSx_hAXrkQldf-rX65sD79Uc-SKXQkvZPNwBU7iD03bMSjmtdPw4cm7R2K0Q-7mN3XXe3eFbY3dY5YklvpV7IhWHTK7Lz2mCVB4SwtnRNY-fPbYFYv06ftRTle1CclVWnajhWb9ATfHLGmqUqikBuJKRYvt	0%	Avira URL Cloud	safe	
http://https://biz-qa.gcp.wazestg.com	0%	Virustotal		Browse
http://https://www.editionsatplay.com	0%	Virustotal		Browse
http://https://console.cloud.google	0%	Avira URL Cloud	safe	
http://https://payments-demoserver-sandbox.corp.cloud.google	0%	Avira URL Cloud	safe	
http://https://3-dot-gweb-io2016-registration.appspot.com	0%	Avira URL Cloud	safe	
http://https://js.wpshsdk.com/npc/sdk/push/styles.css	0%	Avira URL Cloud	safe	
http://https://console.cloud.google	0%	Virustotal		Browse
http://https://payments.cloud.google	0%	Avira URL Cloud	safe	
http://https://biz.gcp.wazestg.com	0%	Avira URL Cloud	safe	
http://https://gweb-nextregistration.appspot.com	0%	Virustotal		Browse
http://https://3-dot-gweb-io2016-registration.appspot.com	0%	Virustotal		Browse
http://https://nik.googlegoro.com	0%	Avira URL Cloud	safe	
http://https://js.wpshsdk.com/npc/sdk/push/styles.css	1%	Virustotal		Browse
http://https://payments-demoserver-sandbox.corp.cloud.google	0%	Virustotal		Browse
http://https://biz.gcp.wazestg.com	0%	Virustotal		Browse
http://https://arctic-ocean-116022.appspot.com	0%	Virustotal		Browse
http://https://arctic-ocean-116022.appspot.com	0%	Avira URL Cloud	safe	
http://https://payments.cloud.google	0%	Virustotal		Browse
http://https://js.wpadmngr.com/push/badges/love-letter.png	0%	Avira URL Cloud	safe	
http://https://notification.tubecup.net/in/multy	0%	Avira URL Cloud	safe	
http://https://taylormarshall-dot-test-dot-402-bslatkin-staging.appspot.com	0%	Avira URL Cloud	safe	
http://https://js.wpshsdk.com/npc/sdk/common/config.js	0%	Avira URL Cloud	safe	
http://https://defjam-staging.appspot.com	0%	Avira URL Cloud	safe	
http://https://googlecommassage-hrd.appspot.com	0%	Avira URL Cloud	safe	
http://https://nik.googlegoro.com	0%	Virustotal		Browse
http://https://clientlog.cloud.google/log?format=json&hasfast=true	0%	Avira URL Cloud	safe	
http://https://taylormarshall-dot-test-dot-402-bslatkin-staging.appspot.com	0%	Virustotal		Browse
http://https://js.wpadmngr.com/push/badges/pill.png	0%	Avira URL Cloud	safe	
http://https://cdn.stgcdn.com/files/439950858060922bf976c7a20645da7a.jpg	0%	Avira URL Cloud	safe	
http://https://website-dot-cl-syd-eap.appspot.com	0%	Avira URL Cloud	safe	
http://https://js.wpshsdk.com/npc/sdk/common/config.js	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://bddb2d2561.62b81f5af3.com/9dc01d48437911a2369d0f0f8dd84903.js	0%	Avira URL Cloud	safe	
http://https://defjam-staging.appspot.com	0%	Virustotal		Browse
http://https://dev-dot-gweb-nextregistration.appspot.com	0%	Avira URL Cloud	safe	
http://https://biz-beta-row.witools.foo	0%	Avira URL Cloud	safe	
http://https://notification.tubecup.net/in/multy	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
storage.multstorage.com	104.21.30.242	true	false	• 0%, Virustotal, Browse	unknown
i.ytimg.com	142.250.141.119	true	false		high
js.nextpsh.top	104.21.39.40	true	false	• 10%, Virustotal, Browse	unknown
mobile-gtalk.l.google.com	142.251.2.188	true	false		high
gossnabgroup.ru	172.67.210.214	true	false	• 0%, Virustotal, Browse	unknown
nereserv.com	94.130.198.6	true	false	• 1%, Virustotal, Browse	unknown
fp2e7a.wpc.phicdn.net	192.229.211.108	true	false	• 0%, Virustotal, Browse	unknown
stats.g.doubleclick.net	142.250.141.155	true	false		high
cdn28786515.ahacdn.me	45.133.44.52	true	false		high
fp.metricswpsh.com	157.90.84.242	true	false	• 2%, Virustotal, Browse	unknown
play-lh.googleusercontent.com	142.251.2.119	true	false		high
www.google.com	142.251.2.99	true	false		high
winrenew-cash.life	185.155.184.32	true	false	• 12%, Virustotal, Browse	unknown
cdn.gdns.revopush.com	95.216.14.117	true	false	• 2%, Virustotal, Browse	unknown
android.l.google.com	142.250.101.100	true	false		high
cdn66489868.ahacdn.me	45.133.44.25	true	false		high
cdn.adx1.com	31.204.132.207	true	false		high
plus.l.google.com	142.251.2.113	true	false		high
cdn44221613.ahacdn.me	45.133.44.53	true	false		high
notification.tubecup.net	88.198.204.166	true	false	• 0%, Virustotal, Browse	unknown
payments.google.com	142.251.2.92	true	false		high
play.google.com	142.250.141.100	true	false		high
ntvpforever.com	94.130.198.6	true	false	• 1%, Virustotal, Browse	unknown
us.superfasti.co	109.200.209.143	true	false	• 0%, Virustotal, Browse	unknown
subscribers.production.wpu.sh	178.62.192.95	true	false	• 0%, Virustotal, Browse	unknown
js.wpadmngr.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
bddb2d2561.62b81f5af3.com	unknown	unknown	false		unknown
img.cdn.house	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
js.wpshsdk.com	unknown	unknown	false	• 2%, Virustotal, Browse	unknown
sw.wpushorg.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
js.capndr.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
e32350d110.84bfe218ba.com	unknown	unknown	false	• 2%, Virustotal, Browse	unknown
cdn.stgcdn.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
e1f6a352a1.3ea94c3718.com	unknown	unknown	false		unknown
static.bookmsg.com	unknown	unknown	false		unknown
apis.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://play-lh.googleusercontent.com/La2XvLnJqNI5JyshQ5RfxM18zHduji9KPgNge93Ibwpjc7znBZVYuuwJ4ycGk6T-DQ=s64-rw	false		high
http://https://play-lh.googleusercontent.com/2YgTmjjbsOwLZ4vwROj2MhYIMFoaNHYbGg50Y-Yt_DG9e6h0-cyIFw701szgbFrgCNo=w526-h296-rw	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j101&tid=UA-19995903-1&cid=1169434221.1709885559&jid=1062486233&gjid=541615713&_gid=1992863761.1709885559&_u=YEBAAEAAAAAAACgDI~&z=1467949968	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://i.ytimg.com/vi/C4uzmiVn8Og/hqdefault.jpg	false		high
http://https://play-lh.googleusercontent.com/z950eFx-wowoAV2KgHast5YFcrxoGJtY18fYd_eMgvEDVn8_tsJwApy4Dbs1iqE2tAjX=s64-rw	false		high
http://https://play-lh.googleusercontent.com/fDpoqIbZ884ylRnMK8Lx9Fu4DsLQk5yt4f9WkxeOAPpGnzc9BTi_YKkMsLvoMdx7Uzg=s256-rw	false		high
http://https://play.google.com/store/apps/details?id=com.tinder	false		high
about:blank	false	• Avira URL Cloud: safe	low
http://https://play-lh.googleusercontent.com/a-/ALV-UjVEDgFjAocMId0v2Cxmm6MLmoD7yzAcB5ZdgKwNXzXXyFM=s32-rw	false		high
http://https://play-lh.googleusercontent.com/a-/ALV-UjWH6jUBtSGI7BBubov7tNbYm6JMKCh-M4rpyCwDH5Hzgz8=s32-rw	false		high
http://https://play-lh.googleusercontent.com/vTMochUbMqk9ehiZ7npCcwvhzOX8x0GlN1EHTW8sg58GBkcF48Vf6fwbvag5KwHxLA=s64-rw	false		high
http://https://cdn.stgcdn.com/files/6b7c183bc5faf7a9ba96b9f945eeaf83.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j101&tid=UA-19995903-1&cid=1169434221.1709885559&jid=1062486233&_u=YEBAAEAAAAAAACgDI~&z=659014817	false		high
http://https://play-lh.googleusercontent.com/12USW7aflgz466ifDehKTnMoAep_VHxDmKJ6jEBoDZWCSefOC-ThRX14Mqe0r8KF9XCzrpMqJts=s20-rw	false		high
http://https://img.cdn.house/i/1/u5KMKIF1XZfyyXSH2MpUbH2gGje5Q5HBBLuJA3hGbrFW1WEPRUiVcPSx_hAXrkQldf-rX65sD79Uc-SKXQkvZPNwBU7iD03bMSjmtdPw4cm7R2K0Q-7mN3XXe3eFbY3dY5YklvpV7IhWHTK7Lz2mCVB4SwtnRNY-fPbYFYv06ftRTIe1CclVWnajhWb9ATfHLGmqUqikBuJKRYvt	false	• Avira URL Cloud: safe	unknown
http://https://play-lh.googleusercontent.com/NVUOs8Vh4nvaP1pTvdrmhfzpy5rYZcWJl13uxyLjRCWZmEubC1PyjihCCi2TCO9FfQ=w526-h296-rw	false		high
http://https://play-lh.googleusercontent.com/D4DUUFQDCsH9NIEa8hjMjQSWdtNhGX1Fd_jT-23ogAb5uMMqttqQDUJcUt4K_u8RYOQ=s64-rw	false		high
http://https://play-lh.googleusercontent.com/KsCewcbhguiV2WXb5o-NM28xhZlhukM1JWU__L7POklqA3CP2DFXVfco8b4acM3wWHg=s64-rw	false		high
http://https://js.wpshsdk.com/npc/sdk/push/styles.css	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://play-lh.googleusercontent.com/Kjxf_QViKaL8tmk2R2gtNr8teHl7Oz9bO5ckWZkvKa5w4h7Q2eb4gYa5cjPhAyn3d3NYAfJ8XQnH=w648-h364-rw	false		high
http://https://js.wpadmngr.com/push/badges/love-letter.png	false	• Avira URL Cloud: safe	unknown
http://https://notification.tubecup.net/in/multy	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://js.wpshsdk.com/npc/sdk/common/config.js	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://play-lh.googleusercontent.com/IEbtDFfx84oGJxAjMuGDOEA3gRpDqhePZ2pAkpdz2GAPBLp8Pyg5SP5AAVstmPSeSQ=s64-rw	false		high
http://https://play-lh.googleusercontent.com/byNQj20XRp7MfIVK7WryqB4jdyZceL087ABgIjwzZqw9y339Nz0_KLS_1B7ak51QLEg=s64-rw	false		high
http://https://play-lh.googleusercontent.com/9u1xt67PewWfe0nfh-ShHdyrNIDUi-eKyc73T2QBUPyWQWBn1Fnr_R2rxquLSnQdrZVe9rbFXi3u=w648-h364-rw	false		high
http://https://js.wpadmngr.com/push/badges/pill.png	false	• Avira URL Cloud: safe	unknown
http://https://cdn.stgcdn.com/files/439950858060922bf976c7a20645da7a.jpg	false	• Avira URL Cloud: safe	unknown
http://https://bddb2d2561.62b81f5af3.com/9dc01d48437911a2369d0f0f8dd84903.js	false	• Avira URL Cloud: safe	unknown
http://https://gossnabgroup.ru/	false		unknown
http://https://www.google.com/tools/feedback/chat_load.js	false		high
http://https://play-lh.googleusercontent.com/Y9BUoMIWfhZDUFZ_MxQmnsgSyb3O8s8Sds65E_j46-vdDSJi_0Xqmoa-fHaQa7fGlw=s64-rw	false		high
http://https://i.ytimg.com/vi/-wpM1XofnD8/hqdefault.jpg	false		high
http://https://play-lh.googleusercontent.com/OmRFgoSS-iZDwzkMpygYEjbBkpY-_fpE2CEiEgj2KG0yoj2DcP01fbGMutWEf8ip2tiv=s64-rw	false		high

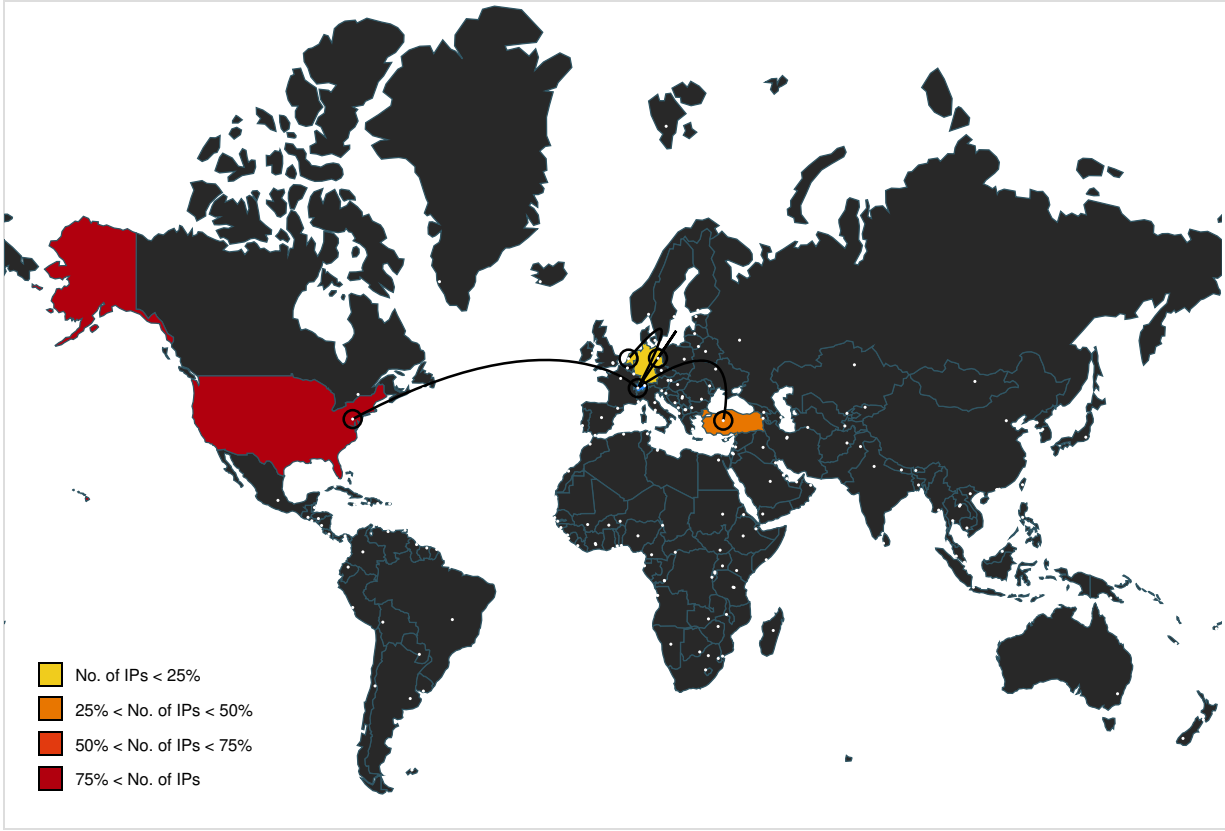
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stats.g.doubleclick.net/g/collect	chromecache_203.2.dr	false		high
http://https://feedback.googleusercontent.com/resources/annotator.css	chromecache_313.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://developers.google.com/recaptcha/docs/faq#localhost_support	chromecache_376.2.dr	false		high
http://https://apis.google.com/js/client.js	chromecache_313.2.dr	false		high
http://https://support.google.com	chromecache_297.2.dr, chromecache_266.2.dr, chromecache_235.2.dr, chromecache_304.2.dr, chromecache_378.2.dr	false		high
http://https://massage-hrd-dev.googleplex.com	chromecache_304.2.dr	false		high
http://https://biz-qa.gcp.wazestg.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://localhost.proxy.googlers.com/inapp/	chromecache_313.2.dr	false	• URL Reputation: safe	unknown
http://https://gweb-nextregistration.appspot.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://stagingqual-feedback-pa-googleapis.sandbox.google.com	chromecache_313.2.dr	false		high
http://https://ampcid.google.com/v1/publisher:getClientId	chromecache_358.2.dr	false		high
http://https://home.ft.nest.com	chromecache_304.2.dr	false		high
http://https://www.youtube.com	chromecache_304.2.dr	false		high
http://https://checkout.youtube.com	chromecache_304.2.dr	false		high
http://https://vector-customer.googleplex.com/	chromecache_304.2.dr	false		high
http://https://www.gstatic.c..?/recaptcha/releases/QquE1_MNjnFHgZF4HPsEcf_2/recaptcha__.	chromecache_376.2.dr	false	• Avira URL Cloud: safe	low
http://https://pay.google.com/gp/v/widget/save	chromecache_212.2.dr	false		high
http://https://www.editionsatplay.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://support.google.com/recaptcha/#6175971	chromecache_376.2.dr	false		high
http://https://policies.google.com/terms;target;_blank;class;cOP9Jc	chromecache_251.2.dr	false		high
http://https://www.google.com/shopping/customerreviews/optin?usegapi=1	chromecache_212.2.dr	false		high
http://https://asx-frontend-autopush.corp.google.co.uk/tools/feedback/	chromecache_313.2.dr	false	• URL Reputation: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	chromecache_358.2.dr	false		high
http://https://support.google.com/googleplay/?p=report_content	chromecache_251.2.dr, chromecache_246.2.dr	false		high
http://https://support.google.com/recaptcha	chromecache_376.2.dr	false		high
http://https://console.cloud.google	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/tools/feedback	chromecache_313.2.dr, chromecache_339.2.dr	false		high
http://https://payments-demoserver-sandbox.corp.cloud.google	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sandbox.google.com/inapp/%	chromecache_313.2.dr	false		high
http://https://3-dot-gweb-io2016-registration.appspot.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://apis.google.com/js/api.js	chromecache_212.2.dr, chromecache_331.2.dr, chromecache_275.2.dr, chromecache_168.2.dr, chromecache_202.2.dr	false		high
http://https://payments.cloud.google	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/tools/feedback/	chromecache_313.2.dr	false		high
http://https://www.youtube.com/subscribe_embed?usegapi=1	chromecache_212.2.dr	false		high
http://https://biz.gcp.wazestg.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://schema.org	chromecache_251.2.dr	false		high
http://https://nik.googlegoro.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://feedback2-test.corp.google.com/tools/feedback/%	chromecache_313.2.dr	false		high
http://https://arctic-ocean-116022.appspot.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://plus.google.com	chromecache_309.2.dr	false		high
http://https://developers.google.com/recaptcha/docs/faq#my-computer-or-network-may-be-sending-automated-que	chromecache_376.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asx-frontend-autopush.corp.google.de/tools/feedback/	chromecache_313.2.dr	false		high
http://https://asx-frontend-autopush.corp.google.com/inapp/	chromecache_313.2.dr	false		high
http://https://feedback.googleusercontent.com/resources/render_frame2.html	chromecache_313.2.dr	false		high
http://https://sandbox.google.com/tools/feedback/%	chromecache_313.2.dr	false		high
http://https://taylormarshall-dot-test-dot-402-bslatkin-staging.appspot.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/g/collect?v=2&	chromecache_203.2.dr	false		high
http://https://play.google.com/work/embedded/search?usegapi=1&usegapi=1	chromecache_212.2.dr	false		high
http://https://policies.google.com/privacy	chromecache_322.2.dr, chromecache_300.2.dr, chromecache_251.2.dr, chromecache_332.2.dr, chromecache_246.2.dr, chromecache_377.2.dr, chromecache_371.2.dr, chromecache_169.2.dr	false		high
http://https://defjam-staging.appspot.com	chromecache_304.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://googlecommassage-hrd.appspot.com	chromecache_304.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://clientlog.cloud.google/log?format=json&hasfast=true	chromecache_304.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://yt-web-release.corp.youtube.com	chromecache_304.2.dr	false		high
http://https://website-dot-cl-syd-eap.appspot.com	chromecache_304.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://payments.sandbox.google.com/payments/v4/js/integrator.js?rk=1	chromecache_207.2.dr, chromecache_345.2.dr	false		high
http://https://play.google.com	chromecache_297.2.dr, chromecache_266.2.dr, chromecache_235.2.dr, chromecache_304.2.dr, chromecache_378.2.dr	false		high
http://https://biz-beta-row.witools.foo	chromecache_304.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://major.home.integration.nestlabs.com	chromecache_304.2.dr	false		high
http://https://www.google.com/log?format=json&hasfast=true	chromecache_331.2.dr, chromecache_275.2.dr, chromecache_168.2.dr, chromecache_202.2.dr	false		high
http://https://support.google.com/inapp/%	chromecache_313.2.dr	false		high
http://https://youtube-xsell-tool-stg.googleplex.com	chromecache_304.2.dr	false		high
http://https://vector-perf-customer.googleplex.com/	chromecache_304.2.dr	false		high
http://https://cloud.google.com/contact	chromecache_376.2.dr	false		high
http://https://www.google.com/shopping/customerreviews/badge?usegapi=1	chromecache_212.2.dr	false		high
http://https://dev-dot-gweb-nextregistration.appspot.com	chromecache_304.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com/savetodrivebutton?usegapi=1	chromecache_212.2.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.133.44.25	cdn66489868.ahacdn.me	Turkey		59447	SAYFANETTR	false
185.155.184.32	winrenew-cash.life	Switzerland		44160	INTERNETONEInternetServicesProviderIT	false
45.133.44.24	unknown	Turkey		59447	SAYFANETTR	false
94.130.198.6	nereserv.com	Germany		24940	HETZNER-ASDE	false
109.200.209.143	us.superfasti.co	Netherlands		49544	I3DNETNL	false
178.62.192.95	subscribers.production.wpu.sh	European Union		14061	DIGITALOCEAN-ASNUS	false
104.21.30.242	storage.multstorage.com	United States		13335	CLOUDFLARENETUS	false
88.198.204.166	notification.tubecup.net	Germany		24940	HETZNER-ASDE	false
142.251.2.119	play-lh.googleusercontent.com	United States		15169	GOOGLEUS	false
157.90.84.242	fp.metricswpsh.com	United States		766	REDIRISRedIRISAutonomousSystemES	false
142.251.2.99	www.google.com	United States		15169	GOOGLEUS	false
104.21.39.40	js.nextpsh.top	United States		13335	CLOUDFLARENETUS	false
167.235.163.216	unknown	United States		3525	ALBERTSONSUS	false
45.133.44.53	cdn44221613.ahacdn.me	Turkey		59447	SAYFANETTR	false
45.133.44.52	cdn28786515.ahacdn.me	Turkey		59447	SAYFANETTR	false
142.250.101.100	android.l.google.com	United States		15169	GOOGLEUS	false
142.251.2.92	payments.google.com	United States		15169	GOOGLEUS	false
142.250.101.99	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.67.210.214	gossnabgroup.ru	United States		13335	CLOUDFLARENETUS	false
142.250.141.119	i.ytimg.com	United States		15169	GOOGLEUS	false
31.204.132.207	cdn.adx1.com	Netherlands		49544	I3DNETNL	false
95.216.14.117	cdn.gdns.revopush.com	Germany		24940	HETZNER-ASDE	false
142.251.2.188	mobile-gtalk.l.google.com	United States		15169	GOOGLEUS	false
142.250.141.155	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.4
192.168.2.5

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1405276
Start date and time:	2024-03-08 09:11:05 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://gossnabgroup.ru
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.win@25/363@84/27
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://play.google.com/store/games • Browse: https://play.google.com/store/apps/dev?id=8070166968320699506 • Browse: https://play.google.com/store/apps/category/DATING

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 74.125.137.94, 142.251.2.139, 142.251.2.101, 142.251.2.100, 142.251.2.102, 142.251.2.113, 142.251.2.138, 142.251.2.84, 34.104.35.123, 40.68.123.157, 23.204.147.9, 23.204.147.16, 20.166.126.56, 192.229.211.108, 142.250.141.94, 142.251.2.94, 142.250.141.102, 142.250.141.139, 142.250.141.113, 142.250.141.138, 142.250.141.101, 142.250.141.100, 142.251.2.97, 142.251.2.95, 142.250.101.94
- Excluded domains from analysis (whitelisted): android.clients.google.com, ssl.gstatic.com, slscr.update.microsoft.com, clientservices.googleapis.com, a767.dspw65.akamai.net, clients2.google.com, ocsp.digicert.com, www.googletagmanager.com, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, update.googleapis.com, www.gstatic.com, glb.sls.prod.dcat.dsp.trafficmanager.net, mtalk.google.com, www.google-analytics.com, clients1.google.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, fonts.gstatic.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, edgedl.me.gvt1.com, clients.l.google.com
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 167

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 100x100, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	486
Entropy (8bit):	7.456735643048542
Encrypted:	false
SSDEEP:	12:rbPqOLycYgACU4do/wZVbEqb0hyCQRdLOdsw:rbyUyXgdo/wZVbEvHObw
MD5:	CEEB4E8840C24621C0E0352B42B38A5B
SHA1:	03CBCEB0134A39267014595938705E2916580644
SHA-256:	50CB77AE9715629235F102DD53A68559DF1B64416F71179DBB4AA942725790B3
SHA-512:	80D4128488580567597BA5EB65DBFF2DD4A8EFC625C64CAC6A027A1BB5C229545206669F04A50A252B54F471BEE4FDC892E6BFE8347A50DD216BBA67BD671A 3
Malicious:	false
Reputation:	low
URL:	http://https://static.bookmsg.com/creatives/SG/SG_083be47dfc3e28c9a68305b76181a5033bc45790_icon.webp? pattern1=0&pattern2=0&pattern3=0&pattern4=0&pattern5=0&format=default-view-b_r-body&mlf=1&mlc=1&st=0.11&cpa=446c008d-62f6-43d5-8007- 6b0144ac2eaf&prev_step_diff=4097
Preview:	RIFF....WEBPVP8 .....*d.d.?9..\/*.&".Z..'.gl.>.". h.q/.O...m..v..>. {.]..AP..F.l....^.O....jd.I$&V.?..'...,z..].&..Q.+.....1Tg..Q...e..!t.....W ...y...)....r...m...3?..C...f.^.....i.K.$B..}...R ..m.g..5....PFg.lZ.\....X8...1m.Q.....).c....t..C.9...&.E.{..x....q..rCl..:.H.N....8.....q:S.VLs.Z.'lF.za..K9nU..Yk.Z.y.....h/5&.U.l.t....:..f...-.~iL....a..O..9..dR...g_(B.....h..p8~..0 ..EWB*..?0.rV.A.....z.Q.c..fZ....*.M.5...D.h:.....#i.u...,BA..aU[.hC5@..

Chrome Cache Entry: 168

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2162)
Category:	downloaded
Size (bytes):	195575
Entropy (8bit):	5.484447098062502
Encrypted:	false
SSDEEP:	3072:ZHARgMLVYxC4rboc7KTgdFiQnBCckeGrxygKxP/toI0QFY3o1u7ojsVFcSFgFlnF:ZHARgMLV4RrboSKTgdFiQBCck7rxygKR
MD5:	AB8804FC24BF364CA1169FF0F7D9192F
SHA1:	4B1E723246EA6F88C1F7E07895777AE99DC3E2C5
SHA-256:	5461579426FD97036CE5C52E27625C2B61085DC38E8FDB81992FD5E825A26DDB
SHA-512:	883BF8FACEC5C3E19274150332F3AF17618C9D5A54C6BA938A4F445DE91A6C66F8FD3E6E9E6ADF30AFB1F691483A374ECD86CBD23ECEF97E6813070B929B0E 1E
Malicious:	false
Reputation:	low

URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/am=022DoYEFBv4jfQ-2/d=1/excm=_b,_tp,appdetailsview/ed=1/dg=0/wt=2/ujg=1/rs=AB1caFU4y67OJEhh6CzWJiwmF9DXNHswJA/m=_b,_tp"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(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)([0x21836dd3, 0x38181606, 0x20f7d23f, 0x2d,]);./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2013 Google LLC.. SPDX-License-Identifier: Apache-2.0.*/.var baa,daa,haa,laa,Ja,Ma,Oa,maa,naa,oaa,paa,Va,Xa,raa,uaa,kb,Haa,Jaa,Gb,lb,Naa,Paa,Qaa,Uaa,bba,hba,iba,jba,lba,oc,nc,oba,Bc,tba,sba,uba,vba,Cc,wba,yba,Hc,Aba,Rc,Bba,Tba,Qc,Vba,Oc,Wba,Dc,bca,ed,Ica,nd,nca,od,rca,tca,xca,yca,Aca,Bca,Fca,Hca,Lca,Mca,Nca,Rca,Zca,Vca,ada,ce,fda,gda,ida,ne,pda,rda,te,sda,uda,vda,zda,Bda,Eda,Fda,Gda,Hda,Ida,Lda,Mda,Qda,Wda,Xda,Yda,$da,dea,eea,fea,aaa,gea,hea,iea,jea;_.p=function(a){return function(){return aaa[a].

Chrome Cache Entry: 169

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1142)
Category:	downloaded
Size (bytes):	18939
Entropy (8bit):	5.671340841999808
Encrypted:	false
SSDEEP:	384:ZlAjJyXrH4i8ViAfav6jfNMy5kuNHk8p4lTqRrNKYugHQ6Og8MDqryIz4pHJriqz:ZlAjQXrYiAfav6jfNM1uNHk8p4oqRrN/
MD5:	B98C43C54254DF5830E5DE6F0C6FAD64
SHA1:	7B49FF8A3F37824C81E45DB4F28938F71C0364FD
SHA-256:	5B8BD1DF219E3CCF74E50FC3229741197475910D1B16AF31E7E079A47987976A
SHA-512:	725EFF6695FA2DC97B30F40775FE9C6E5255C924C1126EA5205CD570ADB49963215A3CA6D8505787F65CC3E7B73799708 35E713E07B0000F7BA514FCE32A29ED
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SWD8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aTwUve,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,e5qFLc,fl4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lpwuxb,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q4UNLc,qfGEyb,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FIoWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=dfkSTe"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.Me(_.yoa);._.u("sOXFj");.var ywa=class extends _.nq{constructor(a){super(a.wa)}H(a){return a()}};_.pq(_.xoa,ywa);._.w();._.u("oGtAuc");._.pwa=new _.ej(_.yoa);._.w();._.qwa=class extends _.rk{static Ja(){return{Th:{EW:function(){return _.De(this)}}}}constructor(a){super(a.wa);this.soy=this.sj=null;if(this.Mj()){var b=_.gj(this.Tg(),[_.Dj,_.Cj]);b=_.re([b[_.Dj],b[_.Cj]]).then(function(c){this.soy=c[0];this.sj=c[1]},null,this);_.qk(this,b)}this.Pa=a.Th.EW}getContext(a){return this.Pa.getContext(a)}getData(a){return this.Pa.getData(a)}Hp(){_.Xk(this.sj.Oe())}rF(){};_.lr=(a,b)=>{_.pk(b);a&&_.dj.lb().register(a,b)};_.u("q0xTif");.var swa=function(a){const b=c=>{_.zk(c)&&(_.zk(c).mc=null,_.Wq(c,null));c.XyHi9&&(c.XyHi9=null)};b(a);a=a.querySelectorAll("[c-wiz]");for(let c=0;c<a.length;c++)b(a[c])};var twa,uwa,vwa,wwa;twa=function(a){const b=a.hb();return(...c)=>a.Ta.H(()=>b(...c))};uwa=fu

Chrome Cache Entry: 170

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	244
Entropy (8bit):	7.153897685834863
Encrypted:	false
SSDEEP:	6:c3Zulvhb4/Ep0/bXorL+jrXTvx2GCTn0LpIaoyl:c3Ql94sp0/jorUXTZ2GS09IaoyI
MD5:	9DEA3CBD9E0F9B455FDE32DCA965B41F
SHA1:	8049A160E77BF9FDD2446113611BB8C99D1E5A53
SHA-256:	3A1344E63287114EAD7F90BE694B7FC95370BF7B215D89BE93A54F39C15011CB
SHA-512:	E559F6BC3C44DC6E793EC98832926FAEB3D2D34811041868244CA89DF67DFAEB899689723C0DDAB5A58063EB4E42539614BEBBA23E09A8697E863F20416DB594
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../....5...Fm4.W#...0D.]....J...r..l.2...6.mU....5.C.(.....'vi...R...Fm.t.....\.._..Y.....c; .....| ....pk..b....`.....p..../.72<.....AQ.....Y..@.ErE.....d..]:..KG.^.@L.S..g..z..^.g.zg..\.JE..

Chrome Cache Entry: 171

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	14288
Entropy (8bit):	7.971123367692374

Encrypted:	false
SSDEEP:	384:DIyi/vxRM2ObnY6l1WPhWvqMjh6TvIll18ccxu:9RA5lAcvld67Nl18n8
MD5:	C20218C9C4795819B8A1B67545D4D0AD
SHA1:	ECE8F6FE9D29B24EB7D0F79559C6D3F093F72A1C
SHA-256:	E23EB256FB8DBCFABA1227A39300D06A182E5FAFE790533EB724A3982026BDD2
SHA-512:	480E9DC7BE3524A465FC542E5AB9E5288E728B38C2C67A5927D042731C247E0134D2B02DC6AB67610225CECC2CC48E3BAAB32FB6E0550CFFEEE7F9D9D8625E F5
Malicious:	false
Reputation:	low
Preview:	RIFF.7..WEBPVP8L.7../..?...m.H..... .....b].....,...`Q.....YjP..(.....$ SO..o..7..2....'.qF..I..D.....T...,2.....c|.....J.J..]...t....n.F..n..3..].1Z#.'\r..n.u.B...w.:.m'...t.L.].....l[..'t....(" "..".b.. 7.....w..O..4V.....C.R..q.M.%...%...`(0h.....GF.F..o..M...0qY.....L.....H,.....C%...`...A&...eP>.....Pq &"..!"..1jl.....+Vc..mV.K..24}..V6..._.N...D...S.i#.)d.....cj... .."7w.u.-.d.~....\.<P....8..m$))....!.....Q....>e...w... %y.l@J6...F..2.M....\ex]E..$J..lq...a.C@..L9-....N...*.A.Q.p.....".h...$.....$*.....G*.(...QA...oc.m...X.k..K.~,9....)GcN..8Y.. ..Rj...DA.P....r..C..luj...M.6...hR3.zq.R..m.Ht.....m[U...=s..>h..(...<...r6.H...^N..>W..4.%p1.d7l..u4..... ...7..i{.Hj..).IR .. ."..9...c.....~G`_...n..n.D@.g}a.{B`.=e...P LU..6rDc.o5]. ....I....(A.v..Z26.M.m7l#l..h_.G...!.=.kW.?Ev...#..Y.....(ff..H.0..V...0../2...ui..l...N.F.Y.`.l..|.y.ec.u#s.v..\.oB.m$l.$YdVW.....VUf.Q..p,.....4*'..s.m.l.l

Chrome Cache Entry: 172	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	11632
Entropy (8bit):	7.973192232256701
Encrypted:	false
SSDEEP:	192:oED+zCUROCFKf4/CRQy5FYX06ZT3SqGRxXTbEhKuXgFRKuajZCLR/:WGUROCPJy5uXYkgFRaYl/
MD5:	7F9AB9B1BC8874296F3F3C957D5AF858
SHA1:	11D165038FF925C972D9C4DAC609C4A64E6FC86D
SHA-256:	2F8CCC9C8D685960B357ACB42C5CCED51B1541716FE381731D73BBB517C5C366
SHA-512:	23E25F620BD9E782C73ACC7A8214B693A99D86B88246E5F0B31660DDDFCAACE5022D3C89A07BA1A21D68017FE431461ADBAD17BF7DEF908E5BD17696B397F4 A6
Malicious:	false
Reputation:	low
Preview:	RIFFh-..WEBPVP8L[-../..;....I.m3...I.L.....;....L>..z.HT...5..U`&yCH......B..Hn%.@...: .....2FCl. ..1.2v..i.1.<.....y.8yn$.Z....Z.....R.b..-4j..Y......2..$.cp.*.n`..D.X.....f.'.9.&.$q. O...\8l#I.....V..?...~...I..>c43..2....2..M:._....L.Gi.?.4.$..().D.@.$.....W.)J.{G....Z..@U....z..d%....!k.....P.W.....P..0.i.\|..F.g..m...8.-..y...1p.uZ...OH..._>0)C...I...E.FL.,^E...G... .....y.v;...m..6$|.....o8l.6.$.u....@DL...9..t.G.9.a...%.*.....*.Z...V/i.h.%..D.W).2.$1.Ba.R...'..#.....7/./,.x..@.g... $!.J.)..v...*...D...<.m.$.,..*....8..3...P....7.s.....<.....F....\."a.{... ./.}...`.m.....w..H.,j ..g..o.....I.$D....0.%...J.....y.xc.v-.UgB.....k`.....I..^k..}....-.$T.3...I...Q.....$m..w....._.....J...m.....z...%[../..MW...'.v)s...m.m.m.m.lk.aU..1F2... {.g.l./...6.....n....Ip.H.$:..X...:3...d.....^.I.....afff....."3.....1K.%... I..Y..HT8.w....._B{.G....c...N....1/4..G.,....X..G".....W....?.Fg.O.,:^..'...f|...

Chrome Cache Entry: 173	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (505)
Category:	downloaded
Size (bytes):	980
Entropy (8bit):	5.269706174882423
Encrypted:	false
SSDEEP:	12:kRZTFkNWAwM/AfzZ1QXBNqjbn5xym4mTAooDsuwv2YNF5QIE5mk9GU1rgGRkbRNl:kzTAwIeHQx8j54pyXmspXLuhkk9hlrl
MD5:	D7A4551E6306EAC7CC6BE1BAC90C0ECD
SHA1:	D19DD85CA64264062B4EAD354CF6ED3D0075FF03
SHA-256:	3E68611DF0C764740D823A475FA692222FDF098FC9B02B0A526634F623AEA34C
SHA-512:	3535444B8C21C398CCF16EC0BF69F17C97E15D89865D328D25484DF6BCEC7F83B603FCF861700D72AEB8B2264F046307A2574712B4BB44B6F47500FAD2BEF43
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5l84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ- 2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,FCpbqb,FuzVxc,GkRiKb,l8lFqf,lJGqxf,IZT63,lcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z, KkXpv,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PHUIyb,PrPYRd,QlhFr,RMhBfe,RQJprf,RqjULd,SWD 8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,UZStuc,Uas9Hd,Ulmmrd,V3dDOb,VXdfxd,VwDzFe,WO9ee,WhJNk,Wt6vjf,XVMNvd,Z5uLle,Z5wzge,ZfAoz,ZwDk9d,_b,_tp,aTwUve ,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,hhhU8,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,la zG7b,lpwuxb,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,q4UNLc,qfGEyb,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,s oHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdet ailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:Sdcw Hb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tl c;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe: VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=qAKInc"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.WCa=_.A("qAKInc");._.u("qAKInc");.var WT=class extends _.Uq{constr uctor(a){super(a.wa);this.H=this.getData("active").Nc(!1);this.O=this.Va("vyyg5");this.na=_.rn(_.sn(this).ze().Mb(function(){var b=this.oa();this.H?b.Cb("qs41qe"):b.Cb("s f4e6b");this.H&&this.O.Ad(b.getData("loadingmessage").string(""));this.H||setTimeout(this.ha.bind(this),500)}))}isActive(){return this.H}qa(a){var b=a.data.Nx;switch(a.da ta.name){case "data-active":this.H="true"==b,this.na()}}ha(){_.rn(_.sn(this).Mb(()=>{var a=this.oa();a.ac("sf4e6b")&&(a.Eb("sf4e6b"),.this.H||a.Eb("qs41qe"),this.O.Ad("") ,this.Ua(_.Ik)))})()}};_.V(WT.prototype,"kWijWc",function(){return this.ha});_.V(WT.prototype,"dyRcpb",function(){return this.qa});_.V(WT.prototype,"qs41qe",function(){re turn this.isActive});_.Bs(_.WCa,WT);._.w();.}catch(e){._.DumpException(e)}.}).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 174	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 5156
Category:	downloaded
Size (bytes):	1767
Entropy (8bit):	7.900952454375473
Encrypted:	false
SSDEEP:	24:XQUA3nkoLDy1UewNFQ2nIyuY7yYeZtNTi82QezdLthA0tdhTGgrsYB0i+W3vXLK2:XxA0OaNy8YatNngdbFdsgr/0VWfLGIv
MD5:	173F2A1D0B062D388633EFCF7DB54DF7
SHA1:	645179997DB997CF42883B47BD4B2097F928B025
SHA-256:	97E9EC7053DB0283691A34CEF728F8C2F8542F8EDA27A06F7D2BDEA22EABD926
SHA-512:	CFC21E9BE8BBBC0DBF1AC77F97FFF355147699B4F91EAF087EB4144C6748470373AB59550E1691D9E44E2AD27F7A94E800699EFB87FA45C345E25FE46F35C1A5
Malicious:	false
Reputation:	low
URL:	http://https://sw.wpushorg.com/ps/sw.js
Preview:	..........Wm..6..+.>...:..P.P.....K.i...5..+.m%..#.u.....II.I%.EQt.....CBh...V..mT..p~'T..{.-E.9...A.qt.....`.I.#yJ.;.....%.....:.&zW.nA.p.RVD..R..>i./.V..y"wWE.\....;Y.G..6...Y.x..NCDa..}..}7}6#q\.x...|.t`.RJe...9...2.ql.>2.P..8...._...|...../?.....&..db<.6..J...?Z.....7....)F`dg.A..uU$&.E .}....P.H..@....+X..=.u..{.....H.;.WP'.$[....T...d...'j.SY..E2:{....h...Nq.....<..+7.s.g..".."..4..P.j...,`.4...i..b...e.....=..^#P$...4...bB.=...Jf...i.....~...E..{4..T.A.s....\h}pb.J...,.....D..fL.x\|d../.h.....[.....PuX.....>.<...IA...._:o..G.U.T.E.z.~.Q.Y.....n0...mn..2.2."..O....c.Y..y.'.*..}o...{p..x?ap._6...P1\...-..Z.!....Q.s..}.c.6R...K.qs....+...y0.....w..Y.-.>]...m....%....lO.H..g.2.rB~.@thDg...lp(J$.....Z.G.@d.m.k..y.d.,....jM&O...-^..\.)...0.KP.....X,...a.d.05fj)W5..<.u..X*i./.o.....m..<w.gD.kk6.....p.w%...o~.Ll.....9..~....c..;.yl.B...u(.C.5.I.;.f.XC..dN.G_..b<..g.]...Z.'4....M.6{.oA;....:Z...y..P..;a

Chrome Cache Entry: 175	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	730
Entropy (8bit):	7.625614246453882
Encrypted:	false
SSDEEP:	12:68ZE4/Fm02TgTqfreyT0Hl+UFNwL7ZEPl8SDA/Xg8k0Y2x3N5GPyIuM0oBummF:BZEcDxTqfKy0bNYE9/A/w8q2FyPK2uvF
MD5:	4737081FEE45348744E1EF8E2191BCA5
SHA1:	612B035AF45C9107D3E362F977A07CAA1EF15329
SHA-256:	C0399F54B71DBD55E21B996F7010B4EE98A06647B51E5FE931882DBEDF381B49
SHA-512:	90C318AB4C47BB268797F048FE7BB8B4534D2A43B19D388E4A5B5E18EA81F65B832C7E7C6A6111E36F3E205A8135FCDE430B6EFD133B858FC51F565CBA1412FF
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../?.....$E.<.-...uw.8.6..! .....6.d.N..g...{...'.q..GU..?}..e-.c..c..c?..v8.GUkY.Z6}\.+..z..GUkY.U._-.>.hY.q\.+....O..hY.-.>...~...U.8..'....~>U.e-{.....~X@"o..6N..... ... .@L8..F.0.P.@!`.....B....(....c.b..c.....@..H..BB.....(@..0...x@.m..<..;Y.....m..\|....wG....ID.'@.....R...1.....w...2..>.:.{.._4d..U*.. ...*.....&.....S....7a!..d.?.....sa.1X..J.:.....7..Un...*.Z.O.&.!..f..^..E\|..>.]....Z.=.v../..... ...B.+...-N....b..9..A28.L.VP..,.....x..&.O..oa..\1...VM.&..U.g..M*...,.....C.m.....30.....F._A...XR....;H...,k(`<...$.t..4.....4..=j.....l.]....pH.d...}...G.K...._a..P/...`@..8..d...A..p!!=..`.[.....6.$..?..IR.....T..G.....

Chrome Cache Entry: 176	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	3514
Entropy (8bit):	7.927281300438779
Encrypted:	false
SSDEEP:	96:P+wI2ZBn/VSoDPiodR4aY5fUbJtAt5Yjot1:Pf1SWBj65WSYQ
MD5:	29DA476E7B5A194FE0ABD9146AE18564
SHA1:	F4DBE0D57051CBFA80D61008C49350AFCBEF0910
SHA-256:	B06A16D5D1CEDF27DB3F42D1E31D665698559B44120904858F72667E6AF04117
SHA-512:	308211509D8C6704DB666ECE0DA0FBCE43E8CD67B836D2DC34D09DEFF913B0054A48CF2CEAB8770193AED96C6BE0A21D7A50A945489677DE8C56C3B53D002BF
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/lwBxT-SXGW_99shrwHIzxUB5nyv248-9b_KfowA0mgBZYtTKftUAX7ewr17hAzWJQYA=s64-rw
Preview:	RIFF....WEBPVP8L..../?...M0l.6.$.l.....[?..c.*.V..~k$j....x.7....$E]..?...E...m.F....E../:l...IRt....zffJ...U.r.....`=.....$..~1.^5.8....K!..$@..D.w.....S4."..*.D...Mj...s...h...Y... w;.S[.-z..a...E.n....a... .....e].&yx`..c.....&.j4\.A..&O..$EU=._:N...(.$E.k.4...r.Ss...Q$l..H....=|zP.z...m.1..#(..hr...9M'.....:.o3.&`.....d.w.3.a...J..r.z.....+.4).~....m#9.dH|oP..+l.Q..q..XE..l.....m...../..T5-333333e{...=.%..l..Qdfff>.....K..0...../.9..J..*..0..1r4Rk..9.....3..s.K....62..6.).2N"l.$E...cx.....3.ngH.m[m.s..b.v.....j..ff.=.@.df..V..0A&MP..j?.....s....*T'..e9Z....9mT...kN...z..x....A.%..tjl...:.J/.L.b...,. X...h..V.....:.(...}...kO'../.....U*h....F....2...J.b..i9..9.%.?.....A.... ....j@...`s.tzv.C.k'.>l.3X.b.b:..W....."(....J8.y...VL...hx.....L.=.F:...Qw-.;.(.P...b.0h.K.....-..\.k.Nb.r..b.....g.\. ..n...+E .sFW...r.-7...o.u<l....$..$J...(.^.....jj.M.....DI(..E....d.G..f,...'N..N.O.s.j...k.....&*h..;

Chrome Cache Entry: 177	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 648x364, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	21244
Entropy (8bit):	7.98833258384387
Encrypted:	false
SSDEEP:	384:APzfxTOmFE4w5KxW2ALrGTGa352Rbag9F4gKBo6834AqAj:gFE4xNALrGkR2g9F4gKi683rqQ
MD5:	03B1DC5DEF3A03B3B513FDD42B8F44E3
SHA1:	DA9BE9F8AA07196AB9D43BC9F86EEC8D4D2CDF03
SHA-256:	1D34D1F432B486C70B71E5ED7A74C054BF2EE85F74CE00C5C2954204C340C82C
SHA-512:	60CC6D3D5D953968BC01A503CD5E28D4D6BE32B3B55D5D1EA19F55DE9DC163CE2DE98E6836A04F3618918C7A48F8866C35B09B7704470256394A96DB3935D0B
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/fWeFmmqEhxgnidTfx0BGIy2ZNWKF1g4zLfnvy0GcQ0_bETqceP_VoB5O0YGAjwhI0osdHS5r4w=w648-h364-rw
Preview:	RIFF.R..WEBPVP8 .R...B...*..l.>A..D.....D.(.....H..l..#.....o...K.....?.Y-.6/6.s...?..?........w..j?.?.{........#.........{~....f...g.../._-..?g...t.]..............}.......?....u.....O..H.....U.....w...?..?.@?...../1?a.q..O..#.7._2.|.....K....?..E.O.....g...{..?...}.?.....,....c...q.....o..._+.....M....._.....8...[.?..}....o.....$ q..ZUU..n-*..q7..Uj...J..\M.UZ.&...T....t.b...q7..Uj...J..FV..B..O.P..x..J.M/....CO.X.:[~Y.SHm...6...i....Q&.|.UW.....~...5.....m.f..U.....f.K9.;j..f.Y`O..Mr?..O.I..^MliiFI).>...o._$..m....v...I*...Fk3...-s.$.....T.v.....H....O.yh.....V;....sEd.F....$.vf.L..T....1.W~.[j5....Ut..:.....0....A.:iV.S.p....5..n?.x..,.Z.Y.M..P.....5...{5b...:|...$...}|,3Q...{....n..p.....fEz...1....*.h+..R.....l.{.z.@.m.z..`M...,..ay...m;N_...7...;...!&M.]. .....qiR.....b.....$L....pr...^..s..;Q.....j.h.z..u0.PB...N..;.i..^9...5R...m..`j.<.:q.a.Pdl.....l.....U..{..`+a../....SL.*3*.8..Z.:

Chrome Cache Entry: 178	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	1909
Entropy (8bit):	5.090327194391798
Encrypted:	false
SSDEEP:	48:YjXZnvndKfkXNLL7uKSXvPMAOdpInG0a790VK/SlATT:Sn/QeNv7uKSX3JYpoZamVYnT
MD5:	8CC669D7A1C5EB42AE06AB66C254F213
SHA1:	5CC28B77545A36C6796BBFE25F2E6E910C2DA245
SHA-256:	3BBBE82FDFB5FC7A0F09FB06A1D248ECDD84247E1FCEDA0D880C44EDAC591832
SHA-512:	4C84D53D46ED848DAA85C834A5835C0939DB29E28D16649F11E86BEA1177745A6C4816F54C30AE9B583860D2484E67126D87558787827E6F878F53D50C2DE0BA
Malicious:	false
Reputation:	low
URL:	http://https://bddb2d2561.62b81f5af3.com/3572bcc7be69f5109a8d2b0b8fa39de1/151659?version_name=a
Preview:	{"label":0,"iabcat":24,"iab_extended":"24-24","default_keywords":[],"cat":"Others","tagId":151659,"script_defer":false,"utm_mapping":[],"tag_id":151659,"adformats":[{"type":"inpage","assets":{"js":["https:\/\/js.wpushsdk.com\/npc\/sdk\/wpu\/npush.js"],"name":"__fp-initev"},"spots":[{"updated_at":"2024-03-04T09:53:17.000000Z","config":{"sub_id":2083435515,"spot_id":513500,"unified_id":400513500,"save_spot_id":false,"tube":"native-push","proxy_domain":"https:\/\/vidvas3.com","auction_url":"https:\/\/ntvpforever.com\/in\/multy ","ip_check_url":"https:\/\/nereserv.com\/in\/dip","type":1,"mtype":1,"disabled":0,"target":0,"ml_close_ratio":50,"ml_close_ratio_modal":50,"eventFrequency":{"type":"show","count":2,"cappingTime":120},"perPageEventsFrequency":{"show":2},"firstShowEvent":{"type":"page","delay":0},"betweenShowEventsDelay":0,"betterAds":false,"betterAdsMobile":false,"branding":true,"startOnFullscreenEnd":true,"paramsToExtend":{"default":1},"tabunder":true,"large_cross_button":false,"is

Chrome Cache Entry: 179	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 165629
Category:	downloaded
Size (bytes):	45441
Entropy (8bit):	**7.994199933239812**
Encrypted:	**true**
SSDEEP:	768:gj9VUZe9MAVQpKd405R+E4uLZxn8SgKQfZCJuFfS5P4vx0kc:gPUuTROArnnPQxWuF/i/
MD5:	3F164CB6FC7CD0AAC0D904F8DE3103FD
SHA1:	F481F86A41742D4B6E727BBA534607D19815365D
SHA-256:	6AAC4A4019D5BADC1F2256DABA0EB13919605C485725A0A6686A3ACE24E9FE11
SHA-512:	7BD3C7565464228D77024482C1C80E7DD25F475729EAA3426719C132D3918371367E8017187C31D82D2FAA08238130411F7209ED45B027815F62F508FF2CA908
Malicious:	false
Reputation:	low
URL:	http://https://bddb2d2561.62b81f5af3.com/11716c69a3d9e5ab14e0d555a9e69583.js

Preview:	.....v.8. .*N~.>R%.....?....r.)..hI.LR.e[....s....o.t#...).....N....@ ....H....We....Z-_Y.....sj.'&.....).....N.....r..&.fe.N.S...n..c....k.#.^..r..tz...G^7u.g,.(..Y.:...z{...vnwT+.....i. .....E.?.L.....Z.n.pS/.L*..'.....Uc.p..w.<...w.v....K7C.y...74.P..43h:..Jk.X.....\+.6..w..{.|..;.....^k.s.../.<...w...I.S.X.k.~^....M.5Lw.R.....;..z....>.....Zz.x..-y.k...g!...I../K.m...Z..i. .+.N....d..xn.^J{..n8Ojv!.P.>...5.....9?.....n.....u\gd.....w\...M....}..wM...Ri...d.~W-...<9j..W7..G... ;....N3././/..?@l....@.2..^.]`W.q.K.H.e...?...4.{...p.z4.wG{.....D.Hh.F.. 9,:Y..%.4n.....zv.k<.|..5.....E.|..?...<...Q...w.....z..~.....@.^.....w./7....p..m..NW..@..c"m.../.k;....$.4..q.,.MJE@....=...[.Zi\.v...^.z....rlv...y.]]..k[..N.wXi.m.=..m.%....S.(.2.]..LHk6..u....U.u.dYN..O3V#{...6....]..n....9.}.W.;..fZ.P..jg~'{Vu._V...c.=..cd\J..jN..9..o.phF.N3...q.ly~i.ml.w...<...&g..q.=..=....j(u.d5.r.....^z..... ..].S.!.V.

Chrome Cache Entry: 180

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	332
Entropy (8bit):	7.358546821442648
Encrypted:	false
SSDEEP:	6:PZVS4Q+recdKlUVHiRQtvCoqYlbJq0AxtC0U8vAzIp9JtOOZkeWbCgfpH:D9Q+recdKlcHiRmC+bJqlAzIpTtOOZTM
MD5:	2F640AA73D5757BA0FE67B74E5D9F41E
SHA1:	A4D29ADF1BA739285BA35AFBD94D51734425429D
SHA-256:	469C936814B431210209150CA7F39A314A333269C07A5C83483D0C3EE0D772D4
SHA-512:	EB2C59AC81D5C2D8DFC90C5A06B283651225A3836A514B47E46009DBE9A9E2AB72EBC77558CD3CD4B3470844D417DE6958A7BFE1AF5BE16C2D7A2F9C314FA 8D
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/12USW7aflgz466ifDehKTnMoAep_VHxDmKJ6jEBoDZWCSefOC-ThRX14Mqe0r8KF9XCzrpMqJts=s20-rw
Preview:	RIFFD...WEBPVP8L7.../.....m..s..c...m..[H.....X.q.|..c[..*.m.#.Jw.E:.uro....z..m[....J..I.I.XNH...D<$A"X.k).....y..W..7T}.....V.G..v4.d....%.Z....y)o.....]~.0jS/.....$..|.K.....8 M...=..I.q....[.9s.../.F:.j...{n..2..d.#A<.T.A.i.../..6.)..9.}. ..%.I..e_..=p.H.....z.n.(^..}/.CJ..:;.G..3.q....ZG.ZF..&.b..;..

Chrome Cache Entry: 181

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1610
Entropy (8bit):	7.861288969735864
Encrypted:	false
SSDEEP:	24:zlw7vjT1GVznWVASYnsaIU9L8oqsgpCDN9FaoDhgLEMo0j2X87302misLc0:zlw7KTWVAnLIKKgDN9FaoNjMqzXFP
MD5:	E002EB245CEDE04193B2DB5C914BD4A0
SHA1:	035FCF0CD9228A0643839CC11FD67F9B659CDE9E
SHA-256:	E76553027E1D9153BA1A4C244C88B2772BA62134EED47FCBA1FC796B71AA0261
SHA-512:	3D154D90B80690A74CF05155A8DACC958A3112B3A4ACC05EA4840CE1490889107D185D0BAA6683B3AE9DCB8F7AAA835BA0EB680C137F230FC93645A0BCEDA E36
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/tH2ui3MqYnTyt7EG9S3DVNDO7SV7eRtts2phjaE-vZNBvf4meAx5_a5LZc_IbZGAFw=s64-rw
Preview:	RIFFB...WEBPVP8L5.../?.....m.IRf.M.?.=...O....a\.@...../..P..c.....m.0e.i...0l..q.....'.....B3.H.....H..>.=.c[[$9.Y5..3K....x*.133.03CWe...3....;.[..;"..|....2.....$I6mU.s.....$Z. .....m.Fv.m.nd.F..:.m.}..#..$.....t.....Ng.37....A3.....H.....z.....U....qP....3..f...+@.u....H..3.Y...},.p..5..y.4.Y.JLg.0..$.1...%.3..0..+...v.-N..)OG.].v&..C...)7....=...i"....V.t..v.. V~...%M4yb.....B.{...)....J....F.....V....7..h..Z&....R.....{j.3t7!?bP.4L5.T....U.|m....R..<.....bn.0.zG.b..k,+...'.H..S.^..g.e.8..^x..8.-y.#.!s2?...\.Gc9R.....|.S.....5..;....dL.Cc. .y..+..O$^..w.w....4..a."{9>.q.[.....qz.9.Y..@._.u....R...~.7..#...F'.....u#....XB..H..e..*w....%.....r.>... z_...(....r...).=V.....\.Z.C...o./nC.c'C..k&..t.....2.&|..._...i.....d.... <1C...G ..[m.o.Y ..d..NZ.s-e0....9.I..x.^=..m...~.H.5.."..B.U.k.....$.%[[..+.C[\.....>g..$..K.#8.sW.>-..t D.8..x.,R..!.....w....|.....(.....Sp]....{ie.(}...z$..^@6..

Chrome Cache Entry: 182

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1560
Entropy (8bit):	7.817152065364505
Encrypted:	false
SSDEEP:	48:SQtBQZz0Vp1ttzhVoLIFLiCaWMYYkSgGqY:S0lp37VoLIDRM0Gv
MD5:	54A07A94ECA1B8328D2F5747D2947754
SHA1:	4883DCE70693CE0170D0EA6D188EAEEA44101536
SHA-256:	98ED54B694FFF89DA78AD01B37DEC85ECD3BDC2F6E4B3714C5EF1B37045A29D1
SHA-512:	569F6D260A0B3E22A5AE25E9B28C90ADE5850DB80DF1D60DE491B46CB2C3BBB7ED6E3BFAC3A1F059FA2A8F1A97F1279928BB05C8133A65088A2B0F1FEA6387 69
Malicious:	false
Reputation:	low

Preview:	RIFF....WEBPVP8L...../?..."........I.[.m.fe.m.6.m...>....Y..V.{..h.T:Ul.N..8.]...S.....?p.......[...K...l$.m...m..m.m.m_.'...m..g$N.U..+..a.N.n.njI..a...B....InFs.s..FRL..oI....H... o.&.S%.G&.w_W...Xt.....r$.I.WO..0...3..I.DM:dJ.Q..2#=.$....={m.e...\Y.n.#..%..*v.E.d..*.R....0..F.V....=...2.L.$...j..H.....I..{$..q..Uz...d/`..Y.v..Jt...y....N.....<.M.SDa.C.$jq ....Ta...C..7.....f.2f.A/.;...v.E|.4..6..D..QaL..,....m.P&....D..{.k.N.JX#?...92Q8.pB...].#|..L..txQ.1..".2;...0.\Zzu.u5..$2.@...qI.....2B....8.....>U?.....ODl.-..<P..V..C.:2:.9,>.M. ..:.C.#X...'V..}...2.....\.5=...V..:..).d$..Px..I...H1E...6.w..-i%.(...T;.]3Q.k6e7..K.....N..r.I..G.I.N;...'.Pb.|.....?%..#..^!..V*y..2S...I.Z.....1......./.....8.U.h[....-..}.T<$v.... .c.q1L..:.:RI.f.....B...|b|}.....Pn..Sv.8...hGr.Ks.....T...f.....&..n..s.oX.....W.....w...e.....H..,Z....[<.K....5.....O.f.5.r.....w.....ua.....>.q.~.Pj.I..z.....9|'..E.

Chrome Cache Entry: 183

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	**7.9932077797451395**
Encrypted:	**true**
SSDEEP:	1536:83UzPjIi8OZoU+3BsShm/HsDk11bMUOL7WO9H10/MGRv:83UgcZF+3mSydRVUWOB6E+
MD5:	C2D7E483FAD2740A6C16BDD8647910C5
SHA1:	85C5B54A7DF4E46955A8EABDC64441BF3F17021A
SHA-256:	B49E99C97D8C1E9E2B3FF7C008718A9CED62014B02E6D4F28F87AA1D14E29D0C
SHA-512:	6E772CC944918CABF62FD8B99AFA63A06609C9F01E8059353F39D04E3C7FD030858B185128CC78C0292D15E1829DD2545D8B11DFBC1BB174E4748C5D75B5C42
Malicious:	false
Reputation:	low
Preview:	RIFFn...WEBPVP8Lb.../..Z..@.d+l3...'.E..... ..... .iG.Q.tlSDP_..m.5...R[H.V~4.....!`QB;JgMK.....G*<_9h..j.)E<WH..,I..T.h..!..O.`.?.b..6X-u.h..i{f.q,V....{...P.=.O..0.w.~AlK.1 ".C.x..?.\..}....\!@...].h.K. {...D.#...7.=b:.....}ut.j.}...O.. 9..H2..p..J.....s.O.,I...t....qO.=....3...y..../6\.....]..lb..a....bZ.....X....$.....Ia. h.H.a.*.J./...V*[.lY.e+...xcN..BA...U.....G+B \|u.^..@-.....3=.1...:...a...Ny.x.V-F+..a...c... .9m\|..K.a.....=....t.OG....D.<;.K...Z.....*ku....M.....S.A.u.j..S...r.....&P..>..s{..N....Z...T.....V.q..M.$.5r.F}.I....G...BG%....U..v .S.6B..43r..K.t/..w].....K[A..%iF8....R%...K....F...VpkA...)].6.*U.....J..QJ..(|....S..betHo..j.6.....Z..a..K}0.e..-M(."...].!..._...5.....V.7.....5....I.M.T.....8.)..4.....Z5H.....`$...+.UE. Z..m#u....m. "& ..s.KZ.*.-.%aM.yG...M#.*..E.t.....d(..aeA..${..pJ.E....2..j..|.Pp....npv.o.K..h.....Y..].U.....U...]..Q.....Yy.2"..#.6.>P.s...b4.. ..9.....5.....Bc`.c.KK.

Chrome Cache Entry: 184

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	37748
Entropy (8bit):	7.972768866355637
Encrypted:	false
SSDEEP:	768:xFvIIIWSGGuFj2uGMLMLMLMLMLMLza6N4FhF1YyDviXSOBAV3:fvIIIyDZ2KIIIIIC4IIYqviXSiAx
MD5:	6B1B3A743B9F68665E74FA4B843EBD53
SHA1:	4ED5E10956E55F909DCBC0415A3E150B011B874D
SHA-256:	72C530F4B20C659C3040084C79F0558DDA42401DA9F60334228FB4FE05CDCC11
SHA-512:	6E4B215674E346C385876D9A1D6B3E1C11AE2AA1D1E5513EAEC6B712EA24F56AC0DB6E2123B2F5A0543CDB021CE59F68CF9A0096261B00D76D533ADB57E451 EE
Malicious:	false
Reputation:	low
Preview:	RIFFl...WEBPVP8X.....o..VP8 $...P....*..p.>=..E"!...d. ...~...!u.....{B~u.u.zA...7i.!...(._.....\|...?T...7.....='...>....i.n.k'..x..?.....e.....O.?.....}..C.....?...../x .....7....z....O....}.....)....O...._.....`...Y.....P.^.:...c.....t.{y..<..A.....5....@...{.w.?....n.....k.....~k..z../.....=.?.7.....].c..?...k....C...1...d.:.M...6LC...1...d.:.M...6LC... 1...d.:.M.p....d.:.A...RI..UI.b.U%'{.M....>.....s.0.....s./:....<:.x{I.....h...\|F.....{.GCK.<\-.Z.Xo.Jw..n....r\.T.....7x...?CUz.#.d...v..;.ZTApDLW..c@\|8.UN..<+..jP.9..s0....,=.....7 ....C-.w.?I.....\x.[V.[.L.v.$.}9.*Kuk..*&f.2...M.d..L.~$~.i_..v4..V..u^..)5....w~.....4..Q._.....4_U(..P..5....;...x.;[...ic.....ma7.....p.....CR..1.V&$..DApP7$Q...2...(cl.1....Gs. J.....f.[XG.L_...{.XMJ..'3.Nf.....a....@.9.g...;k.DLLJ.s.3..._.....`..j.).a#.....[$..`.5(c.#].~%K.....<.I.s....O^.b!14...7

Chrome Cache Entry: 185

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	4.639719888612948
Encrypted:	false
SSDEEP:	96:EdAdhzUooooRoooT0oooooHooooooovqxooooooooA:EkLL
MD5:	A217F758EFDFFF14053678DBE58FA4D0
SHA1:	6E0EB512C2F386D645712D7ECBE339EA85CFCA68
SHA-256:	F343B3015D0545A7D5B719A434135BCAE2AC766ED459AEEA671E3688B79D1875
SHA-512:	9BCF90FED875FFAF3170EF3425949642EB23B4E750CD42BA546D30E1A58C4FEE1A14CCDBD31455A6A442D09372CCB3873BD7477A59853608BC87660FB578119 F
Malicious:	false
Reputation:	low

Preview:	....(... ...@..... .....5C..5C..5C.]5C.5C.5C.`5C..5C..5C..5C..5C..5C..5C..5C..5C..5C..5C..=/..$I..... <../A.8D..5C..5C..5C..5C..5C.:5C..5C..5C..5C..5C..5C..5C..5C..5C..=/..$I.....TN.(?..'>..8D..5C..5C..5C..5C..5C.5C..5C..5C..5C..5C..5C..5C..5C..=/..$I.....2..I...8..&>..8D..5C..5C..5C..5C..5C.5C..5C..5C..5C..5C..=/..$I...../... ..m...8..&>..8D..5C..5C..5C..5C..5C..5C..5C.g5C..5C..5C..5C..5C..=/..$I.....E...>.. ....m...8..%>..8D..5C..5C..5C..5C..5C..5C..5C..5C.?5C..5C..5C..=/..$I.....B..C...>.....m...8..$=..8D..5C

Chrome Cache Entry: 186

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	339
Entropy (8bit):	5.186927421082407
Encrypted:	false
SSDEEP:	6:kRZzRxVvn9vMGgA18G/QVf1M0WDUIfwQRaNw6JpyxZRNlad0:kRZTFLH/Af12DUkbRN20
MD5:	B7C9476DD84697B306F7C037DBC9A1FD
SHA1:	A0A1EE9B4E35EB93212235F2D6D5B8D5C9BCA6EF
SHA-256:	3B9256F826BA1156D7B633E14354D0E2E3ADFD93F3A37ACB8E712A270BD4E640
SHA-512:	87BB6CC435EF3BCAE9D9B7B0DC3D6451B849C705013BDDA9CFF2BF4A346DC5518218DC9A57E4E03A2F90FB3B7407734E4373DC7D56D6213B6EF296232AA3C00
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,AKTwDe,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,FuzVxc,GkRiKb,I8lFqf,IJGqxf,IZT63,IcVnM,IgeFAf,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PH175e,PHUIyb,PrPYRd,QIhFr,RMhBfe,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fPcQoe,fdeHmf,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYClec,pjlCDe,pw70Gc,q0xTif,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appscategoryview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=PZ1hre"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("PZ1hre");._.Ir(_.ZAa,class extends _.mr{constructor(a){super(a.wa)}H(){return"PZ1hre"}O(){return!0}hb(){return _.LCc}});_.Qq.PZ1hre=_.gQa;._.w();.}catch(e){._DumpException(e)}.}).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 187

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	742
Entropy (8bit):	7.704077267990546
Encrypted:	false
SSDEEP:	12:OBqoM5t7CCHRaOpmKiFKW95DotIst+ZcNDZGOU7a5FBsGgDfc0sCXs6u0EGQM8xh:O/M5tjW3otIDeNVlFBxAfc0sC8ljM8xh
MD5:	3AC1FF2C773AE2B5FD6E1581F8BD5D6C
SHA1:	2A76A9A0DFCDB6B9C298AEED1D2BCCA501F3A305
SHA-256:	7F54C2FC512AA005BFE5F434170066DD1BFEA2F1E5022BDDF00638B12247F6D4
SHA-512:	433D94CB3AFCA71683234E237A1D8E839E55067BB7EA93123148B1A2F18F621E9FB156CFA1FAFA7F854050752528E7199D67F1F9164CA6061CB423B3A7910C42
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/mix0TYeOXNQ8vCIKE-dwOlCUrb5RKuJJVdmWmDfjosD1I-Btx08-rZRK0e91ap_gMrw=s64-rw
Preview:	RIFF....WEBPVP8L..../?.....$G...r.....<..A.q.?.CX .m$I...p.....M.P...}sQ.....P...(..C...C(`..!....2-...(..#..!.E..@.#....Z.#..GL....i<..h.#.....!.q!..IG.8..%.....#.8,...#._`.`..,!....N..[....%.^8....BY.JK.....Q.X.....ww.Swww.R.....w.2.....+p.F.1...f.H...p...$R*..D...RR^VV^4..QY.7.RN....".!.T....?...n.q.<`1..{.+B....).Y..-.<-.....)..n.H.....pc.....$.JuL.@.....,.,.....G5G.&...u+.....'..k...Wc.wS.efN.v...;n.....ut=.{,'...k{...uQ..].6b.7.M..&.M0FofcW.L...{...6...~A.h..a...m...[....+O...=.f..0..G....,c.;..SZ.....@..+.....Vo.&..dg.....U'."e...[77.O.....A.I.././.....NY).".*T.d.. k=\D!).v..}.q..^....I.2...B.|m../B...o.sBli.P...:...$I....y.2U.....'...o..L.....I..

Chrome Cache Entry: 188

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1898
Entropy (8bit):	7.829582097243759
Encrypted:	false
SSDEEP:	48:SGer7d4vCL5WzoCPyQOCQDBIP/Rxe6we11gdBMcc:SGerJ4vsWzoCPyUQzIwe112s
MD5:	ED8A4674D2A7886593A3DB41A9895A51
SHA1:	BBE46F09148DEEA5772B616A200F3336436D1AB5

SHA-256:	FCD052789E212D6EF4C3BE74E18F2366A7EAE0D572C25A460B1F73547BB8E19B
SHA-512:	83C52BB59FCB813B3042625C300931C9ECE48EB3C90E0806FB9AB988234C379F635DC4270A95A9B2C0C38A928C3C21859EB11FFACFC2855CC0E7C62FD4828FC
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/a-/ALV-UjVhAJroDG3rFcHCeguJJfqe0ywxWvOANSuyL2sZGhEVwnC1=s32-rw
Preview:	RIFFb...WEBPVP8X.....VP8L..../....M(I...*.#..@.... X(h.....w.gp...4.I@.H0w.H0;..m.t[..... ".F..D.Q...j .....kA[.`..43GI..W.k.m...=z?.O.m.5...M.3...$IR$If.Y.u./.....yd.*.b. .q$..H....p.....m..O~.,2...d..UY.,.b..G.hv....`D...*..L.:=.cOg....%.P...H.(`D.A.V@..C.(.OF.....c...g..N|,.D.J.5.P.@.@f...6.....C.....=.4...h.@.Ae;"HA.H..:.$..0..N{^p.,.....f. 1.O.....Q.Y..V.B.)..P..4.81}..........O..;..s.....q.Z3..4..#J8h4.J.....P...G,%.g..J..U.}.....bQ.....H..R..A}..k.D$@.s@1S.d...Aae.....;F.....k...g.f..q4>..8.%.Re...+v..... m.oQ..s....eW{.x.q.NJ.....qk}..9\s..B@`A!..X....I.^.....I....km....)&....n..#.C.....D*U.`o+..J...K.....;s.?....9..0L.vo.rU...w.|.#.cmPA.....+.....3\...~...g?.`^..]R.j..._....E.\....hc0 .2!.X....YW.T<.n.<.....,..Wy=..g...e.(...gi=...0.1ZZ.D..$..}TB...|.]/.0..c..{..ip6.....,y.p}.[...u.g.d..B.8B.....!....\w.....6.....M.}.Gy=.)[.>.....A..{D!R(.....u..>...{L.i.].}.M...>..... W.....

Chrome Cache Entry: 189	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (700)
Category:	downloaded
Size (bytes):	882
Entropy (8bit):	5.330483457440343
Encrypted:	false
SSDEEP:	24:hYHuVBYPvuNRmo14LNkeKcOBrOYuJAs3wVvsi9s3WPcmgs3AWV4T:DCHuNRr14LNkejOBr3kASwpDSW0BS+T
MD5:	B728CA9CD183D1B7C3F72116B19B22A3
SHA1:	C1FD73F6B02CF00B8BC60B09CC99495E8494B739
SHA-256:	8A7B1CA4BBF273B32EA865D4785A1944D1B2B133678D9B5FE7EE0406F6FD64B2
SHA-512:	CE52C8CAA65B221D0E8A26B7BFE60D20AC628BC8C4D479C72F904FEFD587B87A136D24B32C17E6A87082338E606249463A3C6D8D03E28C50EA81E1C1A408CF48
Malicious:	false
Reputation:	low
URL:	http://https://storage.multstorage.com/log/count.html
Preview:	<!DOCTYPE html>.<html lang='en'>.<head>. <meta charset='UTF-8'>. <meta http-equiv='X-UA-Compatible' content='IE=edge'>. <title></title>.</head>.<body>.<script>var e="_shrdstrg";function a(){try{return JSON.parse(localStorage.getItem(e)||"{}")}catch(e){return{}}}function s(a){localStorage.setItem(e,JSON.stringify(a))}window.addEventListener("message",(function(t){var n=t.data.action,r=t.data.key,l=t.data.value,o=t.data.messageId;switch(n){case"SET":var d=a();d[r]=l,s(d),window.parent.postMessage({key:r,messageId:o,value:null},"*");break;case"GET":var g=a()[r]||null;window.parent.postMessage({key:r,messageId:o,value:g},"*");break;case"REMOVE":var c=a();delete c[r],s(c),window.parent.postMessage({key:r,messageId:o,value:null},"*");break;case"CLEAR":localStorage.setItem(e,"{}"),window.parent.postMessage({key:r,messageId:o,value:null},"*")}})));.</script>.</body>.</html>..

Chrome Cache Entry: 190	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1606
Entropy (8bit):	7.857056769811978
Encrypted:	false
SSDEEP:	48:z62qnO15662L5WDblWCv5KdMINn2Let44tgOyeXXn:uODKqkCvSn2LL4tgOrX
MD5:	D9465D5C85B0AA6CC8AA5C681AFF3BD7
SHA1:	930137B4C6F5719722A44EA814AC208D0173FB04
SHA-256:	B202FF8C6B424BAD43D5446D2D77823A943D9B6C12EFE6F74D43F7AB43297392
SHA-512:	605E37754978681B3C8FD5B2CE6B6F20C3ECAD5801FA510EB50AA8E6548122257DD5D4BD9F5CCD63DAA2BF9C5DA1B52DC6FE65A2763D5DEDB0473C93C7991F44
Malicious:	false
Reputation:	low
Preview:	RIFF>...WEBPVP8L2.../?.....7.mW.'...I.....=..A8.$.m..8g...]G. ....$...+`..$.._.A+....eE.a.F.aE.Z.9..#..>.....G..>....9.Ze..._...F6+Vo...cD.....ls....+....b..u.....<F.....I... ....D.. .JP.6.qX.>.8=h..D.F8..V .....\|d7.PH.{C..&.N.RD.....9.....A..Av.:...D,:..2..4D.!.Ah...@'2 rd4`b..(B(.!G.`.....@.....d..e....w...v.z.....M.....M.d[..m.m..m.....-.g...eWDT....""... ...]O..)...'.sI..I..@ZE...*.....0*.]\6..\l."......".p9..jU(GgW.E.Q.,3.....3W..V....UU.s.QA$.|..D$E.A...L.Dg.6$.....M0.+...I...Zz..x..N....w...X...O...K.....Qj_.}.)&y....5.]\U..[._....= .x.....4.x....o...~.....g?..=`/.sKm..M.S.1sm.u.bv....n...U..R..)-P&....Q..../...4.\ks.!=....M.(.f.q..5K=K<.A..7w.....rUVf5..l.{.0....N..'...v8....._.?.td..4K.l.mj{[...C.{..{.593.6...l. "..r...g.&...}X]....A.W..`w..K.Ui.."....._`..... r....m.R&.X^a.....e..w...sr?['...U.....+.....w..wA....Ye..NLFDUD(A.}...z~z.G.#.9k.X.3..^.<A..\.+k.F./9.*.]-..N..z.+\..B...c.?!

Chrome Cache Entry: 191	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 48 x 36, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	185
Entropy (8bit):	5.9780303893393345
Encrypted:	false

SSDEEP:	3:yionv//thPlSYLl+1IHCRsHrXLRa+dn/23rIIGU5thNnkncm3w4qtmkW7PXl0VMa:6v/lhP0YLkyymvVGtjnUnRq0kW7N0xVp
MD5:	07505E9DAC6DD922116F038EB58C9B88
SHA1:	4DAB9005E4603F76A6FAD92FE78FB9C92D05B62F
SHA-256:	C4DB75F643BB4DD47E39A9601FCC0A14621B588D5E4EBE987EE4828120BDE791
SHA-512:	5A94B97148037E9A25AF768AF67A1AD5D4959E5D5C216DC5353FB159630302A74A990CCA20F787C024C6B7229A12920B287A88A4063514FBA534E7D1DB094C11
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...0...$.....=k.9....PLTE"u.#t."s..OO.PP.OO.....o.....tRNSJ....J..J.j.\...DIDATx.c`T..ec$.. .].A...1..Z..!..%p.A....H...0.....*.....]...Qp...al.....IEND.B`.

Chrome Cache Entry: 192

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	6786
Entropy (8bit):	7.965927930926584
Encrypted:	false
SSDEEP:	192:vcbAACEFzOi9dbk04elkx8Q74m6o69cjdLpHQa8PSV0Aks:v8AAdFSsIeS4Po69SpHkP+tR
MD5:	3B87358A3C47C3286BF61E315EB2C346
SHA1:	ACD64F564368F7015484155D170D27C5E3E966D1
SHA-256:	6838A1BB1F6CCF606B6B23C0CE56B0AD2AB050758888B7EB42A186472C581B02
SHA-512:	7A4DEE0F5B8D1E63A3E1EA488A4FDF4D8850DF2CAD3548439DD8899ACB55C0BA94AEF01B48560259D01A3284DCF1D7947CF1EC754A7F49878832F1CA40446A CE
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/TcHgSH30vCBCtQfyFLWvvPJdpOAJrSp1OtqopwMue3yRiXa7wT5Fs8gUbA3oJylGW991=s256-rw
Preview:	RIFFz...WEBPVP8Ln.../..?..Gn.9.lk....<.j.5.....A.}TY.....+..dN]....O'.H..-3.....Y.%...h.;..$l6.\|.mc.[<...WQ.F....@X.... .6.....}...6..mk.....M.B.....`.....1K.5..t.c..l..*..... M..P...d;..R..d.....@.l...(AC.lW@..C.dK.....6.....e."..1..Z.j..,..}NweDL@.+.1G..:qa..u.....#.:B-'.T=a.h%..EK.....c.m.m.m.e..].].S...u.F=..^.pG.....b..N.u.F}b'.=.qf.....0....H.. ..?J.....@..v.{m.{.m{i.X.m.v1.....6..d...;.B.h.].~.....ylx\| ~.H%xSCY.~`lH .....D".. ../....b.T..E...6.$'..`.,H..q....;.m...?u...bp..:...h.""....T..a..v..L.+..H..d..B...aR...e.zb...+....+... .....5.}.8.5....O.....H%/.g./.]S...@.w Q5z.$..w..M.r.....}.-&.....3.....]-.gR"..C..<...>Q..E.....I..0.....e..D....._S.v.7...a%..V..3.H.....n...0..kBe.4....TzM...[i...C.X1..`..s....[...h..V^..... w.Y....A.....b...5...?.%#..,.%.]\....9C.G.".IKB...x.....=.....'.[.7....*V.n.4..S.O..\..M....$a.D,:.s.z.G..*..`...U.m0..t2.Q_T%..g.'i9..?B.....u.....m.[Gx;.#...)H....L.....

Chrome Cache Entry: 193

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	8990
Entropy (8bit):	7.959388167722879
Encrypted:	false
SSDEEP:	192:qL+8F5flrsw2TNllSoGp5DRBcFOC41pMvNjC1O4BCJXn5tzmgb:K+83flr7BRBcFO9SCwjzzt
MD5:	7367103A0E06381FB02DE1C6E95DD998
SHA1:	C2A6FF6A9EC8AD29584C6E2D01B15C17658664AB
SHA-256:	162FAB3FA3AE06EAFE7E688D8628A6896E99139D18B34EEEEADCAB541565A8AF
SHA-512:	C45351B6AB639FD72D3A7CDB34D2F95CC4DC82BC46ACD029F2388FF091E48FCA84E66F698D419F8E6CC2537EE706ECD199F52D94DE69AD900E41706F43EC9 8E
Malicious:	false
Reputation:	low
Preview:	RIFF.#..WEBPVP8L.#../?...M0h.H.&.....$.)..v._.0J.ki..[t.$E.e...o.1....$+../.....E..$..<...p,..5.?^.B&"".I...."<(.d.S....$*.....N....t.....8.....0.....+...g..^..@..._F.>.....:y3.....? ...XrNN<.B..wj.....2.^..*sw}....5www..`.. q;..{.....}..N...`.m.m.m{..{.$....=Q{.W...}0.....1(.....Zf9:.M.RB.[.....$.....G..P...L.'..S<wHr0e...8X..i%R;....Z..s{.Y..@(.*..ze9;.. ....4.$.....J..iAN...r.Osh.....!.4o.w..xs..u.....z.?.}.r._:..gw...3.rddc.....^..Z...k..N`_.I....H.....'.z..<L..`>.....7....w..aS...;..W..$.\.p~...../.P..H.....k.,=..9=..^.'.(...t_..N.W6# .+....e.<...(...8s.^.X{.QE~9.....).`..p;.....`.....P"6P?..p..Z.N.."(j...@.R.s.o.S.x.c".I.xxs.`z.....^..x...LI..`.....{..1P...~..#J...R.....[....}...Bd..{"M..g(..G..a.c..kz?y.l.D....0A. .....I.....q.@..H.i(R..o6..!.X.y...i'..Z....%..~..?,.*./ck.)...c.....E...o....~$.....Cz...T.....3.C<N.I....i4M.....*=).p./$.....

Chrome Cache Entry: 194

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (17227), with no line terminators
Category:	downloaded
Size (bytes):	17227
Entropy (8bit):	5.573217276068648
Encrypted:	false
SSDEEP:	384:RqH0uDlQ8hqe04GqmMb4EH4qnxJh+aPQN5XKq:RYZ5hqejNbjHnngbj
MD5:	9EDAB1C568F66A838F45722D37C07D57
SHA1:	56020CA13F1524A44AEF551C68ECF06009CC17A6

SHA-256:	B0B3C8A08AFFF51D87D6F144EB76C25BDFD19943CC6CB93E5F22B00C0728D06E
SHA-512:	A9D1B51BA6BA540EB0DA14C261B696E065BDD015820B4D0472187E506071B275137824DFF5D37DDE1EB1B5FA0F55595145589694EFA5699B03AA8BC75E266BD3
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/js/bg/sLPIoIr_9R2H1vFE63bCW9_RmUPMbLk-XyKwDAco0G4.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var u=this||self,D=function(K){return K},e=function(K,M){if(M=(K=null,u.trustedTypes),!M||!M.createPolicy)return K;try{K=M.createPolicy("bg",{createHTML:D,createScript:D,createScriptURL:D})}catch(f){u.console&&u.console.error(f.message)}return K};(0,eval)(function(K,M){return(M=e())&&1===K.eval(M.createScript("1"))?function(f){return M.createScript(f)}:function(f){return""+f}}(u)(Array(7824*Math.random()|0).join("\n")+'(function(){var Kw=function(M,K){return M[K]<<24|M[(K|0)+1]<<16|M[(K|0)+2]<<8|M[(K|0)+3]},h=function(M,K,u,D,H,B){if(u.J==u)for(B=V(K,u),436==K||86==K?(K=function(S,f,e,y){if((e=B.length,y=(e|0)-4>>3,B).SV!=y){f=[0,(y=(y<<(B.SV=y,3))-4,0),H[1],H[2]];try{B.RE=MS(Kw(B,(y|0)+4),Kw(B,y),f)}catch(O){throw O;}}B.push(B.RE[e&7]^S)},H=V(410,u)):K=function(S){B.push(S)},D&&K(D&255),u=M.length,D=0;D<u;D++)K(M[D])},fw=function(M,K,u){return u=J[K.B](K.Ch),u[K.B]=function(){return M

Chrome Cache Entry: 195	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	6786
Entropy (8bit):	7.965927930926584
Encrypted:	false
SSDEEP:	192:vcbAACEFzOi9dbk04elkx8Q74m6o69cjdLpHQa8PSV0Aks:v8AAdFSsIeS4Po69SpHkP+tR
MD5:	3B87358A3C47C3286BF61E315EB2C346
SHA1:	ACD64F564368F7015484155D170D27C5E3E966D1
SHA-256:	6838A1BB1F6CCF606B6B23C0CE56B0AD2AB050758888B7EB42A186472C581B02
SHA-512:	7A4DEE0F5B8D1E63A3E1EA488A4FDF4D8850DF2CAD3548439DD8899ACB55C0BA94AEF01B48560259D01A3284DCF1D7947CF1EC754A7F49878832F1CA40446ACE
Malicious:	false
Reputation:	low
Preview:	RIFFz...WEBPVP8Ln.../..?..Gn.9.Ik....<.j.5.....A.}TY.....+..dN]....O'.H..-3.....Y.%...h.;..$I6.\|.mc.[<...WQ.F....@X.... .6.....}...6..mk.....M.B.....`.....1K.5..t.c..I..*.....M..P...d;..R..d.....@.I...(AC.lW@..C.dK.....6.....e."..1..Z.j.,..}NweDL@.+.1G..:qa..u.....#.:B-'.T=a.h%..EK.....c.m.m.m.e..].].S...u.F=..^.pG.....b..N.u.F}b'.=.qf....0....H.....?J.....@..v.{m.{.m{i.X.m.v1.....6..d....;.B.h.].~.....ylx\| ~.H%xSCY.~`IH .....D".. ../....b.T..E...6.$'..`.,H..q....;.m...?u...bp..:...h.""....T..a..v..L.+..H..d..B...aR...e.zb...+....+.....5.}.8.5....O.....H%/.g./.]S...@.w Q5z.$..w..M.r.....}.-&.....3.....]-.gR"..C..<...>Q..E.....I..0.....e..D....._S.v.7...a%..V..3.H.....n...0..kBe.4....TzM...[i...C.X1..`..s....[...h..V^.....w.Y....A.....b...5...?.%#..,.%.]\....9C.G.".IKB...x.....=.....'.[.7....*V.n.4..S.O..\..M....$a.D,:.s.z.G..*..`...U.m0..t2.Q_T%..g.'i9..?B.....u.....m.[Gx;.#...)H....L.....

Chrome Cache Entry: 196	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	8594
Entropy (8bit):	7.966296411345263
Encrypted:	false
SSDEEP:	192:uBP/bR7pJfOTI3Nqeuo+gbCHvU0gMJ6FuAaPa2ZPStvh+YI8:aPzRqTMUTgAvU0JMwAEaDI8
MD5:	4AEA614380B998263508C1153B9DDEC6
SHA1:	6160ABF08D74CE8A9BAED61A8634935147AC1700
SHA-256:	393065BD8ACF1D886E07030B1DAE40B2387EC3AA631C46774A43FCEAAF9689D7
SHA-512:	F427D3CAC274F57F1A307C19B9A31760DF4D05F066199EAC6B7778694E53216BD214F9FA2AB139013875E64209FD55D710347FC5908FFC07A29DDB6ABDB1ED9
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/vTMochUbMqk9ehiZ7npCcwvhzOX8x0GlN1EHTW8sg58GBkcF48Vf6fwbvag5KwHxLA=s64-rw
Preview:	RIFF.!..WEBPVP8X.....?..?..VP8LA!../?...M(.$.2c....$"..T5L..'L3Tf.....0..S..w8...A$I.T._.33.O....m+9.....q"B"w.;..HRT.w..X.cf....4Cq..0EG.8.....{.-.2.ap...(.....i}J.".H..MMvN.... T8....~.dQ.f#Yx..A..!..pA.....!e...9...D..._..H...PY.....[jf...effffff.aff...L3.`.R.J..._....!c)c^.....2.6B&E..'3-...l.dZF..of.....!33..]\|.v<.msn;..H*).2..~!.^....m.6....y.N..$G.c...m.m..I....q&.J...i_=..m>.m.m.O..m.v.T.R.y.{L.....4.|..]N.....W}.Qk..i.j.....^...:..w...P.....s...k)Am.$...91}.t...._v....4....I3..j$.*H....WG..d.2f.....f...x5..N...-....utsy.m|."Z<....@.(..7g..qd\Z..w...L..9./.B]{.9.'leu..l#.{g.:go..D....4S....-q..C.....&...haAC.-....\;.v.^.....9...>=d'..c.....RF..N._.e.b.FVM.....|.T..)q..u.....,..0*9X.I.....6Vf..AH.....!..@.uwf.{@0%w..u..a.etU.'.N.....j .4.tN_.6.~...|.4..+C..W.n.P..XA.....x.GN3.DJ@J...',.Z9.J.....O..0].=...k....wi\.....&....Fl.i.+..1...[...ez0.y.V>....I.4.I-..c..D.....P.<4.. .0..b...`$...?m

Chrome Cache Entry: 197	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	266
Entropy (8bit):	7.052421013235357
Encrypted:	false
SSDEEP:	6:yk5ZYChDBpEnS96WesGKsxdRM8Zj5elkndH7xLiGE6CAYdr0jSKIz/zZwE4:34CRBpEnLID3Pb5e+LE6CACgmKIzLZwT

MD5:	0923A53B64E64DB75177B6972F016A42
SHA1:	6915D871CBEA8A3B8F4E54367DCA538DA0AC3082
SHA-256:	E0106DC1C0490A432C08671994F87FCBB982B7B25B4F9CBB640D49A03BD89CE3
SHA-512:	5054B69C1A895FEEC0CECD471FE317149D8F804E15CDC0ED51F8BA6B3FB61E092C5C78A92768D31273DBCBD189148D305BA4EB1EB210174DC6B0724615B1B F4
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../.....$g.....r^.E.$E.....~8...A.H....A8...%l#.Vr....b9.P.....N..[n.P.....6\.w.+.....X....U'...#.}...Y....A.xdB.....$%.ww....t. ....Q|.....,.....q...D.@!H.N. p.5.....*`...ms.~.l....\.[/..u=..@...X...4j=.}..edi.i...%..0u~.MH..

Chrome Cache Entry: 198	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	1798
Entropy (8bit):	7.849963237802661
Encrypted:	false
SSDEEP:	48:T3ye9MK9OVdLYYPjnPHKJ5dSgTDbzVS1UjV4bCGbC1e:u3f0Y7nPHKJ5VTXzIM4bCEC1e
MD5:	D3BA16BA660F19113FA5034379485C10
SHA1:	C23BE1B2F5B85B40F19B50E9CDFD47C4706CD40E
SHA-256:	9BDBD6817C5B5917609CCAF9DEE48146C62298159EC9804860FD1EC9C606BDC4
SHA-512:	75D68AD4136757106253132DFFD952521B10F215133F618CEA7DB3E709A719C7D19A2340A1C0F526F89E63C3C792C6B0F792400BB8354898DAD2D4FACD70288E
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/fDpoqIbZ884ylRnMK8Lx9Fu4DsLQk5yt4f9WkxeOAPpGnzc9BTi_YKkMsLvoMdx7Uzg=s64-rw
Preview:	RIFF....WEBPVP8L..../?....Em.I.....;.!...0:A...h.Mj....R.:Y.m$IQY....h.>..@....#L@.....##.....@.....8.N.4.!....m....m.....Zqe.m.5V.3.1..US...6y..w.u5....M...`.m$...?q-E .e.....q..$:.DuX.+p..H.O.%.d.I..g...$)g.n..}...4.7..6{.ds..;W../.....1.1.D...x...o.<b.<...k.G..P..;..mO.z.Hy1P... ...SH..X%L.....[..y..[.+&YA@.<..W6..x`=.....7.....9.....!F9 hsda.L..Aos.}.....ba`.n..Gb.|...2"....J&xE&7(.M.....6h.s?G.!.Q.Z..O.j.Ar+...:...Q...O. ...A.....S.w...w.nt.d...;...X].#YMs...i.fK.O....]..>.8..#.y.`....X}W...&b....._'L..9D...)R .i..$@..H.....)m...D."....G".4..Y.j..sC..h.vA..O`l9.$...&K.&.Y..AeF...h....P>);..MvG..]<*n.cP.....D.....&P...l.[B...Z-..V.....<.E2...n....z .EV27..9.>...QR.....C"x{...3.I_...K.....n. (..).....p..e|s...[.$u..h.h....Z.R`....&..O~/.YO.fv.....)bJ ....4....X...1.....7.....9..)b.....<n...b.<h...+<...[.....kdE.lt0.....*.byU.ul,.E.1e!].W.....-.B..7.`..A.rN.h.j!m...0t..A ...j

Chrome Cache Entry: 199	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	7114
Entropy (8bit):	7.949066568760502
Encrypted:	false
SSDEEP:	192:fSsvvBv3D6GRt1wC7xRQ2N2KLb6X30dGN4gFlF9+l:fSi5v5Rrf7/QxYb6HZ4W9+l
MD5:	794D878D3F3333508C9270AF3E2EADA2
SHA1:	1AB7FAA454D5EF9A1599B106C8002B7B2B22677E
SHA-256:	669AF012E2BBC4A3665B8BBE67DFAF6C65E31C5601FAD90B78C66E297C077730
SHA-512:	7F17E2EB5975129EE51039A746D6D8EB64EECB7DDFA429B90EFC405EE1E4181488FFBEE8F52430C98B2189980135BE40D28647811E58074C526EF086E9FE5FC F
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/Y9BUoMIWfhZDUFZ_MxQmnsgSyb3O8s8Sds65E_j46-vdDSJi_0Xqmoa-fHaQa7fGlw=s64-rw
Preview:	RIFF....WEBPVP8L..../?...M(l..Avw.....}.w...)..E..... Y8.$Y.....`q..d..l....T....{3l#.V.pw.)... "uww....G.:-z...^~u..Z.D.~.....'h.....K.V.....S....}.....w...7+W'....S.*..-. Z2.@._y`..k^.....i....!"&...O....<..H.m[..)s...,f..Z..^.X.Zl[Affc3..1..[.J..k.V$9..h....,.].ki&.....k..P6.....01.E.....P.m..t..o.....m.n...qDd.2.....l.m..'.m..u..\Y....q..m.....C..m...8##. U..j./.m.6~.m.5....3+.q..7.M.m-.R[o]..m....m[sn.m.....^k.s...h...B..j..G....%.....<Z..d.....}.P.....D.d.E.!@=;....g..t.2g...A...lq-i.4...h....L.....d....a..).&*s..q.....t..t.@ ..BG.T.Ub.....l.....AO.....ZO ...-....Qs..1!.=....P...]...L..XfP(.b.....w.}c.?.....!A).D."..*c..-..A....(!D).Rg{;'.MU...R&HO..n.....^k...<.K...H.W..W@...y..AF.$.l.....{/[S.&.(-..8..... ;.....&....H;.....-?=.i...(...I..w..~....3.....w..~g....:.I.K.....~..u{..RAr C.c.L..7.....j7....t..k.....'.8..[..@.....Z..YQg..-.....

Chrome Cache Entry: 200	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (4048)
Category:	downloaded
Size (bytes):	16755
Entropy (8bit):	5.4581596618045864
Encrypted:	false
SSDEEP:	384:TJPw7nfFalTPq8TC9q1ZJ/xFhJTqLG2QQR83DqjCx2pgLsQCbHkepKwV1FpTsXUW:Nw7nfFal+8X1ZJ/xFhJWLqA83Dt2pg1/

MD5:	28307CB3ADE9AFE8774EAE4F6B31D27B
SHA1:	F2B16D17015502A7BE8EA101A1C409063AF0BDF3
SHA-256:	B5830D09EA4F2C592F13B38398261825AD55ABC4E6803A03B2F6DAB7E3C39606
SHA-512:	D18FBC72D10550E45EE9FE401668627BEF3229B045E750002B55349500010D53E0B487AFAFEEA17FFF840E46A22B11E219BD8DF722EC61D0754659B36750C841
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,CvxVpd,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,M2Qezd,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,gKWqec,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=RqjULd"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("RqjULd");.var X8a=function(a){if(_.aa&&_.aa.performance&&_.aa.performance.memory){var b=_.aa.performance.memory;if(b){const c=new W8a;isNaN(b.jsHeapSizeLimit)||_.Jh(c,1,Math.round(b.jsHeapSizeLimit).toString());isNaN(b.totalJSHeapSize)||_.Jh(c,2,Math.round(b.totalJSHeapSize).toString());isNaN(b.usedJSHeapSize)||_.Jh(c,3,Math.round(b.usedJSHeapSize).toString());_.H(a,W8a,1,c)}}},a9a=function(a){if(Y8a()){var b=performance.getEntriesByType("navigation");if(b&&b.length){var c=new Z8a;if(b=b[0]){switch(b.type){case "navigate":c.Ke(1);.break;case "reload":c.Ke(2);break;case "back_forward":c.Ke(3);break;case "prerender":c.Ke(4);break;default:c.Ke(0)}var d=_.Gh(c,2,Math.round(b.startTime));d=_.Gh(d,3,Math.round(b.fetchStart));d=_.Gh(d,4,Math.round(b.domainLookupStart));d=_.Gh(d,5,Math.round(b.domainLookupEnd));d=_.Gh(d,6,Math.round(b.connectStart));d=_.Gh(d,7,Math.round(b.connectEnd));d=

Chrome Cache Entry: 201	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (4048)
Category:	downloaded
Size (bytes):	16755
Entropy (8bit):	5.4581596618045864
Encrypted:	false
SSDEEP:	384:TJPw7nfFalTPq8TC9q1ZJ/xFhJTqLG2QQR83DqjCx2pgLsQCbHkepKwV1FpTsXUW:Nw7nfFal+8X1ZJ/xFhJWLqA83Dt2pg1/
MD5:	28307CB3ADE9AFE8774EAE4F6B31D27B
SHA1:	F2B16D17015502A7BE8EA101A1C409063AF0BDF3
SHA-256:	B5830D09EA4F2C592F13B38398261825AD55ABC4E6803A03B2F6DAB7E3C39606
SHA-512:	D18FBC72D10550E45EE9FE401668627BEF3229B045E750002B55349500010D53E0B487AFAFEEA17FFF840E46A22B11E219BD8DF722EC61D0754659B36750C841
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,SdcwHb,SpsfSb,TSrO,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,chfSwc,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,gychg,hKSk3e,hc6Ubd,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,developerdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=RqjULd"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("RqjULd");.var X8a=function(a){if(_.aa&&_.aa.performance&&_.aa.performance.memory){var b=_.aa.performance.memory;if(b){const c=new W8a;isNaN(b.jsHeapSizeLimit)||_.Jh(c,1,Math.round(b.jsHeapSizeLimit).toString());isNaN(b.totalJSHeapSize)||_.Jh(c,2,Math.round(b.totalJSHeapSize).toString());isNaN(b.usedJSHeapSize)||_.Jh(c,3,Math.round(b.usedJSHeapSize).toString());_.H(a,W8a,1,c)}}},a9a=function(a){if(Y8a()){var b=performance.getEntriesByType("navigation");if(b&&b.length){var c=new Z8a;if(b=b[0]){switch(b.type){case "navigate":c.Ke(1);.break;case "reload":c.Ke(2);break;case "back_forward":c.Ke(3);break;case "prerender":c.Ke(4);break;default:c.Ke(0)}var d=_.Gh(c,2,Math.round(b.startTime));d=_.Gh(d,3,Math.round(b.fetchStart));d=_.Gh(d,4,Math.round(b.domainLookupStart));d=_.Gh(d,5,Math.round(b.domainLookupEnd));d=_.Gh(d,6,Math.round(b.connectStart));d=_.Gh(d,7,Math.round(b.connectEnd));d=

Chrome Cache Entry: 202	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2162)
Category:	downloaded
Size (bytes):	195575
Entropy (8bit):	5.484447098062502
Encrypted:	false
SSDEEP:	3072:ZHARgMLVYxC4rboc7KTgdFiQnBCckeGrxygKxP/toI0QFY3o1u7ojsVFcSFgFlnF:ZHARgMLV4RrboSKTgdFiQBCck7rxygKR
MD5:	AB8804FC24BF364CA1169FF0F7D9192F
SHA1:	4B1E723246EA6F88C1F7E07895777AE99DC3E2C5
SHA-256:	5461579426FD97036CE5C52E27625C2B61085DC38E8FDB81992FD5E825A26DDB
SHA-512:	883BF8FACEC5C3E19274150332F3AF17618C9D5A54C6BA938A4F445DE91A6C66F8FD3E6E9E6ADF30AFB1F691483A374ECD86CBD23ECEF97E6813070B929B0E1E

Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/am=022DoYEFBv4jfQ-2/d=1/excm=_b,_tp,appscategoryview/ed=1/dg=0/wt=2/ujg=1/rs=AB1caFU4y67OJEhh6CzWJiwmF9DXNHswJA/m=_b,_tp"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(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)([0x21836dd3, 0x38181606, 0x20f7d23f, 0x2d,]);./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2013 Google LLC.. SPDX-License-Identifier: Apache-2.0.*/.var baa,daa,haa,laa,Ja,Ma,Oa,maa,naa,oaa,paa,Va,Xa,raa,uaa,kb,Haa,Jaa,Gb,lb,Naa,Paa,Qaa,Uaa,bba,hba,iba,jba,lba,oc,nc,oba,Bc,tba,sba,uba,vba,Cc,wba,yba,Hc,Aba,Rc,Bba,Tba,Qc,Vba,Oc,Wba,Dc,bca,ed,Ica,nd,nca,od,rca,tca,xca,yca,Aca,Bca,Fca,Hca,Lca,Mca,Nca,Rca,Zca,Vca,ada,ce,fda,gda,ida,ne,pda,rda,te,sda,uda,vda,zda,Bda,Eda,Fda,Gda,Hda,Ida,Lda,Mda,Qda,Wda,Xda,Yda,$da,dea,eea,fea,aaa,gea,hea,iea,jea;_.p=function(a){return function(){return aaa[a].

Chrome Cache Entry: 203	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (5955)
Category:	downloaded
Size (bytes):	232417
Entropy (8bit):	5.569478189750226
Encrypted:	false
SSDEEP:	6144:BWODkSPMZjG5Kni1AdWds8GWlzAt2E9vTfzCL:/lPISllzAt2ovTr+
MD5:	3B06C5D64E8AED7450A9DA117068C18E
SHA1:	A7060FCD6D58A1962A038A319F85DFDDA7ED7F90
SHA-256:	43F7F2598561A79DD543794763DE5DB5280D7D53BC1897EE348BAE872BE04955
SHA-512:	03736FF064D8ACBD4687A3B37B9204F8C7F48E235A1F47D6D9D4BAB6E5AE692721624E5307464E718D6B544A8BAC5B5C48192C57B1251FA8CC6C4418B06D62E3
Malicious:	false
Reputation:	low
URL:	**http**://https://www.googletagmanager.com/gtag/js?id=G-6VGGZHMLM2&l=dataLayer&cx=c
Preview:	.// Copyright 2012 Google Inc. All rights reserved.. .(function(){..var data = {."resource": {. "version":"5",. . "macros":[{"function":"__e"},{"vtp_signal":0,"function":"__c","vtp_value":0},{"function":"__c","vtp_value":""},{"function":"__c","vtp_value":0},{"vtp_signal":0,"function":"__c","vtp_value":0},{"function":"__c","vtp_value":""},{"function":"__c","vtp_value":0}],. "tags":[{"function":"__ogt_cross_domain","priority":17,"vtp_rules":["list","play\\.google\\.com"],"vtp_enableSuggestedDomains":false,"tag_id":15},{"function":"__ogt_referral_exclusion","priority":7,"vtp_includeConditions":["list","play\\.google\\.com"],"tag_id":17},{"function":"__ogt_1p_data_v2","priority":7,"vtp_isAutoEnabled":true,"vtp_autoCollectExclusionSelectors":["list",["map","exclusionSelector",""]],"vtp_isEnabled":true,"vtp_autoEmailEnabled":true,"vtp_autoPhoneEnabled":false,"vtp_autoAddressEnabled":false,"vtp_isAutoCollectPiiEnabledFlag":false,"tag_id":18},{"function":"__ccd_ga_first","priority":6,"vtp_

Chrome Cache Entry: 204	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1798
Entropy (8bit):	7.849963237802661
Encrypted:	false
SSDEEP:	48:T3ye9MK9OVdLYYPjnPHKJ5dSgTDbzVS1UjV4bCGbC1e:u3f0Y7nPHKJ5VTXzIM4bCEC1e
MD5:	D3BA16BA660F19113FA5034379485C10
SHA1:	C23BE1B2F5B85B40F19B50E9CDFD47C4706CD40E
SHA-256:	9BDBD6817C5B5917609CCAF9DEE48146C62298159EC9804860FD1EC9C606BDC4
SHA-512:	75D68AD4136757106253132DFFD952521B10F215133F618CEA7DB3E709A719C7D19A2340A1C0F526F89E63C3C792C6B0F792400BB8354898DAD2D4FACD70288E
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../?....Em.I.....;.!...0:A...h.Mj....R.:Y.m$IQY....h.>..@....#L@.....##.....@.....8.N.4.!....m....m.....Zqe.m.5V.3.1..US...6y..w.u5....M...`.m$...?q-E.e.....q..$:.DuX.+p..H.O.%.d.I..g...$)g.n..}...4.7..6{.ds..;W../.....1.1.D...x...o.<b.<...k.G..P..;..mO.z.Hy1P... ...SH..X%L.....[..y..[.+&YA@.<..W6..x`=.....7.....9.....!F9hsda.L..Aos.}.....ba`.n..Gb.|...2"....J&xE&7(.M.....6h.s?G.!.Q.Z..O.j.Ar+...:...Q...O. ...A.....S.w...w.nt.d...;...X].#YMs...i.fK.O....]..>.8..#.y.`....X}W...&b....._'L..9D...)R.i..$@..H.....)m...D."....G".4..Y.j..sC..h.vA..O`l9.$...&K.&.Y..AeF...h....P>);..MvG..]<*n.cP.....D.....&P...l.[B...Z-..V.....<.E2...n....z .EV27..9.>...QR.....C"x{...3.I_...K.....n.(..).....p..e|s...[.$u..h.h....Z.R`....&..O~/.YO.fv.....)bJ ....4....X...1.....7.....9..)b.....<n...b.<h...+<...[.....kdE.lt0.....*.byU.ul,.E.1e!].W.....-.B..7.`..A.rN.h.j!m...0t..A...j

Chrome Cache Entry: 205	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 492x328, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	21832
Entropy (8bit):	**7.990590814222627**
Encrypted:	**true**
SSDEEP:	384:D3+9ModnYb9qCCuG97KA/BW552stD5U/N8LweN5SXyAH/Ma+laOZQ:Cuo8qPuG97vM2stDPN5SmWQ

MD5:	C08171D45D3A9DC7ADD2943A50384AC3
SHA1:	5972E27EEDA5CFC5D0F5B4C232AA5D5B230E5E88
SHA-256:	2CF9528CE001570CAA1BBDFE7D45F60F797DC2302583F587F722CEC5180F096D
SHA-512:	A113CD62EED4FF57866423E3FF3965248C92969D235D4D66234625EDD1CFAA93643F9DDB4F24B25B7017EC51F845178555A5520ABFB7890A0E524AA7ECB392E
Malicious:	false
Reputation:	low
URL:	http://https://img.cdn.house/files/ads/56661/65ea33056122f.png
Preview:	RIFF@U..WEBPVP8 4U...5...*..H.>.:.G.#.,..H...In._...\c.2?..O.....W.g.....o..C.K....E...k./.....H.....g..._...{..K.....onOY....T.!.....}.....O..w._e..`...?..K.....e.....w.s.....I?. .B.z.K....|.]..............@...4O..W.2...?.....7..NoH.D.0....N.8f_.....q.A.q.#E..9...a..{`"..ZMV`...Lgj..g,....../.....S.O.w.C....Rp[... ....Xx2../<.O.../<..7..>.?.A{p.....t..[.i.Ru2.....| ..X.....{.....3.h../QK.Y....b....(...C..\3c.I>...'...\x.....jT...]..-_5I.Fb.x.....='...gT...mg}....B#..-FMW4{.C.Q....\hI..w..z.Ob.X.&./.E..^.&i ....,.y..ybcB..z...G..m...i...+O.1...p>=...S B9.....p.Z....)R..1..1{nyqGt.R..V..A_Y..v.ZE..M:.e3.B.....~..}.....{;r.g...Jy...bY..U...`=..Z/.....tn7..Q...S.....3R...;....F(.P..8...M0..UG.<o.....L.pf-....5"WOU.R..C..(X.....4.....ST. {...<.....e.Sy].djXN..@....?...."V...x.p`.xx@$k.3.$k.3.$f.'..b.Fx..V..63&..|.d...5..`?Q....2`..AI...I.....\.':Q..3....r@j....X.v.]-#.?.~.Gp..Z4h.....8.

Chrome Cache Entry: 206	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	downloaded
Size (bytes):	39909
Entropy (8bit):	7.976805543329996
Encrypted:	false
SSDEEP:	768:RH5XX+GbkfLohh7BRsSrRq/oiREkzqNZJsLjt1DUaJNmjgftLEYZjT9:RZ9bkDcBRsyk/oiRuNfsLQaJNqgVLEAp
MD5:	ED6B32D646E747CD9BBD172A3764C098
SHA1:	EEAEE2B6587AAB5280C9131B73BC17C62BC7B02C
SHA-256:	9B860B3327FD3D017F15B8589D08DD6CD9E01CF7FD59910DE16416B28FD4FFBB
SHA-512:	90C9C43F95FB7E173DEC3396782F7438677CFE7E125B80B4255CAA46C2F5BA4C281328DD9E676FAE761B2651A26CAF58FFFDCA73A4D9D59528DF43BF9828FF4 5
Malicious:	false
Reputation:	low
URL:	http://https://i.ytimg.com/vi/uWsQ5IWViIM/hqdefault.jpg
Preview:	......JFIF.....h...."...N.....!1..A."Qaq.2..B... ....#R.Sbr.....3C...$..s...4c.....?.....!1.AQaq."......2....#B..Rbr.$3C.....?..eE.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE .E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.! .QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.E.P.QE.!.QE.E.QB.En..-q..._...^...f;l.....8...`.W.<?..k.../.....}.....{....Q...D.p.....'....._...Q.....pG.....fc..r..X.....p..^. ..^W.d...-.....Z..P...X.....z.....*'...EJ.....E~..~.\lw..>./..QU.....0.....O..s#.>...El....W.....E...v.....j...Q.....1q..p..^...\....W.....l/v.x...)Em....W.....

Chrome Cache Entry: 207	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (8117)
Category:	downloaded
Size (bytes):	220791
Entropy (8bit):	5.696164391289731
Encrypted:	false
SSDEEP:	6144:8nLSrtlRFNMPAlFFOMnxPhEJ4EngPgTV1r0sHSJyW/qnypjEHOkVfsPwKInkPawz:8nLSrtlRFNdFFOMnxPhEtZr0sHS0Jypd
MD5:	C9951DEE13CE6250791F1EC702389A45
SHA1:	D86FBB78D351505D86153079DAB462E42DD9F7DF
SHA-256:	D0950FE8EB786945C11EDC3C18873043D6DB4413BEF094710C39F9CFD4EA58B6
SHA-512:	1C6001B4C4CE10338440BC171A599623D52B7353259FB3FA81BCA0DCBFFF25EE091410FB28160117B32FCFC44E13D58F0BE6E7AF20A8C7B3BC7106A33EC6A1E 7
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,IcVnM,JNoxi,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,fl2Zj,gychg,hKSk3e,hc6Ubd,j9sf1,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,ovKuLd,pYClec,pjICDe,pw70Gc,q4UNLc,s39S4,vrGZEc,w9hDv,wW2D8b,ws9Tlc,xQtZb,xUdipf,yDVVkb,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=vNKqzc,fl4Vwc,sJhETb,JWUKXe,t1sulf,JH2zc,tBvKNb,soHxf,lJGqxf,wg1P6b,ywOR5c,PHUIyb,BfdUQc,oEJvKc,kJXwXb,chfSwc,aTwUve,indMcf,RQJprf,lpwuxb,NkbkFd,nKuFpb,zBPctc,jX6UVc,qfGEyb,fdeHmf,SWD8cc,tKHFxf,rpbmN"
Preview:	"use strict";_F_installCss(".H1RBrd{max-width:500px}.UIeOBe{margin-top:30px;min-height:120px}.k2cXo{margin:0}.XWz5yd{margin-left:160px;padding:0 20px 20px}@media screen and (max-width:480px){.XWz5yd{margin-left:0;padding-left:0}}.iCVHHc{height:215px;text-align:center;width:160px}.FOYkDe{max-height:215px;max-width:160px}.Dtwbxf{font-size:28px}.Hv8szf{text-align:right}.rYrxJf,.rYrxJf:visited{color:#00838f;padding-left:3px}.F9JOfb{margin-right:3px}@media (max-height:fit-content48px){.ZDGq3b .VfPpkd-P5QLlc{max-height:calc(100% - 48px)}}@media (min-height:fit-content48px){.ZDGq3b .VfPpkd-P5QLlc{max-height:fit-content}}@media (-ms-high-contrast:active) and (min-height:fit-content48px),(-ms-high-contrast:none) and (min-height:fit-content48px){.ZDGq3b .VfPpkd-wzTsW{align-items:stretch;height:auto}}@media (max-width:528px){.ZDGq3b .VfPpkd-P5QLlc{max-width:calc(100vw - 48px)}}@media (min-width:528px){.ZDGq3b .VfPpkd-P5QLlc{max-width:480px}}.ZDGq3b .VfPpkd-P5QLlc{min-width:calc(100vw - 32px)}.ZDG

Chrome Cache Entry: 208	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1692)
Category:	downloaded
Size (bytes):	36071
Entropy (8bit):	5.427759367605427
Encrypted:	false
SSDEEP:	768:kODeBRUnFSleydV1oqAFhY7XjbiZxchFHqv5ZgWh1RRlEtIMbh7nxEKXOMI0Jxz8:KeydDoqAie2h4gkRRWaWJnxEYOpG7l3d
MD5:	92527A50FD03CAEECF2B9136D03E2A23
SHA1:	8BB29676DE788A6BF670C7F12444F693803B02E2
SHA-256:	82CCBE7C6CE15AC8B756F13078B27F21CC84B800B3277F13F52AF3DE4AB88568
SHA-512:	B1B9FD82CF5B5F248CC26CD10EA8509CDE6300EFE4C2604AD9F0BA35739099281736EBD64CB30856C31D955207EC350920748E94014388A1487AC5FAE3B7CB8A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=_b,_tp/excm=_b,_tp,developerdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=byfTOb,lsjVmc,LEikZe"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.Spa=function(a){let b=0;for(const c in a)b++;return b};_.Tpa=function(a,b){for(const c in a)if(a[c]==b)return!0;return!1};_.Upa=function(a){return a.Lh&&"function"==typeof a.Lh?a.Lh():_.ea(a)||"string"===typeof a?a.length:_.Spa(a)};_.Gn=function(a){if(a.Vh&&"function"==typeof a.Vh)return a.Vh();if("undefined"!==typeof Map&&a instanceof Map||"undefined"!==typeof Set&&a instanceof Set)return Array.from(a.values());if("string"===typeof a)return a.split("");if(_.ea(a)){for(var b=[],c=a.length,d=0;d<c;d++)b.push(a[d]);return b}return _.eb(a)};_.Vpa=function(a){if(a.Wl&&"function"==typeof a.Wl)return a.Wl();if(!a.Vh||"function"!=typeof a.Vh){if("undefined"!==typeof Map&&a instanceof Map)return Array.from(a.keys());if(!("undefined"!==typeof Set&&a instanceof Set)){if(_.ea(a)||"string"===typeof a){var b=[];a=a.length;for(var c=0;c<a;c++)b.push(c);return b}return _.fb(a)}}};.var Xpa,Vn,fqa,

Chrome Cache Entry: 209	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1402)
Category:	downloaded
Size (bytes):	125062
Entropy (8bit):	5.654590268726825
Encrypted:	false
SSDEEP:	3072:2nLSrtlRFNtPAlFFOMn7RhEJ4EngPgTV1r0hRtOa57SJyW/qnypjEBJOkVfsYQnB:2nLSrtlRFNtPAlFFOMn7RhEJ4EngPgT3
MD5:	44FFA59EA8CC0A0FBD268896F4BE56CA
SHA1:	BE07274980FCE0AFBF7316424CC9E00676A6ECE8
SHA-256:	C66B30E65DADD44A412F04B67C6710CEC168DFC6E94FB947C039EF328A431C68
SHA-512:	7E699A3CEA6BA19B3C47E6BAFA99EE8788490DD2979FFC92804D3F4CAE68D5357017CEC0040A95EA3911489A0BCE2FB6E3E319FCBB984B29ABF0854490C7FD76
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,IcVnM,IgeFAf,JNoxi,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,fPcQoe,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,ovKuLd,pYClec,pjICDe,pw70Gc,s39S4,vrGZEc,w9hDv,wW2D8b,ws9Tlc,xQtZb,xUdipf,yDVVkb,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appscategoryview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=vNKqzc,fl4Vwc,sJhETb,JWUKXe,t1sulf,JH2zc,tBvKNb,soHxf,lJGqxf,wg1P6b,ywOR5c,PHUIyb,BfdUQc,oEJvKc,PH175e,fdeHmf,rpbmN"
Preview:	"use strict";_F_installCss("@media (max-height:732px){.vFondc .VfPpkd-P5QLlc{max-height:calc(100% - 32px)}}@media (min-height:732px){.vFondc .VfPpkd-P5QLlc{max-height:700px}}@media (-ms-high-contrast:active) and (min-height:732px),(-ms-high-contrast:none) and (min-height:732px){.vFondc .VfPpkd-wzTsW{align-items:stretch;height:auto}}.xoKNSc{margin:0 -24px;padding:0 40px}.Ud1OW{background-color:#e9f0fe}sentinel{}");.this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.tCa=_.A("vNKqzc",[_.Uj]);._.u("vNKqzc");.var J6b=class extends _.Uq{static Ja(){return{service:{view:_.cL}}}constructor(a){super(a.wa);this.we=a.service.view}H(a){(a=a.event.target)&&(a=a.getAttribute("href"))&&_.aL(this.we,a,!0)}};_.V(J6b.prototype,"fAsfBd",function(){return this.H});_.Bs(_.tCa,J6b);._.w();._.u("r0aiGd");._.qAb=_.Ek("efhmcb");._.w();._.sLa=_.A("sJhETb",[]);._.uLa=_.A("tBvKNb",[]);._.vLa=_.A("fl4Vwc",[]);._.pN=function(a){a.getData("enableSkip").H()&&_.$d(a.el(),()=>!0)

Chrome Cache Entry: 210	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	244
Entropy (8bit):	7.153897685834863
Encrypted:	false
SSDEEP:	6:c3Zulvhb4/Ep0/bXorL+jrXTvx2GCTn0LpIaoyI:c3Ql94sp0/jorUXTZ2GS09IaoyI
MD5:	9DEA3CBD9E0F9B455FDE32DCA965B41F
SHA1:	8049A160E77BF9FDD2446113611BB8C99D1E5A53
SHA-256:	3A1344E63287114EAD7F90BE694B7FC95370BF7B215D89BE93A54F39C15011CB
SHA-512:	E559F6BC3C44DC6E793EC98832926FAEB3D2D34811041868244CA89DF67DFAEB899689723C0DDAB5A58063EB4E42539614BEBBA23E09A8697E863F20416DB59 4
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/iFstqoxDElUVv4T3KxkxP3OTcuFvWF5ZQQjT7aIxy4n2uaVigCCykxeG6EZV9FQ10X1itPj1oORm=s20-rw
Preview:	RIFF....WEBPVP8L..../....5...Fm4.W#...0D.]....J...r..l.2...6.mU....5.C.(.....'vi...R...Fm.t.......\.._..Y.....c; ....| ....pk..b....`..........p..../.72<.........AQ.........Y..@.ErE.....d..]:..KG .^.@L.S..g..z..^.g.zg..\.JE..

Chrome Cache Entry: 211	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (56398), with no line terminators
Category:	downloaded
Size (bytes):	56398
Entropy (8bit):	5.907604034780877
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKYlebyB5lxRx54PHSGdXXwW7MFWwXVuE2:4UcW6v+0B5chXwW49z2
MD5:	EB4BC511F79F7A1573B45F5775B3A99B
SHA1:	D910FB51AD7316AA54F055079374574698E74B35
SHA-256:	7859A62E04B0ACB06516EB12454DE6673883ECFAEAED6C254659BCA7CD59C050
SHA-512:	EC9BDF1C91B6262B183FD23F640EAC22016D1F42DB631380676ED34B962E01BADDA91F9CBDFA189B42FE3182A992F1B95A7353AF41E41B2D6E1DAB17E87637 A0
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/releases/QquE1_MNjnFHgZF4HPsEcf_2/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url();background-repeat:no-repeat}

Chrome Cache Entry: 212	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2056)
Category:	downloaded
Size (bytes):	18372
Entropy (8bit):	5.452504565468757
Encrypted:	false
SSDEEP:	384:hcXfX9yALAULgMEcqdeydhPN+A+F4+5SYOelHO91XErIuW:hcXfXtLAUL405dzOGPi
MD5:	9E2ADB386B5EE3DCC04AFB8A4131FCC0
SHA1:	C98CB6D8F6FDE39D496DBA4C7D75E692C32C499F
SHA-256:	B9D589B80851934997657F105F130F05FFAD98478DFE8B0BE4313DC7EFAADC95
SHA-512:	A3FFA25575014B62CA4E55F08CD45206A211837A4ACD1A2DC2C92AC6C1D7BAB8F0ABC47CF70D391D5192397234BC746990E43489E7E0770E7377B2345AE993
Malicious:	false
Reputation:	low
URL:	http://https://apis.google.com/js/api.js

Preview:	(function(){var aa=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},g="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ea=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");},fa=ea(this),h=function(a,b){if(b)a:{var c=fa;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&g(c,a,{configurable:!0,writable:!0,value:b})}};h("Symbol",function(a){if(a)return a;var b=function(f,k){this.B=f;g(this,"description",{configurable:!0,writable:!0,value:k})};b.prototype.toString=function(){return this.B};var c="jscomp_symbol_"+(1E9*Math.random()>>>0)+"_",d=0,e=function(f){if(

Chrome Cache Entry: 213	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	792
Entropy (8bit):	5.271423979636484
Encrypted:	false
SSDEEP:	12:kRZTFMTaH/Af1RDyBmH/Af1ODTGiw1YZH/Af1oAWD3GXQvnFpH/Af1sDZ2kbRN20:kzeTafoffR6iw1GfLnFpfLdrl
MD5:	4394984BDFC2465754EAC8C70F384628
SHA1:	A43018C1513B1AC900DC05201E5D636FB5954E9C
SHA-256:	38A273950BF3FC4C8A97644A01BEC26894EB2026C37C91A8900689914E969650
SHA-512:	09B0352BF9386351DFE79B795BB6333CE1D76541C15B82BDD5FB3A61D31201384181962A8CBAF0065113A57A85C2D487F9692EBF43447794459F0B450581B68A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,CvxVpd,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,M2Qezd,Ml6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RjJvI,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fPcQoe,gKWqec,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=yNB6me,qqarmf,FuzVxc,l8lFqf"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("yNB6me");._.lr(_.BBa,class extends _.mr{constructor(a){super(a.wa)}H(){return"yNB6me"}O(){return!0}hb(){return _.g2b}});._.Qq.yNB6me=_.l2b;._.w();._.u("qqarmf");._.lr(_.nCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"qqarmf"}O(){return!0}hb(){return _.S5b}});._.Qq.FuzVxc=_.V5b;._.w();._.u("l8lFqf");._.lr(_.sCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"l8lFqf"}O(){return!0}hb(){return _.Y5b}});._.Qq.l8lFqf=_.$5b;._.w();.}catch(e){._.DumpException(e)}.}).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 214	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1524
Entropy (8bit):	7.867931299726191
Encrypted:	false
SSDEEP:	24:cHWkHLH7Y106ScPyQtVmBrNb22/i4UID/Vn83YxViQ/l8AV+ZoXkNGAVayhdFr3b:c2sH7l6S2yQ2rk2/GID983YFCekN7Amv
MD5:	765391F2F78961FF2B9317EA1F4A4A23
SHA1:	D09773D7CDE72481574D23224E04A38754CE3F0E
SHA-256:	B8A5F9C559C011C6FBCC4E66A59D4691F507B164196B09E3340E81CE66D6F8A2
SHA-512:	C1A96B6134B6CF369C02E207FD80C0DC68BADBDB893A754D8280B73D0FD784F990FE96A0FCBEA188CF6BF7D424E4C84AE7EE0EA9EEB6BB68ACB30A56497AD343
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../?.....m.0J.....O..0...N..HR.....E.."..h.M.....Y.Dd..4..mv.....1.q.b.YG.....$.$.....d.\....Bm...nV/....P}...5m..m..;..6.l.m..k..f...SS..+...l....{....#: ...h...\f*.h.....n.)..K.w.{.~).....,\..a..r.}....P...b./.o...%.h..\T~.....".l.t.<..1Mq.2.(.b.D..e..,ij9.H.G2..$..._.^.F..7..}....p..-..4.d.....r..j.....?..Xn..<.....H.Ul.Z4ZnMl.Z.?9.../.}z.m..s...R..f.8 ..C..I.[...A.P!.20.....lr.o.w....}..S....&..6.(..{...Kb.v^.B...JV.`...k...a..7.....|pb...YJj$....u.....R.m.0..h.B.SDZ.O...t.....{.C.q.0..o>.mg)..$.....G"..j.%u....>._.K.kg.c(.^..?.N.S.....N..1..j`+ 4U.)....(x.4...D{.&.2r..!.w.W...9c.....!A#.w#YQ..#.R.EW..NW..;_".$!.yR.....f87.N6+..,bw..(.....LZ-.D. M"..;./9/Z..LZm>.Xk..l...%.^.9.....,n.c.),.....^.dl2.O..Z.G....;|"x...%.a/.....^...\..}.3C.*v...wq.....(.#x...q....n.78j<.._....u]....d.@...DA.....,"....H....O<..N..v2&.'z...`.....B@...PVS..c...|h4.@.....r.fG5.5]..Y5

Chrome Cache Entry: 215	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	6384
Entropy (8bit):	7.956987109259552
Encrypted:	false
SSDEEP:	192:72Z3tJlNEJCM++MkNrKZN2YPHRRxf1BfnEdQSOVk2EGU:72DuDBIZN2Ef1BTfV5E1

MD5:	348FF1C2E2160906063F6A951ADECC1C
SHA1:	2C1F1A51A4C9B69990A253ECC45D1743DEF5C200
SHA-256:	867FFB53745AB55C63D8D55D91CCDDEC25EB1175123154062243D9322BF03802
SHA-512:	98DB445431B1B9260E29EA2A3B487D9A6EFEB5352163371B18F52414D9EE6D0BFFED3A5A22FA9EFEF4564C9BBB0DC44FD3051E1200A71EC2BC9821F2FBF85E99
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/NVUOs8Vh4nvaP1pTvdrmhfzpy5rYZcWJl13uxyLjRCWZmEubC1PyjihCCi2TCO9FfQ=w526-h296-rw
Preview:	RIFF....WEBPVP8 .....f...*..(.>E..E"...xE.(.D..]...<...C....8.....0..?...<.~.~.....U...I.n.g.....-..]._.....'..Y{...._..../.=....!..<...S.?...?..&...'....._.....G.o...7.....d.....Y....S?.~Z.R..)...........o.{...;.....+...../.?....y.w.#.o./...7.....?.O.....#.....o.....%.]..........P...&9.....h..1.T.....=..hi.Mr.>v.&.N:w5..a>.w..j.n...|...J...s...=Iw.8g\.T.xs'.R.b...,.;*H..<...../@.jiwQ....7.?.?I..LB...7.a.kp..".....R.IM.Q...)P...23.....s....e*..... .....!x..`.H..Z.W!%.Eu...../..'vJ.7.|_..W..'>u.....0?$r.....<..v...I...t.V..T..pA...$.%..G.Fnf.x^C|7..\..6)...nyf.N.....  ..uJ.7.+y5(..).{..|..1.nb.K.t..G.i...O.g...k...<...g.0...>.}.$D...h.....UK.9..3b.....o..D.6....\.C.gb.....L.t.E.%r.(^m1/z.,..(...:.../..$..J.Y.i;.2.^....?.....{. ^....`..R.H....t.....K.... M...Avl .....'_."......h!...fK*v..%.FZ3.9ya...S{...s..&...y.....U.i...J....x6.*1...L.Z..j.1.}#..-.._;.O..oh.O...x..S...

Chrome Cache Entry: 216	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.883997494668443
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKMQcoX/gjxGECWaee:PLKdXNQKD/0eL
MD5:	5734E3C2032FB7E4B757980F70C5867E
SHA1:	22D3E354A89C167D3BEBF6B73D6E11E550213A38
SHA-256:	91E9008A809223CA505257C7CB9232B7BF13E7FBF45E3F6DD2CFCA538E7141EB
SHA-512:	1F748444532BC406964C1BE8F3128C47144DE38ADD5C78809BBCDAE21BF3D26600A376DF41BF91C4CD3C74A9FAE598D51C76D653A23357310343C58B3B6D773
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=QquE1_MNjnFHgZF4HPsEcf_2
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/QquE1_MNjnFHgZF4HPsEcf_2/recaptcha__en.js');

Chrome Cache Entry: 217	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 360x240, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	1066
Entropy (8bit):	7.748167067702273
Encrypted:	false
SSDEEP:	24:w/OKbJVu9UWk9jCGKPV+M0eFk9lkdesuSijQ5F4U+S6a7:w9bJVutcpGAeaGesu98j4U+k
MD5:	2A11E13B2BD67BB9A6CB347D7C73DF13
SHA1:	B85460A33F9B229F42C08A6A94AE433A4D5C32AB
SHA-256:	1D0D6B5176D6A48B3042A107F929BBFCEFD4A057273AC488BBB7F7AFFD909B56
SHA-512:	059DD018BBF13A669D73F07442288F165BC6B305AFB0DF955773A0EFB7454B8204095196231179FAB4CB625E189C7C735FE41DC5B67FB8666D584214277186E6
Malicious:	false
Reputation:	low
URL:	http://https://static.bookmsg.com/creatives/SG/SG_083be47dfc3e28c9a68305b76181a5033bc45790.webp
Preview:	RIFF"...WEBPVP8 .....6...*h...?9..[/+.....'.in.`N.....k..!L..B..$.0.I.`.....$)..HS.....!K.....q.-y.....-...>.~.rc..Aw.O...A6....n@pk.WL.....t..IL"M7*..u.....>...W#.....F^+....e..=. ...].....P,.p.....m...;..&.I...ws .-..$u.U8.# ..X._.K.....N&".*.8..8\|..R....4B.f}.K%.d...st8.$\}....HI.eO.>.T,0^...g.)d...).%*.>|..m.....X.e....W.P.,?B.i....H..I..)....F.....!kY.....j.(.|.o_E.'.j..1...?.....>^.$...!l>.Nh...~.%.....T..6.#.....I....$+g..0.....p...<.t.<y.....a.0..BG.^gK...b8.C..X..~...5....f;.P.L.x!..I.X.o.s9.....S..... .L&.).aa.Gm.....#.7.N....)I. M.....PL.sM.u...0T....w.....'...F....h.....gIo....E.....oq....=..3.T.B%a..:.....e.....$.d"..U]..P`]iI.`..1.p".!..`...D6h..X..K}.....A{..~....F..?m.)....7..~...;f..oN..w{t.....Q.Hy.'\l.....~5S.K!J.y....G.zjs.._L .G.....*..@ig..$.....!...._..'.U.q.\...yn. ..{...YT".O.....yp0...&6..j...S.f..h3!B.....L...~....x.J...F.....C.....*x.OhC`_.G.s..c

Chrome Cache Entry: 218	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 106754
Category:	downloaded
Size (bytes):	35202
Entropy (8bit):	**7.992174396966344**
Encrypted:	**true**
SSDEEP:	768:niJE6Df2KzA9+artH/bqUd4HkL9CxvNXwxJ06Wp2y4oGt+hQnkHXzxv2:n1Kz0+adNCk+yE/p2yMt41XzA
MD5:	E101D38F26587914C937124AE0EB5E05

SHA1:	AC662B476F60DA3A27A2A8867EB9C711A7B687F9
SHA-256:	8C573A0DCFF2428F0A483D51CD0875E46F1DFEF228AAE10D49768FBB99259B1D
SHA-512:	3A880C73FC3E64DC58DB3085F75AB2E6445B37EF3F873345ADAB0CBE43A5CA925001A89260E49BF56A7AD992293A005F216FAFB5154568BD7890C14AF4F5778B
Malicious:	false
Reputation:	low
URL:	http://https://bddb2d2561.62b81f5af3.com/b313026a748183b52dfbacb3ef471b45.js
Preview:	.....s.8.(.Wh.Y/.S...m*..q.Ivc'c;..4.EB.c...!.1u..O.....%....Sugwb.@.h4....h.n.zT..(I..n...N...q.#..=.B7..P.....F.o.`l;}X.h.L.h..73?.c.fq(.....!Y)oE.....v..idwC+?...h.....s.0I..~L..Y.N...8..Y.....0t.Zd..F.C.JTcl..P..V.4...jxdy.y....@.p...9III..7...[.Q..pBgJ._)....,..X..Q.....F...G...P...R.....#a.O|..sR..0..S.0:..(I.8..3wB.p.$..o...[@,.....q=.`\.X..8.;....d.I4...q6.MU7...k..I.....$=T.?....q...X 6._.Z..R.$..E.O.6..DY...,...i..8.G;..e.....y.e).z..Jy...bA<... .=..\.MA9....SL.....K...../..=..r...J._._.\....q...y...{....VH.-...@.p.S.QN}..)9.O.^[{.'N..0.T.e..C...,....x.i.C...bi.y....[....eaZ...@5...*....K.....$..0/-+`.u...$Q.G:ac.t.k.H.=S.D.....%...dLH..H..h.k?.DZ.^.....uF..S...q..O.u.GJ..Q.....V.^9q...R.?..h.N..../t.U-*bi.\....f-D.B.e.Fl...T.I...V...x...(Zl.....h..FT....IR;....j!../~....d.5 !..v..RV...G.T...E../F.s....H.....d.R..f.1...M.....B.. 7..]..@.l..r..S.c...`....l UD.G.k#*i.#..G.a..R....Mt

Chrome Cache Entry: 219	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 64x64, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	798
Entropy (8bit):	7.6748306110830615
Encrypted:	false
SSDEEP:	12:E1HW3rHM54yVoxHcAZeLdCRxBEFO0wdV70leN8uOiTS658clmJiBKKKWjS15pSyp:4WbHM+y+KAldSZN8Oec8cl8lWy9
MD5:	5966064C221FB185939E00C2E8CE0ED3
SHA1:	C3F9DF3805F48DF56CDA976D9593C22BEC2609CD
SHA-256:	AB4ABABE52E48E2D44F788AD615AD95BF1762C08A5BD60E6B4C4FF1D8B7214EF
SHA-512:	9331B343F2028850B71F3AC51E4B5C0EC140100BCA839A513B85AD4FA6F3958F1F03422D0BE95308A308040F87A7BEF0F54D84A3116AF768C93055FC42B0249F
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/7odIr8zuMI5ddrSG6KtefaVNEvKBoiGzo6Q96lowbP5tLFhqiqUl3Mc16PMk2E1m9g=s64-rw
Preview:	RIFF....WEBPVP8 ....0....*@.@.>U .D..!...H8.D..`....8~....Ol.....C>......g+..L.x....;.#........<......o...O."..J.....U.g..>:...jM......}.R.%=..f..1K....aS6..W.....K..Q2j...........w.b.....1...3.s..<W.o.v.Z.~.<_.5..AF.....Xa....\ T.u./...*.J.....Y..b.....eb.....j.f87).....G!j.....u~.......2b?6....._*..*@f...l....{.c.;2.}.a....y...../g!o\?...8H.}.3\.M.{Z'.]A\....F.....g...0.....F#2...7w^...1../.....zcT....`..~....31.....m.'<..+....\.N...u?3../w...^...4...X:....n.h...G%7s.....VK.....q*H/.....Zo..-.....}.!(.G.g.8..&.o...:.h.....`E.*...T...m....A....1.....UJ F.1wJ.^..&Sg.....w.v.....k.....$.?....%.o..%..... .\F]6F1.w.....9h..u...+.Z...5.S..:.W.O`..O.e.D....x..~/?!..-x.W....M..`.._.I*...^..[.a....}.Q..X....._.h..N)..

Chrome Cache Entry: 220	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	2572
Entropy (8bit):	7.883630092374087
Encrypted:	false
SSDEEP:	48:l/zazUMipN3s67CpzzuvocggeVWrT4nz3UfxyNpoM0pSc+9UAjB5Glxn:tLN867CpzawHZkT4z3Cy4rSc+9gzn
MD5:	7BD516C53A3978EB3EF8F0F3A0ED587B
SHA1:	1FC3634798108F2BBB2ADDAAE65151187A8CA699
SHA-256:	DE8C047445DE3ED5AE2F9EAAEC09FBF852E66967BD9BA964410B72C7FAB4B678
SHA-512:	2B9578573672A9708DFBCB016B54E216F26F606CAE5B4A9EF195E868F85583EDA4D0F8432E8ED03D7EAD5AA4DF9B491DAE7FB260DD3609643DD1F61A480D138
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/rCNE1TGBN3EgPecrC-B5ALFplkW_QWTa3TAA8QDtcXmDK8TeMFW2fzqraMQAx5GRFw=s94-rw
Preview:	RIFF....WEBPVP8L..../]@....m.FBl.....&iG..........DI.U.lg...&i..A.M.@lj/.7..H.\..ef.....`.m.....T.dS.ER.'.....R.....(..P3.t%..........'.((...$.In.z'8..z..;.H....+..#....|.m...3J..6<..l..m^.m..m..6.&..[....[-...I.$)..0.n..O7..k.i.c.}|m;|.^d.#..3.....q...R.m[.....E.&....1...v0.M..p.>.Y...i.p.....6.$..Ge3.j...U...'C..h.VmP...8....P..|;...n4.p..........)u[..h.p..b..........Yp...C.4B5.....F&.~.I.0.....B.....#...@..p08A..p.F.~...QB..e.=J...A..@.#K.....>]QY?_..b.I.....U.Q....>..U..s._...G.Qk..w..*.p...vmP..t....j+...7.%5E..U.L...Ux.1....[<.u...S..R-.._.+.c..|..pb#...Z>.S..A..q..*...X.\)....D.c...V.....E=.BM Z.b.....h.y@....:P!Q.....^O..[.|h\....p..(.D..?]..3,.....MN.`kZ....'..7L.C.4....q.........q...F.b...Kf2.. ..DJ"...@.u..cv7.."F...n)Q....O.8U....Eu....v..E."..v..P.....I...k....i;L.Ap...*.v.r..M.....[c.. B=...Y.X..B.S0.."..M.e..B.....B..f.)]....`H3...SL.B`.D.....-...|.....)..._F.u._s&.W`?.q.CX.._s-j..3*3.)[7.@.E.Z.

Chrome Cache Entry: 221	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	8990
Entropy (8bit):	7.959388167722879
Encrypted:	false
SSDEEP:	192:qL+8F5flrsw2TNllSoGp5DRBcFOC41pMvNjC1O4BCJXn5tzmgb:K+83flr7BRBcFO9SCwjzzt

MD5:	7367103A0E06381FB02DE1C6E95DD998
SHA1:	C2A6FF6A9EC8AD29584C6E2D01B15C17658664AB
SHA-256:	162FAB3FA3AE06EAFE7E688D8628A6896E99139D18B34EEEEADCAB541565A8AF
SHA-512:	C45351B6AB639FD72D3A7CDB34D2F95CC4DC82BC46ACD029F2388FF091E48FCA84E66F698D419F8E6CC2537EE706ECD199F52D94DE69AD900E41706F43EC98E
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/D4DUUFQDCsH9NIEa8hjMjQSWdtNhGX1Fd_jT-23ogAb5uMMqttqQDUJcUt4K_u8RYOQ=s64-rw
Preview:	RIFF.#..WEBPVP8L.#../?...M0h.H.&.........$.)..v._.0J.ki..[t.$E.e...o.1....$+../.....E..$..<...p,..5.?^.B&"".I...."<(.d.S....$*.....N....t.....8.....0.....+...g..^..@..._F.>.....:y3.....?...XrNN<.B..wj.....2.^..*sw}....5www..`.. q;..{.....}..N...`.m.m.m{..{.$....=Q{.W...}0.....1(.....Zf9:.M.RB.[.....$.....G..P...L.'..S<wHr0e...8X..i%R;....Z..s{.Y..@(.*..ze9;.....4.$.....J..iAN...r.Osh.....!.4o.w..xs..u.....z.?.}.r._:..gw...3.rddc.....^..Z...k..N`_.I....H.....'.z..<L..`>.....7....w..aS...;..W..$.\.p~...../.P..H.....k.,=..9=..^.'.(...t_..N.W6#.+....e.<...(...8s.^.X{.QE~9.....}..p;.....`.....P"6P?..p..Z.N.."(j...@.R.s.o.S.x.c".!.xxs.`z.....^..x...Ll..`.....{..1P...~..#J...R.....[....}...Bd..{"M..g(..G..a.c..kz?y.I.D....0A.....I.....q.@..H.i(R..o6..!.X.y...i'..Z....%..~..?,.*./ck.)...c.....E...o....~$.....Cz...T.....3.C<N.I.....i4M.....*=).p./$.....

Chrome Cache Entry: 222

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1692)
Category:	downloaded
Size (bytes):	36071
Entropy (8bit):	5.427759367605427
Encrypted:	false
SSDEEP:	768:kODeBRUnFSleydV1oqAFhY7XjbiZxchFHqv5ZgWh1RRlEtIMbh7nxEKXOMI0Jxz8:KeydDoqAie2h4gkRRWaWJnxEYOpG7I3d
MD5:	92527A50FD03CAEECF2B9136D03E2A23
SHA1:	8BB29676DE788A6BF670C7F12444F693803B02E2
SHA-256:	82CCBE7C6CE15AC8B756F13078B27F21CC84B800B3277F13F52AF3DE4AB88568
SHA-512:	B1B9FD82CF5B5F248CC26CD10EA8509CDE6300EFE4C2604AD9F0BA357390992817 36EBD64CB30856C31D955207EC350920748E94014388A1487AC5FAE3B7CB8A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=_b,_tp/excm=_b,_tp,appscategoryview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=byfTOb,lsjVmc,LEikZe"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.Spa=function(a){let b=0;for(const c in a)b++;return b};_.Tpa=function(a,b){for(const c in a)if(a[c]==b)return!0;return!1};_.Upa=function(a){return a.Lh&&"function"==typeof a.Lh?a.Lh():_.ea(a)||"string"===typeof a?a.length:_.Spa(a)};_.Gn=function(a){if(a.Vh&&"function"==typeof a.Vh)return a.Vh();if("undefined"!==typeof Map&&a instanceof Map||"undefined"!==typeof Set&&a instanceof Set)return Array.from(a.values());if("string"===typeof a)return a.split("");if(_.ea(a)){for(var b=[],c=a.length,d=0;d<c;d++)b.push(a[d]);return b}return _.eb(a)};_.Vpa=function(a){if(a.Wl&&"function"==typeof a.Wl)return a.Wl();if(!a.Vh||"function"!=typeof a.Vh){if("undefined"!==typeof Map&&a instanceof Map)return Array.from(a.keys());if(!("undefined"!==typeof Set&&a instanceof Set)){if(_.ea(a)||"string"===typeof a){var b=[];a=a.length;for(var c=0;c<a;c++)b.push(c);return b}return _.fb(a)}}};.var Xpa,Vn,fqa,

Chrome Cache Entry: 223

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 100x100, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	486
Entropy (8bit):	7.456735643048542
Encrypted:	false
SSDEEP:	12:rbPqOLycYgACU4do/wZVbEqb0hyCQRdLOdsw:rbyUyXgdo/wZVbEvHObw
MD5:	CEEB4E8840C24621C0E0352B42B38A5B
SHA1:	03CBCEB0134A39267014595938705E2916580644
SHA-256:	50CB77AE9715629235F102DD53A68559DF1B64416F71179DBB4AA942725790B3
SHA-512:	80D4128488580567597BA5EB65DBFF2DD4A8EFC625C64CAC6A027A1BB5C229545206669F04A50A252B54F471BEE4FDC892E6BFE8347A50DD216BBA67BD671A63
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8 .....*d.d.?9..\/*.&".Z..'.gl.>.". h.q/.O...m..v..>. {.]..AP..F.I....^.O....jd.I$&V.?..'...,z..].&..Q.+.....1Tg..Q...e..!t.....W ...y...)....r...m...3?..C...f.^.....i.K.$B..}...R..m.g..5....PFg.lZ.\....X8...1m.Q.....).c....t..C.9...&.E.{..x....q..rCI..:.H.N....8.....q:S.VLs.Z.'lF.za..K9nU..Yk.Z.y.....h/5&.U.l.t....:..f...-.~iL....a..O..9..dR...g_(B.....h..p8~..0..EWB*..?0.rV.A.....z.Q.c..fZ....*.M.5...D.h:.....#.u...,BA..aU[.hC5@..

Chrome Cache Entry: 224

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded

Size (bytes):	11016
Entropy (8bit):	7.981378648560577
Encrypted:	false
SSDEEP:	192:81+5YBdagqk5t72EXnl/Q6hD8mXXJf5uJ/Nxnz+CIrgGT6LVz+ud2NXX2cXiIs8o:8JDaKr7pXnl/QaYc5uJ/NxCC5LVkpGcG
MD5:	CCF32A218C433ABF66324FCDA65D2FDB
SHA1:	029CC35F87EBDA0706422DA0E610BF611A78B4C4
SHA-256:	FB14C3B073F972C32246C26FDD135F1277A65219656DC39C8C12976506D1A4EE
SHA-512:	FF277620A37259F98CCB17599287C3698481A896752A96ECBC7CCD7C508824249E1CD043BD183A446CDD7640EFEEE74E1C85969341FAAB25EF04BF292223E6C
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/NfjNow7xCVioIcwYKiH3bKUIgvUqsg1fRjI9m1d3NliEd0Fj38A4lUrS94JHZ05Kxg=w526-h296-rw
Preview:	RIFF.+..WEBPVP8 .*.....*..(.>a(.E."..|.X@.....b.a...~^{p[..~;...y....'.....=[~....N.e.g.K.W._.....c.....z....P.....+....M..._._.?I>..d....z.j.....r...o.?.}.2...~..&.....j.+.....}. ..~a...W._..._..O.....~..k.....-...o...g.....>..M...._._.....K...._.?....].[.O.....?y..?..W.....z....~....6.....4.$b.T..:.,7.E>...Ei0".&Q.k.3.;....9.r.S.DNE.Y4.!R.R..*....z. A...|w/.E...R..tsB.....R.0$.&J.^;c...,.AkU>.N.Uk..4-%...A<.."..~...Q._.!.?....;....i.....E.~.u... .a.|*...Uy..]\@.D..v..Nd...=*.....R..3..gE.Q.7.h.$^..;.<.....7....(0.....>I.i.K....%+. `..h.x.....=L..q,..d1k..`.-).u.W.....s..1.....R*.J.....o`...Tf.r.@..u=.K..[{.m...m..Y...(...\.....u}..1.....oa.<.8..6.5.{T.$.d.X.n>.p./GW].-'...a.....z.<=w.h.naW.#..}.....S.Y7....'.../!.f. ...G.N...{.,a...o....L..&.Aqjx.p.:...{.zr.b.(~.\q2geJ.nn.$p.....D.B..h..\.....`....C.....L.....*._....C8.*.Uk.....|...4.j....C..H....xvW..B/.]....ppL;..

Chrome Cache Entry: 225	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (706)
Category:	downloaded
Size (bytes):	3382
Entropy (8bit):	5.564544645695353
Encrypted:	false
SSDEEP:	96:kwMWtfGkOT8K9G69klyEYtdE59AFYaNJHHfGFWXZFQl:iWtfHWHAFY6fbH2
MD5:	416A2FAA5DD240821E3382521B9B0ED7
SHA1:	3A30F3060E941A089F2D035FE962CB5DBCDB49FF
SHA-256:	A3E4DCDFD45D304B5AC6F77A5E0B41D3D9A0105689DFD22A066D58F17503C839
SHA-512:	30885C6548D743C0ED4DA8CAC9647DF39B6C0163026ED87F84576C7C03E867DE60E25BF9424E3986D3BC50EE69397AAB15FF6CBBBB661E890A51F185A7CBDEC1
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,CvxVpd,DRmmld,EEDORb,EFQ78c,FuzVxc,GjTCAc,GkRiKb,I8IFqf,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,M2Qezd,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PHUIyb,PrPYRd,QIhFr,RBsfwb,RMhBfe,RjJvI,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,gKWqec,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,mI3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=Wt6vjf,hhhU8,FCpbqb,WhJNk"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("Wt6vjf");.var w$a=class extends _.x{constructor(a){super(a,0,w$a.Sd)}tc(){return _.Yg(this,1)}We(a){return _.Eh(this,1,a)}};w$a.Sd="f.bo";var x$a=function(a){a.pG&&(window.clearTimeout(a.pG),a.pG=0)},y$a=function(a){const b=_.rL.get("https:"==window.location.protocol?"SAPISID":"APISID","");a.ZE=""!==a.aD&&""===b;a.oM=a.aD!=b;a.aD=b},A$a=function(a){a.yy=!0;const b=z$a(a);let c="rt=r&f_uid="+encodeURIComponent(String(a.dH));_.fk(b,(0,_.Ke)(a.O,a),"POST",c)},xM=function(a){if(a.uK||a.yy)x$a(a),a.pG=window.setTimeout((0,_.Ke)(a.H,a),1E3*Math.max(3,a.iD))},z$a=function(a){const b=new _.Jn(a.IT);null!=a.bI&&_.Xn(b,"authuser",a.bI);return b},.B$a=function(a){a.ZE||(a.yy=!0,a.iD=Math.min(2*(a.iD||3),60),xM(a))},C$a=class extends _.uj{Xc(){this.uK=!1;x$a(this);super.Xc()}H(){y$a(this);if(this.yy)return A$a(this),!1;if(!this.oM)return xM(this),!0;this.dispatchEvent("p");if(!this.dH)return

Chrome Cache Entry: 226	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	339
Entropy (8bit):	5.206167536518377
Encrypted:	false
SSDEEP:	6:kRZzRxVvn4G2bUA18G/QVf1NyDNcUnwQRaNw6JpyxZRNlad0:kRZTFoPH/Af1YDyU8kbRN20
MD5:	4273B6A78AB79F2FCAE19423FC01EF19
SHA1:	DB8FAA4C988AA1D30C5C7DF7F2C536993F3F517E
SHA-256:	879EFAA323F60FF74BB0F980B3ACC0F755D91D6AD056965856E5109578801A6F
SHA-512:	EA59B5B7613EB9A6A9F533453C86E9CD4C6164A719E86D91B30F859FB77938DECB6E10C42B899578477018C5AA139F20099F7B02CFD1B89D7E53F0243CDB225
Malicious:	false
Reputation:	low

URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,CvxVpd,DRmmld,EEDORb,EFQ78c,FuzVxc,GjTCAc,GkRiKb,I8lFqf,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,M2Qezd,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RjJvI,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fPcQoe,gKWqec,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,mI3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=RBsfwb"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("RBsfwb");._.lr(_.SAa,class extends _.mr{constructor(a){super(a.wa)}H(){return"RBsfwb"}O(){return!0}hb(){return _.eCc}});_.Qq.RBsfwb=_.YPa;._.w();.}catch(e){_._DumpException(e)}.}).call(this,this.default_PlayStoreUi);// Google Inc..

Chrome Cache Entry: 227

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	332
Entropy (8bit):	7.358546821442648
Encrypted:	false
SSDEEP:	6:PZVS4Q+recdKlUVHiRQtvCoqYlbJq0AxtC0U8vAzIp9JtOOZkeWbCgfpH:D9Q+recdKlcHiRmC+bJqlAzIpTtOOZTM
MD5:	2F640AA73D5757BA0FE67B74E5D9F41E
SHA1:	A4D29ADF1BA739285BA35AFBD94D51734425429D
SHA-256:	469C936814B431210209150CA7F39A314A333269C07A5C83483D0C3EE0D772D4
SHA-512:	EB2C59AC81D5C2D8DFC90C5A06B283651225A3836A514B47E46009DBE9A9E2AB72EBC77558CD3CD4B3470844D417DE6958A7BFE1AF5BE16C2D7A2F9C314FA8D
Malicious:	false
Reputation:	low
Preview:	RIFFD...WEBPVP8L7.../.....m..s..c...m..[H.....X.q.|..c[..*.m.#.Jw.E:.uro....z..m[....J..l.l.XNH...D<$A"X.k).....y..W..7T}.....V.G..v4.d....%.Z....y)o.....]~.0jS/.....$..|.K.....8M...=..l.q....[.9s.../.F:.j...{n..2..d.#A<.T.A.i.../..6.)..9.}. ..%.l..e_..=p.H.....z.n.(^..}/.CJ..:;.G..3.q....ZG.ZF..&.b..;..

Chrome Cache Entry: 228

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	119998
Entropy (8bit):	**7.994984946815762**
Encrypted:	**true**
SSDEEP:	3072:Eh/bxy7XUBx5qJCjtlKlf6GbdSRHkbIegSgWFhX:EVYArE9boH4gwhX
MD5:	22C7ED1AB596E487E55E682C86778E29
SHA1:	2D9CE014B97C62F22AE7BC3399394D4661E820DD
SHA-256:	B4EC15C15FD70884F5F959292F0A3AD0A30FFFEF013C962DF8E2525414E7803
SHA-512:	E8C0553D8C3F6A40D3235D8398ED4D01D1E09523AE9D4091667AE2C2F47CEB0EA8DDC4B23C30CE5EAB29DBFC209D245496DE4ACF370E07FBF3F40A6A9799E26B
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../..Z..@p.6..;.dZe....)p..........W...~.2.%.4.F..p|.....W.....&=.....$W.y1..o.OI....#.{.....l(.y.....RN....&N...y....tF.....o.O.:..5..........ZQU....).....*.. .p...Zm.....;..........>..Z6.m...>Q]!=..H...$...y@.v"K.$.v...i?.F.k..)y.....).....HV$.,.(..(.\-N}.....{.z4rd.N$..03Y...1g...t..l,...?....n..&@....\..&..... ..'O.....w.<.x4...h.....g..._;O'cj.....AW._....H*....S.....w.<..'.....0|...F.....p*.....m.@.....{.r.....E.S.&]..I.0.....f.L.....S.e}Q.2.. 4.x..p..x...)...Hn.|q\36(..z....'..f...~....7.1.a..B@p...-..B4,..0..1.....(P.eG=.]......ado...aX..m&.`X..#...Z"12(..+t.X.4..VQ.j.&.....+-.u...W...W...8".}.(s..{.....0..:.(Y.D...]....\R.....A.*H..u.>...j..rF.)....=..].4.s.f}...R.GrZH.X..f".g.)...q.L.&].7.V2..<.'#..D.0.J....0..oh.....t3Q.....p..X.."..$k.k.....>8....L..i..#Y.o.Q.h.y7.....DFF.@.. .....2D...S.(...b8[.7.QQ..5.n.i. .....@.1.T..8,.d-..@.tL.(S|..nb.....&`.u..i..B:L..e.

Chrome Cache Entry: 229

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	645
Entropy (8bit):	7.631563068517978
Encrypted:	false
SSDEEP:	12:6v/7ihaL0Z6T2rkLv0cLSbLzKlRv+reS0TZPhnv8NuKS8jrRJI1b3g0hfue9:riS+v05bLzK7CmTRhnUTJjk1b3Jhfj
MD5:	EA2722D3B676D5CDD4F7225E65695112
SHA1:	97E5E94CFF5B62F60BA76C7DD9F606304AF8B10C
SHA-256:	317E5FDAA14E548C0045D5E662709CFE0B692E0384A8396CF22054BF0A1E1C48

SHA-512:	BF06CE48B306A0EA13EBC7BE92CB56440DDF1C35C214BA7C164DECFDA6E2E7AAAB31605196D0690BE4FF509404701CA620C504A5EDF0C3E6A12C6FA5A73C78DA
Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/i/productlogos/avatar_anonymous/v4/web-32dp/logo_avatar_anonymous_color_1x_web_32dp.png
Preview:	.PNG.....IHDR... ... .szz....LIDATx.b .<|...P|.h(.E.0.....|.x.....a.....!.....q{.t.U...(.A.g.....w.3,&.s.~..h2.....lp=..4!..[.....r.p6.R.....R.....19]z.....%.E.q.....6".#. ..9..Y.n.U.ZU.ZMu:.Q:t%..y`<.+.0T6.=.i.0.e..a.f...b.\..Ax..e...K...$7..BAk@.\f..}bG.K....\Nk@.T.ha.+.w.%x.5.....k..OJr...$Gd.....,.0....n.{..b.....%]....K.....?....f....w....j4. ..@%p{?...|>.....hH.h.....r....h..s.J..@X.j..3#h>.`@Xw..I.K.;).c..>....V.b. T....0B.4....%G.....a[..P.....G..B"..!*...m9rj%.....E.AD*...0....!..y``....o.z...1J.FF,..sEr3.s.&....b.m.+.... .....'.m3(D..{..:...So.Ja..*.....#..'....IEND.B`.

Chrome Cache Entry: 230

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (706)
Category:	downloaded
Size (bytes):	3382
Entropy (8bit):	5.564544645695353
Encrypted:	false
SSDEEP:	96:kwMWtfGkOT8K9G69kIyEYtdE59AFYaNJHHfGFWXZFQI:iWtfHWHAFY6fbH2
MD5:	416A2FAA5DD240821E3382521B9B0ED7
SHA1:	3A30F3060E941A089F2D035FE962CB5DBCDB49FF
SHA-256:	A3E4DCDFD45D304B5AC6F77A5E0B41D3D9A0105689DFD22A066D58F17503C839
SHA-512:	30885C6548D743C0ED4DA8CAC9647DF39B6C0163026ED87F84576C7C03E867DE60E25BF9424E3986D3BC50EE69397AAB15FF6CBBBB661E890A51F185A7CBDEC1
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,FuzVxc,GkRiKb,I8IFqf,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SWD8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,UZStuc,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,Z5wzge,ZfAoz,ZwDk9d,_b,_tp,aTwUve,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lpwuxb,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,q4UNLc,qfGEyb,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=Wt6vjf,hhhU8,FCpbqb,WhJNk"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("Wt6vjf");.var w$a=class extends _.x{constructor(a){super(a,0,w$a.Sd)}tc(){return _.Yg(this,1)}We(a){return _.Eh(this,1,a)}};w$a.Sd="f.bo";var x$a=function(a){a.pG&&(window.clearTimeout(a.pG),a.pG=0)},y$a=function(a){const b=_.rL.get("https:"==window.location.protocol?"SAPISID":"APISID","");a.ZE=""!==a.aD&&""===b;a.oM=a.aD!=b;a.aD=b},A$a=function(a){a.yy=!0;const b=z$a(a);let c="rt=r&f_uid="+encodeURIComponent(String(a.dH));_.fk(b,(0,_.Ke)(a.O,a),"POST",c)},xM=function(a){if(a.uK\|\|a.yy)x$a(a),a.pG=window.setTimeout((0,_.Ke)(a.H,a),1E3*Math.max(3,a.iD))},z$a=function(a){const b=new _.Jn(a.IT);null!=a.bI&&_.Xn(b,"authuser",a.bI);return b},.B$a=function(a){a.ZE||(a.yy=!0,a.iD=Math.min(2*(a.iD||3),60),xM(a))},C$a=class extends _.uj{Xc(){this.uK=!1;x$a(this);super.Xc()}H(){y$a(this);if(this.yy)return A$a(this),!1;if(!this.oM)return xM(this),!0;this.dispatchEvent("p");if(!this.dH)return

Chrome Cache Entry: 231

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 5318
Category:	downloaded
Size (bytes):	1236
Entropy (8bit):	7.8450254010275735
Encrypted:	false
SSDEEP:	24:XAl5R7E1DKfnrrueX8WVeZ7le8JxCrrsWjoc/l/pQwln:XXkTrHMWVeZpe/rrs0ocw/pZl
MD5:	A651959998EB05A41E6B1EAC5930B191
SHA1:	6A87727DC2B250F9F47B6C4BEAF1F0D7FD6AE88F
SHA-256:	980C864A7AA2F2E7833CC5D38669ED8B451725685C37CA4235549DF151BDE3AE
SHA-512:	3F8E3E52106528D1328BE3015F200B97E4844F0C9BCFAFBB5D6D249797B7851807FAA428814ABC79CF5EA63800386E1FE9C5B38C217B8A8033BED684B1D72F78
Malicious:	false
Reputation:	low
URL:	http://https://js.wpshsdk.com/npc/sdk/push/styles.css
Preview:	.....XK..6...0fQ`.D...|io=.....u...<&..^I.m.....-.x.DR....`....%o;.J.....Y.E...7"A.x.9.(%.....{.!.,ID.....Kq..w.T..R....?.E8.....[.VQ..:....1.....%I.....}.....Q...$.r.I....Y.."/..&.$...q .IV...@r..Zq$..$W.<_x9..qo..bn...w6g...'z.,.>i..H...)Y]A.V.w...2&.8f.Z.pO....DR...@G.; 4.g...6|}.}.ca...X...*...n.r.zF~.8....I..n.'*.....1..V..Fk..(V2K.M. P....`.].F9.Q.(2.m....d 9.S..C.D.Y#..."G.....hMq.....08 .;.K.Y:....r.F.JSBwp....@=...L.kRr.\^0b,."..%...w.J....4*..t.=;*...-.L.).....k.I..{.XkbC.....]V. 9 g.I....x7..Y2`.i..dM.G\3m..i..e .a!.2.tm.K..txK..Q\..x ..q.....K.....uxg..r.8..p.z.bk..M2mt....g.>.B.#A..,P"..U..UvUg^&. N....@R...1M[0r(.....+..?K!lv...0..=.h...k.k..=;...wg.?..._..]....#...Q.....n....:/.....*/:...y~...&.|.)A.....z.....A.I.V .ov.._M}X.O.\..?....O...N..Z...q...;*.G...#....-.N..?...!.....7.w...D..]...;.qw.Y..~7u....4.....>nA...'k 0.>s]..u.N^...U..<~.....2..;+'wLf..|.A..w..Q...W....4..2>....[

Chrome Cache Entry: 232

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

File Type:	ASCII text, with very long lines (706)
Category:	downloaded
Size (bytes):	3382
Entropy (8bit):	5.564544645695353
Encrypted:	false
SSDEEP:	96:kwMWtfGkOT8K9G69klyEYtdE59AFYaNJHHfGFWXZFQl:iWtfHWHAFY6fbH2
MD5:	416A2FAA5DD240821E3382521B9B0ED7
SHA1:	3A30F3060E941A089F2D035FE962CB5DBCDB49FF
SHA-256:	A3E4DCDFD45D304B5AC6F77A5E0B41D3D9A0105689DFD22A066D58F17503C839
SHA-512:	30885C6548D743C0ED4DA8CAC9647DF39B6C0163026ED87F84576C7C03E867DE60E25BF9424E3986D3BC50EE69397AAB15FF6CBBBB661E890A51F185A7CBDEC1
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,AKTwDe,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,FuzVxc,GkRiKb,I8lFqf,IJGqxf,IZT63,IcVnM,IgeFAf,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PH175e,PHUlyb,PZ1hre,PrPYRd,QlhFr,RMhBfe,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,fdeHmf,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appscategoryview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QlhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=Wt6vjf,hhhU8,FCpbqb,WhJNk"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("Wt6vjf");.var w$a=class extends _.x{constructor(a){super(a,0,w$a.Sd)}tc(){return _.Yg(this,1)}We(a){return _.Eh(this,1,a)}};w$a.Sd="f.bo";var x$a=function(a){a.pG&&(window.clearTimeout(a.pG),a.pG=0)},y$a=function(a){const b=_.rL.get("https:"==window.location.protocol?"SAPISID":"APISID","");a.ZE=""!==a.aD&&""===b;a.oM=a.aD!=b;a.aD=b},A$a=function(a){a.yy=!0;const b=z$a(a);let c="rt=r&f_uid="+encodeURIComponent(String(a.dH));_.fk(b,(0,_.Ke)(a.O,a),"POST",c)},xM=function(a){if(a.uK||a.yy)x$a(a),a.pG=window.setTimeout((0,_.Ke)(a.H,a),1E3*Math.max(3,a.iD))},z$a=function(a){const b=new _.Jn(a.lT);null!=a.bI&&_.Xn(b,"authuser",a.bI);return b},.B$a=function(a){a.ZE||(a.yy=!0,a.iD=Math.min(2*(a.iD||3),60),xM(a))},C$a=class extends _.uj{Xc(){this.uK=!1;x$a(this);super.Xc()}H(){y$a(this);if(this.yy)return A$a(this),!1;if(!this.oM)return xM(this),!0;this.dispatchEvent("p");if(!this.dH)return

Chrome Cache Entry: 233

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	11208
Entropy (8bit):	7.981551403260864
Encrypted:	false
SSDEEP:	192:E1ZEL90lv5quXl+OHRbm0orqZ3cKTsOYmwPHhybVmlzLB1qmXSYayOrlc2iuyC0T:E46IRquXl+O5m0kqXNYmIhybVmlzdkmA
MD5:	C151B65794E92ADC68B3E99664FAF189
SHA1:	4F0FF89AEAA084188F8CFA71F26885EC8FB43093
SHA-256:	9400EE73EAF60FA2C9CBA1AAEF6AEDCCAD0DD76B62C8FBC71B702307148911C59
SHA-512:	2DEDC1F6463DEB96206CF216EDCF71437F4EF1884E784B08C02E815DF73B184D810D216095D8032E3AF72650AB16819788D8DDC46E872C11562CB17BA9B0468
Malicious:	false
Reputation:	low
Preview:	RIFF.+..WEBPVP8 .+..P....*..(.>]&.E#.!.+..8...9)(..N...`l...~\.E..k?'.....W...~..^.....k....._....R..?.~.....W...?.....M...C.;.K.....m..7^G~/.#.....C.....Q.....W...../.../...?3..-...Q.z~.....Mo.'.....g.....?..~x.....=.?..Z.....o./....n...7.W.7.O.....K...o.O.....6..m+t9.)EG.@.d...kj.`.m.cP.V....}n...l=l)J..B"E?....._...pqLe....i5....h").Q...u.. ....R(..wP..:.-sUFg.m...h...#`...D+o3...8..%..C..Q&.D..:...1O~.o....z..._...^P...g..c.....+...at...#.|.....'.=;R)3k...O..xy;..!.V0y...i\h.....<u..E.U`P.^.R7...M.M..X....nz...w.c x...%0WOG.k.A.7.....<....'../.....p|$@.2.....@.....6..Q...|%.'...~..-.w%LO.Q..n..j...8.G.....<..<m..=5C.L....O.2.n....H...U.%.q.....-35...@....<....J.W...2kp..A.c.*..ky]$ha..{U.. H.aDkPv.....#[p...1...;.....Y>"C.R#W.5.Z.R..I..[NP.....};P.....i...sR.JQ..D.."..c...HL..j..x.Q.....A.....'.Y&.=....f..?>>-.w.#-!)'.W.!...\.NQ..G.....>.F.6L.[q.e.].-.N..EG.4I..m...u=...2..*

Chrome Cache Entry: 234

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	2222
Entropy (8bit):	7.892968104781668
Encrypted:	false
SSDEEP:	48:+OFML6l0KRqayHtroAJ4AkzEnMNwmPYbpHOiyv3Kn:TMX2AJ4AkzEFbpHVwK
MD5:	8101E612BF08949C7951093F776BBB38
SHA1:	709512B3CE7BB2E74D2278B6793901FB492DC64E
SHA-256:	7050C993F4A8B3BB4FC77C6126D099EA45E73E349B5F11F7B31A4EAF630CE23E
SHA-512:	E452FBB6EFADA78E7D3BC9AB0D8EC1FB6118A8243F8FA63FD1E327BAE52237A2159CE50E14163CCEFD79C333A53A2167C3437AF909949C9EDD54A174AB2B26F8
Malicious:	false
Reputation:	low

URL:	http://https://play-lh.googleusercontent.com/a2HLOHpXniFGGEOxr6fcAkhmjQTT_r9IK2p23c9RDdvJAioZrSsyIwBdaxqRF7qScW0=s64-rw
Preview:	RIFF....WEBPVP8L..../?.....m#9...y.._.!....<0..IE...-.9..i$.....m.a=.L90l.lq.:.{.g.I.....}@.H.E.Q.B.....}..q..tv..A.H:..v...C.n.?.t..=.....g.A @...Z..6.....$....l..533C..33V...233 3.nb....%..T..>...9..,o.%.MK...#.#..3.m..n.....h.....}w.....u.....2.@.d..2.T.m}x....P.$..i../cW..U.....t.....kL...xZD..V.....U!#.....>.?"d.,....>L..i..>2..../.+...4~.3.9..b....y....." !....M; ^e..!.....G.....Tb..^d...(..s.5..Q.pH.0.u.?x4WZ0;'...5.d..p.....Q".x..x.M.C.D.....S. c<#.b"..h.i.;.A.t].U.#.....[..V....3.]..}.T.U..m,P....j..g...$...r \.....v.fx.._.IbQ.....dI _.....L_..U|..k....D"..6..H..~...}'..q=&K....S....)...k....*>...2`.PU...s=..:..Cp.....O.7...n./...|.#..Q...._g#B....%i.j..t!..H..C..1.2D..8..g.>.k.p..|.O....Z..-..C8J.o...$.=.L....sc.1S...3 .q.;.T...A.S#y...e.+..)@.n.$...M!..w^.....[..QE..".G1@...\%.h.8.^.H...U..|....t.....MHnEk@./aC.H..e...!...)....H.....[.P....`..:.K.3...tf..D6...6.K..z.y...B.k.m<..p..6.L.

Chrome Cache Entry: 235	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6193)
Category:	downloaded
Size (bytes):	822887
Entropy (8bit):	5.63881706273612
Encrypted:	false
SSDEEP:	24576:1k8CBGe2dChzP2tmpJpIShwPdQUAbmsSb1UNoSF1bAiGosICXsJUiu8waZD5y4De:1k8CBGe2dChzP2tmpJpIShwPdQUAbmsS
MD5:	ED64A2EB5DBE63CD14889222C9CEDD53
SHA1:	CE8108B91EDB0801E6FFE13A785826686173AE1B
SHA-256:	F27761977A0D9C72DAA8795BE584B464509495C77C223BD567C44347F19769BC
SHA-512:	1F0A9E62CFCE245F35D4DA374B004EDEAD3C23936400F7E25FE1115FB44A25A287DC95E7BEDA11B0AEBD4D8FFDE9CB836605E5CDFA4DDDC0C49B10325F98E06
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,developerdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=ws9Tlc,n73qwf,GkRiKb,e5qFLc,lZT63,UUJqVe,O1Gjze,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,WO9ee,mI3LFb,m9oV,z5Gxfe,ArluEf,lcVnM,fPcQoe,vrGZEc,TSrO,LCkxpb,kr6Nlf,O6y8ed,PrPYRd,MpJwZc,NwH0H,OmgaI,lazG7b,XVMNvd,L1AAkb,KUM7Z,Mlhmy,pYCIec,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,mdR7q,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QIhFr,ovKuLd,hKSk3e,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,BBI74,VwDzFe,MdUzUe,A7fCU,zbML3c,zr1jrb,Uas9Hd,pjICDe"
Preview:	"use strict";_F_installCss(".EDId0c{position:relative}.nhh4Ic{position:absolute;left:0;right:0;top:0;z-index:1;pointer-events:none}.nhh4Ic[data-state=snapping],.nhh4Ic[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}.nhh4Ic[data-state=resting] .MGUFnf,.nhh4Ic[data-state=cooldown] .MGUFnf{transform:scale(0);transition:transform 150ms}.nhh4Ic .LLCa0e{stroke-width:3.6px;transform:translateZ(1px)}.nhh4Ic[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: 236	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	660
Entropy (8bit):	7.559727689613209
Encrypted:	false
SSDEEP:	12:CPtXDzhxTyuv+KFYrU701108ACYvNybe5Lq2TRQufUv18rAX6tk6ySl:6XDzhvler1086ybe5LqoOdStYW
MD5:	35C28E9A4F538FB6307DD68240313766
SHA1:	E25D101C2363140DB55C6FFC6F8203E805822077
SHA-256:	59AF6D38E2E8871E2EF6214749F6315A37F8F0A1620EC564D89092D715BF4408
SHA-512:	52DB7C19C9D7886B55C1011C1FE5066335640E2FDCADBE5616AA83E217CC5BFEB6ED7DE9C0A6078E1136F1DC419CBCB0792635658EF9851A4E11678956B8A1BA
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/5P5svqXNCWqE0NtHSV91pl2YUGKJ2aitjaUWIVZd-65AtskDVO2o9bpYx1oAV9fr0-nt=s64-rw
Preview:	RIFF....WEBPVP8L..../?...'.$G..t.~.v&..m#9..t...lK..Fr$M....mIm.6..L.....W @.....<.......$..B...@.....s?..E..E...81eL.Q....u]..... @...}....0U2...I.QUT....<..|>_.u.........u.LRQ...G ..R.h....B.,...Q.... [.I....m..\.8...#..{.....;p.I.\.{.:...BMeI=I..Q.$..yQo..._..PQ[).).H..A.....~...{.O^ ....*..J,..F.].kcG.VZ".F....b#9;.....f...S.gvS.....<..)]..:){.... ..T.}.<.ir....p.r.....3... .).%..*s.hY7{...I.@.....7o...W...?..Hb3.i...f\.S....^.....8...`.;....|S.#O...6.XH...g....9....P...R3.....?..m...Z.U..K....ue\Y...zWZ.1...9$..f...R.Iy.B.....).....I...O.~....r.~'.&..G.....H/..... ....1.....<eO...7o.....r.@....ZT'MU..

Chrome Cache Entry: 237	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	240
Entropy (8bit):	6.9991712725025685

Encrypted:	false
SSDEEP:	6:Y/PZql/KiDZfb08qzALLJRn3PRB8y1BLqmX45oBezn:Y3Ul/KMb0tzALL3391t1o5oBezn
MD5:	BA44425C00D3898F79D74B5748E49934
SHA1:	BB2CFD3AC724BDAF3C1F3A3A61030671C79D1B60
SHA-256:	35F1F26A525AFA469CEC210657087027502D02CE5ADC3BB1C431A29C4544FECD
SHA-512:	23D0D7732B4E677FA0E464C3BB834DD28BB232E0460AB6918AACA4CEB1AF7D149A7BA50035B4F39C102472F30B1840EEEF73310517FFDE7810EEE2B4F0F7864 7
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/ohRyQRA9rNfhp7xLW0MtW1soD8SEX45Oec7MyH3FaxtukWUG_6GKVpvh3JiugzryLi7Bia02HPw=s20-rw
Preview:	RIFF....WEBPVP8L..../.....$e...'..6.F..u....H....m$'....P.>;L..L3f.S...+Q....Y.....j.s...)...w...B?.V.y?..9.....~`..C..1.b...$)Y.....?O.....y+..g.i.V.\.q*.f....5...1. (2.s..R....w=.b...)..0...(.....e.....n.n.

Chrome Cache Entry: 238	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	792
Entropy (8bit):	5.271423979636484
Encrypted:	false
SSDEEP:	12:kRZTFMTaH/Af1RDyBmH/Af1ODTGiw1YZH/Af1oAWD3GXQvnFpH/Af1sDZ2kbRN20:kzeTafoffR6iw1GfLnFpfLdrl
MD5:	4394984BDFC2465754EAC8C70F384628
SHA1:	A43018C1513B1AC900DC05201E5D636FB5954E9C
SHA-256:	38A273950BF3FC4C8A97644A01BEC26894EB2026C37C91A8900689914E969650
SHA-512:	09B0352BF9386351DFE79B795BB6333CE1D76541C15B82BDD5FB3A61D31201384181962A8CBAF0065113A57A85C2D487F9692EBF43447794459F0B450581B68A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SWD8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,Z5wzge,ZfAoz,ZwDk9d,_b,_tp,aTwUve,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lpwuxb,lsjVmc,lwddkf,m9oV,mI3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,q4UNLc,qfGEyb,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=yNB6me,qqarmf,FuzVxc,l8lFqf"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("yNB6me");._.lr(_.BBa,class extends _.mr{constructor(a){super(a.wa)}H(){return"yNB6me"}O(){return!0}hb(){return _.g2b}});_.Qq.yNB6me=_.l2b;._.w();._.u("qqarmf");._.lr(_.nCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"qqarmf"}O(){return!0}hb(){return _.Y3b}});_.Qq.qqarmf=_.w5b;._.w();._.u("FuzVxc");._.lr(_.pCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"FuzVxc"}O(){return!0}hb(){return _.S5b}});_.Qq.FuzVxc=_.V5b;._.w();._.u("l8lFqf");._.lr(_.sCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"l8lFqf"}O(){return!0}hb(){return _.Y5b}});_.Qq.l8lFqf=_.$5b;._.w();}catch(e){_._DumpException(e)}.})).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 239	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	11208
Entropy (8bit):	7.981551403260864
Encrypted:	false
SSDEEP:	192:E1ZEL90lv5quXI+OHRbm0orqZ3cKTsOYmwPHhybVmlzLB1qmXSYayOrIc2iuyC0T:E46IRquXI+O5m0kqXNYmIhybVmlzdkmA
MD5:	C151B65794E92ADC68B3E99664FAF189
SHA1:	4F0FF89AEAA084188F8CFA71F26885EC8FB43093
SHA-256:	9400EE73EAF60FA2C9CBA1AAEF6AEDCCAD0DD76B62C8FBC71B702307148491C59
SHA-512:	2DEDC1F6463DEB96206CF216EDCF71437F4EF1884E784B08C02E815DF73B184D810D216095D8032E3AF72650AB16819788D8DDC46E872C11562CB17BA9B0468
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/12sfBhw4O0sk8Bs9qKLJf2t4Cj_n6PJ10ficezyllp_lW6bc5UadmNtNS0rFdhkglLeP=w526-h296-rw
Preview:	RIFF.+..WEBPVP8 .+..P....*..(.>]&.E#.!.+..8...9)(..N...`l...~\.E..k?'.....W...~..^.....k....._....R..?.~.....W...?.....M...C.;.K.....m..7^G~/.#.....C.....Q.....W...../.../...?3..-...Q.z~.....Mo.'.....g.....?..~x.....=.?..Z.....o./....n...7.W.7.O.....K...o.O.....6..m+t9.)EG.@.d...kj.`.m.cP.V....}n...I=I)J..B"E?....._...pqLe....i5....h").Q...u.. ....R(..wP..:.-sUFg.m...h...#`...D+o3...8..%..C..Q&.D..:....1O~.o....z..._...^P...g..c.....+..at...#.|.....'.=;R)3k...O..xy;..!.V0y...i\h.....<u..E.U`P.^.R7...M.M..X....nz...w.c x...%0WOG.k.A.7.....<....'../.....p|$@.2.....@.....6..Q...|%.'...~..-.w%LO.Q..n..j...8.G.....<..<m..=5C.L....O.2.n....H...U.%.q.....-35...@....<....J.W...2kp..A.c.*..ky]$ha..{U.. H.aDkPv.....#[p...1...;....Y>"C.R#W.5.Z.R..l..[NP.....};P.....i...sR.JQ..D.."..c...HL..j..x.Q.....A.....'.Y&.=....f..?>>-.w.#-!)'.W.!...\.NQ..G.....>.F.6L.[q.e.].-.N..EG.4I..m...u=...2..*

Chrome Cache Entry: 240

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	3054
Entropy (8bit):	7.910076776321541
Encrypted:	false
SSDEEP:	48:S9skh+s2qz4kX0614PMHhJoKmjnZA1UegndbMF1KmwWGcMAgwmx7bEzF4hEkvQhB:QBh+/qtGPMBJlmjuWegn1BWoAgF7bEGI
MD5:	61374F426AE0866DD88D32A073C6AE47
SHA1:	D62C0C600141009A6882B56F94AD0F6BDF5896CE
SHA-256:	D45C08D891324AC0723D3A95B0AFED9FF0092B4082C8ADF262CC5D452C36C485
SHA-512:	DAA42C80BB0939088412E024E719B6B3C534DC11D64214392A0EBA667D0E314A5B02B2163F604B8F85CAAB214BE4ECBD087570EBA035C935FEBFFE31FB54F5 B6
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/TymHl9J6thzg_3mSBPcEb-JCcgBujUXZWjMQIe2HPWm0xukLUZ6BxtDK9qyExfY0n-4=s64-rw
Preview:	RIFF....WEBPVP8L..../?.....m...._...n.f.....%..^.....V.....,.G...y._z...J.m$I.....#>.o.K.l#Ir....01...'.....2........&3u.2.;);.l........3...jjz^.c......{..x......m..m.... I...]\...m.m.m.m?..L.<...L... ..x.m[.l.r.c.-fff96.........wl...bf\<.....l[..h...y...,W........&..e....`2...U<...=Ca....+.......(.....o..[.}.........u.H7..!....K.!..ml..g.{.w..&.G=.s3>..`h...._L.B....]........O..6.aI.F..$... .'..?.&...]hP-.X o..7~z.7...t7......t..0|.q..k"tS..8jY...._[...W.(.(.F....\....\..(...T.rk1.%.*........k.Vj...c....v...8..._...QJ..+q.KZGF.$...k..^.V`._...J..I..,..".....-j....r..\.I../. ..@@C....3..^..}..M...o...........t...x. .c+RTe..+....A.~......}...x(<..CE.~.~b....5=.....Wz.7.N. .E.Z...^.....<......8.-P.....6...^I\Jow~...Z..@%d.Y2N..]~...i.L...`@..c~K.....L.......7.d..(...8K..?8...S.....` 7..[d......gZ.GS....L |X<..*.V.......2r........x..0......8..-f...5....|...iv..J...G..D*V.....#...........}..r....#..L&.3../:z...gs=.......|v..:.D0....J.y..

Chrome Cache Entry: 241

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 480x360, components 3
Category:	dropped
Size (bytes):	39997
Entropy (8bit):	7.97375484107102
Encrypted:	false
SSDEEP:	768:gviOwqkxt4KkDuUR0nFMNGI9/2KRIzePd9m6g6pD1ielvE6f:idTa6Kkp8GEI9/jAKm6of6f
MD5:	CD5881AE4C1F96CA24D28DB455826360
SHA1:	033E3303FD048FC96B8E2FACADD8F9468AA0BCA8
SHA-256:	DD5062DE1DDEC283F55C40DB7E293FA9126E2E932DFD3A527346F9169DECE5BF
SHA-512:	427E0B600921DE49C18D1AB8DD25E51BF6B75496A1C91F635998A74CB38839529B90E2D5AFC70A07D710D3DF2EAEC5B85613E170457D4D1CE423FBA568127D4 E
Malicious:	false
Reputation:	low
Preview:	......JFIF...h...."..U.......................!..1A.."Qaq.2....# BR....br...3.....$CS..Tc....4s...%...5DE................................8......................!.1AQ...aq..."....2R..#B..3r$b............?..*(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(.... (B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....(..".(....(B(....*K......*.6#......cy.:..QtT.n...}[.kj..]<.z......T. <..]..,.y|.k_....[+.$.k_.s..@.D?.).9....EY.3..e.DF....W=.K1.5......|.......c.7.2<.a.."G.....9BJy#.B.(..j..6..6..^+....Y....*>.A.....5..5Y..cPV...iUu.c..q|......f.......B......]..~...?.*.......2.k*G..f ....k.^ ..d..j..GGm...v...aHtU........N...\G.....4v.?p]......%QMX...Z...Ei>...%=

Chrome Cache Entry: 242

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	8086
Entropy (8bit):	7.96079286623829
Encrypted:	false
SSDEEP:	192:C/p2NUmgrtCLI4+vUSf31ESZLaegozslnytMWa7TkDcop:C/UNzgrtCLI4GUaESpzsgA7TKZ
MD5:	7BFC640FA12EC8BEAFFFF8CA1CCD9BCA
SHA1:	1AA8C0219571A38E8C1600E4A1862FE5B4190B54
SHA-256:	9BDE6D454CCD3BDFD0CB82052F4B559F91BCDE1ACD09C200B25CEAB5D8441178
SHA-512:	BF5A9BE7E0D4F221CD0CA7C9C13F07997507762F6AB48CDC6E69030635867281CC3DA8154B28FDC89A3670EC27F61099F7C87CAD55D0EEA2394E5EC9157908 3
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/z950eFx-wowoAV2KgHast5YFcrxoGJtY18fYd_eMgvEDVn8_tsJwApy4Dbs1iqE2tAjX=s64-rw

Preview:	RIFF....WEBPVP8L..../?...M0h.H...{...xID.?...,.0...<L.....6.`.I..).p.(...sz.u..$.I.#,.....u$.....g...BKu.D.....i.&.....a.n@..wU..#y"BDE*A.....t.. ....o..... .....Ir..#5..g. .m.U.m...c..k.-i.,..N.effff...<.....en.....,.....)..../R.m.....gf.[.F...v44..H...pwwwwwwwww..nqO...(.X`agw...'Z.N.m.y../.6w.[.m...2l.m.mN.....{k..R.7..m.t..p.7.....&....`..@....!a..d..b< ....7d9..}.....0.f.....~).x.g.Fe....K.RP..,2 .....q....Rc{...a.m...@..ET .@. .S..Y.#}..?.{x+.Ad.k.2.k....Vw.6..l.9...:..."@..".. .)R..... .....).....V.A...0<...{.....IW...[...=1...|..;.t.]. ..8...A....[5....W.._'...~.?z..b$..)....B..!.....T1"R` .....9....]+>.g?[_}.V... E#P `.f.....N....Uw.:.....y.a(..A.:[.B..3.9.....^...Y.C{.og.w9..".HQ.P.x.Vy(.....dG.....t.....y.'.q.o.9.d@A. ...\P...S..&%pQZ..Oq.5OD_C.rm.e..6d.+8.P)..@...z...u.....J0b.$.....T....C.....V7.J.....{...../.!.....6(...>..T.$:o..N..tW..x..V...,.....1;.....,F.....k..!..T....

Chrome Cache Entry: 243	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (923)
Category:	downloaded
Size (bytes):	1365
Entropy (8bit):	5.298186704852222
Encrypted:	false
SSDEEP:	24:kziQY2JWvbAfRFbsQy/Fyq5QXKzGAciGbn64Gbh9V+5o6yZkwey5fuXkT5egrMol:kiQY9vEby1GAciGbnHGb7sRyZkbUTsKf
MD5:	F6A63B70E6AAC6796031067CE6AB78B0
SHA1:	B482DE10C65EE85785F9AB9A7A4DC7C594BD003B
SHA-256:	40E90D27329BCC81D228EB400AEC58ECE7963B137B2CD411F30E04C93E1E230B
SHA-512:	B6F86528B55066F1BC813077B6EA32A40175CA0BE24E11B457A7A7DAC17DED6EB703DE3A25EF12589B031FBB1E135943CA3607DCD3E9BFCEA13CF7A27D2A7FA1
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,lJGqxf,lZT63,lcVnM,lgeFAf,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PH175e,PHUIyb,PrPYRd,QIhFr,RMhBfe,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fl4Vwc,fKUV3e,fPcQoe,fdeHmf,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYClec,pjICDe,pw70Gc,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appscategoryview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=bm51tf"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("bm51tf");.var k7a=!!(_.Ue[2]&128);var m7a=function(a){const b={};_.za(a.va(),e=>{b[e]=!0});const c=a.O(),d=a.qa();return new l7a(a.na(),1E3*_.vh(c,1),a.H(),1E3*_.vh(d,1),b)},n7a=function(a){return Math.random()*Math.min(a.qa*Math.pow(a.na,a.H),a.va)},iL=function(a,b){return a.H>=a.ha?!1:null!=b?!!a.Ba[b]:!0},l7a=class{constructor(a,b,c,d,e){this.ha=a;this.qa=b;this.na=c;this.va=d;this.Ba=e;this.H=0;this.O=n7a(this)}};var o7a=function(a,b,c,d){return c.then(e=>e,e=>{if(k7a)if(e instanceof _.Ed){if(!e.status||!iL(d,e.status.H()))throw e;}else{if("function"==typeof _.Mp&&e instanceof _.Mp&&103!==e.O&&7!==e.O)throw e;}else if(!e.status||!iL(d,e.status.H()))throw e;return _.zd(d.O).then(()=>{if(!iL(d))throw Error("fc`"+d.ha);++d.H;d.O=n7a(d);b=_.zi(b,_.Hha,d.H);return o7a(a,b,a.O(b),d)})},a)},p7a=class extends _.nq{static Ja(){return{service:{aM:_.i7a,metadata:_.j7a,XY:_.h7a}}}construc

Chrome Cache Entry: 244	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	337
Entropy (8bit):	5.135617493816446
Encrypted:	false
SSDEEP:	6:kRZzRxVvnQYUGbA18G/QVf1324BIDbeNFMwQRaNw6JpyxZRNlad0:kRZTFfeH/Af1G4WDbelkbRN20
MD5:	8E6076A4445A16A48ACC94DC8E5685E5
SHA1:	89FBE0FBC99F0920AA4736F6960517E1C413628D
SHA-256:	3886D233A350C461D64DD7E5048FA82325745DE773B16C3D9D4780E9EC9AFA7D
SHA-512:	B56BEAEED0FF90F50CB1956FD7F615EBE8008B9A2E93109EE2C76210A934F464F6D8495F1130318BD05E11B797C0B21D9813242D8DF67AF7D9CFA65E7FB6422A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,FuzVxc,GkRiKb,l8lFqf,lJGqxf,lZT63,lcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SWD8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,Z5wzge,ZfAoz,ZwDk9d,_b,_tp,aTwUve,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lpwuxb,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYClec,pjICDe,pw70Gc,q0xTif,q4UNLc,qfGEyb,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=UZStuc"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("UZStuc");._.lr(_.lza,class extends _.mr{constructor(a){super(a.wa)}H(){return"UZStuc"}O(){return!0}hb(){return _.r5}});_.Qq.UZStuc=_.rz;._.w();}catch(e){._DumpException(e)}.}).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 245	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:H0hCkY:UUkY
MD5:	AFB69DF47958EB78B4E941270772BD6A
SHA1:	D9FE9A625E906FF25C1F165E7872B1D9C731E78E
SHA-256:	874809FB1235F80831B706B9E9B903D80BD5662D036B7712CC76F8C684118878
SHA-512:	FD92B98859FFCCFD12AD57830887259F03C7396DA6569C0629B64604CD964E0DF15D695F1A770D2E7F8DF238140F0E6DA7E7D176B54E31C3BB75DDE9B9127C4
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAk4BRY1LvFEvhIFDVNaR8U=?alt=proto
Preview:	CgkKBw1TWkfFGgA=

Chrome Cache Entry: 246

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1223)
Category:	downloaded
Size (bytes):	131327
Entropy (8bit):	5.716164634933234
Encrypted:	false
SSDEEP:	1536:rtazmz4go7eqIDSlH764hFq2Pp7OTBlEolTYzgyJa2TLR3llNoxicd1xEHTa7+Uy:rwzmzo7jFl2JKOJYIOxJxV6UgTYnU
MD5:	5FED19F4245CD3AA5AF428989B725987
SHA1:	7F9E7508B2B536D5B03327D51B1053332C358A62
SHA-256:	FE20127D9363865CB621000C73F41B07B967A438D91F8A319D87A2A0D69BC0F9
SHA-512:	80AEE99AE9978515046F4029B20A26A0AA45F646BC18C5100558B348A2063C72DBC11441B3F7A5C0F3A8D052FBD46124D6C4F7A02D96D4DD0DBEFAC0E267382 4
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SdcwHb,SpsfSb,TSrO,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,gychg,hKSk3e,hc6Ubd,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,developerdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=sOXFj,q0xTif,tucRse"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{.var Epa;_.un=function(a,b){if(!Number.isFinite(a))return String(a);a=String(a);let c=a.indexOf(".");-1===c&&(c=a.length);const d="-"===a[0]?"-":"";d&&(a=a.substring(1));return d+(0,_.Vf)("0",Math.max(0,b-c))+a};.Epa={MN:["BC","AD"],JT:["Before Christ","Anno Domini"],gU:"JFMAMJJASOND".split(""),zU:"JFMAMJJASOND".split(""),dO:"January February March April May June July August September October November December".split(" "),qO:"January February March April May June July August September October November December".split(" "),nO:"Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec".split(" "),rO:"Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec".split(" "),xO:"Sunday Monday Tuesday Wednesday Thursday Friday Saturday".split(" "),.CU:"Sunday Monday Tuesday Wednesday Thursday Friday Saturday".split(" "),pO:"Sun Mon Tue Wed Thu Fri Sat".split(" "),BU:"Sun Mon Tue Wed Thu Fri Sat".split(" "),hU:"SMTW

Chrome Cache Entry: 247

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	3054
Entropy (8bit):	7.910076776321541
Encrypted:	false
SSDEEP:	48:S9skh+s2qz4kX0614PMHhJoKmjnZA1UegndbMF1KmwWGcMAgwmx7bEzF4hEkvQhB:QBh+/qtGPMBJlmjuWegn1BWoAgF7bEGI
MD5:	61374F426AE0866DD88D32A073C6AE47
SHA1:	D62C0C600141009A6882B56F94AD0F6BDF5896CE
SHA-256:	D45C08D891324AC0723D3A95B0AFED9FF0092B4082C8ADF262CC5D452C36C485
SHA-512:	DAA42C80BB0939088412E024E719B6B3C534DC11D64214392A0EBA667D0E314A5B02B2163F604B8F85CAAB214BE4ECBD087570EBA035C935FEBFFE31FB54F5B6
Malicious:	false
Reputation:	low

Preview:	RIFF....WEBPVP8L..../?.....m...._...n.f.....%..^.....V......,.G...y._z...J.m$l.....#>.o.K.l#Ir....01...'.....2........&3u.2.;);.l.......3...jjz^.c.....{..x......m..m.... I...]\...m.m.m.m?..L.<...L... ..x.m[.l.r.c.-fff96.........wl...bf\<.....l[..h...y...,W........&..e....`2...U<...=Ca....+.......(.....o..[.}.........u.H7..!....K.!..ml..g.{.w..&.G=.s3>..`h...._L.B....]........O..6.aI.F..$... .'..?.&...]hP-.X o..7~z.7...t7......t..0|.q..k"tS..8jY...._[...W.(.(.F....\....\..(...T.rk1.%.*........k.Vj...c....v...8..._...QJ..+q.KZGF.$...k..^.V`._...J.I...,.".....-j....r..\.I../. ..@@C....3..^..}..M...o..........t...x. .c+RTe..+....A.~......}...x(<..CE.~.~b....5=.....Wz.7.N. .E.Z...^.....<.....8.-P.....6...^l\Jow~...Z..@%d.Y2N..}~...i.L...`@..c~K.....L.......7.d..(...8K..?8...S.....` 7..[d......gZ.GS....L |X<..*.V.......2r........x..0.....8..-f...5....|...iv..J...G..D*V.....#...........}..r....#..L&.3../:z...gs=.....|v..:.D0....J.y..

Chrome Cache Entry: 248

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	7.974695271372103
Encrypted:	false
SSDEEP:	192:RyC8XLOf/agEPYLnalf6O6lgARkHb1UrTYwfwLcZP9c4iNaVbH4WqN:ECgL+WialiBjCHbiTpAqP9XiNgcWqN
MD5:	0C33BA3576410B21607EEF5294EEFA5D
SHA1:	08EBD96F18C6A4B6BA398B37E67499BECB96EFEF
SHA-256:	76EF2DBF0EC33757A35FD3895F6F73536224FB8D11857AD46B882DE1DF9324A2
SHA-512:	5FDDF33D5A5BF64E256FA0D3D0813FF3F4E343AEB9D6C48722CB88F48FFB97AF2DF7E5C9EEB5EDDCAFED15BC578F67FB3AAF534918225153B2EB1F301865F F9B
Malicious:	false
Reputation:	low
Preview:	RIFF. ..WEBPVP8 . ...r...*..(.>Q$.E#.!....8....H.,...l...._mk...H.a.....m...l.g.;..._...0\|.~.........e.....7.g..e.._.}..m.5.j~..l.j~..e?..2......=...?).ht7..B.....?....~.........=B?..g...#.W.Of.... ...?..q.....^.....+...[.C.G...?.....w.....,~.?..Q.1../.....W...s.o.....g._....{.....g..s..?...Da.....\|.U....A..[...1}.rw...'.5.....v..k.Y`.>.M5.V..^..Y.ESK,q..O.x...j.q"Ej.5.k.R .....r..u.....:.f1sx....h.9.c:%./.Ur@....Z9.IxO..!s$Q....C.[....v.....4h.Hy.$.....QR."I...P....\S..5..(%.r..!..Cq.`.....7^....At...&...e...j~.r.)wUA<....jy..6...2k(.K...D.j.ik...r...#M.v..d.R.... ..J...].....y2.....fX=...<..^..O...b.-.t.5.O.....q1...?...Q.b[.2...%..p$.C6(.=L4..q...z .B.U....M..p.b.r...<#Y..v.....U{U.oq.y.+CR.w.S.N...g.l..T...5.T.....1...P...#.-..Ty+...*....~C.F. ...0....#..~....Z....IPP$.0N.)=^pe.t.!..D....-..u.l8ZkICOT@e.,....A....N.`.2...m.......<.....*.....[.w...4I.p.b....N..:..n.[.!.-...._.".\l.a.....^..V%...5..|Y..

Chrome Cache Entry: 249

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1104
Entropy (8bit):	7.8340659828453205
Encrypted:	false
SSDEEP:	24:PFUcWKnpazsGnPF4r/7/OAEf3Bdy1Wr+CLU6Y7qdd gsSW8HA9Bd8:PRW49GN47rEvBoljUiddgPdUD8
MD5:	3247CDEE38829D74BF9D441EF0FC31A1
SHA1:	DA1D5FA95C28BFB726D66F03E700B1922EC51875
SHA-256:	3F215ADCE75131E4D514D73BC7A600D17779A2DAE3A0A663653245CB915E6CBB
SHA-512:	36DFC2517A09A0BBD242906E02752989D91F8CD633CBA99BB3C2105FDBACA1E77AE6B5F1007BB51D212A74DEB99F445539A90C1F65DF4A08C3D06D1BB4751E 02
Malicious:	false
Reputation:	low
Preview:	RIFFH...WEBPVP8L;.../?....Em.17....<)D.........}.J#IRV.=.z.....A.M..Ow.!.H.'..^..F..5.!.........m..).....%3.$..j$33333333c..z....XA.:.&.P.....K...K(.[(W..0..(nW.@.6..k..n.v~.. ..l.koj.........l..!~.....Qr...w;/A....KXi...9]..^.>...<.j..\6.........5Es-....G..../P.\|.....fh.RZ...\|.L.^A. ..0..AJNs3.....z.Ve,..t...g..r.....z.6.....w...l..v.:.X>.\|.H..x.-/{...'..7.P.}.f$.....d.w....- ;M..&C.....7.....@....k.+.k.e.,G...\....*{..}aH./.(.d....5.c.+0...g.u...+lo..)9..}A#.Zy..2....t./....~....r..?.cT.?4.....u.dt...V...O.....4".~....f#G>..sE...3j....W.....l'.?..F.....<y.".....9O..... ..m..y.!..K.3..)u..,.t...}@R@.p..# (d...;<8.....n...-...y...:.2{..:s...=>.B.I.`.C.....j.3p...[...}...@..7.....I.a|FCed.Q.\..'.....x.....X..b....n$.1 ....pH....u..6}U.HWV..@..B.K...V....qd..(.. /.Z. ..y%....A...........[1.Q.zt*p.....4f.{....K.+.j([...!.8.a,}...T.....VU....D....Y.p....*@$..^>...u .X.....:.nOV...z....w..#

Chrome Cache Entry: 250

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	266
Entropy (8bit):	7.052421013235357
Encrypted:	false
SSDEEP:	6:yk5ZYChDBpEnS96WesGKsxdRM8Zj5elkndH7xLiGE6CAYdr0jSKlz/zZwE4:34CRBpEnLlD3Pb5e+LE6CACgmKlzLZwT
MD5:	0923A53B64E64DB75177B6972F016A42
SHA1:	6915D871CBEA8A3B8F4E54367DCA538DA0AC3082
SHA-256:	E0106DC1C0490A432C08671994F87FCBB982B7B25B4F9CBB640D49A03BD89CE3
SHA-512:	5054B69C1A895FEEC0CECD471FE317149D8F804E15CDC0ED51F8BA6B3FB61E092C5C78A92768D31273DBCBD189148D305BA4EB1EB210174DC6B0724615B1B1 F4
Malicious:	false
Reputation:	low

URL:	http://https://play-lh.googleusercontent.com/W5DPtvB8Fhmkn5LbFZki_OHL3ZI1Rdc-AFuI19UK4f7np2NMjLE5QquD6H0HAeEJ977u3WH4yaQ=s20-rw
Preview:	RIFF....WEBPVP8L..../.....$g.....r^.E.$E.....~8...A.H....A8...%I#.Vr....b9.P.....N..[n.P.....6\.w.+.....X....U'...#.}...Y....A.xdB.....$%.ww....t. ....Q|.....,.....q...D.@!H.N.p.5.....*`...ms.~.l....\.[/..u=..@...X...4j=.}..edi.i...%..0u~.MH..

Chrome Cache Entry: 251	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (802)
Category:	downloaded
Size (bytes):	113437
Entropy (8bit):	5.70515118121591
Encrypted:	false
SSDEEP:	1536:qbio3oMCweFn5tB0607F6LBZtVW1AjQn7JFNPYmaEb0ycB:qm0oMOFWf7F6LBZtVW1AjgwEA
MD5:	A76B94979136A756B4085DAB914A4250
SHA1:	2B44B64F806A77FDD5CD3EF880E758975D78FFD5
SHA-256:	9B1E5D98B49D1672A5EE6807807089185944766 3AC7AE44E1D3A0BE93D2A39FF
SHA-512:	C65D410FA612DD09118A19F30592B424847EBC8D0CDF8AF7175DD2AAB9628F793399D1881B045AC55A9D24BFC1CBE11EA036F34F6B6DB9EDF3C9836465E9D29
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NkbkFd,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SWD8cc,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aTwUve,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fdeHmf,fl2Zj,gychg,hKSk3e,hc6Ubd,indMcf,j9sf1,jX6UVc,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lpwuxb,lsjVmc,lwddkf,m9oV,ml3LFb,mdR7q,n73qwf,nKuFpb,oEJvKc,ovKuLd,pYClec,pjICDe,pw70Gc,q4UNLc,qfGEyb,rpbmN,s39S4,sJhETb,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zBPctc,zbML3c,zr1jrb/excm=_b,_tp,appdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=sOXFj,q0xTif,Z5wzge"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.rX=function(a){return"Rated "+a+" stars out of five stars"};.var tKb,uKb;_.YY=function(a,b){b=b||{};_.XY(a,_.zo({Ha:tKb(b)},b))};_.$Y=function(a,b){_.ZY(a,_.zo({Ha:tKb(b)},b))};tKb=function(a){a=a||{};const b=a.lg,c=a.Gh,d=a.Be;a=a.jv;let e;e=_.aZ();e=e+" "+(null!=b?b:a?"cKScvc":"IfEcue")+" "+(null!=c?c:"HPiPcc");return e+" "+(d??"")};_.XY=function(a,b){b=b||{};const c=b.content;a.open("button","J4hqjc");uKb(a,b);a.W();a.print(c??"");a.Ga()};._.ZY=function(a,b){const c=b.href,d=b.target,e=b.content;a.open("a","BDhSBd");uKb(a,b);a.ma("href",_.Lo(c));d&&a.ma("target",d);a.W();a.print(e??"");a.Ga()};.uKb=function(a,b){b=b||{};const c=b.Ha,d=b.Kf,e=b.Se,f=b.ariaLabel,g=b.jscontroller,h=b.jsaction,k=b.jsname,m=b.jsmodel,n=b.jslog,q=b.id,t=b.attributes,v=b.hidden,z=b.disabled;b=b.autofocus;f&&a.ma("aria-label",f);a.ma("class",(c?c:"")+(null!=e?" id-track-click":"")+(z?" hf6Ybc":""));null!=

Chrome Cache Entry: 252	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	14288
Entropy (8bit):	7.971123367692374
Encrypted:	false
SSDEEP:	384:DIyi/vxRM2ObnY6l1WPhWvqMjh6TvilI18ccxu:9RA5lAcvld67NI18n8
MD5:	C20218C9C4795819B8A1B67545D4D0AD
SHA1:	ECE8F6FE9D29B24EB7D0F79559C6D3F093F72A1C
SHA-256:	E23EB256FB8DBCFABA1227A39300D06A182E5FAFE790533EB724A3982026BDD2
SHA-512:	480E9DC7BE3524A465FC542E5AB9E5288E728B38C2C67A5927D042731C247E0134D2B02DC6AB67610225CECC2CC48E3BAAB32FB6E0550CFFEEE7F9D9D86255F5
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/fDpoqIbZ884ylRnMK8Lx9Fu4DsLQk5yt4f9WkxeOAPpGnzc9BTi_YKkMsLvoMdx7Uzg=s256-rw
Preview:	RIFF.7..WEBPVP8L.7../..?...m.H..... .....b]....,...`Q.....YjP..(.....$ SO..o..7..2....'.qF..I..D.....T...,2.....c|.....J.J..]...t....n.F..n..3..].1Z#.'\r..n.u.B...w.:.m'...t.L.]....l[..'t....(" "..".b.. 7.....w..O..4V.....C.R..q.M.%....%...`(0h.....GF.F..o..M...0qY.....L.....H,.....C%...`...A&...eP>.....Pq &"..!"..1jl.....+Vc..mV.K..24}..V6.._.N...D...S.i#.)d.....cj...."7w.u.-.d.~....\.<P....8..m$))....!.....Q....>e...w... %y.l@J6...F..2.M....\ex]E..$J..lq...a.C@..L9-....N...*.A.Q.p....."h...$.....$*.....G*.(...QA...oc.m...X.k..K.~,9....)GcN..8Y.....Rj...DA.P....r..C..luj...M.6...hR3.zq.R..m.Ht.....m[U...=s..>h..(...<...r6.H...^N..>W..4.%p1.d7l..u4..... ...7..i{.Hj..).IR .. ."..9...c.....~G`_...n..n.D@.g}a.{B`.=e...P LU..6rDc.o5]. ....I....(A.v..Z26.M.m7l#I..h_.G...!.=.kW.?Ev...#..Y.....(ff..H.0..V...0../2...ui..l...N.F.Y.`.l..|.y.ec.u#s.v..\.oB.m$I.$YdVW.....VUf.Q..p,.....4*'..s.m.l.l

Chrome Cache Entry: 253	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (804)
Category:	downloaded
Size (bytes):	23587
Entropy (8bit):	5.601761987333268
Encrypted:	false

SSDEEP:	384:wMk2o2ePZ1Ar3DSrDkO4tk+MUVMVJ6Qr/IsrDGM7mkJtrruHmasr2hROXdrbCxEx:wMktZ1ALor4tkjUS36QLIs/GM7mkJtrD
MD5:	17EEB696E89799AF587349622BB39DB4
SHA1:	B6F581B91AB359C4B31288D39B1205F6C644DE1B
SHA-256:	B6132CD08E4FC9A31951BAC7C02821700BB3A3C0A2C7E6E1456EDB06A37DABF4
SHA-512:	C5E264860A39137839D9B40DAC0FF7B8A6A1409D36A5D87A9D2790EF58BA04B29BEC4D1194CECE07FAFAC5DAA36C7CAB6582E9713A5E49D9605865CADC124AC
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,CvxVpd,DRmmld,EEDORb,EFQ78c,FuzVxc,GkRiKb,I8lFqf,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,M2Qezd,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,RjJvI,RqjULd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,dfkSTe,e5qFLc,fI4Vwc,fKUV3e,fPcQoe,gKWqec,gychg,hKSk3e,hc6Ubd,kWgXee,kjKdXe,kr6NIf,lazG7b,lsjVmc,lwddkf,m9oV,mI3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,qqarmf,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,vNKqzc,vrGZEc,w9hDv,wW2D8b,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,yNB6me,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=GjTCAc"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{.var AEb,BEb,CEb,DEb,EEb,FEb,GEb,HEb;AEb=function(a,b,c,d,e,f,g,h,k,m,n,q){const t=void 0===q?!1:q;var v=void 0===v?!0:v;b.print(_.Y(z=>{var y="nCP5yc AjY5Oe"+(null!=g?"":" DuMIQc");y+=v?" LQeN7":"";y+=e?" "+e:"";const D=_.ON(C=>{_.Z(n)&&_.PN(C,_.eO(n))});z.T("ldWeFd");_.pO(a,z,c,d,void 0,y,!0,void 0,f,g,h,k,D,m,1,t);z.V())});.BEb=function(a,b,c,d,e,f,g,h,k,m,n){const q=void 0===n?!1:n;var t=void 0===t?!0:t;b.print(_.Y(v=>{var z="nCP5yc AjY5Oe"+(null!=h?"":" DuMIQc");z+=t?" LQeN7":"";z+=g?" "+g:"";const y=_.ON(C=>{_.Z(m)&&_.PN(C,_.eO(m))}),D=_.ON(C=>{_.Z()&&_.PN(C,_.eO())});v.T("rFER7");_.tdb(a,v,c,d,e,D,f,z,!0,void 0,h,void 0,k,y,1,q);v.V())});.CEb=function(a,b,c,d,e,f,g,h,k,m,n,q,t){const v=void 0===t?!1:t;var z=void 0===z?!0:z;b.print(_.Y(y=>{var D="ksBjEc lKxP2d"+(null!=k&&m?" HDnnrf":"");D+=z?" LQeN7":"";D+=h?" "+h:"";const C=_.ON(J=>{_.Z(q)&&_.PN(J,_.eO(q))}),I=_.ON(J=>{_.Z(f)&&

Chrome Cache Entry: 254

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 192x192, components 3
Category:	dropped
Size (bytes):	9510
Entropy (8bit):	7.83625996695091
Encrypted:	false
SSDEEP:	192:9w8ANqyqq4YoTqHi0DAFL3RblxYhsOOHJO4XKEwy/av0V1sw:9wZNzqRGHi8AFL3VvvpOAA6a88w
MD5:	5A661ECF18FD74DD9E3197A72A3110A0
SHA1:	2DA2C482A7F289F6DE11014948D279599B919281
SHA-256:	E2892D26AA66B12F01D0831E0F30D084D1A9FD1EBCBF2A07374CA944D474E156
SHA-512:	F75FAE29AA0815D6840F1A55341ECE13CEECA24408700582D32EAB6C165F228419FB52FE90856CD5227F52EED1F87D4835EEF24807942E586F184372973C0497
Malicious:	false
Reputation:	low
Preview:	......JFIF.....ICC_PROFILE.....0..mntrRGB XYZ .....acsp.....-.....desc.....$rXYZ.....gXYZ...(....bXYZ...<....wtpt...P....rTRC...d...(gTRC...d...(bTRC...d...(cprt.....<mluc.....enUS.....s.R.G.BXYZ .....o...8.....XYZ .....b.....XYZ .....$.....XYZ .....-para.....ff .....Y.....[.....mluc.....enUS... .....G.o.o.g.l.e. .I.n.c... .2.0.1.6...C.....C.....".....Y.....!.....1VW."8Aa.....2QXqv.....U..#$3BRS.69Gbru...5Cgs.....7.....Q...!1...3ARaq."2.B...$.#br.....?...!..+..W..wF..I.5.....:&....3.....b@$.(s.E..B/.gy.....9..7..^K..O).....j..^\.....%..s;.og^.....y&./0..E...1..

Chrome Cache Entry: 255

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 467697
Category:	downloaded
Size (bytes):	109226
Entropy (8bit):	**7.995960071386688**
Encrypted:	**true**
SSDEEP:	3072:mJYehMLlbR4bMPrHe0EQ9DCMJBW1DoNDbRwDEWq:mJYomPrHe09vaNoNDb+ox
MD5:	2691C0B5A94D6C055173C614952E5716
SHA1:	F18A78EA1901B4843A5A9BF5EB38423B143A6E1C
SHA-256:	6183D53E9D9DA3CAE78CF668D32EB8A63AADDBF27C978EA1D50AF8D88D7C5652
SHA-512:	4AA0034C54B9B9EB694555CBE9FC46D0B61B86E41824C5C8DEE83A4741A254B79E6B5BEFE3713A0BDF94AFF8694CAF80FD0944126214A9F00E869BA642ECB0D4
Malicious:	false
Reputation:	low
URL:	**http**://https://bddb2d2561.62b81f5af3.com/9dc01d48437911a2369d0f0f8dd84903.js
Preview:	.....s...&.W.qj..e.F.r..2...B.H...0...?...lJ.gf.{...$.q..~:.>;.y.8.yU..t.....?..kf..O.....?^..._.xY9..$|N."g_./.....S..5...../../_.|Q.....1....._..9{.j_....I&.+L5.....h.;:..\x..]5.uO^./.Iz..C...X[Sz1tS.g..%.....IV..."-+J.7E.....C..Iv....."..h..... ?...?.../.m.....?....].$.....&...% ..X../.....6/I...`A...A._...=}'.....M{5 +Gnp.j.xX....I...m.n..H..4.b.a.N....Z.....E..>..k.x....'.p..a~.=.~...g.....pc.....GVJv.y.X{&.^../...? .m....._.....g$..._....;..am..5.qe..<3....._.GC..._.n./.c..(.z.M...i.g.|....s{<g9.w...=.ty_.....yB..:....[...k._.....m...?.....1O..c.*x.a.'2.b...X.....D_.D.#...'.....E.....(.c(.).F.r..>.X.!S.....k....7.n.b.d.....I",..ZH...#q.9..x..s...1h%.....s....3_c....FI...>wd[...:.....Q....[.kO.....\...VR.k.....&@...-`"..../..4.2.4P....R..y..Y....q.2.9.:.M...MP..Gm.....k..P..Wf..Y.....{f....Y.E.....e&9.TN6.....4.\.w..g.9....7.-.:.c.0..x..\x6%Q.%..^..tG..?z.vm&

Chrome Cache Entry: 256	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from Unix, original size modulo 2^32 123040
Category:	downloaded
Size (bytes):	40277
Entropy (8bit):	**7.994307373042056**
Encrypted:	**true**
SSDEEP:	768:2hUEdDr5OIfguJJtmXjXQoM9QSjxGmCUbX5N7nACGaVFBZJ1pC:2hUEJtJfZJJtsbQf9w+X59ACGaV731pC
MD5:	14BFD8290FBC97E738620D36BB5CB70E
SHA1:	A50086460CCE47880B71558012F617AC42057901
SHA-256:	067EB0521589BC9063628B1E095C6CDE459650401E22E8D5090E9677C1927F61
SHA-512:	54E5801023183FCD8D6115F6738F5E0E25B090F4FDC5E48B42295ECD69C110BC9E1F988FB2777C80ECB5FD239F72D2960DDF12A3D745894FCD7E1C59E8053A0
Malicious:	false
Reputation:	low
URL:	**http**://https://js.wpshsdk.com/npc/sdk/common/core.js
Preview:	.....v.F.(.+$V...J4.....sl.N..c;q..G.....(Y!..w?..Bv.;..Y.feY.P(.c.~?.8..n.u#{.....ITOf.....o.....*{*.E!*.\.....JU.:/.....?..'b....=.L..z....\|....a.>.o.#q._....I^.eu.{Z.U...Mvr. ....T.nWrx./...\|8...L6.DPs..R.Z.Q....:...*I.\|...},.Uv....\|..^<.\|..&...#..i... I&..._.....A._.\|.t.~I.:....2....jY.8....t:.E6...:..Y..f)U....q.... .0X3Z.....Nk.+.e...*.e...m5..... VY.]c.....LM.f..~.... ./f.(..us.o..2..r.\.....\_G..6.D"./.x>.g3..(e.=N.....j..*S..o..o....}..d*.....\|_V7%CD$.d....\..&...N...n.q.m.5..i.H.B..P.W.t-...Tw/.e.,...p4.E;....i$.;.`..\.\|.....Sz=./...\|..2..\..i%dy].Uy..O.!? @'.FU..i34?.T.....}IC....B{..u.t.....u.0.n.kh..C..Z..$...|..2{.o....S1....'.SY.....]....v0..a\*....5.F..f.4.E....Nl..i.X.0NX.K./`0.....*Kx.....(.M.....2=..\]. W.=...e.<...m\&c. ..F.Ez...2 .....^.*>.v..U...Q..{y.}.....e.?....Ul.....i.....H.U....7'/..meq~._.Dv.7..e.s.|Z.z..\&....2.gY..rZ...._5...M...O.....z.S..Yr..u^...,.?.

Chrome Cache Entry: 257	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	458
Entropy (8bit):	7.165896275783275
Encrypted:	false
SSDEEP:	12:3WZnPvWx6wgG56N9q8XXVkGQklgyr02hC28TTta/:GZPvG6K6zLJcywSr8T8/
MD5:	6222F809059D9C06243EC20D40F6F1DE
SHA1:	E0B203D35DDC1F5AFEF671A654501CD234E374BA
SHA-256:	EBA0DB705381E35605B2AB2F954C612F09EED0FBBB9A90B928DABC824041588F
SHA-512:	51E2259911C49FCCD5BEC5F914EC79E1E81673861351D6B3ECEC9F443429F1DD379AC6E1CD969DC66916038C4F2CF384369692DC33FB30465294B8DAF776BB 0
Malicious:	false
Reputation:	low
URL:	**http**://https://play-lh.googleusercontent.com/a-/ALV-UjVEDgFjAocMId0v2Cxmm6MLmoD7yzAcB5ZdgKwNXzXXyFM=s32-rw
Preview:	RIFF....WEBPVP8X.....VP8 z...P....* . .>.6.G.#"!0.....g....+.2..G)8.T.D.E...i.&a.i.....x.....m\...m.....&Mw'.f...L@S<..o..L.....+b.Cc,..8.....p.t.$#.;.EV..V...$. .....i..3Ef.....2E..U.$....V..Pf.^m.....^....(.~=.....Z.>./G.....7.I....b. ..k.X..j^.....>...L...\./.S...+P@...r..L-.U.g>L<Z..".....*.`.)..wU#...c..[]I2<.?d.[..S.9..6..T=.Y<z&\;).d|.~..}..'. ..EDA..^...EXIF"...II*.....1.....Google..

Chrome Cache Entry: 258	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	3.972163460365541
Encrypted:	false
SSDEEP:	3:YIzMaXwLnDWWn:YIHUDWWn
MD5:	0849660B654E3A313882A44C0E7DC08A
SHA1:	B1493D6CE204EB99837D9B33849D1458093A6E6D
SHA-256:	6E73B83AE8FCDAF81421A4236C9F817A9E4EA0FA931BF696F72872B266BD83E6
SHA-512:	A2405A2F44E82CC439D5848C5B719E2E48EBC31F7659F2A7D319994DFB2563443A16BF237B03FF5B2F4AF4EC4CC04B6E28D7B2B525DF9BDE73EA433B0163916 7
Malicious:	false
Reputation:	low

Preview:	{"message":"Internal Server Error"}.

Chrome Cache Entry: 259	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	792
Entropy (8bit):	5.271423979636484
Encrypted:	false
SSDEEP:	12:kRZTFMTaH/Af1RDyBmH/Af1ODTGiw1YZH/Af1oAWD3GXQvnFpH/Af1sDZ2kbRN20:kzeTafoffR6iw1GfLnFpfLdrl
MD5:	4394984BDFC2465754EAC8C70F384628
SHA1:	A43018C1513B1AC900DC05201E5D636FB5954E9C
SHA-256:	38A273950BF3FC4C8A97644A01BEC26894EB2026C37C91A8900689914E969650
SHA-512:	09B0352BF9386351DFE79B795BB6333CE1D76541C15B82BDD5FB3A61D31201384181962A8CBAF0065113A57A85C2D487F9692EBF43447794459F0B450581B68A
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=A7fCU,ArluEf,BBI74,BVgquf,BfdUQc,COQbmf,EEDORb,EFQ78c,GkRiKb,IJGqxf,IZT63,IcVnM,JH2zc,JNoxi,JWUKXe,KG2eXe,KUM7Z,L1AAkb,LCkxpb,LEikZe,MI6k7c,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,Omgal,PHUIyb,PrPYRd,QIhFr,RMhBfe,RQJprf,RqjULd,SdcwHb,SpsfSb,TSrO,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WO9ee,XVMNvd,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,chfSwc,dfkSTe,e5qFLc,fl4Vwc,fKUV3e,fPcQoe,gychg,hKSk3e,hc6Ubd,kJXwXb,kWgXee,kjKdXe,kr6Nlf,lazG7b,lsjVmc,lwddkf,m9oV,mI3LFb,mdR7q,n73qwf,oEJvKc,ovKuLd,pYCIec,pjICDe,pw70Gc,q0xTif,rpbmN,s39S4,sJhETb,sOXFj,soHxf,t1sulf,tBvKNb,tKHFxf,tucRse,vNKqzc,vrGZEc,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,yDVVkb,ywOR5c,z5Gxfe,zbML3c,zr1jrb/excm=_b,_tp,developerdetailsview/ed=1/wt=2/ujg=1/rs=AB1caFWkNlDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=yNB6me,qqarmf,FuzVxc,I8lFqf"
Preview:	"use strict";this.default_PlayStoreUi=this.default_PlayStoreUi||{};(function(_){var window=this;.try{._.u("yNB6me");._.lr(_.BBa,class extends _.mr{constructor(a){super(a.wa)}H(){return"yNB6me"}O(){return!0}hb(){return _.g2b}});_.Qq.yNB6me=_.I2b;._.w();._.u("qqarmf");._.lr(_.nCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"qqarmf"}O(){return!0}hb(){return _.Y3b}});_.Qq.qqarmf=_.w5b;._.w();._.u("FuzVxc");._.lr(_.pCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"FuzVxc"}O(){return!0}hb(){return _.S5b}});_.Qq.FuzVxc=_.V5b;._.w();._.u("I8lFqf");._.lr(_.sCa,class extends _.mr{constructor(a){super(a.wa)}H(){return"I8lFqf"}O(){return!0}hb(){return _.Y5b}});_.Qq.I8lFqf=_.$5b;._.w();.}catch(e){_._DumpException(e)}.}).call(this,this.default_PlayStoreUi);.// Google Inc..

Chrome Cache Entry: 260	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1909
Entropy (8bit):	5.090327194391798
Encrypted:	false
SSDEEP:	48:YjXZnvndKfkXNLL7uKSXvPMAOdpInG0a790VK/SlATT:Sn/QeNv7uKSX3JYpoZamVYnT
MD5:	8CC669D7A1C5EB42AE06AB66C254F213
SHA1:	5CC28B77545A36C6796BBFE25F2E6E910C2DA245
SHA-256:	3BBBE82FDFB5FC7A0F09FB06A1D248ECDD84247E1FCEDA0D880C44EDAC591832
SHA-512:	4C84D53D46ED848DAA85C834A5835C0939DB29E28D16649F11E86BEA1177745A6C4816F54C30AE9B583860D2484E67126D87558787827E6F878F53D50C2DE0BA
Malicious:	false
Reputation:	low
Preview:	{"label":0,"iabcat":24,"iab_extended":"24-24","default_keywords":[],"cat":"Others","tagId":151659,"script_defer":false,"utm_mapping":[],"tag_id":151659,"adformats":[{"type":"inpage","assets":{"js":["https:\/\/js.wpushsdk.com\/npc\/sdk\/wpu\/npush.js"],"name":"__fp-initev"},"spots":[{"updated_at":"2024-03-04T09:53:17.000000Z","config":{"sub_id":2083435515,"spot_id":513500,"unified_id":400513500,"save_spot_id":false,"tube":"native-push","proxy_domain":"https:\/\/vidvas3.com","auction_url":"https:\/\/ntvpforever.com\/in\/multy ","ip_check_url":"https:\/\/nereserv.com\/in\/dip","type":1,"mtype":1,"disabled":0,"target":0,"ml_close_ratio":50,"ml_close_ratio_modal":50,"eventFrequency":{"type":"show","count":2,"cappingTime":120},"perPageEventsFrequency":{"show":2},"firstShowEvent":{"type":"page","delay":0},"betweenShowEventsDelay":0,"betterAds":false,"betterAdsMobile":false,"branding":true,"startOnFullscreenEnd":true,"paramsToExtend":{"default":1},"tabunder":true,"large_cross_button":false,"is

Chrome Cache Entry: 261	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	8856
Entropy (8bit):	7.976046282619352
Encrypted:	false
SSDEEP:	192:a4PAaT1kN2+c8m07ipWzIILsflahx9ESoThpqidkl:ac6A+cj7ksOxHoFwidkl
MD5:	41B50D204BFC68658E97EAE2C301CB08
SHA1:	0ADB97DF5F0A85144AD1B70A75B5226AD5BF7A0B
SHA-256:	2CC382E0C7A870879CB7B3DC5F35261C33098F0AED8DEA4903C4593DD9F61FE5

SHA-512:	2CAC73A9B49BEF4220546B1B53CEBF1834803579D6281DCF38124570E7BB7BF84085D0CDED10C569FEF68A23105C4281D90739B52DA2047296D3AA6C4E5FF0E7
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/KGCN_wYPWmCvGaLY8VmRLJOV1KYWJ_U68ceJSPt4DLKbcxvYBdxw_5ivLfDog0J3UA=w526-h296-rw
Preview:	RIFF"..WEBPVP8 ."...v...*..(.>U$.E#.!..-.8.D.7]...,.....-.....~.\|kZ?..C.....2....o.4..z....S...s...w.....y..?.?.....}e...?.zj.../.x...../^=....O.><...../...~..)...._..<...}.[f./.c.../.?F.;...S.'.....k....i?.x0.....Op.....s...l...7....k.....g...?.....~U\|.....w.u...]....S.=...:.9.j..H..]...zm..._..n./*s'n...s-.g.T.....sR.....r_...?.....}z!9U>.;../.....:.&s+..4.Z...d....Z..~.3.....7)..c..33...VY{52.*<...u.V..b..... .W\| .H..0..".9....E:.....F..w..^.....5.v.~1nD.....l.n.!l..H....!.dB.../...*....Z...s'...g"...-.....\|Hp..<..1o..$....]3e.....#..7.X...sq...Dp...'.._..hx..;.....-.s.....U9..}S...D.!..1.'.%..Y..".i._.@.E..F,...v.f.D....Z>.[..... ..gf...^.YC.x.{...i...P..XK0&...X)o....|]...OfP.....!#.b-k.G.....{r...a...U].....{..?.gy.D.{.MU.{..)`XN.....|...fp.a)..D.%..fx..L.`...ex....TvRyU....."......M....^Fn...1k.sM.....-|G.d..{A...v.|....#.-..T.;|HFu.....n.lk.7~{...&..l..m

Chrome Cache Entry: 262	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	8702
Entropy (8bit):	7.9696964543351285
Encrypted:	false
SSDEEP:	192:TrvdHcjIL1CgrJpPkFl3pEYBMLXUcVbihGASU9Jd:Hvd8jurmxYBMLXihgc
MD5:	B6BE4795BF0D1F02932D61E99BCBB817
SHA1:	095A9C547B263E78CA6E0AF7B3A39554E636BF9E
SHA-256:	A1665EE004EF4B4C931E492D70B706374CF028A6D284C5E40FE691061EAFAAA2
SHA-512:	B2289F54FF75C1A4F74CB238D0D262D754047E5E89C455362831FE240AA7DD750AE820A2A7255B680821FF9DF5594732E0F400E906E4E8ECD1044F2FD4FB8C91
Malicious:	false
Reputation:	low
Preview:	RIFF.!..WEBPVP8X.....?..?..VP8L.!../?...M0h.H.....Z..."UW..A.....z....D.l..T._....7$z.#.N.....5+. .H...u.Xl.d.....E=..~....*.z....J..:...&...x....Sfb.)..UT..o....f5.4u.g`.~.F.C}....f" .ea.\.`QO..*ZZ....w..?.1..m..a.B...._.Y....m..j..:....]RrB..F..R.w.).9.f.....9{...l....k+.:.="j.6.aB.>Krl....wk.dF"..m. ...h..{{....m.t..?...mW.6.c..B.bfl.v..Cef.Eeff.\Tfff.4..S;.Mk..c.-l..< /.....L.....\|....h.n.b_....m.m.m./.v.,6.}%.ds43O_.m.rk.V...>..B.l...s13333..._..'333333Mf6.lY...P.....$.}2.....Y..]-}..S..($.$'.$.....,+s.ko....w(.9...9.7.....Wc(.</..SzN>....x.2...~.. .....y.....e./.@".....m.u.v-?HF.....R.....1Y T6=.....v.=b..x9..(X }TV.J.'...z...\.L*wv.\.6..."...].u.L.b.*....Xg....3..E;..x*.*.....@f.....p...,.....9<.u*..!...~.9.....u....1d(y..k.[.....l...B. ..g.;8.A3....F;fu.....@d...5//.z.F.i.UWGz$...$bZ2.....Wn....d8.|.....5..&v..0.....e.a.}...O.I'l..A>.N.Q3...\...v!a...t.Ol.....R.....G..G....Se.!.^...4V.....~..-.3.

Chrome Cache Entry: 263	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image, VP8 encoding, 166x296, Scaling: [none]x[none], YUV color, decoders should clamp
Category:	downloaded
Size (bytes):	7314
Entropy (8bit):	7.971125199825403
Encrypted:	false
SSDEEP:	192:j2IcbcwWAa7V7ttCWoihjxd8GBpl2TpXHdzhCRnEX:eYws5Jhj38GB/UH9hCRnEX
MD5:	BE6BA74B67B4A8A63852DBC95B9609AE
SHA1:	437F21C611E76DA9EF4474974A38DD61E3A47C7E
SHA-256:	2FBDD2051B22EAAF7E4C7C27B01FFD0450EB5634FEB6E935BA8FCE2D69492475
SHA-512:	DC5D350272A3AA82037DF59139DEDEB70A6323F71AE3EDFC50679DA52620159237FA63A001991D60DC6B45D032A2CA64DC44C20F5A67496E38642AD360F3CA59
Malicious:	false
Reputation:	low
URL:	http://https://play-lh.googleusercontent.com/JLTSXDb4jBkaSMI_NsNPfUR9Ysw6WJy6nVJ5Iuh9lLuJiXogo4zwZckJoL7gywuxZ9o=w526-h296-rw
Preview:	RIFF....WEBPVP8 ~....s...*..(.>I .D..!.zF.(........G.?._..=8...~D.........R...j..~.~...z&.....G.....g.o...._.^....?.....?.=.5..z.../...O{.c.".7.-....._.....g.....k.../..m.....|.M.....}....%...{..... _.....~.....p?.....f.....o.>....k....._`..?.....s.../.....}...{.....S../I..W..l<E..f3.dUE5.cR.b0.u_..C?..j.....0.z..+.E4CE.C.....c..8.....6....8..i..1.qW.p.il.r.....i.N.....r.. c....c..cbGL3 ..=-6}L.A..V..X%.....,.-..@J..2....Be.aAg...ey._.QoH.;-#/.K...J.w...v?U~...@]'..'[..:\iS..A...B~L.c*...z.....X .3..G.j.<.a..a;QT.....I....v.>.z.c..I....}R...)h..B.=:.b.e..K.....q.JH..1k.(S ..+.....9.....?._.S=.....v.....n'.K.....~7.d..LA.\../I.\Y....4..Kp.|...M%v#..;/.#y-.+.N..P..$>.:\|....1..w..;..$LPM..e....-..B3.....`.FX./.WL.).|gM.B%.....J...$..b....+.r....g.Z^.ht...jsc.....(; C.....s...:.~...Xe.....?....h..w.o{/...5.Y5.fM.y....Uy&.....h.....m.....H...m+5Y ..T{*...I.$7:..(..1.....u..u.....J..Pj3<.....u..\".Lqt...+

Chrome Cache Entry: 264	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	742
Entropy (8bit):	7.704077267990546
Encrypted:	false
SSDEEP:	12:OBqoM5t7CCHRaOpmKiFKW95DotIst+ZcNDZGOU7a5FBsGgDfc0sCXs6u0EGQM8xh:O/M5tjW3otIDeNVlFBxAfc0sC8ljM8xh
MD5:	3AC1FF2C773AE2B5FD6E1581F8BD5D6C
SHA1:	2A76A9A0DFCDB6B9C298AEED1D2BCCA501F3A305

SHA-256:	7F54C2FC512AA005BFE5F434170066DD1BFEA2F1E5022BDDF00638B12247F6D4
SHA-512:	433D94CB3AFCA71683234E237A1D8E839E55067BB7EA93123148B1A2F18F621E9FB156CFA1FAFA7F854050752528E7199D67F1F9164CA6061CB423B3A7910C42
Malicious:	false
Reputation:	low
Preview:	RIFF....WEBPVP8L..../?.....$G...r.....<..A.q.?.CX .m$I...p.....M.P...}sQ.....P...(..C...C(`..!....2-...(..#..!.E..@.#....Z.#..GL....i<..h.#.....!.q!..IG.8..%.....#.8,...#._`.`..,!....N..[....%.^8....BY.JK.....Q.X.....ww.Swww.R.....w.2.....+p.F.1...f.H...p...$R*..D...RR^VV^4..QY.7.RN....".."..!.T....?...n.q.<`1..{.+B....).Y..-.<-.....)..n.H.....pc.....$.JuL.@....._.,.....G5G.&...u+.....'..k...Wc.wS.efN.v...;n.....ut=.{,'...k{...uQ..].6b.7.M..&.M0FofcW.L...{...6...~A.h..a...m...[....+O...=.f..0..G....,c.;..SZ.....@..+.....Vo.&..dg.....U'."e...[77.O...A.I.././.....NY)."."*T.d.. k=\D!).v..}.q..^....I.2...B.|m../B...o.sBIi.P...:...$I....y.2U.....'...o..L.....I..

Chrome Cache Entry: 265

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	dropped
Size (bytes):	1610
Entropy (8bit):	7.861288969735864
Encrypted:	false
SSDEEP:	24:zlw7vjT1GVznWVASYnsaIU9L8oqsgpCDN9FaoDhgLEMo0j2X87302misLc0:zlw7KTWVAnLlKKgDN9FaoNjMqzXFP
MD5:	E002EB245CEDE04193B2DB5C914BD4A0
SHA1:	035FCF0CD9228A0643839CC11FD67F9B659CDE9E
SHA-256:	E76553027E1D9153BA1A4C244C88B2772BA62134EED47FCBA1FC796B71AA0261
SHA-512:	3D154D90B80690A74CF05155A8DACC958A3112B3A4ACC05EA4840CE1490889107D185D0BAA6683B3AE9DCB8F7AAA835BA0EB680C137F230FC93645A0BCEDAE36
Malicious:	false
Reputation:	low
Preview:	RIFFB...WEBPVP8L5.../?.....m.IRf.M.?.=...O....a\.@...../..P..c.....m.0e.i...0l..q.....'.....B3.H.....H..>.=.c[[$9.Y5..3K....x*.133.03CWe...3....;.[..;"..|....2.....$I6mU.s.....$Z.....m.Fv.m.nd.F..:.m.}..#..$.....t.....Ng.37....A3.....H.....z.....U....qP....3..f...+@.u....H..3.Y...},.p..5..y.4.Y.JLg.0..$.1...%.3..0..+...v.-N..)OG.].v&..C...)7....=...i"....V.t..v..V~...%M4yb.....B.{...)....J...F.....V....7..h..Z&....R.....{j.3t7!?bP.4L5.T....U.|m....R..<.....bn.0.zG.b..k,+...'.H..S.^..g.e.8..^x..8.-y.#.!s2?...\.Gc9R.....|.S.....5..;....dL.Cc.y..+..O$^..w.w....4..a."{9>.q.[.............qz.9.Y..@.._.u....R...~.7..#...F'.....u#....XB..H..e..*w....%.....r.>... z_...(....r...).=V.....\.Z.C...o./nC.c'C..k&..t.....2.&|..._...i.....d....<1C...G ..[m.o.Y ..d..NZ.s-e0....9.I..x.^=..m...~.H.5.."..B.U.k.....$.%[[..+.C[\.....>g..$..K.#8.sW.>-..t D.8..x.,R..!.....w....|.....(.....Sp]....{ie.(}...z$..^@6..

Chrome Cache Entry: 266

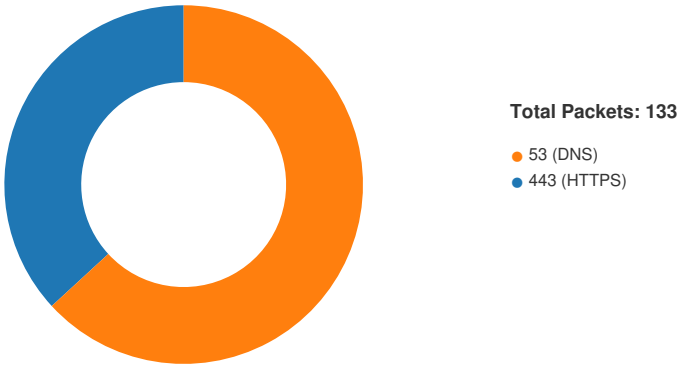
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (5770)
Category:	downloaded
Size (bytes):	786195
Entropy (8bit):	5.618151986379679
Encrypted:	false
SSDEEP:	12288:lKk8lCBGe2dChzP2tAnpJpIShwPdQUAbmsSb1UNoSF1bAiGos3tyFzCXsJUoUYz1:Ek8CBGe2dChzP2tmpJpIShwPdQUAbmsV
MD5:	5A685C122E699AE05F6F72574B909C5F
SHA1:	2FF881F91D7463F46E2070E58E19C87B93526512
SHA-256:	A74027A261B14B6B0C742D2215AD3CB27F835E6FCD8C52F71DC35F60DACA23E1
SHA-512:	7696E6CF421EF7E49BBF96D3C9ADE2E892CCF588F2C1A232EDB68FDCBDEBCC83BB4BC10F83A053EB4C4FC88867FF9F4A5504AF9F6BA3E8DB71245B9FF3583638
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/boq-play/_/js/k=boq-play.PlayStoreUi.en_US.Q_BxHty5I84.2021.O/ck=boq-play.PlayStoreUi.yLOfNYXhHv8.L.B1.O/am=022DoYEFBv4jfQ-2/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,appshomeview/ed=1/wt=2/ujg=1/rs=AB1caFWkNIDOp0fBemB9CcPjGshi9lHtFg/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;Hs0fpd:jLUKge;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;Rdd4dc:WXw8B;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;nAu0tf:z5Gxfe;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;sgjhQc:bQAegc;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:BBI74;yEQyxe:TLjaTd;yxTchf:KUM7Z;zxnPse:GkRiKb/m=ws9Tlc,n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,WO9ee,mI3LFb,m9oV,z5Gxfe,ArluEf,lcVnM,wW2D8b,vrGZEc,fPcQoe,LCkxpb,kr6Nlf,O6y8ed,PrPYRd,MpJwZc,NwH0H,OmgaI,lazG7b,XVMNvd,L1AAkb,KUM7Z,Mlhmy,pYCIec,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,UImmrd,ZfAoz,mdR7q,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QIhFr,ovKuLd,hKSk3e,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,BBI74,VwDzFe,MdUzUe,A7fCU,zbML3c,zr1jrb,Uas9Hd,pjICDe"
Preview:	"use strict";_F_installCss(".EDId0c{position:relative}.nhh4Ic{position:absolute;left:0;right:0;top:0;z-index:1;pointer-events:none}.nhh4Ic[data-state=snapping],.nhh4Ic[data-state=cancelled]{transition:transform 200ms}.MGUFnf{display:block;width:28px;height:28px;padding:15px;margin:0 auto;transform:scale(0.7);background-color:#fafa;border:1px solid #e0e0e0;border-radius:50%;box-shadow:0 2px 2px 0 rgba(0,0,0,.2);transition:opacity 400ms}.nhh4Ic[data-state=resting] .MGUFnf,.nhh4Ic[data-state=cooldown] .MGUFnf{transform:scale(0);transition:transform 150ms}.nhh4Ic .LLCa0e{stroke-width:3.6px;transform:translateZ(1px)}.nhh4Ic[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

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:11:52.077917099 CET	49675	443	192.168.2.4	173.222.162.32
Mar 8, 2024 09:12:01.782766104 CET	49675	443	192.168.2.4	173.222.162.32
Mar 8, 2024 09:12:04.408004045 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.408055067 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.408123016 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.408442974 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.408457994 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.736741066 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.737176895 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.737205029 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.738733053 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.738817930 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.740255117 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.740329027 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.741003990 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:04.741010904 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:04.787267923 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399188995 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399260998 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399302006 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399337053 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399354935 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399396896 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399404049 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399486065 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399537086 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399549007 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399561882 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399621010 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399626017 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399730921 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.399774075 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.399780035 CET	443	49736	172.67.210.214	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:05.400526047 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.400573015 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.400579929 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.401182890 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.401230097 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.401236057 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.401299000 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.401338100 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.401345015 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.402033091 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.402085066 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.402091026 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.402237892 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.402308941 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.464854956 CET	49736	443	192.168.2.4	172.67.210.214
Mar 8, 2024 09:12:05.464886904 CET	443	49736	172.67.210.214	192.168.2.4
Mar 8, 2024 09:12:05.775003910 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:05.775080919 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:05.775167942 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:05.776503086 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:05.776537895 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:05.928159952 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:05.928196907 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:05.928266048 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:05.929121971 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:05.929140091 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.146512985 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:06.146903992 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:06.146965981 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:06.148458004 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:06.148536921 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:06.262893915 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.263556004 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.263585091 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.265089989 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.265152931 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.313271046 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.331804037 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:06.332079887 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:06.333187103 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.333260059 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.333368063 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.374865055 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.374891996 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.374933004 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:06.374990940 CET	443	49737	142.251.2.99	192.168.2.4
Mar 8, 2024 09:12:06.420697927 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.420819044 CET	49737	443	192.168.2.4	142.251.2.99
Mar 8, 2024 09:12:06.602186918 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:06.602210999 CET	443	49739	23.202.57.177	192.168.2.4
Mar 8, 2024 09:12:06.602330923 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:06.606462002 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:06.606471062 CET	443	49739	23.202.57.177	192.168.2.4
Mar 8, 2024 09:12:06.926927090 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.927207947 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.927346945 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.927964926 CET	49738	443	192.168.2.4	104.21.39.40
Mar 8, 2024 09:12:06.927984953 CET	443	49738	104.21.39.40	192.168.2.4
Mar 8, 2024 09:12:06.954680920 CET	443	49739	23.202.57.177	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:06.954881907 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:06.980309963 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:06.980330944 CET	443	49739	23.202.57.177	192.168.2.4
Mar 8, 2024 09:12:06.981236935 CET	443	49739	23.202.57.177	192.168.2.4
Mar 8, 2024 09:12:07.030402899 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:07.081847906 CET	49739	443	192.168.2.4	23.202.57.177
Mar 8, 2024 09:12:07.128238916 CET	443	49739	23.202.57.177	192.168.2.4
Mar 8, 2024 09:12:07.138323069 CET	49740	443	192.168.2.4	45.133.44.52

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:01.816157103 CET	53	57707	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:01.931332111 CET	53	58577	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:03.750606060 CET	61833	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:03.751085997 CET	65198	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:03.932265997 CET	53	50449	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:04.247452021 CET	53	61833	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:04.247869968 CET	53	65198	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:04.251435995 CET	60549	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:04.251576900 CET	49301	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:04.406781912 CET	53	60549	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:04.407143116 CET	53	49301	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:05.474977016 CET	49607	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:05.476145983 CET	52636	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:05.616224051 CET	51237	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:05.616722107 CET	62717	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:05.771434069 CET	53	51237	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:05.771500111 CET	53	62717	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:05.926214933 CET	53	49607	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:05.926326990 CET	53	52636	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:06.981843948 CET	62939	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:06.982451916 CET	58660	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:07.137588024 CET	53	62939	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:07.137634039 CET	53	58660	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:08.153665066 CET	55500	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:08.153930902 CET	57409	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:08.309452057 CET	53	55500	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:08.309499979 CET	53	57409	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.291646957 CET	64841	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.292347908 CET	59895	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.292592049 CET	49253	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.294979095 CET	50941	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.352161884 CET	50504	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.352672100 CET	61838	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.354243040 CET	56255	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.354629040 CET	55500	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.369925022 CET	54366	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.370467901 CET	63985	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:09.447449923 CET	53	49253	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.447540045 CET	53	59895	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.448215961 CET	53	64841	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.450058937 CET	53	50941	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.507214069 CET	53	50504	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.507333040 CET	53	61838	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.509114027 CET	53	55500	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.509193897 CET	53	56255	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.524912119 CET	53	54366	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:09.525443077 CET	53	63985	1.1.1.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:10.618345022 CET	52092	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:10.618957996 CET	54069	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:10.650882006 CET	63763	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:10.651665926 CET	56440	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:10.705724955 CET	53	52470	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:10.773355961 CET	53	52092	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:10.806869984 CET	53	56440	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:10.824035883 CET	53	63763	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:10.978207111 CET	53	54069	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.294271946 CET	62230	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.294491053 CET	65489	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.449306011 CET	53	62230	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.450572968 CET	53	65489	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.540030003 CET	50327	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.540450096 CET	57652	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.648438931 CET	61330	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.648948908 CET	53753	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:12.695254087 CET	53	50327	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.695420027 CET	53	57652	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.868590117 CET	53	53753	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:12.869323969 CET	53	61330	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:13.402642965 CET	56721	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:13.411117077 CET	62830	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:13.557892084 CET	53	56721	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:13.566356897 CET	53	62830	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.404321909 CET	53148	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.410892010 CET	57458	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.417076111 CET	58193	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.417740107 CET	57157	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.418551922 CET	56882	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.418823957 CET	58989	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:15.559638023 CET	53	53148	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.566610098 CET	53	57458	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.641114950 CET	53	58193	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.641294003 CET	53	57157	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.643142939 CET	53	56882	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:15.643224001 CET	53	58989	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:16.758594036 CET	64061	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:16.758991957 CET	62132	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:16.832560062 CET	59517	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:16.833002090 CET	49344	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:16.913563013 CET	53	62132	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:16.987978935 CET	53	59517	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:16.988333941 CET	53	49344	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:17.051561117 CET	53	64061	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:17.143495083 CET	50902	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:17.144490957 CET	64269	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:17.299006939 CET	53	50902	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:17.299181938 CET	53	64269	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:19.035655022 CET	60416	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:19.038242102 CET	56089	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:19.191184044 CET	53	60416	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:19.193603039 CET	53	56089	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:19.997683048 CET	138	138	192.168.2.4	192.168.2.255
Mar 8, 2024 09:12:20.452008963 CET	56547	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:20.452677965 CET	63312	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:20.607666969 CET	53	56547	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:20.608216047 CET	53	63312	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:22.284010887 CET	53	61010	1.1.1.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:30.159965992 CET	55072	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:30.163701057 CET	55306	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:30.413796902 CET	53	55072	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:30.413815975 CET	53	55306	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:31.777200937 CET	65270	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:31.777384043 CET	54879	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:31.932189941 CET	53	54879	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:31.932261944 CET	53	65270	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:33.756242990 CET	56392	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:33.756602049 CET	57011	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:33.881679058 CET	53	59930	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:33.902201891 CET	53	53719	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:33.910976887 CET	53	56392	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:33.944654942 CET	53	57011	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:34.700253963 CET	60422	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:34.700593948 CET	50175	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:34.792063951 CET	53	54569	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:34.854743004 CET	53	60422	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:34.856384039 CET	53	50175	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:36.350462914 CET	53	56703	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:37.235322952 CET	53	61615	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:39.070031881 CET	53	60995	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:39.072134972 CET	53	65120	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:40.918587923 CET	62751	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:40.918966055 CET	50076	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:41.067455053 CET	53	64663	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.073646069 CET	53	62751	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.073728085 CET	53	50076	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.084203005 CET	53	51843	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.629056931 CET	53	64940	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.818464994 CET	49477	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:41.818464994 CET	56370	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:41.973175049 CET	53	49477	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:41.973444939 CET	53	56370	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:42.594067097 CET	55634	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:42.596007109 CET	56290	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:42.749085903 CET	53	55634	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:42.750535011 CET	53	56290	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:43.087387085 CET	61745	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:43.088254929 CET	55822	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:43.242106915 CET	53	61745	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:43.243180990 CET	53	55822	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:46.634991884 CET	53	53073	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:53.075536966 CET	57191	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:53.076508999 CET	64741	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:53.082935095 CET	53516	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:53.083529949 CET	49823	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:53.231154919 CET	53	57191	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:53.231643915 CET	53	64741	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:53.238109112 CET	53	53516	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:53.238243103 CET	53	49823	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:55.960808992 CET	64160	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:55.960846901 CET	52289	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:56.115976095 CET	53	64160	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:56.116712093 CET	53	52289	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:56.330061913 CET	57931	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:56.330249071 CET	63355	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:56.590627909 CET	53	57931	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:56.590656042 CET	53	63355	1.1.1.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2024 09:12:56.923827887 CET	59191	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:56.924098015 CET	59520	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:12:57.078161001 CET	53	59191	1.1.1.1	192.168.2.4
Mar 8, 2024 09:12:57.078700066 CET	53	59520	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:01.313594103 CET	53	54805	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:04.080365896 CET	53	51043	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:17.719887018 CET	57594	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:17.722456932 CET	64776	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:17.722853899 CET	65226	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:17.723079920 CET	64584	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:17.877674103 CET	53	64776	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:17.877888918 CET	53	65226	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:17.878180027 CET	53	64584	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:18.031425953 CET	53	57594	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:30.560456991 CET	53	51727	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:33.438971996 CET	61900	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:33.439390898 CET	52816	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:33.594059944 CET	53	52816	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:33.594104052 CET	53	61900	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:52.942486048 CET	55394	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:52.942972898 CET	50962	53	192.168.2.4	1.1.1.1
Mar 8, 2024 09:13:53.098212004 CET	53	55394	1.1.1.1	192.168.2.4
Mar 8, 2024 09:13:53.098659039 CET	53	50962	1.1.1.1	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 8, 2024 09:12:10.978310108 CET	192.168.2.4	1.1.1.1	c249	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:03.750606060 CET	192.168.2.4	1.1.1.1	0x55d2	Standard query (0)	gossnabgroup.ru	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:03.751085997 CET	192.168.2.4	1.1.1.1	0x7e47	Standard query (0)	gossnabgroup.ru	65	IN (0x0001)	false
Mar 8, 2024 09:12:04.251435995 CET	192.168.2.4	1.1.1.1	0xc67b	Standard query (0)	gossnabgroup.ru	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:04.251576900 CET	192.168.2.4	1.1.1.1	0x8bda	Standard query (0)	gossnabgroup.ru	65	IN (0x0001)	false
Mar 8, 2024 09:12:05.474977016 CET	192.168.2.4	1.1.1.1	0x5ccc	Standard query (0)	js.nextpsh.top	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.476145983 CET	192.168.2.4	1.1.1.1	0x7fdb	Standard query (0)	js.nextpsh.top	65	IN (0x0001)	false
Mar 8, 2024 09:12:05.616224051 CET	192.168.2.4	1.1.1.1	0x74f9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.616722107 CET	192.168.2.4	1.1.1.1	0x23fa	Standard query (0)	www.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:06.981843948 CET	192.168.2.4	1.1.1.1	0x8d1f	Standard query (0)	bddb2d2561.62b81f5af3.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:06.982451916 CET	192.168.2.4	1.1.1.1	0xf2b	Standard query (0)	bddb2d2561.62b81f5af3.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:08.153665066 CET	192.168.2.4	1.1.1.1	0x712f	Standard query (0)	js.capndr.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:08.153930902 CET	192.168.2.4	1.1.1.1	0x14a4	Standard query (0)	js.capndr.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:09.291646957 CET	192.168.2.4	1.1.1.1	0xedfe	Standard query (0)	storage.multstorage.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.292347908 CET	192.168.2.4	1.1.1.1	0xf3cb	Standard query (0)	storage.multstorage.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:09.292592049 CET	192.168.2.4	1.1.1.1	0x306d	Standard query (0)	fp.metrics wpsh.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.294979095 CET	192.168.2.4	1.1.1.1	0x3318	Standard query (0)	fp.metrics wpsh.com	65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:09.352161884 CET	192.168.2.4	1.1.1.1	0x4b48	Standard query (0)	e1f6a352a1.3ea94c3718.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.352672100 CET	192.168.2.4	1.1.1.1	0x1f4c	Standard query (0)	e1f6a352a1.3ea94c3718.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:09.354243040 CET	192.168.2.4	1.1.1.1	0x3dca	Standard query (0)	js.wpshsdk.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.354629040 CET	192.168.2.4	1.1.1.1	0xa907	Standard query (0)	js.wpshsdk.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:09.369925022 CET	192.168.2.4	1.1.1.1	0x4443	Standard query (0)	bddb2d2561.62b81f5af3.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.370467901 CET	192.168.2.4	1.1.1.1	0xbfa6	Standard query (0)	bddb2d2561.62b81f5af3.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:10.618345022 CET	192.168.2.4	1.1.1.1	0x2a91	Standard query (0)	e32350d110.84bfe218ba.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.618957996 CET	192.168.2.4	1.1.1.1	0x5154	Standard query (0)	e32350d110.84bfe218ba.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:10.650882006 CET	192.168.2.4	1.1.1.1	0xa407	Standard query (0)	nereserv.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.651665926 CET	192.168.2.4	1.1.1.1	0x660	Standard query (0)	nereserv.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:12.294271946 CET	192.168.2.4	1.1.1.1	0x6c08	Standard query (0)	e1f6a352a1.3ea94c3718.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.294491053 CET	192.168.2.4	1.1.1.1	0x7db4	Standard query (0)	e1f6a352a1.3ea94c3718.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:12.540030003 CET	192.168.2.4	1.1.1.1	0xffe3	Standard query (0)	nereserv.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.540450096 CET	192.168.2.4	1.1.1.1	0x8763	Standard query (0)	nereserv.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:12.648438931 CET	192.168.2.4	1.1.1.1	0xf44e	Standard query (0)	sw.wpushorg.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.648948908 CET	192.168.2.4	1.1.1.1	0x6eb0	Standard query (0)	sw.wpushorg.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:13.402642965 CET	192.168.2.4	1.1.1.1	0x453b	Standard query (0)	fp.metricswpsh.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:13.411117077 CET	192.168.2.4	1.1.1.1	0x45d1	Standard query (0)	fp.metricswpsh.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:15.404321909 CET	192.168.2.4	1.1.1.1	0x2cd	Standard query (0)	static.bookmsg.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.410892010 CET	192.168.2.4	1.1.1.1	0xb13a	Standard query (0)	static.bookmsg.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:15.417076111 CET	192.168.2.4	1.1.1.1	0xe5be	Standard query (0)	us.superfasti.co	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.417740107 CET	192.168.2.4	1.1.1.1	0x93a5	Standard query (0)	us.superfasti.co	65	IN (0x0001)	false
Mar 8, 2024 09:12:15.418551922 CET	192.168.2.4	1.1.1.1	0xf1f1	Standard query (0)	cdn.stgcdn.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.418823957 CET	192.168.2.4	1.1.1.1	0x7dda	Standard query (0)	cdn.stgcdn.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:16.758594036 CET	192.168.2.4	1.1.1.1	0x22d8	Standard query (0)	e32350d110.84bfe218ba.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:16.758991957 CET	192.168.2.4	1.1.1.1	0xc189	Standard query (0)	e32350d110.84bfe218ba.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:16.832560062 CET	192.168.2.4	1.1.1.1	0xc5f9	Standard query (0)	static.bookmsg.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:16.833002090 CET	192.168.2.4	1.1.1.1	0x359	Standard query (0)	static.bookmsg.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:17.143495083 CET	192.168.2.4	1.1.1.1	0x63fa	Standard query (0)	cdn.stgcdn.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.144490957 CET	192.168.2.4	1.1.1.1	0x2c03	Standard query (0)	cdn.stgcdn.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:19.035655022 CET	192.168.2.4	1.1.1.1	0xea74	Standard query (0)	notification.tubecup.net	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:19.038242102 CET	192.168.2.4	1.1.1.1	0x3866	Standard query (0)	notification.tubecup.net	65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:20.452008963 CET	192.168.2.4	1.1.1.1	0xc0ff	Standard query (0)	notificati on.tubecup.net	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.452677965 CET	192.168.2.4	1.1.1.1	0xe55c	Standard query (0)	notificati on.tubecup.net	65	IN (0x0001)	false
Mar 8, 2024 09:12:30.159965992 CET	192.168.2.4	1.1.1.1	0x21a2	Standard query (0)	winrenew-c ash.life	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:30.163701057 CET	192.168.2.4	1.1.1.1	0x8225	Standard query (0)	winrenew-c ash.life	65	IN (0x0001)	false
Mar 8, 2024 09:12:31.777200937 CET	192.168.2.4	1.1.1.1	0x77d	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.777384043 CET	192.168.2.4	1.1.1.1	0xe8c3	Standard query (0)	play.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:33.756242990 CET	192.168.2.4	1.1.1.1	0xe892	Standard query (0)	play-lh.go ogleuserco ntent.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:33.756602049 CET	192.168.2.4	1.1.1.1	0x857b	Standard query (0)	play-lh.go ogleuserco ntent.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:34.700253963 CET	192.168.2.4	1.1.1.1	0xac75	Standard query (0)	play-lh.go ogleuserco ntent.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:34.700593948 CET	192.168.2.4	1.1.1.1	0x4e86	Standard query (0)	play-lh.go ogleuserco ntent.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:40.918587923 CET	192.168.2.4	1.1.1.1	0xe2e6	Standard query (0)	stats.g.do ubleclick.net	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:40.918966055 CET	192.168.2.4	1.1.1.1	0x46fa	Standard query (0)	stats.g.do ubleclick.net	65	IN (0x0001)	false
Mar 8, 2024 09:12:41.818464994 CET	192.168.2.4	1.1.1.1	0xe771	Standard query (0)	stats.g.do ubleclick.net	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.818464994 CET	192.168.2.4	1.1.1.1	0xcb36	Standard query (0)	stats.g.do ubleclick.net	65	IN (0x0001)	false
Mar 8, 2024 09:12:42.594067097 CET	192.168.2.4	1.1.1.1	0x58b7	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.596007109 CET	192.168.2.4	1.1.1.1	0x5025	Standard query (0)	www.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:43.087387085 CET	192.168.2.4	1.1.1.1	0xe92	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.088254929 CET	192.168.2.4	1.1.1.1	0xec3e	Standard query (0)	play.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:53.075536966 CET	192.168.2.4	1.1.1.1	0x4007	Standard query (0)	payments.g oogle.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.076508999 CET	192.168.2.4	1.1.1.1	0x3e56	Standard query (0)	payments.g oogle.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:53.082935095 CET	192.168.2.4	1.1.1.1	0xf8d6	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.083529949 CET	192.168.2.4	1.1.1.1	0x4efa	Standard query (0)	apis.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:55.960808992 CET	192.168.2.4	1.1.1.1	0xec1b	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:55.960846901 CET	192.168.2.4	1.1.1.1	0x9f91	Standard query (0)	i.ytimg.com	65	IN (0x0001)	false
Mar 8, 2024 09:12:56.330061913 CET	192.168.2.4	1.1.1.1	0x11ef	Standard query (0)	subscriber s.producti on.wpu.sh	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:56.330249071 CET	192.168.2.4	1.1.1.1	0xce46	Standard query (0)	subscriber s.producti on.wpu.sh	65	IN (0x0001)	false
Mar 8, 2024 09:12:56.923827887 CET	192.168.2.4	1.1.1.1	0x9331	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:56.924098015 CET	192.168.2.4	1.1.1.1	0x56a9	Standard query (0)	i.ytimg.com	65	IN (0x0001)	false
Mar 8, 2024 09:13:17.719887018 CET	192.168.2.4	1.1.1.1	0x20dc	Standard query (0)	img.cdn.house	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:17.722456932 CET	192.168.2.4	1.1.1.1	0xbcd2	Standard query (0)	img.cdn.house	65	IN (0x0001)	false
Mar 8, 2024 09:13:17.722853899 CET	192.168.2.4	1.1.1.1	0x773f	Standard query (0)	js.wpadmng r.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:17.723079920 CET	192.168.2.4	1.1.1.1	0xb1ef	Standard query (0)	js.wpadmng r.com	65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 8, 2024 09:13:33.438971996 CET	192.168.2.4	1.1.1.1	0x395e	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.439390898 CET	192.168.2.4	1.1.1.1	0xf74a	Standard query (0)	play.google.com	65	IN (0x0001)	false
Mar 8, 2024 09:13:52.942486048 CET	192.168.2.4	1.1.1.1	0x8f39	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:52.942972898 CET	192.168.2.4	1.1.1.1	0x5e02	Standard query (0)	play.google.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:04.247452021 CET	1.1.1.1	192.168.2.4	0x55d2	No error (0)	gossnabgroup.ru		172.67.210.214	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:04.247452021 CET	1.1.1.1	192.168.2.4	0x55d2	No error (0)	gossnabgroup.ru		104.21.23.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:04.247869968 CET	1.1.1.1	192.168.2.4	0x7e47	No error (0)	gossnabgroup.ru			65	IN (0x0001)	false
Mar 8, 2024 09:12:04.406781912 CET	1.1.1.1	192.168.2.4	0xc67b	No error (0)	gossnabgroup.ru		172.67.210.214	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:04.406781912 CET	1.1.1.1	192.168.2.4	0xc67b	No error (0)	gossnabgroup.ru		104.21.23.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:04.407143116 CET	1.1.1.1	192.168.2.4	0x8bda	No error (0)	gossnabgroup.ru			65	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.99	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.147	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.105	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.103	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.104	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771434069 CET	1.1.1.1	192.168.2.4	0x74f9	No error (0)	www.google.com		142.251.2.106	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.771500111 CET	1.1.1.1	192.168.2.4	0x23fa	No error (0)	www.google.com			65	IN (0x0001)	false
Mar 8, 2024 09:12:05.926214933 CET	1.1.1.1	192.168.2.4	0x5ccc	No error (0)	js.nextpsh.top		104.21.39.40	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.926214933 CET	1.1.1.1	192.168.2.4	0x5ccc	No error (0)	js.nextpsh.top		172.67.142.186	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:05.926326990 CET	1.1.1.1	192.168.2.4	0x7fdb	No error (0)	js.nextpsh.top			65	IN (0x0001)	false
Mar 8, 2024 09:12:07.137588024 CET	1.1.1.1	192.168.2.4	0x8d1f	No error (0)	bddb2d2561.62b81f5af3.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:07.137588024 CET	1.1.1.1	192.168.2.4	0x8d1f	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:07.137588024 CET	1.1.1.1	192.168.2.4	0x8d1f	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:07.137634039 CET	1.1.1.1	192.168.2.4	0xf2b	No error (0)	bddb2d2561.62b81f5af3.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:08.309452057 CET	1.1.1.1	192.168.2.4	0x712f	No error (0)	js.capndr.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:08.309452057 CET	1.1.1.1	192.168.2.4	0x712f	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:08.309452057 CET	1.1.1.1	192.168.2.4	0x712f	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:08.309499979 CET	1.1.1.1	192.168.2.4	0x14a4	No error (0)	js.capndr.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.447449923 CET	1.1.1.1	192.168.2.4	0x306d	No error (0)	fp.metricswpsh.com		157.90.84.242	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.447540045 CET	1.1.1.1	192.168.2.4	0xf3cb	No error (0)	storage.multstorage.com			65	IN (0x0001)	false
Mar 8, 2024 09:12:09.448215961 CET	1.1.1.1	192.168.2.4	0xedfe	No error (0)	storage.multstorage.com		104.21.30.242	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.448215961 CET	1.1.1.1	192.168.2.4	0xedfe	No error (0)	storage.multstorage.com		172.67.174.51	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.507214069 CET	1.1.1.1	192.168.2.4	0x4b48	No error (0)	e1f6a352a1.3ea94c3718.com	cdn44221613.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.507214069 CET	1.1.1.1	192.168.2.4	0x4b48	No error (0)	cdn44221613.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.507214069 CET	1.1.1.1	192.168.2.4	0x4b48	No error (0)	cdn44221613.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.507333040 CET	1.1.1.1	192.168.2.4	0x1f4c	No error (0)	e1f6a352a1.3ea94c3718.com	cdn44221613.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.509114027 CET	1.1.1.1	192.168.2.4	0xa907	No error (0)	js.wpshsdk.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.509193897 CET	1.1.1.1	192.168.2.4	0x3dca	No error (0)	js.wpshsdk.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.509193897 CET	1.1.1.1	192.168.2.4	0x3dca	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.509193897 CET	1.1.1.1	192.168.2.4	0x3dca	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.524912119 CET	1.1.1.1	192.168.2.4	0x4443	No error (0)	bddb2d2561.62b81f5af3.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:09.524912119 CET	1.1.1.1	192.168.2.4	0x4443	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.524912119 CET	1.1.1.1	192.168.2.4	0x4443	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:09.525443077 CET	1.1.1.1	192.168.2.4	0xbfa6	No error (0)	bddb2d2561.62b81f5af3.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:10.773355961 CET	1.1.1.1	192.168.2.4	0x2a91	No error (0)	e32350d110.84bfe218ba.com	ntvpforever.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:10.773355961 CET	1.1.1.1	192.168.2.4	0x2a91	No error (0)	ntvpforever.com		94.130.198.6	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.773355961 CET	1.1.1.1	192.168.2.4	0x2a91	No error (0)	ntvpforever.com		157.90.84.246	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.773355961 CET	1.1.1.1	192.168.2.4	0x2a91	No error (0)	ntvpforever.com		168.119.25.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.773355961 CET	1.1.1.1	192.168.2.4	0x2a91	No error (0)	ntvpforever.com		167.235.163.216	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:10.824035883 CET	1.1.1.1	192.168.2.4	0xa407	No error (0)	nereserv.com		94.130.198.6	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.824035883 CET	1.1.1.1	192.168.2.4	0xa407	No error (0)	nereserv.com		168.119.25.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.824035883 CET	1.1.1.1	192.168.2.4	0xa407	No error (0)	nereserv.com		157.90.84.246	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.824035883 CET	1.1.1.1	192.168.2.4	0xa407	No error (0)	nereserv.com		167.235.163.216	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:10.978207111 CET	1.1.1.1	192.168.2.4	0x5154	No error (0)	e32350d110.84bfe218ba.com	ntvpforever.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:12.449306011 CET	1.1.1.1	192.168.2.4	0x6c08	No error (0)	e1f6a352a1.3ea94c3718.com	cdn44221613.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:12.449306011 CET	1.1.1.1	192.168.2.4	0x6c08	No error (0)	cdn44221613.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.449306011 CET	1.1.1.1	192.168.2.4	0x6c08	No error (0)	cdn44221613.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.450572968 CET	1.1.1.1	192.168.2.4	0x7db4	No error (0)	e1f6a352a1.3ea94c3718.com	cdn44221613.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:12.695254087 CET	1.1.1.1	192.168.2.4	0xffe3	No error (0)	nereserv.com		167.235.163.216	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.695254087 CET	1.1.1.1	192.168.2.4	0xffe3	No error (0)	nereserv.com		157.90.84.246	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.695254087 CET	1.1.1.1	192.168.2.4	0xffe3	No error (0)	nereserv.com		168.119.25.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.695254087 CET	1.1.1.1	192.168.2.4	0xffe3	No error (0)	nereserv.com		94.130.198.6	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.868590117 CET	1.1.1.1	192.168.2.4	0x6eb0	No error (0)	sw.wpushorg.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:12.869323969 CET	1.1.1.1	192.168.2.4	0xf44e	No error (0)	sw.wpushorg.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:12.869323969 CET	1.1.1.1	192.168.2.4	0xf44e	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:12.869323969 CET	1.1.1.1	192.168.2.4	0xf44e	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:13.557892084 CET	1.1.1.1	192.168.2.4	0x453b	No error (0)	fp.metrics wpsh.com		157.90.84.242	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.559638023 CET	1.1.1.1	192.168.2.4	0x2cd	No error (0)	static.boo kmsg.com	cdn66489868.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:15.559638023 CET	1.1.1.1	192.168.2.4	0x2cd	No error (0)	cdn664898688.ahacdn.me		45.133.44.25	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.559638023 CET	1.1.1.1	192.168.2.4	0x2cd	No error (0)	cdn664898688.ahacdn.me		45.133.44.24	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.566610098 CET	1.1.1.1	192.168.2.4	0xb13a	No error (0)	static.boo kmsg.com	cdn66489868.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:15.641114950 CET	1.1.1.1	192.168.2.4	0xe5be	No error (0)	us.superfasti.co		109.200.209.143	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.641114950 CET	1.1.1.1	192.168.2.4	0xe5be	No error (0)	us.superfasti.co		31.204.132.207	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.641114950 CET	1.1.1.1	192.168.2.4	0xe5be	No error (0)	us.superfasti.co		109.200.209.144	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:15.641114950 CET	1.1.1.1	192.168.2.4	0xe5be	No error (0)	us.superfasti.co		31.204.132.208	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.643142939 CET	1.1.1.1	192.168.2.4	0xf1f1	No error (0)	cdn.stgcdn.com	cdn.adx1.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:15.643142939 CET	1.1.1.1	192.168.2.4	0xf1f1	No error (0)	cdn.adx1.com		31.204.132.207	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:15.643224001 CET	1.1.1.1	192.168.2.4	0x7dda	No error (0)	cdn.stgcdn.com	cdn.adx1.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:16.913563013 CET	1.1.1.1	192.168.2.4	0xc189	No error (0)	e32350d110.84bfe218ba.com	ntvpforever.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:16.987978935 CET	1.1.1.1	192.168.2.4	0xc5f9	No error (0)	static.bookmsg.com	cdn66489868.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:16.987978935 CET	1.1.1.1	192.168.2.4	0xc5f9	No error (0)	cdn66489868.ahacdn.me		45.133.44.24	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:16.987978935 CET	1.1.1.1	192.168.2.4	0xc5f9	No error (0)	cdn66489868.ahacdn.me		45.133.44.25	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:16.988333941 CET	1.1.1.1	192.168.2.4	0x359	No error (0)	static.bookmsg.com	cdn66489868.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:17.051561117 CET	1.1.1.1	192.168.2.4	0x22d8	No error (0)	e32350d110.84bfe218ba.com	ntvpforever.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:17.051561117 CET	1.1.1.1	192.168.2.4	0x22d8	No error (0)	ntvpforever.com		94.130.198.6	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.051561117 CET	1.1.1.1	192.168.2.4	0x22d8	No error (0)	ntvpforever.com		168.119.25.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.051561117 CET	1.1.1.1	192.168.2.4	0x22d8	No error (0)	ntvpforever.com		167.235.163.216	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.051561117 CET	1.1.1.1	192.168.2.4	0x22d8	No error (0)	ntvpforever.com		157.90.84.246	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.299006939 CET	1.1.1.1	192.168.2.4	0x63fa	No error (0)	cdn.stgcdn.com	cdn.adx1.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:17.299006939 CET	1.1.1.1	192.168.2.4	0x63fa	No error (0)	cdn.adx1.com		31.204.132.207	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:17.299181938 CET	1.1.1.1	192.168.2.4	0x2c03	No error (0)	cdn.stgcdn.com	cdn.adx1.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:19.191184044 CET	1.1.1.1	192.168.2.4	0xea74	No error (0)	notification.tubecup.net		88.198.204.166	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:19.191184044 CET	1.1.1.1	192.168.2.4	0xea74	No error (0)	notification.tubecup.net		94.130.197.136	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:19.191184044 CET	1.1.1.1	192.168.2.4	0xea74	No error (0)	notification.tubecup.net		94.130.197.140	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:19.191184044 CET	1.1.1.1	192.168.2.4	0xea74	No error (0)	notification.tubecup.net		78.47.181.156	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:19.191184044 CET	1.1.1.1	192.168.2.4	0xea74	No error (0)	notification.tubecup.net		116.202.204.10	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.166819096 CET	1.1.1.1	192.168.2.4	0x37f1	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:20.166819096 CET	1.1.1.1	192.168.2.4	0x37f1	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.607666969 CET	1.1.1.1	192.168.2.4	0xc0ff	No error (0)	notification.tubecup.net		88.198.204.166	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:20.607666969 CET	1.1.1.1	192.168.2.4	0xc0ff	No error (0)	notification.tubecup.net		116.202.204.10	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.607666969 CET	1.1.1.1	192.168.2.4	0xc0ff	No error (0)	notification.tubecup.net		94.130.197.140	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.607666969 CET	1.1.1.1	192.168.2.4	0xc0ff	No error (0)	notification.tubecup.net		78.47.181.156	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:20.607666969 CET	1.1.1.1	192.168.2.4	0xc0ff	No error (0)	notification.tubecup.net		94.130.197.136	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.250.101.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.250.141.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.250.141.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.139	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.251.2.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		74.125.137.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:25.851249933 CET	1.1.1.1	192.168.2.4	0xd08	No error (0)	android.l.google.com		142.250.101.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:26.816361904 CET	1.1.1.1	192.168.2.4	0xe4e7	No error (0)	mobile-gtalk.l.google.com		142.251.2.188	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:30.413796902 CET	1.1.1.1	192.168.2.4	0x21a2	No error (0)	winrenew-cash.life		185.155.184.32	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.139	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:31.932261944 CET	1.1.1.1	192.168.2.4	0x77d	No error (0)	play.google.com		142.250.141.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:33.910976887 CET	1.1.1.1	192.168.2.4	0xe892	No error (0)	play-lh.googleusercontent.com		142.251.2.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:34.854743004 CET	1.1.1.1	192.168.2.4	0xac75	No error (0)	play-lh.googleusercontent.com		142.251.2.119	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:37.409640074 CET	1.1.1.1	192.168.2.4	0x62bc	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:37.409640074 CET	1.1.1.1	192.168.2.4	0x62bc	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.073646069 CET	1.1.1.1	192.168.2.4	0xe2e6	No error (0)	stats.g.doubleclick.net		142.250.141.155	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.073646069 CET	1.1.1.1	192.168.2.4	0xe2e6	No error (0)	stats.g.doubleclick.net		142.250.141.157	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.073646069 CET	1.1.1.1	192.168.2.4	0xe2e6	No error (0)	stats.g.doubleclick.net		142.250.141.154	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.073646069 CET	1.1.1.1	192.168.2.4	0xe2e6	No error (0)	stats.g.doubleclick.net		142.250.141.156	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.973175049 CET	1.1.1.1	192.168.2.4	0xe771	No error (0)	stats.g.doubleclick.net		142.250.141.155	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.973175049 CET	1.1.1.1	192.168.2.4	0xe771	No error (0)	stats.g.doubleclick.net		142.250.141.156	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.973175049 CET	1.1.1.1	192.168.2.4	0xe771	No error (0)	stats.g.doubleclick.net		142.250.141.154	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:41.973175049 CET	1.1.1.1	192.168.2.4	0xe771	No error (0)	stats.g.doubleclick.net		142.250.141.157	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.99	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.106	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.103	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.104	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.105	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.749085903 CET	1.1.1.1	192.168.2.4	0x58b7	No error (0)	www.google.com		142.250.101.147	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:42.750535011 CET	1.1.1.1	192.168.2.4	0x5025	No error (0)	www.google.com			65	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.139	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:43.242106915 CET	1.1.1.1	192.168.2.4	0xe92	No error (0)	play.google.com		142.250.141.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.231154919 CET	1.1.1.1	192.168.2.4	0x4007	No error (0)	payments.google.com		142.251.2.92	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.139	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238109112 CET	1.1.1.1	192.168.2.4	0xf8d6	No error (0)	plus.l.google.com		142.251.2.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:53.238243103 CET	1.1.1.1	192.168.2.4	0x4efa	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:56.115976095 CET	1.1.1.1	192.168.2.4	0xec1b	No error (0)	i.ytimg.com		142.250.141.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:56.115976095 CET	1.1.1.1	192.168.2.4	0xec1b	No error (0)	i.ytimg.com		142.251.2.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:56.207729101 CET	1.1.1.1	192.168.2.4	0x14c7	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:12:56.207729101 CET	1.1.1.1	192.168.2.4	0x14c7	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:56.590627909 CET	1.1.1.1	192.168.2.4	0x11ef	No error (0)	subscribers.production.wpu.sh		178.62.192.95	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:57.078161001 CET	1.1.1.1	192.168.2.4	0x9331	No error (0)	i.ytimg.com		142.251.2.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:57.078161001 CET	1.1.1.1	192.168.2.4	0x9331	No error (0)	i.ytimg.com		74.125.137.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:12:57.078161001 CET	1.1.1.1	192.168.2.4	0x9331	No error (0)	i.ytimg.com		142.250.101.119	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:14.586148024 CET	1.1.1.1	192.168.2.4	0xce35	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:14.586148024 CET	1.1.1.1	192.168.2.4	0xce35	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:17.877674103 CET	1.1.1.1	192.168.2.4	0xbcd2	No error (0)	img.cdn.house	cdn.gdns.revopush.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:17.877888918 CET	1.1.1.1	192.168.2.4	0x773f	No error (0)	js.wpadmngr.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:17.877888918 CET	1.1.1.1	192.168.2.4	0x773f	No error (0)	cdn28786515.ahacdn.me		45.133.44.52	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:17.877888918 CET	1.1.1.1	192.168.2.4	0x773f	No error (0)	cdn28786515.ahacdn.me		45.133.44.53	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:17.878180027 CET	1.1.1.1	192.168.2.4	0xb1ef	No error (0)	js.wpadmngr.com	cdn28786515.ahacdn.me		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	img.cdn.house	cdn.gdns.revopush.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		95.216.14.117	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		136.243.133.155	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		88.99.102.201	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		95.216.74.110	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		148.251.151.229	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		136.243.35.87	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		178.63.83.79	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		46.4.122.24	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		176.9.1.39	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:18.031425953 CET	1.1.1.1	192.168.2.4	0x20dc	No error (0)	cdn.gdns.revopush.com		78.46.45.185	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.139	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:33.594104052 CET	1.1.1.1	192.168.2.4	0x395e	No error (0)	play.google.com		142.250.141.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:44.123898983 CET	1.1.1.1	192.168.2.4	0x89bc	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 8, 2024 09:13:44.123898983 CET	1.1.1.1	192.168.2.4	0x89bc	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.100	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.102	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.113	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.138	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.101	A (IP address)	IN (0x0001)	false
Mar 8, 2024 09:13:53.098212004 CET	1.1.1.1	192.168.2.4	0x8f39	No error (0)	play.google.com		142.250.141.139	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- gossnabgroup.ru
- https:
  - js.nextpsh.top
  - bddb2d2561.62b81f5af3.com
  - js.capndr.com
  - storage.multstorage.com
  - js.wpshsdk.com
  - e1f6a352a1.3ea94c3718.com
  - nereserv.com
  - fp.metricswpsh.com
  - e32350d110.84bfe218ba.com
  - sw.wpushorg.com
  - static.bookmsg.com
  - notification.tubecup.net
  - winrenew-cash.life
  - play-lh.googleusercontent.com
  - www.google.com
  - stats.g.doubleclick.net
  - payments.google.com
  - i.ytimg.com
  - subscribers.production.wpu.sh
  - js.wpadmngr.com
  - img.cdn.house
- fs.microsoft.com
- cdn.stgcdn.com
- us.superfasti.co
- android.clients.google.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: **5084**, Parent PID: **6092**

General

Target ID:	0
Start time:	09:11:55
Start date:	08/03/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Has exited:	false

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5932**, Parent PID: **5084**

General

Target ID:	2
Start time:	09:12:00
Start date:	08/03/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2344 --field-trial-handle=2284,i,3100902536086182891,1735761918452591964,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6428**, Parent PID: **6092**

General

Target ID:	3
Start time:	09:12:02
Start date:	08/03/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://gossnabgroup.ru
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly