




**ID:** 553494
**Cookbook:** browseurl.jbs
**Time:** 02:45:00
**Date:** 15/01/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Windows Analysis Report http://Syphilisdating.com 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
Private 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 42
No static file info 42
Network Behavior 42
Network Port Distribution 42
TCP Packets 42
DNS Queries 42
DNS Answers 43
HTTP Request Dependency Graph 47
Code Manipulations 47
Statistics 47
Behavior 47
System Behavior 47
Analysis Process: chrome.exe PID: 3144 Parent PID: 568 47
General 47
File Activities 48
Registry Activities 48
Key Value Modified 48
Analysis Process: chrome.exe PID: 3092 Parent PID: 3144 48
General 48
File Activities 48
Analysis Process: chrome.exe PID: 7876 Parent PID: 3144 48
General 48
Disassembly 48
Code Analysis 48


Copyright Joe Security LLC 2022

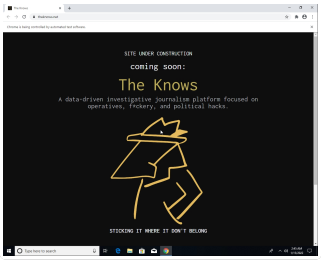
# Windows Analysis Report http://Syphilisdating.com

## Overview

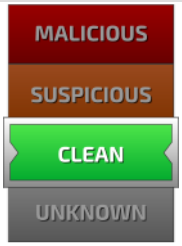
### General Information

| | |
|---|---|
| Sample URL: | http://Syphilisdating.com |
| Analysis ID: | 553494 |
| Infos: | |

Most interesting Screenshot:




### Detection

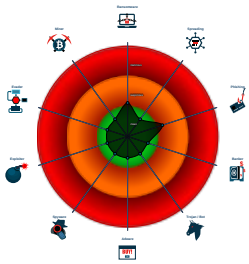



| | |
|---|---|
| Score: | 0 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

HTML body contains low number of ...

### Classification



## Process Tree

- **System is w10x64**
- chrome.exe (PID: 3144 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://Syphilisdating.com MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3092 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1608,3812998973630460944,2125780019593285875,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7876 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1608,3812998973630460944,2125780019593285875,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3636 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Copyright Joe Security LLC 2022

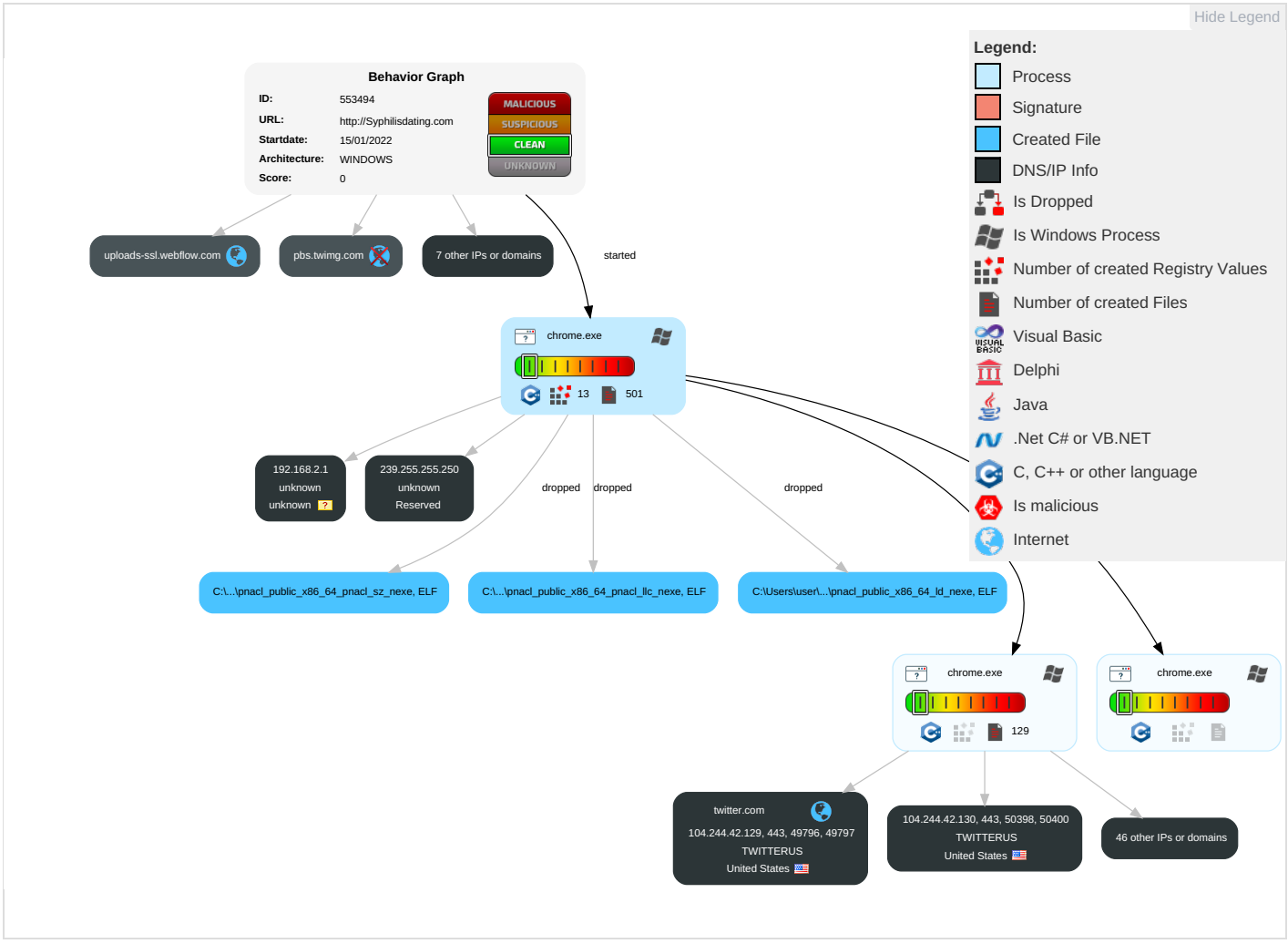
Click to jump to signature section

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

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impa |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Masquerading 3 | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 2 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modif Syste Partit |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Application Layer Protocol 2 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Devic Lock |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 3 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delet Devic Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Ingress Tool Transfer 1 | SIM Card Swap | | Carri Billin Fraud |

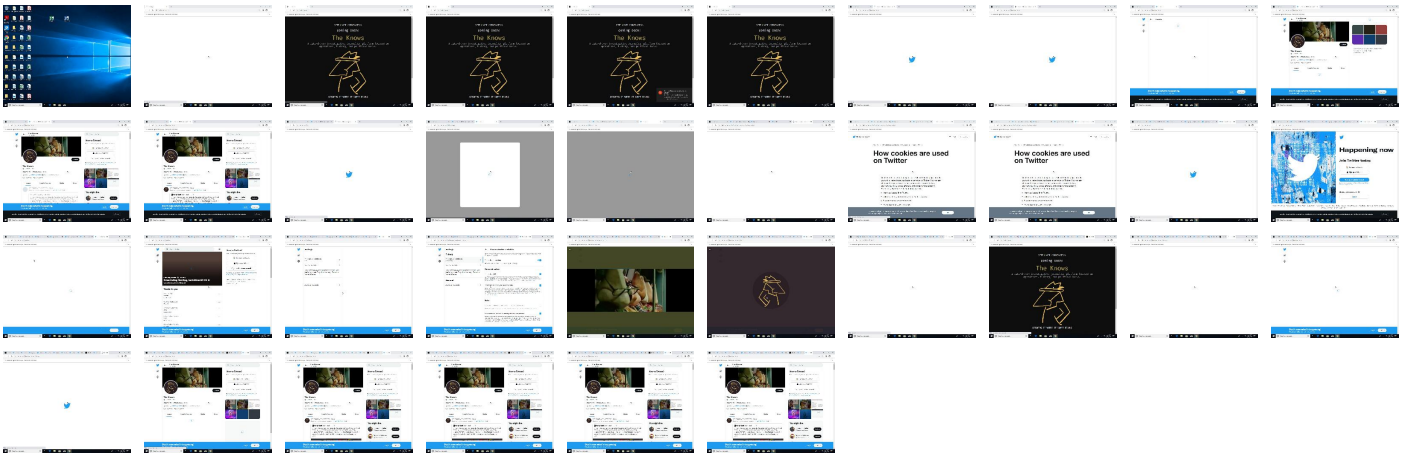
## Behavior Graph

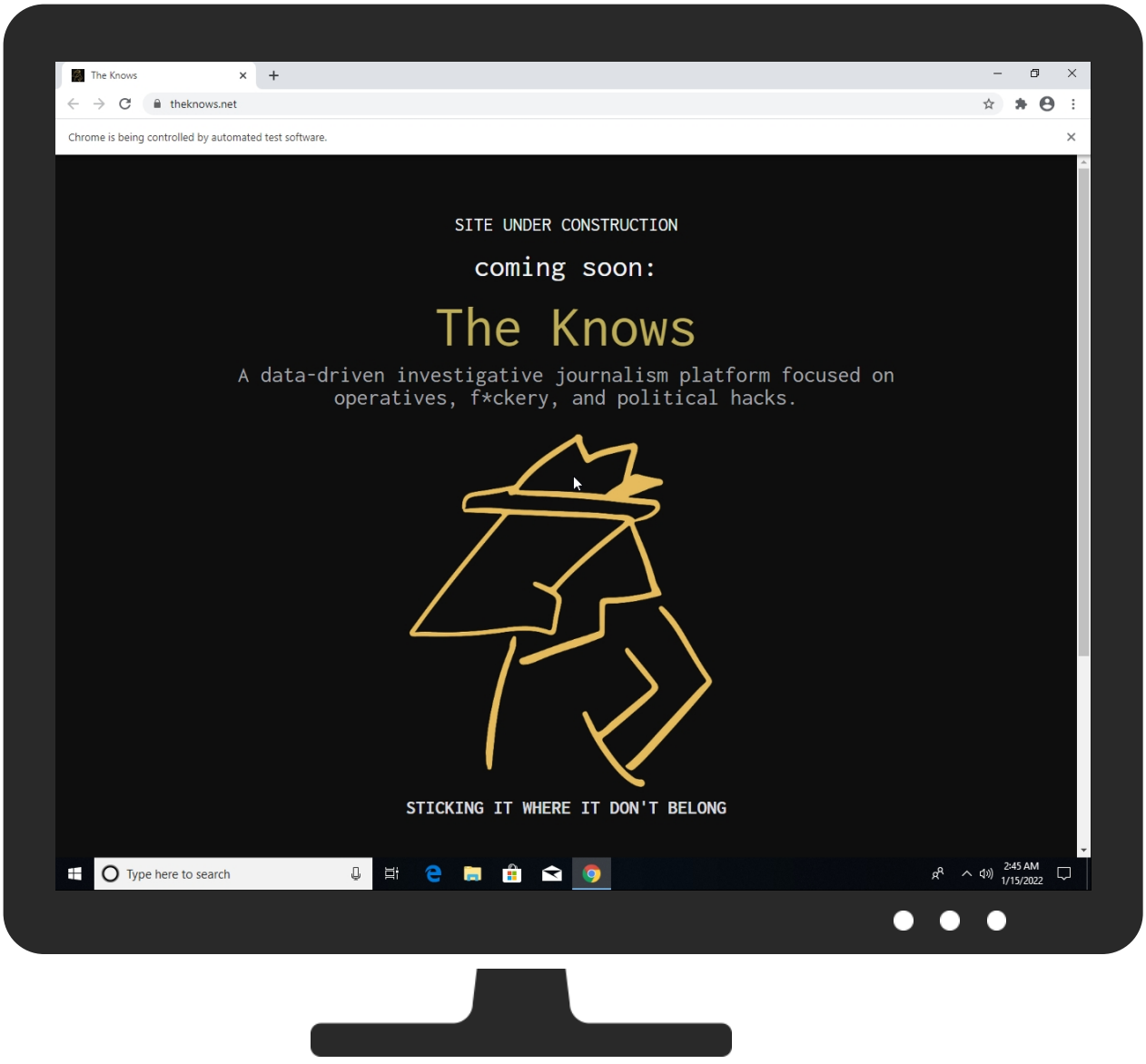


# Screenshots

## Thumbnails

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




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://Syphilisdating.com | 0% | Virustotal | | Browse |
| http://Syphilisdating.com | 0% | Avira URL Cloud | safe | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\3144_2076936835_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe | 0% | ReversingLabs | | |

### Unpacked PE Files

**No Antivirus matches**

### Domains

**No Antivirus matches**

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://redux.js.org/Errors?code= | 0% | URL Reputation | safe | |
| http://https://dwo3ckksxlb0v.cloudfront.net; | 0% | Avira URL Cloud | safe | |
| http://https://mobile.twitter.comVary: | 0% | Avira URL Cloud | safe | |
| http://https://imgix.revue.co; | 0% | Avira URL Cloud | safe | |
| http://https://twitter.github.io/birdwatch/about/overview/#transparency-and-visibility | 0% | Avira URL Cloud | safe | |
| http://theknows.net/ | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| gstaticadssl.l.google.com | 142.250.186.163 | true | false | | high |
| twitter.com | 104.244.42.129 | true | false | | high |
| syphilisdating.com | 216.70.123.100 | true | false | | unknown |
| accounts.google.com | 142.250.184.205 | true | false | | high |
| www-google-analytics.l.google.com | 142.250.186.78 | true | false | | high |
| s.twitter.com | 104.244.42.195 | true | false | | high |
| stats.l.doubleclick.net | 74.125.140.155 | true | false | | high |
| cs45.wac.edgecastcdn.net | 93.184.220.70 | true | false | | high |
| www-googletagmanager.l.google.com | 142.250.186.136 | true | false | | high |
| theknows.net | 99.83.190.102 | true | false | | unknown |
| cs41.wac.edgecastcdn.net | 93.184.220.66 | true | false | | high |
| syndication.twitter.com | 104.244.42.136 | true | false | | high |
| proxy-ssl-geo.webflow.com | 3.248.8.137 | true | false | | high |
| d3e54v103j8qbb.cloudfront.net | 13.224.98.50 | true | false | | high |
| tpop-api.twitter.com | 104.244.42.2 | true | false | | high |
| t.co | 104.244.42.69 | true | false | | high |
| abs-zero.twimg.com | 104.244.43.131 | true | false | | high |
| cs672.wac.edgecastcdn.net | 192.229.233.50 | true | false | | high |
| www.google.com | 142.250.185.164 | true | false | | high |
| clients.l.google.com | 142.250.181.238 | true | false | | high |
| uploads-ssl.webflow.com | 13.224.96.82 | true | false | | high |

Copyright Joe Security LLC 2022

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| googlehosted.l.googleusercontent.com | 142.250.181.225 | true | false | | high |
| cs510.wpc.edgecastcdn.net | 152.199.21.141 | true | false | | high |
| cs189.wpc.edgecastcdn.net | 68.232.34.217 | true | false | | high |
| www.theknows.net | unknown | unknown | false | | unknown |
| abs.twimg.com | unknown | unknown | false | | high |
| pbs.twimg.com | unknown | unknown | false | | high |
| abs-0.twimg.com | unknown | unknown | false | | high |
| api.twitter.com | unknown | unknown | false | | high |
| stats.g.doubleclick.net | unknown | unknown | false | | high |
| clients2.googleusercontent.com | unknown | unknown | false | | high |
| clients2.google.com | unknown | unknown | false | | high |
| help.twitter.com | unknown | unknown | false | | high |
| video.twimg.com | unknown | unknown | false | | high |
| platform.twitter.com | unknown | unknown | false | | high |
| fonts.twitter.com | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://twitter.com/settings/account/personalization | false | | high |
| http://theknows.net/ | false | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 104.244.42.129 | twitter.com | United States | | 13414 | TWITTERUS | false |
| 216.70.123.100 | syphilisdating.com | United States | | 31815 | MEDIATEMPLEUS | false |
| 93.184.220.66 | cs41.wac.edgecastcdn.net | European Union | | 15133 | EDGECASTUS | false |
| 3.248.8.137 | proxy-ssl-geo.webflow.com | United States | | 16509 | AMAZON-02US | false |
| 68.232.34.217 | cs189.wpc.edgecastcdn.net | United States | | 15133 | EDGECASTUS | false |
| 142.250.181.238 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.185.164 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 104.244.43.131 | abs-zero.twimg.com | United States | | 54113 | FASTLYUS | false |
| 152.199.21.141 | cs510.wpc.edgecastcdn.net | United States | | 15133 | EDGECASTUS | false |
| 142.250.184.205 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.186.136 | www-googletagmanager.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 13.224.98.50 | d3e54v103j8qbb.cloudfront.net | United States | | 16509 | AMAZON-02US | false |
| 142.250.186.78 | www-google-analytics.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 99.83.190.102 | theknows.net | United States | | 16509 | AMAZON-02US | false |
| 104.244.42.2 | tpop-api.twitter.com | United States | | 13414 | TWITTERUS | false |
| 104.244.42.69 | t.co | United States | | 13414 | TWITTERUS | false |
| 104.244.42.136 | syndication.twitter.com | United States | | 13414 | TWITTERUS | false |
| 142.250.186.163 | gstaticadssl.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 192.229.233.50 | cs672.wac.edgecastcdn.net | United States | | 15133 | EDGECASTUS | false |
| 104.244.42.3 | unknown | United States | | 13414 | TWITTERUS | false |
| 104.244.42.130 | unknown | United States | | 13414 | TWITTERUS | false |
| 104.244.42.195 | s.twitter.com | United States | | 13414 | TWITTERUS | false |
| 104.244.42.193 | unknown | United States | | 13414 | TWITTERUS | false |
| 142.250.181.225 | googlehosted.l.googleusercontent.com | United States | | 15169 | GOOGLEUS | false |
| 74.125.140.155 | stats.l.doubleclick.net | United States | | 15169 | GOOGLEUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 52.49.198.28 | unknown | United States | | 16509 | AMAZON-02US | false |
| 13.224.96.82 | uploads-ssl.webflow.com | United States | | 16509 | AMAZON-02US | false |

Copyright Joe Security LLC 2022

### Private

| IP |
|---|
| 192.168.2.1 |
| 127.0.0.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 553494 |
| Start date: | 15.01.2022 |
| Start time: | 02:45:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 37s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | browseurl.jbs |
| Sample URL: | http://Syphilisdating.com |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 19 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | CLEAN |
| Classification: | clean0.win@55/486@30/30 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Browse: https://twitter.com/theknowsnews<br>• Browse: https://twitter.com/login<br>• Browse: https://twitter.com/i/flow/signup<br>• Browse: https://help.twitter.com/rules-and-policies/twitter-cookies<br>• Browse: https://twitter.com/<br>• Browse: https://twitter.com/explore<br>• Browse: https://twitter.com/settings<br>• Browse: https://twitter.com/theknowsnews/header_photo<br>• Browse: https://twitter.com/theknowsnews/photo<br>• Browse: https://t.co/HfNZOOxhoP<br>• Browse: https://twitter.com/theknowsnews/following<br>• Browse: https://twitter.com/theknowsnews/followers |
| Warnings: | Show All |

## Simulations

### Behavior and APIs

| No simulations |
|---|

# Joe Sandbox View / Context

## IPs

No context

## Domains

No context

## ASN

No context

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 451603 |
| Entropy (8bit): | 5.009711072558331 |
| Encrypted: | false |
| SSDEEP: | 12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ |
| MD5: | A78AD14E77147E7DE3647E61964C0335 |
| SHA1: | CECC3DD41F4CEA0192B24300C71E1911BD4FCE45 |
| SHA-256: | 0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA |
| SHA-512: | DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101 |
| Malicious: | false |
| Reputation: | low |
| Preview: | BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\27cace04-743a-42e0-8c33-5b546207540b.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 94052 |
| Entropy (8bit): | 3.7494329962109245 |
| Encrypted: | false |
| SSDEEP: | 384:E7XkU2ZDiNGgVRjADNMr9vIU3nkyDHeTGTmrxG0mxXKSKVrBsm1CV2kgITOW6gNo:2Oq1pqqHXUefyIS0HPegK2YAnO |
| MD5: | 30D0F6B18BB8F1180D8D6BBFD37C7922 |
| SHA1: | BFDCAFD383A2D3E945CE101CE2A0A324ACE0D649 |
| SHA-256: | E89FF2CE5B84732FAEE5080E51B3A317AD59AE1CB1F768E0CE6F75B76299C0DC |
| SHA-512: | AE0E060377BD738FB482B6910FC03D32D8C0F718283F10F7C51C6E2E063C359BDE957494BD8560C53059B0B886BBC1103679AED130947143BA550525F4417615 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\27cace04-743a-42e0-8c33-5b546207540b.tmp | |
|---|---|
| Preview: | `o.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....Q8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\58d03010-ac37-4643-bcd1-5349850fb2ff.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 193431 |
| Entropy (8bit): | 6.045036113390477 |
| Encrypted: | false |
| SSDEEP: | 3072:Q2peUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGD7FcbXafIB0u1GOJmA3iuRZ:xh2qOAOntfJ/MQxglD5aqfIlUOoSiuRZ |
| MD5: | C445FD386D1B189020D8F9ABCF15CA4F |
| SHA1: | 7F3F2B1FB585F546D8B101E88E24B05F7F14B484 |
| SHA-256: | 0D5FBD536CB3FFE6370DBA09FB836B154EC1BC04E98CB9AE6DE25F4ACFAE0AA5 |
| SHA-512: | 73A31185B0A51AC17E99BDAFCFD0F81DE3D2F76D62956FC2394833A7EDCFA9FA45554701FDEA93B2D0353636E8D09E501E4AA0D94A7F1B3026669D3CC265DC1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642243551377976e+12,"network":1.642211153e+12,"ticks":130372452.0,"uncertainty":3963030.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799416751"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\5abde186-addb-4829-abe0-5edf17b646d3.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 201811 |
| Entropy (8bit): | 6.073524149425148 |
| Encrypted: | false |
| SSDEEP: | 6144:DNh2qOAOntfJ/MQxglD5aqfIlUOoSiuRZ:DrhOAAtWHlDKoi |
| MD5: | EB54BC8FA23119324EC7C3403D6F51EC |
| SHA1: | 57C0366C29F7BB119CA101C01FC9B1CE7717ABA6 |
| SHA-256: | 510D4CCC63A4B79473DA0577B34EF216E4E5E49F89BF5D88DD1709E2DCFFAA54 |
| SHA-512: | EE6FBA67520DBA6F22162C618C974D596EE859604A4F3F96B468A263B5D7653F4ED3C2A33AFA09E5B5A7A7078584C6674F2820C008333717BBD9115ADAB7CCD |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642243551377976e+12,"network":1.642211153e+12,"ticks":130372452.0,"uncertainty":3963030.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\5f19cc2d-b295-478a-83b1-ac37f1d9e14a.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 193337 |
| Entropy (8bit): | 6.044774661226077 |
| Encrypted: | false |
| SSDEEP: | 3072:QqpeUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGD7FcbXafIB0u1GOJmA3iuRZ:ph2qOAOntfJ/MQxglD5aqfIlUOoSiuRZ |
| MD5: | F275F9F8344D9D5FA20C356EC877771C |
| SHA1: | ED4E0F74DDDAFBE67011A54D06C6ABFD2938273B |
| SHA-256: | 1D1F7A07E4A4D3999FEDA1B16C2906C9DB979684C248A9C0ECBD328571071D2E |
| SHA-512: | BE32CE19CBF7471DFFD8F1A79E9B9A1D2707110E07BB1A74FD61DFB24CC45BBA9AC0699F2A2370D8B309D0DA81B87E24D722BC86233C315E7E4A3BF237031ED9 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\5f19cc2d-b295-478a-83b1-ac37f1d9e14a.tmp | |
|---|---|
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642243551377976e+12,"network":1.642211153e+12,"ticks":130372452.0,"uncertainty":3963030.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799416751"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\6214624d-ff25-428a-a722-fa37378d300a.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 94772 |
| Entropy (8bit): | 3.7494265744220074 |
| Encrypted: | false |
| SSDEEP: | 384:S7XkU2ZDiNGgVRjADNMr9vIU3nkyDHeTGTmrxG0mxXKSKVrBsm1JbV2kgITOW6gi:AOq1pqqQXUefyIS0HPegK2YAn61 |
| MD5: | 0DAFEE297BE2F2F1D7CA3E9437B5BB56 |
| SHA1: | 57DF45CDB079953688486D8397F4D3C14711237E |
| SHA-256: | 7D2760B29A85244210AB5F738C8065B29C826F9F0D0582DE2DE68FDC5D0ECBF2 |
| SHA-512: | 4F3C0248F273B2E4579117DD8112053FD2747F410408E5F10297BCD34095F2797203A11CC01A0684664E26536FEFCECF8439821790316A1A2C80425B4C2C9396 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0r.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....Q8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\649c457a-2b3b-4b4d-96e4-126e35196a61.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 92068 |
| Entropy (8bit): | 3.749149945344734 |
| Encrypted: | false |
| SSDEEP: | 384:77XkU2ZDeGBADNMr9vIU3nkyDHeTGTmrxG0mxXKSKVrBsm1CV2kgITOW6gNp10t5:hq1pqqHXUefyIS0HPegK2YAnBk |
| MD5: | CD19B334217EEE5574E8D4A7A722AA03 |
| SHA1: | 647B41934A0C1129FBCAED661A3C01C0EAB02199 |
| SHA-256: | 314F64AC0E0D2198D5BEF83A46C06BAC69B3618A19A134B94990004A1B89DB1E |
| SHA-512: | C6F14B3CBF10ED528E56D39878AC0383C00EA717EF273E6014BB8E1989944F80D4C435359D067D545100FFCBD2936F68BF943EE5C1A60F2A0E29788AFD1D2DC |
| Malicious: | false |
| Reputation: | low |
| Preview: | .g.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....Q8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\9dc02b3a-548b-47a2-b951-c02d11790c9c.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 193337 |
| Entropy (8bit): | 6.044774837503846 |
| Encrypted: | false |
| SSDEEP: | 3072:Q6peUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGD7FcbXafIB0u1GOJmA3iuRZ:Jh2qOAOntfJ/MQxgID5aqfIlUOoSiuRZ |
| MD5: | 62B7EB42CEE83DCE59485CE2799D145B |
| SHA1: | 7CA4C854CF10918F0B289329B6207E830DA1F574 |
| SHA-256: | BC51DD3E7AF4301508C9300C3F21236A043783F9AC16D2AE04C4E840B23DA240 |
| SHA-512: | 96D6A14AE2C0A78EBFB018A91ECFFF3B3DC923C7B60407DC5CE64286AF33E50178F27C12F566230F893CC2CCC9AF027C3CEF14B3F4AC90C9AD1AB858A9A2E91 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\9dc02b3a-548b-47a2-b951-c02d11790c9c.tmp | |
|---|---|
| Preview: | {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642243551377976e+12,"network":1.642211153e+12,"ticks":130372452.0,"uncertainty":3963030.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799416751"},"plugins":{"metadata":{"adobe-flash-player":{"disp |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 40 |
| Entropy (8bit): | 3.254162526001658 |
| Encrypted: | false |
| SSDEEP: | 3:FkXft0xE1n:+ftIE1n |
| MD5: | BD4642AD6C750A12D912B20BCB92E14D |
| SHA1: | C549F0F48FDD4FBC62E51AC26D7E185160CE2123 |
| SHA-256: | 4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C |
| SHA-512: | 04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF |
| Malicious: | false |
| Reputation: | low |
| Preview: | sdPC.....s}.....M..2.!..% |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40289732-ef8d-4358-a4b4-97dd770280c5.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 19181 |
| Entropy (8bit): | 5.570214818795944 |
| Encrypted: | false |
| SSDEEP: | 384:zngtdLlKlX91kXqKf/pUZNCgVLH2HfDcrUJHGxt5DnMO4d:oLlO91kXqKf/pUZNCgVLH2HfIrUtGxAj |
| MD5: | FD66D6DC7A50C39AD34D43E00C07F312 |
| SHA1: | 89E1D5302E4A0A792ADB415881EA6AF62B1A1263 |
| SHA-256: | FCCDB78E475447FBD8A1F708A33ED4B56C60FAA22995C341E8143B58D3ECAE8E |
| SHA-512: | B07C074403CE124D4D579CFEF74C3FBFBF17C4358E0C00FD9E963DB663993D2B4DD3F402B7A1BA032A73333CA474F41F36F3CA14028D8CBC8A8AA1CDC5F3CA0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286717149419869","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\44349d8a-f734-47b8-aad5-bfc86348d48c.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 370 |
| Entropy (8bit): | 5.470706561613585 |
| Encrypted: | false |
| SSDEEP: | 6:YAQNnXE9RfSHJR8wXwlmUUAnIMp5zfJmPWUEDMbFLggE6HdB8wXwlmUUAnIMp5zz:Y1XE9RAJ9+UAnIYJmUDMpL/fN+UAnIaF |
| MD5: | 12A8A11A7A11B7A8F0705AB7641CA9AD |
| SHA1: | 3740BACF7A34E328568439772AAAE63D84CB93E5 |
| SHA-256: | EECE13A1F7128BF9878CAA884A041C863DE5BB739133918E7C41B00308AF191C |
| SHA-512: | CF465497F40D957013E13C1ECA525D57CF15327E9A3D37C88CFE43B8EEA64103BF2886E339282025F9DDC22FA6454E2B11882B44D1020AB24F1A0F9D05AED02 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"expect_ct":[],"sts":[{"expiry":1673779614.069488,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642243614.069493},{"expiry":1653129967.951105,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642243567.951113}],"version":2} |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4fda0e8f-6f32-4668-94e8-3d0a463e0ab8.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | UTF-8 Unicode text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 17092 |
| Entropy (8bit): | 5.5830776994711195 |
| Encrypted: | false |
| SSDEEP: | 384:zngtdLlKlX91kXqKf/pUZNCgVLH2HfDcrUmt5DOMO4E:oLlO91kXqKf/pUZNCgVLH2HflrU89Or |
| MD5: | 2EA759B34C435647B1C3F60D378F5665 |
| SHA1: | FA293281ADA7475DEF8B5A2A32F53E5D713E99A6 |
| SHA-256: | 3EC7686AC37006488E543216E84BA503FB6404011888CA130BA1D70C7B5BFA9D |
| SHA-512: | 5C6D55BDFC431FAEF44D4FD21BA56251A63D1A616331FE07CD88536AD0F82AD541C40919EF7C44CE3B353644F6CF1F88F63108D0CC7DA457A5406986F46983C |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286717149419869","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ff000b4-d38a-471e-9387-50f82f3571c9.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 5419 |
| Entropy (8bit): | 5.001120515900457 |
| Encrypted: | false |
| SSDEEP: | 96:noC/s5l9pcKI+9ok0JCKL8UkLhak/16ubOTQVuwn:noC/i9pcF4KdkLYk/g8 |
| MD5: | 2A974B0CF533F0006EBEE687C6891E1E |
| SHA1: | 1F30628653E3C2E409FFCD43846A0B33E66499DB |
| SHA-256: | CA3AFDCDFB60AB1AF53DF20DE535261325B3D136B5B334DA282299D5DA3F6684 |
| SHA-512: | 6D0C6A4581FA7A61DB3BA74D21ACDA9E81B4357CFE08C4BE195BD0204F642B6E977E8650D8A33DD97ACF77F753CD735CCBC0C0529A5FD99C1946BF06C1E6D0F |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13286717149943779","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6820b3ec-029f-4b11-8b32-dda7a16da2ef.tmp | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 384:zngtdLlKlX91kXqKf/pUZNCgVLH2HfDcrUJHGWt5DBMO4d:oLlO91kXqKf/pUZNCgVLH2HflrUtGMir |
| MD5: | 586CF69406AC6DD45E407CA24E7DB5C5 |
| SHA1: | 1DE2FC586888C70C0CA08BBA80452969F4D38C18 |
| SHA-256: | 0344AAA9C666EF161BC56D119518EDF9C7AE148CDAD8BEB4C76729B4F40BC58F |
| SHA-512: | 37B8979C24B0861EC33406878DCE9EF88117F212A325B3967725C4809FC78A70299DCC9533F6742E39F8594EF6CAD67FAD5DB07B4C9A937C3CC307AA69A50D9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286717149419869","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c51c9f9-e8b5-4ee9-8342-057f7f824439.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 370 |
| Entropy (8bit): | 5.4666652582449204 |
| Encrypted: | false |
| SSDEEP: | 6:YAQN6z73E9RfSHJR8wXwlmUUAnIMp5zMWMmPWUEDMbFLggE6HdB8wXwlmUUAnIM/:Y2DE9RAJ9+UAnI9WMmUDMpL/fN+UAnIE |
| MD5: | 5C0B43AE22F7D8BEEC424B16512F47B6 |
| SHA1: | 54F5EA0E5C4442C137A5FFEBBA0D9A181B12E0CC |
| SHA-256: | 739283595817DAC1D16C2E30276D8AAD86BD7D20B73E96DA51250D6CF684A9C2 |
| SHA-512: | F9F085F40F509756452BFC81DDA121CCBFEBFDAACEC78473C4F73C03E0632A665FA9FCD4A5F55965A3DB0D8C0BFF283A339B824D18FC6DB7E876EEE41C0841F |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"expect_ct":[],"sts":[{"expiry":1673779592.102448,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642243592.102453},{"expiry":1653129967.951105,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642243567.951113}],"version":2} |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f69411f-00b3-4f13-9f2e-1275ec6ef0c0.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 3403 |
| Entropy (8bit): | 4.912696853186566 |
| Encrypted: | false |
| SSDEEP: | 96:JTOXGDHazCTrj2Gn6V/WzRGjGKoKGKGHpGGfH:JTOXGDHazCTX2W6V/WzRAPXMp |
| MD5: | 780BB6809B21820FDFE2FD1B146D53B2 |
| SHA1: | 1CFE874CEFCE4274E034048963E970A8214D3796 |
| SHA-256: | 49A9269877B2C4FEFB0E872614BFACE0646F0BB2CEADA766EB61B7DF1B2A6EE2 |
| SHA-512: | 2921E7AA5DE2A7ADB5A82BB6A9226A2B20E4D05A18629AE8F664D7D201BBB1B1A0BFDEFDE7247E3568E84425F868390D832A20CABF6057AECF773A83E59178AF |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289309151333599","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289309151474376","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13289309151474380","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r4---sn-4g5lznle.gvt1.co |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f9c0ca8-2857-44e4-989a-51ae6fac9802.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4219 |
| Entropy (8bit): | 4.871684703914691 |
| Encrypted: | false |
| SSDEEP: | 48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH |
| MD5: | EDC4A4E22003A711AEF67FAED28DB603 |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f9c0ca8-2857-44e4-989a-51ae6fac9802.tmp | |
|---|---|
| SHA1: | 977E551B9ED5F60D018C030B0B4AA2E33B954556 |
| SHA-256: | DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453 |
| SHA-512: | 84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true}, |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9652df07-d7e4-4028-9801-82b04b71d6ee.tmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 3248 |
| Entropy (8bit): | 4.913365893686501 |
| Encrypted: | false |
| SSDEEP: | 48:Y2TtwXGDH3qz5sZGsH5rtsIRs8/sYyKswK7sHMHqsXAQsTZ6VLs+SsfA5sDRLsvg:JTOXGDHazCTrfz1HKqGNAF6V/608KfH |
| MD5: | 87E9F778D0782A0C07471A910D0E275D |
| SHA1: | 44F448C94DC9A63E35B14FFEEE1523E2FBEBCBFF |
| SHA-256: | 625BF1775C4E713FA276F3370B3E72495AE6884EEA29626CB9DF8932AC369DE1 |
| SHA-512: | 1D81475DE9C251C159DB2E8011917E86FFA1E6212B17C8AAC4E836F5D8182D986C3448BED98F42C12BB1D6615B1D39B78EB92192495C104C96E67652554FD137 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289309151333599","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289309151474376","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13289309151474380","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r4---sn-4g5lznle.gvt1.co |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 11217 |
| Entropy (8bit): | 6.069602775336632 |
| Encrypted: | false |
| SSDEEP: | 192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT |
| MD5: | 90F880064A42B29CCFF51FE5425BF1A3 |
| SHA1: | 6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF |
| SHA-256: | 965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268 |
| SHA-512: | D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 38 |
| Entropy (8bit): | 1.8784775129881184 |
| Encrypted: | false |
| SSDEEP: | 3:FQxlXNQxlX:qTCT |
| MD5: | 51A2CBB807F5085530DEC18E45CB8569 |
| SHA1: | 7AD88CD3DE5844C7FC269C4500228A630016AB5B |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log | |
|---|---|
| SHA-256: | 1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC |
| SHA-512: | B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF |
| Malicious: | false |
| Reputation: | low |
| Preview: | .f.5.....f.5..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 369 |
| Entropy (8bit): | 5.273392028942894 |
| Encrypted: | false |
| SSDEEP: | 6:MCXAQL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTCsG1ZmwYVTCcRHwQLVkwOWXc:MoAQyva5KkTXfchI3FUtuFg/0F2QR5fk |
| MD5: | 419DC62537BEC2E1E666627396AF211D |
| SHA1: | AA26DFC00FC637CCB6DAE8A084EA697BD4638426 |
| SHA-256: | DD8E069AD45D6097C85C3FF2D8507D747FB1E19752EBD89F080E4928DC31D7BF |
| SHA-512: | A2F0E73871BB864D5B9051B48841C964CF89EE936D3E82345ED62F5336881C70A7722981F75DF37A5EBABD9AD2E71A68E0D9E0AF62A91D83CCFA61D2EDB6FDF |
| Malicious: | false |
| Reputation: | low |
| Preview: | 2022/01/15-02:45:54.832 418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/15-02:45:54.898 418 Recovering log #3.2022/01/15-02:45:54.901 418 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log . |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.. (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 369 |
| Entropy (8bit): | 5.273392028942894 |
| Encrypted: | false |
| SSDEEP: | 6:MCXAQL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTCsG1ZmwYVTCcRHwQLVkwOWXc:MoAQyva5KkTXfchI3FUtuFg/0F2QR5fk |
| MD5: | 419DC62537BEC2E1E666627396AF211D |
| SHA1: | AA26DFC00FC637CCB6DAE8A084EA697BD4638426 |
| SHA-256: | DD8E069AD45D6097C85C3FF2D8507D747FB1E19752EBD89F080E4928DC31D7BF |
| SHA-512: | A2F0E73871BB864D5B9051B48841C964CF89EE936D3E82345ED62F5336881C70A7722981F75DF37A5EBABD9AD2E71A68E0D9E0AF62A91D83CCFA61D2EDB6FDF |
| Malicious: | false |
| Reputation: | low |
| Preview: | 2022/01/15-02:45:54.832 418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/15-02:45:54.898 418 Recovering log #3.2022/01/15-02:45:54.901 418 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log . |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | zlib compressed data |
| Category: | dropped |
| Size (bytes): | 644 |
| Entropy (8bit): | 5.276161248878741 |
| Encrypted: | false |
| SSDEEP: | 12:VT5b5TgeCSWtLsmqDD72702MESeX9NlWFBkMgNSZvGSClJUS/T8inLNA//G4U:B5d7RALsmqDDy13XUAN0qIoJsU |
| MD5: | 6D4AD10AA86F5906B352B05A01318792 |
| SHA1: | D520C2CD137A3D68E22A489FA5FB0FCD566FA0E3 |
| SHA-256: | 5CB22458EFA7700DA224814A56990DAB49462456FD2936C73A4B853C9ABBD3A5 |
| SHA-512: | 8D0C11F42E4C04D82356A7BDF85EDFC35E1E0FA3EBD4C32FB8D7A84FA99D0F6F14FCFBE8A0C709088213D481D48507AFDD0A25232CDB661AB174632DBF0C32A |
| Malicious: | false |
| Reputation: | low |
| Preview: | ....."D....com..http..knows..syphilisdating..the..https..net..theknows..www*h.....com.....http.....https.....knows.....net.....syphilisdating.....the.....theknows.....www..2.....a.....c.....d.....e.....g.....h.....i.....k.....l.....m.....n.....o.....p.....s.....t.....w.....y...:U.....B.....G..... .....*.http://syphilisdating.com/2.The Knows:.....K..... .....*.https://www.theknows.net/2.The Knows:.....J..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_twitter.com_0.indexeddb.leveldb\000001.dbtmp | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 16 |
| Entropy (8bit): | 3.2743974703476995 |
| Encrypted: | false |
| SSDEEP: | 3:1sjgWIV//Uv:1qIFUv |
| MD5: | 46295CAC801E5D4857D09837238A6394 |
| SHA1: | 44E0FA1B517DBF802B18FAF0785EEEA6AC51594B |
| SHA-256: | 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443 |
| SHA-512: | 8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MANIFEST-000001. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_twitter.com_0.indexeddb.leveldb\CURRENT (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 16 |
| Entropy (8bit): | 3.2743974703476995 |
| Encrypted: | false |
| SSDEEP: | 3:1sjgWIV//Uv:1qIFUv |
| MD5: | 46295CAC801E5D4857D09837238A6394 |
| SHA1: | 44E0FA1B517DBF802B18FAF0785EEEA6AC51594B |
| SHA-256: | 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443 |
| SHA-512: | 8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MANIFEST-000001. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_twitter.com_0.indexeddb.leveldb\MANIFEST-000001 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 23 |
| Entropy (8bit): | 4.142914673354254 |
| Encrypted: | false |
| SSDEEP: | 3:Fdb+4Ll:Zl |
| MD5: | 3FD11FF447C1EE23538DC4D9724427A3 |
| SHA1: | 1335E6F71CC4E3CF7025233523B4760F8893E9C9 |
| SHA-256: | 720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED |
| SHA-512: | 10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....idb_cmp1..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State} (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4219 |
| Entropy (8bit): | 4.871684703914691 |
| Encrypted: | false |
| SSDEEP: | 48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH |
| MD5: | EDC4A4E22003A711AEF67FAED28DB603 |
| SHA1: | 977E551B9ED5F60D018C030B0B4AA2E33B954556 |
| SHA-256: | DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453 |
| SHA-512: | 84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State} (copy) | |
|---|---|
| Preview: | {"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true}, |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 5625 |
| Entropy (8bit): | 5.01538907145425 |
| Encrypted: | false |
| SSDEEP: | 96:noC/scl9pcKI+Aok0JCWRWL8CktSArtk/1EbOTQVuwn:noC/L9pcq4WYvkkik/A |
| MD5: | D9F04E55A0BCC2B10CF708BB61648FFA |
| SHA1: | 0D679729CAA751869A3D45A6FF30F9E6FCB1D00A |
| SHA-256: | 43A2FA45874187A9826F61094C1BC944FEA69CB78AD5FCF3F077B22FE0C08373 |
| SHA-512: | 0CC79315566B1E042E240F69B1AA56DB163E4AF23D6E5B1BC3491F2AFDD7FDF3E067D40D7ED46BB4A1DD8C7B766CC3F4E6DFFD7F7B93F3A7EB80CAFDEA44B58 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13286717149943779","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy) | |
|---|---|
| Preview: | {"account_id_migration_state":2,"account_tracker_service_last_update":"13286717149943779","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\2359ebe4-684b-4ca3-8b2c-81cd4eb2afdc\af47be93e4c33dc6_0 | |
|---|---|
| Preview: | 0\r..m.....#....F.....https://twitter.com/home?precache=1<!DOCTYPE html>.<html dir="ltr" lang="en">.<meta charset="utf-8" />.<meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0,viewport-fit=cover" /><link rel="preconnect" href="//abs.twimg.com" /><link rel="dns-prefetch" href="//abs.twimg.com" /><link rel="preconnect" href="//api.twitter.com" /><link rel="dns-prefetch" href="//api.twitter.com" /><link rel="preconnect" href="//pbs.twimg.com" /><link rel="dns-prefetch" href="//pbs.twimg.com" /><link rel="preconnect" href="//t.co" /><link rel="dns-prefetch" href="//t.co" /><link rel="preconnect" href="//video.twimg.com" /><link rel="dns-prefetch" href="//video.twimg.com" /><link rel="preload" as="script" crossorigin="anonymous" href="https://abs.twimg.com/responsive-web/client-web/polyfills.cad508b5.js" nonce="YmU1ZDg1ZjgtZGU3Yy00YTMyLWI1YmEtMGIyMGY0MDdkY2Nj" /><link rel="preload" as="script" crossorigin="anonymous" href="https://abs.twimg.c |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\2359ebe4-684b-4ca3-8b2c-81cd4eb2afdc\index | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ISO-8859 text, with no line terminators, with escape sequences |
| Category: | dropped |
| Size (bytes): | 24 |
| Entropy (8bit): | 2.1431558784658327 |
| Encrypted: | false |
| SSDEEP: | 3:m+l:m |
| MD5: | 54CB446F628B2EA4A5BCE5769910512E |
| SHA1: | C27CA848427FE87F5CF4D0E0E3CD57151B0D820D |
| SHA-256: | FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D |
| SHA-512: | 8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\2359ebe4-684b-4ca3-8b2c-81cd4eb2afdc\index-dir\temp-index | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 3.5549278751195694 |
| Encrypted: | false |
| SSDEEP: | 3:pQAyXl/lv/HlvB2bR/R:aAKv/nm/R |
| MD5: | ACEA7D0D3D6C8951984FED247B38A4FD |
| SHA1: | B11C34BA91DA05E162F915322A7CEAE5C7B3C244 |
| SHA-256: | BD0AD95AD46D970385DC5DA91795E2F0FD8E7E48ECBAEDDD40C060D2A378245F |
| SHA-512: | 23851C5A5952642AE7C45B6914280E91A7CD60FBF2067D3AC84991110A2E90E3C7EDC4F615A483B29DBD02D96EAE3E4F0879E1E207FCDF525DAA28FD91F284ED |
| Malicious: | false |
| Reputation: | low |
| Preview: | @.....~.oy retne.....k.....=..G.....k.....R.<.24/. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\2359ebe4-684b-4ca3-8b2c-81cd4eb2afdc\index-dir\the-real-index (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 3.5549278751195694 |
| Encrypted: | false |
| SSDEEP: | 3:pQAyXl/lv/HlvB2bR/R:aAKv/nm/R |
| MD5: | ACEA7D0D3D6C8951984FED247B38A4FD |
| SHA1: | B11C34BA91DA05E162F915322A7CEAE5C7B3C244 |
| SHA-256: | BD0AD95AD46D970385DC5DA91795E2F0FD8E7E48ECBAEDDD40C060D2A378245F |
| SHA-512: | 23851C5A5952642AE7C45B6914280E91A7CD60FBF2067D3AC84991110A2E90E3C7EDC4F615A483B29DBD02D96EAE3E4F0879E1E207FCDF525DAA28FD91F284ED |
| Malicious: | false |
| Reputation: | low |
| Preview: | @.....~.oy retne.....k.....=..G.....k.....R.<.24/. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\2359ebe4-684b-4ca3-8b2c-81cd4eb2afdc\index-dir\the-real-index. (copy) | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 3.5549278751195694 |
| Encrypted: | false |
| SSDEEP: | 3:pQAyXl/lv/HlvB2bR/R:aAKv/nm/R |
| MD5: | ACEA7D0D3D6C8951984FED247B38A4FD |
| SHA1: | B11C34BA91DA05E162F915322A7CEAE5C7B3C244 |
| SHA-256: | BD0AD95AD46D970385DC5DA91795E2F0FD8E7E48ECBAEDDD40C060D2A378245F |
| SHA-512: | 23851C5A5952642AE7C45B6914280E91A7CD60FBF2067D3AC84991110A2E90E3C7EDC4F615A483B29DBD02D96EAE3E4F0879E1E207FCDF525DAA28FD91F284E<br>D |
| Malicious: | false |
| Reputation: | low |
| Preview: | @.....~.oy retne.....k.....=..G.....k.....R.<.24/. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\08406be60bab548c_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3748 |
| Entropy (8bit): | 5.797803009429955 |
| Encrypted: | false |
| SSDEEP: | 96:CfWRQNQhzmTa0qGU35yxOoD/dnCtZMJF/ocMFTFgw3:KWRuQzmTa0J+5yIoD/dCtZMJFX8 |
| MD5: | 6941AD008DDA385DD7C602C0C5C21AEB |
| SHA1: | 6D6256C9F447CBC163C62FFCF561228609F860AE |
| SHA-256: | BD511C074ADE4B29375263C01E76AADE54D486BA5E4B0433CC0D8E9C72C3E441 |
| SHA-512: | 3B72072DB47042DE48B79C6297945100F1313007A6814C75A0C439103C52B9A3FE393278D64B34A43C6107E147A4E6068CE2C7CBF594E850124334EE27AB5E30 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....P...U.7.....https://abs.twimg.com/responsive-web/client-web/bundle.ExploreTopics.4137a9b5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[56],{PH3B:function(e,t,a){"use strict";var n=a("ezF+");var o=Object.freeze({Cell:"Cell",PreviewCard:"PreviewCard"}),r=a("XBtf");const i={loader:()=>a.e(337).then(a.bind(null,"a+ad")),loaderKey:"newsCellLoader",strategy:r.a.Critical},c={loader:()=>a.e(339).then(a.bind(null,"hX2d")),loaderKey:"newsPreviewCardLoader",strategy:r.a.Critical};t.a=n.c({selectDisplayType:e=>e.content.newsDisplayType,handlers:{[o.Cell]:i,[o.PreviewCard]:c}})},gRxV:function(e,t,a){"use strict";a.r(t),a.d(t,"ExploreTopicsScreen",(function()ion(){return K})};var n=a("ERkP"),o=a("es0u"),r=a("hqKg"),i=a("ZNT5");const c={news:"url",sim_cluster:"cluster_id",ttt:"ttt_id",semantic_core:"entity_id"};var l=a("kGix"),s=a("3XMw"),d=a.n(s),p=a("rxPX");const u=d.a.fcf3e54b,m=(e,t)=>t.match.params.topicId,y=(e,t)=>t.match.params.taxonomy,w=Object(r.createSelector)(m,y,((e,t)=>( |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\08406be60bab548c_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9008 |
| Entropy (8bit): | 5.969816924420091 |
| Encrypted: | false |
| SSDEEP: | 192:oyHjwgNFZriMo6viW792nOankVbrt+oL3fQZTNJGLE6Fv5K:jDw+TrQ692UdIZfyFBK |
| MD5: | 742C107C4F9C334D943CEED885C03E37 |
| SHA1: | A369AD246D3F11B60C0ADF924B456B6BC73AEDE7 |
| SHA-256: | 60F2B79CB0AA6D0A9B7BB26EF459E4FD495FA043BF440A4F0858131AEF818DCC |
| SHA-512: | A54753BA2C349A37CFB87206F057268AF136F27390BE2E61E9356EDC8DA65D165A0CDD1EB66AADDAF544B04B2FF3CAE224EC4D63918423E800E354A948F0090<br>3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....P...U.7.....https://abs.twimg.com/responsive-web/client-web/bundle.ExploreTopics.4137a9b5.js.....'.....O....h"..%.....(S.t..`.....,L<br>`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....p...`.....a.....Qb.....PH3BC..Qbv.-.....gRxVC.(S..`.....`L`,....0Rc.....M.`$....<br>.Q.`....Da.....Qb.T.....ezF+.....Qc.BG^....freeze.....a.....QbR.....Cell..A...Qd6.. ....PreviewCard.....Qb.+.....XBtf.$.a.....QcR.....loader..C..Qd.....loaderKey....<br>.Qe.....newsCellLoader....Qc^m7.....strategyC.(S.`.`x....L`.....Qb.Lh@....e.....Qb~.G.....a+ad..K`....Dr0.....&.(...&...Q.&.Y....&.(...&...&.(...&..&...&.Z.....&.Y.....<br>.,Rc.....`....Da.....c.....P...@..@.-....\P.a.....P...https://abs.twimg.com/responsive-web/client-web/bundle.ExploreTopics.4137a9b5.jsa.....D`....D`@...D`...<br>..X...`(...&...&....&..!.&.(S.` |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0a4536a5f6afb4b3_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0a4536a5f6afb4b3_0**

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 4801 |
| Entropy (8bit): | 5.666784130888207 |
| Encrypted: | false |
| SSDEEP: | 96:/tnjmaAjHsYGsCMUYCuuJCUBQtVs50yYm+VYGC9lLeYCuuDNMUFNFsSwUP+:/tndAjHlGbM9u1BaVK0yumGiljuZb3P+ |
| MD5: | 5656AECAD359441189A19CBEB9E987E8 |
| SHA1: | DE736DCE32BBC1DE53988A5D01A3ED08327EE1EC |
| SHA-256: | BE1AE31D09EBD74F637F2A8F48B35C8D5C3D93911954C0EA410E0C0D3090F81E |
| SHA-512: | 389D4D10A1715750044D6E3DC52B37AF81D38F1ACDA147E41EFC47EB077FC307C746ACCE36835DE0443DBFF5F0BC6AF4F7383F81B3A41FE5FE41D841A2B900<br>6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....M....#.....https://abs.twimg.com/responsive-web/client-web/bundle.UserAvatar.56a23385.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[103],{ "3Zg8":function(e,t,r){"use strict";r.r(t),r.d(t,"UserAvatarScreen",(function(){return N}));var a=r("ERkP"),n=r("rxPX"),o=r("0KEI"),c=r("kGix"),s=r("G6rE");const i=Object(s.g) ([s.a]),d=(e,t)=>{const r=l(e,t);return r?i(e,r):c.a.LOADING},l=(e,t)=>t.match.params.screenName,m=(e,t)=>{const r=l(e,t);return r?s.e.selectByScreenName(e,r):void 0};var u=Object(n.a)().propsFromState(((()=>({fetchStatus:d,screenName:l,user:m})))).adjustStateProps((({fetchStatus:e,screenName:t,user:r})=>({fetchStatus:e,screenName:t,user:r,mediaItem:r?{id_str:r.id_str,expanded_url:r.profile_image_url_https,media_url_https:r.profile_image_url_https,ext_alt_text:r.profile_image_extensions_alt_text,type:" photo",original_info:{width:400,height:400}}:void 0}))).propsFromActions(((()=>({createLocalApiErrorHandler:Object(o.createLocalApiErrorHandlerWithContextFactory |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0a4536a5f6afb4b3_1**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 11301 |
| Entropy (8bit): | 5.846073755248347 |
| Encrypted: | false |
| SSDEEP: | 192:SdE7bATcCHIg7wRS/+1zNj3JckD5RCNyf2etRc5IDGbsksFKOM5Xy5R9n5hh0L3k:s+HsIHccJRxMKtM5XyR5hh0L3k |
| MD5: | 64DD78C191DA74B8188FE960E11DB262 |
| SHA1: | AC49E48D03B8EE3978BD2FF089E8B62D7A3030F5 |
| SHA-256: | 97AB91360F2C19F9B0336237BB068E0B301225CAAC5E61F561B77913D97D8404 |
| SHA-512: | 28D71DB5A478A155D2E4AF70DB36EBC9A236AC797528F1CABB077FF5B7B07BD4A20351B0B569AA4B57C99A6C22D2203ABD10E14BCFDC8C59A873CFA848F3B<br>36 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....M....#.....https://abs.twimg.com/responsive-web/client-web/bundle.UserAvatar.56a23385.js.....'.....O....X+...E.`.....(S.t..`.....,L`.... ..Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....a.....Qb&.....3Zg8C..Qbv@.+....ac3pC.(S....`.....L`@.....RcP..... ..... M...QbV.<.....o.....Qb.i.....c.....Qb2.....s.....S...Qb..{....d.....Qb.....l.....QbJ!.....m.....QbR.....h.....Qb.....p.....Qb.%.....f.....Qb.#....._.....Qb...*....E.....Qb..(&....S..... O...Qb..#.....N...o.....Q.`....Da.....Qb..\.....r.....Qe.5.....UserAvatarScreen.(S.(.`.....L`.....1...K`....Dd.....,Rc..... ..I`....Da....(.....@.-....\P.a.....M...https://abs.twimg.com/responsive-web/client-web/bundle.UserAvatar.56a23385.js...a.....D`....D`....D`.....\|...`:...&...&....&..!.&.(S.P |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0b55e678a1eb8a24_0**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9323 |
| Entropy (8bit): | 5.456071963477303 |
| Encrypted: | false |
| SSDEEP: | 192:wTcwUI7rWdyWmf5+nakdB8Lvj9dEIuZSaOk8mwBfL2UsOq81RI:eTUI7rWdyWmfEnddB8LrbElZSaR8mwEB |
| MD5: | 47DFB9C186EF8DD22D54A2200C92D22A |
| SHA1: | 1FFBB9CCCBCA337A602537C2FD0245B13DBA57FA |
| SHA-256: | EFFEFD67CE0D7E66800BC11D21B7B9B1E8CF83F4175FAF1F2A24C6B243ECAB75 |
| SHA-512: | 8F6E60937A001BB8DF579AD99BD1F41C1D659DF2D1220ACDED77E0158415B25CE6CB4D3454FCB595B1B499EBD82CB053743604226C9AFBD2FD76D9F1492BB<br>D |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....S.....>.....https://abs.twimg.com/responsive-web/client-web/bundle.AudioSpaceDetail.c9b2a775.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[32], {"Fg/a":function(e,t,i){"use strict";i.d(t,"a",(function(){return v}));var r=i("KEM+"),n=i.n(r),a=i("ERkP"),s=i("Pc/x"),o=i("6/RC"),c=i("Z5jE"),p=i("rxPX");const u=(e,t)=>Objec t(c.a)(t.match),l=e=>(t,i,{api:r})=>r.AudioSpaces.byId(e,{isMetatagsQuery:!0});var h=Object(p.a)().propsFromState(((()=> ({fetchAudioSpace:l})))),d=i("3XMw"),m=i.n(d),g=i("rJoH"),S=i("Rumh"),f=i("AooF");function b(e){const t=e.space;if(!t)return null;const i=function(e){const{canonical:t,de scription:i,title:r,ttl:n}=function(e){var t;const i=null==e\|\|null===(t=e.host)\|\|void 0===t?void 0:t.display_name,r=i?E.hostSpace({name:i}):E.hostSpaceFallback,n=e.title\| \|r,a=E.descriptionGeneric,s=(null==e?void 0:e.participants.total)\|\|0,o=S.a.formatCountShort(s),c=E.descriptionListening({count:o});let p,u,l;if(e.state===f.a.Sp |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0b55e678a1eb8a24_1**

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

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\0b55e678a1eb8a24_1**

| | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 25547 |
| Entropy (8bit): | 5.856044625639801 |
| Encrypted: | false |
| SSDEEP: | 384:d3p6lys1skhLsoWaN3zuIgUvWWJnVI6Zp717px+NBJno40EC/:d3peys1sgLDN3zVZWCnTzepo4h8 |
| MD5: | E92E8A6A1776A945DF907D22D64FADD3 |
| SHA1: | 881F4053F4AFADB5E3D559129D9146A4D54E4470 |
| SHA-256: | 27A5CC7C736510A19368CE2C79848B6B018D34109D3676FD52E13105B1CF0574 |
| SHA-512: | FC7C5CD024AC6121E385D9E27297B960D84C793CFBC8A0B03310DAD25F48F338C6D97ADC819AAFC0F95C0B378A502C991B9C610BD3E745EEBC25FDF89FAE36B |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....S.....>.....https://abs.twimg.com/responsive-web/client-web/bundle.AudioSpaceDetail.c9b2a775.js.....'.s ....O.....b..V. .....`.....(S....`.....<L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....@...`.....,..a.....Qb..r.....Fg/aC..Qb..Z....Pc/xC..QbR .....Z5jEC..Qb.. .....qTXfC.(S.]..`r.....L`x.....RcL.....Qb.~d....n.....M...Qb2.....s.....QbV.<.....o.....Qb.i.....c.....R....Qb.....l.....Qb..(&....S.....Qb.%.....f.....O...Qb...*....E.....Q b&..u....P.....Qb.#.....\_.....Qbj.B.....v...n.....`....Da.....(S.T.`b.....L`.....Qc.=.....space....(S..`R....LL`"....(S....`.....L`\.....Qbv+.s....host..Q dr=.Y....display_name..A...Qd.o3.....hostSpace.....a.....C.. Qfz.}P....hostSpaceFallback.....Qc.+.7....title.... Qf.....descriptionGeneric....Qd..5]....participants..... |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\12405e797f3bdc55_0**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 202696 |
| Entropy (8bit): | 5.53723630912214 |
| Encrypted: | false |
| SSDEEP: | 3072:dGW+B9qLRGHvqoXX46B1vnWnGSgz32oSidtyCfWmWQibAruLu5JWTbRVIxg6Epi3:NZRGHvqoXXrQvL4 |
| MD5: | 97C85691502D3410008E25A75170D9D0 |
| SHA1: | CB899FE6E457F103EB16B0057F642E2515AF76BC |
| SHA-256: | 141BB0A0843EBF383D34DAEA2DAEB3FA70CDA4365D95056C50D9BD915E9BBFE5 |
| SHA-512: | BD16209795024B68F5D3F387C2B9B52DD5FE46BAB5C5AEC3098660AA129B5F9DAE986775724E7C54AEC427500610BCEE73C079FE5DD3AAB1998151164DEDF36 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....https://abs.twimg.com/responsive-web/client-web/shared~ondemand.EmojiPickerData~ondemand.ParticipantReaction~ondemand.EmojiPicker.b5aa2cc5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[18],{"+cai":function(a,f,k){"use strict";k.r(f);var d=k("3XMw"),e=k.n(d);const b={compressed:!0,spriteSheetColumns:50,spriteSheetRows:69,categories:[{id:"people",name:e.a.i506b71f,emojis:".. .. .. .

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\148c8941f3f417fe_0**

| | |
|---|---|
| Size (bytes): | 1678 |
| Entropy (8bit): | 6.0483523937521 |
| Encrypted: | false |
| SSDEEP: | 48:pn58bD3fHEJeTgnLWXwrOK4BVNCch3FFlfM3jaww:qHEJogLvroHMiF7foGww |
| MD5: | C7CD6BC48A5208771635B06548151150 |
| SHA1: | 3F8671E1856456EFDF73443314944C7F815F1A46 |
| SHA-256: | 5D247EE63E64D80EEFF9B632B93469B33B969EB808B80A2191801BAC2CF4E8AF |
| SHA-512: | 9AF3143B9F6BBF66FDDCDC56169B93D0243B9CD12F16871C63C5A640C472E4AAA5FE2046C702E4D886591DDD25FF9BA11EA112BAB342E2D11DEA6AEC85A03<br>44 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....N...5..q....https://abs.twimg.com/responsive-web/client-web/bundle.AboutThisAd.da621335.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[26],{ bv0X:function(e,t,s){"use strict";s.r(t),s.d(t,"AboutThisAdScreen",(function(){return m}));var r=s("ERkP"),a=s("rxPX");const o=(e,t)=>t.match.params.impressionId;var n=Ob ject(a.a)().propsFromState(((()=>({impressionId:o}))),i=s("jHSc"),c=s("3XMw"),p=s.n(c),b=s("bPFD"),d=s("rHpw");const l=p.a.fb4ee11c,m=({history:e,impressionId:t} )=>r.createElement(i.b,{history:e,title:l},r.createElement(b.a,{allowForms:!0,src:`/about-ads?aid=${t\|\|""}`,style:d.a.absoluteFill}));t.default=n(m)}]);.//# sourceMappin gURL=https://ton.local.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.AboutThisAd.da621335.js.map.A..Eo.....?z].....GET.....OK.."…Age..251 6681"...Connection..close"...Content-Length..673"5..Content-Type.%application/javascript; charset=utf-8"%..Date..Sat, 15 Jan 2022 01:46:10 GMT"(..Etag. "94BJJNI 7kHyVLFpjb |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\148c8941f3f417fe_1**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2502 |
| Entropy (8bit): | 5.761568642550696 |
| Encrypted: | false |
| SSDEEP: | 48:prtxTAAHF185EaPLFKauDUQEwsqW2p19LQ78o/sEqb7:dLTAiibPLFK5DUQEwDlxE78o/4 |
| MD5: | 6A1DB5C1D458B47A8F24DB15EA36DF0E |
| SHA1: | B84E94CB2085333EA0E8444BEE87BFEBC6BF22BC |
| SHA-256: | 23E0723B8DA0392E94A14CA8336C01E2FE47518A2AADB55B45BD26A640D1FE6C |
| SHA-512: | 05EE460CF88243EC1D70D438C1E4D6C8B4A35D475936E7D567FED64CF8A5BFFDBE1120FCA36D68F8DE91796192D41AF2F6B6015291E4B6D2714308D7962C6A6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....N...5..q....https://abs.twimg.com/responsive-web/client-web/bundle.AboutThisAd.da621335.js.....'.....O.....h.....(S.l..`.....$L`.....Qcv .I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....4...`.....a.....Qb:jO....bv0XC.(S..`.....XL`(....`Rc,.....Qb..\.....r.....QbV.<.....o.....S. ...O...Qb..{....d.....Qb.....l.....QbJ!.....m...f.....`....Da....2.....q..... Qf.j.....AboutThisAdScreen....(S.(.`.....L`.....q...K`....Dd.....,Rc.....l`....Da. ...$.....@.-....\P.a.....N...https://abs.twimg.com/responsive-web/client-web/bundle.AboutThisAd.da621335.js..a.....D`....D`....D`..... ...`....&...&..1.&..1.&.(S.4..`"....L`.....Qc*.....match.....Qcf1.....params....Qd...B....impressionId..K`....Dg.....(...&.(...&.(.....,Rc.....`....Dar.....b.....P...q.d.....I..@.....&.(S |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\14c4235ea4350d22_0**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 259160 |
| Entropy (8bit): | 5.472871298074857 |
| Encrypted: | false |
| SSDEEP: | 3072:4n5JvcdN7dqPfDBFy0pkEqWsdgq80X+ahCf2xcOuY2Vlk/:0kdN7d07y0tqWot80X+wCPV8 |
| MD5: | 95A0EF37662E1DB6E788E80F0D01B45A |
| SHA1: | EB55F2CB4EC962723424A9BF99D6606324531201 |
| SHA-256: | 44D43E3C5B18972E469467B2D6C1D6FA8C17911443456C982C8EEF0FCCCE5A1A |
| SHA-512: | 1364CAFACEEEC163C981C68901E630F9E33CA5915E29EB3F677FD769478D0E7E2CEA5D198747A64FECBF2024862501DAAD80689A3B36D17ACC60D473192E5E5<br>D |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....U....].....https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls14.1dff23b5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[187], {"6Ag2":function(e,t,r){var i;"undefined"!=typeof window&&(i=function(){return function(e){var t={};function r(i){if(t[i])return t[i].exports;var a=t[i]={i:i,l:!1,exports:{}};return e [i].call(a.exports,a,a.exports,r),a.l=!0,a.exports}return r.m=e,r.c=t,r.d=function(e,t,i){r.o(e,t)\|\|Object.defineProperty(e,t,{enumerable:!0,get:i})},r.r=function(e){"undefined"!=t ypeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t) {if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(r.r(i),Object.defineProperty(i,"default",{enumerable:!0 ,value:e}),2&t&&"string"!=typeof e)for(var a in e)r.d(i,a,function(t){return e[t]}.bind(null,a));return i},r.n=function(e){var t=e&&e.__esMo |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\14c4235ea4350d22_1**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\14c4235ea4350d22_1**

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 454325 |
| Entropy (8bit): | 6.190080218468467 |
| Encrypted: | false |
| SSDEEP: | 6144:N7mfJmFuBWsVg+GtxiVLs2o/HWeVJ2jqoubj:xmfPLVVs2o/2OQ8bj |
| MD5: | C8FCBCE56AE82B9D115A8DFCEAA0F09B |
| SHA1: | AB2268AC82CD85A09F5133051F065F2BD1A902FD |
| SHA-256: | B87C9256CF38474C416388921655E379686D9C68FE3C6BBDEE692015F7132BDE |
| SHA-512: | C4C2DB6100D39E9F5067FEABB62643E5BA557C9FD48FD9C7F6E49151EE67658B74AF8A8E033743D1CEF02E31BA66A36EBC4055FB32A1A0B2F6722D424444032F |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....U....].....https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls14.1dff23b5.js.....'.p.....O.....].c`.....x.....p.....H.....,.....H.....p.....l.....\|.....X.....@.....h.....H.....l.....d.....4.....l.....\|.....,.....p.....$.....(S.t..`.....L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....v...`.....a.....Qb.y.....6Ag2C..Qb.f.....xy/+C.(S.@.`6.....L`.....!..(S...`.....L`>....(S...`.....PL`$.....@Rc.....Qb.Lh@....e.....QbF!.....t.....Qb..\.....r...b$.....l`. |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\164518db471458d5_0**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3638 |
| Entropy (8bit): | 5.682536818013807 |
| Encrypted: | false |
| SSDEEP: | 48:4Y58clPHA5JTQ3Hk0JrEU4nReyU7WONod9YvaQONI7UkjyFJYW0QaK4vOUNC3FFA:lwOHFrPEs76Pb54UCA02UeFph+OK |
| MD5: | 2B6C5A24F454C61EAD99D3DA60BBF604 |
| SHA1: | 8D9FB5A04CCE19DCEE8D0A74B4FB80C37B91F877 |
| SHA-256: | 9479EACF9AAD9CD5FC421676035561DF71269ADA51E8A8BADE742AC95A05F70D |
| SHA-512: | 5E1E8E1F975E34359DB60884E68EA04CF3EBEFEA556830963A2B83EA95A494F1D7E2683811344AE42C4DBFC2FDE3BF271F49A6B7EC32F17F642E1A48B9E25EFD |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O.....https://abs.twimg.com/responsive-web/client-web/loader.SignupModule.5959f915.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[179],{Ukpf:function(e,t,n){"use strict";const s={inject({callback:e,scriptId:t,src:n}){if(document.getElementById(t))e&&e();else{const s=document.createElement("script");s.src=n,s.id=t,s.async=!0,s.defer=!0,document.body.appendChild(s),s.onload=()=>{e&&e()}}},replace({callback:e,scriptId:t,src:n}){const a=document.getElementById(t);var o;a&&(null===(o=a.parentNode)\|\|void 0===o\|\|o.removeChild(a));s.inject({callback:e,scriptId:t,src:n})}};t.a=s},sojc:function(e,t,n){"use strict";n.r(t),n.d(t,"SignupModuleContainer",(function(){return B}));var s=n("KEM+"),a=n.n(s),o=n("ERkP"),c=n("UpKB"),i=n("v6aA"),l=n("0+0m"),r=n("kG2l"),u=n("3XMw"),p=n.n(u),d=n("MWbm"),m=n("rHpw"),b=n("6vad"),g=n("t62R"),y=n("/yvb"),S=n("1zbE");const k=p.a.a565833d,E=p.a.aa95ddc0,f=p.a.b50ea616,h=p.a.ie8e1ffc,C=m.a.create((e=>({buttonContainer:{marginTop:e.spaces.sp |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\164518db471458d5_1**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7263 |
| Entropy (8bit): | 6.081487113431314 |
| Encrypted: | false |
| SSDEEP: | 192:ru0iYdjfArMxiD6990uuUP/k6uxUu7lz0EL4xuv0GBWZr/Rv:IOjfArMxG6990IPNG7lsuv02WZrR |
| MD5: | 9514CF7EF5BD050E60DD201A97CCFB1B |
| SHA1: | 616AE4082C3B1064526DF8FC79DAC95859CC0FAF |
| SHA-256: | 1052A951519041011AE30119CA6ADCE8564CAB2F01469153E14DD0E4D4840FE7 |
| SHA-512: | 71585F4977B9F499F903B1048886DE212CBC24E4BBBC5C1D522535ECA1686DD49C96A11054406B87758EBE3995AB5F9C12B65E4B6594327118878D1FBD61E074 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O.....https://abs.twimg.com/responsive-web/client-web/loader.SignupModule.5959f915.js.....'.a.....O.....u.(.....(S.t..`.....,L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....f...`.....a.....Qb"..9....UkpfC..Qb"}.o....sojcC.(S.L.`T....$L`.....0Rc.....Qb2.....s...`....Q.`....Da.....a.....Qcz.)Z....inject..C..Qc._8.....replace.C.(S...`.....DL`.....4Rc.....Qb.Lh@....e...`.....`....Da....p.....1...Qcf..}....callback..Qc*.v.....scriptId..QbjLj.....src...Qc.N.u....document..Qe.X.8....getElementById....QeZ.....createElement....9...Qb.....id.....Qc.....defer.....Qb..(+....body..Qd28.....appendChild..(S.4.`"....L`.....a...K`....Dg.....&.\.....,Rc.....I`....DaT...l.....b.....@.-....\P.a.....O...https://abs.twimg.com/responsive-web/client-web/loader.SignupModule.5959f915.js.a. |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\16748c84e647c086_0**

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

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\16748c84e647c086_0**

| | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 225377 |
| Entropy (8bit): | 5.304612124984646 |
| Encrypted: | false |
| SSDEEP: | 6144:Vy0gCa/AlToRJ2jWJZwAf/QZnFtfl5HKGVhSbicXWpQXSd:Vy0g5/AlTs2kZwLZnFtfl5HKGVh0ibQE |
| MD5: | 1CFA7D6DA375519AC378B6063670E864 |
| SHA1: | CB25D6CFCA929E985D12D4AB5CF5FEC9633DA80A |
| SHA-256: | B773A6863E3EF075A0B72AE67FE3D3681A8CED24A26C6B6A5BAF0F7314A979DA |
| SHA-512: | 39753B5E93B8429B40DB52EAB5C0509E0D6CC3D381C8D626127070D9055A42561A8EAB991415EA9700491CBA93D46821D963609749BC663511C40BEF80396563 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....F....*.b....https://abs.twimg.com/responsive-web/client-web/bundle.Ocf.b6692a75.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[76,172],{"0ULw":function(e,t,a){"use strict";var s=a("ERkP"),n=a("Lsrn"),i=a("k/Ka");const r=(e={})=>Object(i.a)("svg",{...e,accessibilityHidden:void 0===e.accessibilityLabel,style:[n.a.root,e.style],viewBox:"0 0 24 24"},s.createElement("g",null,s.createElement("path",{d:"M12 22.75C6.072 22.75 1.25 17.928 1.25 12S6.072 1.25 12 1.25 22.75 6.072 22.75 12 17.928 22.75 12 22.75zm0-20C6.9 2.75 2.75 6.9 2.75 12S6.9 21.25 12 21.25s9.25-4.15 9.25-9.25S17.1 2.75 12 2.75z"})));r.metadata={width:24,height:24},t.a=r},"12XZ":function(e,t,a){"use strict";a.r(t);var s=a("97Jx"),n=a.n(s),i=a("ERkP"),r=a("9D1O"),o=a("gPQO");t.default=e=>i.createElement(o.a,n()({},e,{ocfModule:r.i}))},"180P":function(e,t,a){"use strict";a.d(t,"a",(function(){return s}));const s=e=>{const t=(JSON.stringify(e)\|\|"").split("");t.sort();const a=t.join("");return n(a,0).toString()} |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\16748c84e647c086_1**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 475974 |
| Entropy (8bit): | 6.196187917675436 |
| Encrypted: | false |
| SSDEEP: | 6144:LevZyPwvJvXzhiPRV0umtqaMS5bSX+QD6+ds/cycFK5LCqPKPGO+N:4gPwvJ/zhhoPs9ueO+N |
| MD5: | B943AAB06253D7BFFDEB8D31E6C25044 |
| SHA1: | A1F86A573F4B263ABE7B957BF4C1175D87487DAC |
| SHA-256: | 96793AAB111B4F6B206E286DFD32151804B95AEF0E47037369E0C72BD3901E38 |
| SHA-512: | 9EA6A740804A8FAD9ECFF98A661495BB05E48DFDD82F37BD49A091DFBEC838CFCA83B183F2F4BC0D0CCCB225B5C8957954CB5907BD8996B800CB261B52B8BEA |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....F....*.b....https://abs.twimg.com/responsive-web/client-web/bundle.Ocf.b6692a75.js.....'..l....O.....@...S.....l.....H.....d.....\.....P....8.....X.....d.....X.....$.....8..... .....l.....L.....<...D.....x.....(S....`.....U.L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Mb.....X...`.....E...a.....Qb*/.....0ULwC..QbN@g.....12XZC..QbvB.s....180PC..Qb../.....2DawC..Qb2.%.....3GUVC..Qb...8....4BrDC..Qb.$k.....53j7C..QbVS#.....5UIDC..Qb. .....6D0RC..QbB.....6XNvC. |

**C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\189f452556e62e81_0**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1672 |
| Entropy (8bit): | 6.071742849351518 |
| Encrypted: | false |
| SSDEEP: | 48:X458ekjTmsb32j0QWUJeK4409NY3FFuBY2Oj7y1ktG/:fjTvGj0QPYPAFABY2Yv0 |
| MD5: | 2FA2A8952C3FB2A98C4C8C242430934E |
| SHA1: | 7C184AEA56A92601FB1B622D118B40B704A0A0A0 |
| SHA-256: | BF9160F97D77FED55FE5708F5E679F4FF17A2FB8340D02F559A2D9A11EA3EA8C |
| SHA-512: | C9492FD7A399AFA3EF385D52332EAE5D14BE9230DD2649A3FBA23BBBA4AE2AE637ACC7C53192BBDA63864C592D171827822D118C3D9197FD4F3A343AF8682EE0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....L.....e.....https://abs.twimg.com/responsive-web/client-web/loader.AudioDock.66ab3be5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[164],{"8W85":function(e,n,t){"use strict";t("ERkP");var c=t("zb92");n.a=Object(c.a)({loader:()=>Promise.all([t.e(24),t.e(165)]).then(t.bind(null,"u2Vg")).then((e=>({default:e.__DANGEROUS_IMPORT__}))))}},KfhW:function(e,n,t){"use strict";t.r(n),t.d(n,"__DANGEROUS_IMPORT__",(function(){return u}));var c=t("ERkP"),r=t("8W85"),a=t("LxAE");function o(e){const{config:n}=Object(a.a)();return c.createElement(c.Fragment,null,n.dock(e),c.createElement(r.a,n.player()))}const u=function(e){return c.createElement(o,e)}}]);.//# sourceMappingURL=https://ton.local.twitter.com/responsive-web-internal/sourcemaps/client-web/loader.AudioDock.66ab3be5.js.map.A..Eo.....F.....GET.....OK.."...Age..2516662"...Content-Length..699"5..Content-Type.%application/javascript; charset=utf-8"%..Date..Sat, 15 Jan 2022 01:46:06 GMT"(..Etag. "lgFF5Eb84z5U1v |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\189f452556e62e81_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2692 |
| Entropy (8bit): | 5.601246413434071 |
| Encrypted: | false |
| SSDEEP: | 48:XWrMccXbohyN9FIo/3ngH5FAI8CwqWyZG1dzqsow/sEFe+:mgcBy1XgH5r8C3jZG3zqfw/1 |
| MD5: | AA82D9AA8A8E60A6603F21EF9DD6EB67 |
| SHA1: | 122B341761B51DD232934C2773B29DF6903936C3 |
| SHA-256: | CA4FE021332FB9A60867F43E08951B15B30DC1BFBD94B2545A1FA32328B66ED7 |
| SHA-512: | 7F0EBDCA617ECCAA3FAF5D10061F8912F2038CF45300027A68A5DE8EF39D7A042DE9072541941FAE03EA5F275EEA43BEBF9442AFFA23A3235A30DDA216467A74 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....L.....e.....https://abs.twimg.com/responsive-web/client-web/loader.AudioDock.66ab3be5.js.....'.....O.....[CCB.....@.....(S.t..`.....,L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....H...`.....a.....QbNqe.....8W85C..Qb*.....KfhWC.(S.p.`.....(L`.....0Rc.....QbF!.....t...`$.....Q.`....Da.....Qb>..>....ERkP..Qb..^q....zb92.....M....a.....QcR.....loader..C.(S...`.....(L`.....:....`.....Lb.....Qb.Lh@....e.....Qb..E.....u2Vg.(S.4..`".....L`.....a.....a.C. Qf..._....__DANGEROUS_IMPORT__...K`....Dg.....}..)&.(.../...%....,Rc.....I`....Da.....b.....@.-....XP.Q.....L...https://abs.twimg.com/responsive-web/client-web/loader.AudioDock.66ab3be5.jsa.....D`....D`....D`.....(...`....&...&....&....&....&.(S.|..`.....0L`.....PRc$.....Qb.i.....c.....Qb..\.....r.....M...QbV.<.....o.....R..d... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1cc133455a4ec66f_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1694 |
| Entropy (8bit): | 6.036274433240379 |
| Encrypted: | false |
| SSDEEP: | 48:99OT58Jz4OmUmPX391WODeFK4ZX3FFxgi1DOuwThSl:9RmLPN1IfdFzL1NwTYl |
| MD5: | 21450E444816E8347D5808FDECFB0D51 |
| SHA1: | B2A38658DA9D0ED81898966D72DA42F66999CF99 |
| SHA-256: | C6003D21889AECA65E3C0FAAF093D3D2E42ABCDDED84D5040BC394BF34C896E1 |
| SHA-512: | 178B2ECD309DF6D984A12CBF8EA41D25A09043B7E9CA2D8F92682CE2837B2001907F7FBFC12A42047FA0EEE29A0B0E007C69FBB642F5503F0F3D639D6335CB5A |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....R...y.....https://abs.twimg.com/responsive-web/client-web/bundle.ProfileRedirect.aab51c95.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[79],{dgvO:function(e,r,t){"use strict";t.r(r),t.d(r,"ProfileRedirect",(function(){return p}));t("MvUL");var n=t("ERkP"),c=t("G6rE"),s=t("rxPX");const o=e=>{const r=c.e.selectLoggedInUser(e);return r?r.screen_name:void 0};var a=Object(s.a)().propsFromState(((()=>({screenName:o})))),u=t("kGix"),i=t("v//M");const d=()=>null,p=e=>{const{history:r,screenName:t}=e;return n.useEffect(((()=>{r.replace(`/${t\|\|""}`)})),[r,t]),n.createElement(i.a,{fetchStatus:u.a.LOADING,render:d})};r.default=a(p)}]);.//# sourceMappingURL=https://ton.local.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.ProfileRedirect.aab51c95.js.map.A..Eo.....JN.....GET.....OK.."...Age..3721962"...Connection..close"...Content-Length..681"5..Content-Type.%application/javascript; charset=utf-8"%..Date..Sat, 15 Jan 2022 01:46:25 GMT"(..Etag. "fcRvT |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1cc133455a4ec66f_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2850 |
| Entropy (8bit): | 5.609833994271585 |
| Encrypted: | false |
| SSDEEP: | 48:99OUhuSJilnvOwbBaW1uF+PNylSvwaG2uc+DWOHwo/sEq37jI:9bzcln7lF1Mg8SYaG2ucQyo/gE |
| MD5: | E49DD9E37B4AE89A0D245C5B14E01A18 |
| SHA1: | 501D81B7BC233001483869D268F9A706368BBE40 |
| SHA-256: | 0F4168A731D122633ED579D24F2BC6557F34C3B8B1BD8E14D1D5C3FACFD65838 |
| SHA-512: | 271C338768DE50863A9A23102D4CE28A3ED3B8F06BF5476D1A5FC5F2DAC2E518C5AC912C2ECA1B2EBAD5BC411DBAD0A546DED088D7888103F9F27CAE720D69C |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....R...y.....https://abs.twimg.com/responsive-web/client-web/bundle.ProfileRedirect.aab51c95.js.....'.....O....`....d.....(S.l..`.....$L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....a.....Qb.6.M....dgvOC.(S..`n....TL`&....`Rc,.....Qb.~d....n.....Qb.i.....c.....QbV.<.....o.....R.....S...Qb..{....d.....Qb.....p...f.....`....Da....:.....Qb..\.....r.....Qe.....ProfileRedirect..(S.(.`.....L`.....K`....Dd.....,Rc.....I`....Da.... .....@.-....`P.q.....R...https://abs.twimg.com/responsive-web/client-web/bundle.ProfileRedirect.aab51c95.js..a.....D`....D`n...D`.....(...`....&...&..1.&....&.(S.D..`B.....L`.....Qb.Lh@....e.... Qf.....selectLoggedInUser....Qd..1.....screen_name...K`....Dk.....&.(...&.(...&.Y....&...(.....,Rc.....`....Da....".....c. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1e03bb4be0212ad9_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7971 |
| Entropy (8bit): | 5.518866059494555 |
| Encrypted: | false |
| SSDEEP: | 96:n6dy5Kr59l0tpb7BHK/RKqd/T5V+vGC+lkrkxiUiTlLsYj26Hk/FrGJ26j1aCxxY:n6dy5KrnxVER+vv+S75LsfMJtYCxP1o |
| MD5: | CC36E9981FA6B73CF2705ADCE6545AF4 |
| SHA1: | A00917349C5B57CB4CC37C610A1D7E9331A4330B |
| SHA-256: | CDAEB6F41D2118A60B9AED3EF36C81E36B22BA0BE0C78FC4DDD1C18CE63BB16B |
| SHA-512: | 8925A57C00E4C2B8B8111540A2D0C544109634B7CD7CFEE4B6F030ABD6605606E32C0CC6039141B63C2693AE508F63AE3CBCAF21B6ED2271D30F9B8D90EE512 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....^... >.....https://abs.twimg.com/responsive-web/client-web/bundle.SettingsProfessionalProfile.9a16b4b5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[89],{"6kA7":function(e,t,a){"use strict";a.r(t),a.d(t,"ProfessionalProfileScreen",(function(){return G}));var o=a("mC9n"),n=a("ERkP"),r=a("1YZw"),s=a("G6rE"),i=a("rxPX"),c=a("0KEI");var l=Object(i.a)().propsFromState((()=>({loggedInUser:s.e.selectLoggedInUser}))).propsFromActions((()=>({addToast:r.b,createLocalApiErrorHandler:Object(c.createLocalApiErrorHandlerWithContextFactory)("SETTINGS_PROFESSIONAL_PROFILE_SCREEN"),switchToNonProfessional:s.e.switchToNonProfessional,updateProfessionalCategoryDisplay:s.e.updateProfessionalCategoryDisplay,updateProfessionalType:s.e.updateProfessionalType}))).withAnalytics((()=>({page:"professional_settings"})),p=a("jHSc"),d=a("3XMw"),u=a.n(d),m=a("tl3i"),b=a.n(m),f=a("MWbm"),y=a("feu+"),g=a("cHvH"),h=a("rHpw"),L=a("sgih"),w=a("/yvb");const C=u.a.cfd2f35d,E={actionLabel:u.a.ia492079,seconda |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1e03bb4be0212ad9_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 18694 |
| Entropy (8bit): | 6.227103102132686 |
| Encrypted: | false |
| SSDEEP: | 384:r8iBREcCAhvb1FKQN+HkNz1kimdtexpS1J5w1ivBZ9DyJ4hGzSbid:IwCAB6doYw2yIu |
| MD5: | D7E4A663346894675C5D54613BBC89CE |
| SHA1: | E65BA87FF38AB993DD4A91259B78056875DA5ED0 |
| SHA-256: | E0E14652397B4EF6D9A64F058441ECB0B97FB72E4BD6A5E4F405EB3857EED983 |
| SHA-512: | 1C7CF267596A71E2B9AE13EC6A8A472E88B72A09B41A6ECAC249367BDB0881116DDA6E7531EDC34DEC4BE6ABEAB5B559D17520ECC645DE1F7B564E6E02A926D9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....^... >.....https://abs.twimg.com/responsive-web/client-web/bundle.SettingsProfessionalProfile.9a16b4b5.js.....'.....O.... H..%Aq.....h.....\|.....(S.t..`.....,L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....a.....Qb:.....6kA7C..Qb.....jtO7C.(S.]..`r....9.L`.....I.Rc.....H.....QbV.<.....o.....Qb.~d....n.....Qb..\.....r.....Qb2.....s.....Qb.i.....c.....Qb.....p.....O...Qb.%.....f.....Qb.....y.....QbR.....h.....Qb.~k.....L.....Qb.G.....w....Qb";.....C.....Qb...*....E.....Qbz.\|.....T.....Qb.....D.....Qb>. .....k.....Qb&..u....P.....Qb..(&....S.....QbvP4C....I.....Qb.#....._.....Qbj.B.....v.....Qb.&U.....H.....Qb.1.2....x.....Qb...}...A.....Qb..]....B.....Qb..y.....z.....Qb6h.....j.....Qb2.....F.....QbF.....R.....Qb..J.....O.....Qb..}.....M.....Qb..#.....N.....Qb^L'.....G.....Qb"r.....U....A..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1e3a9727aa406da6_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8802 |
| Entropy (8bit): | 5.557200396821371 |
| Encrypted: | false |
| SSDEEP: | 192:hibTwRTZ1paxNJeIt2BMUOMUeMUqDFA8Tf81Wr1roqTf4EKTRubaJZRm:h/RTZ1aNJVt2BMUOMUeMUqZAcP1oHpu/ |
| MD5: | BAE0978EB950E657945EEC1D9843E331 |
| SHA1: | D07369D447A84150D9A9CA224CDEE23F4A926C9D |
| SHA-256: | 39F3A58A9D5BC685F7F71F389056F3349FDC2599034B8BD38C9F1C836C3D5164 |
| SHA-512: | FA72CAF4804BCA8D8D5FD1BDEA8E16F3661A3D6A27F9B2F8BE788412BDA03D672CACABE04ECC2E50C4370137E9259B31A02B35FD85EE2E59D7B59B1D7E73F5E8 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....U...aq8'....https://abs.twimg.com/responsive-web/client-web/bundle.QuoteTweetActivity.6fdbbba5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[80],{"3X8/":function(e,t,r){"use strict";r.d(t,"a",(function(){return c}));var a=r("k49u"),n=r("LVU8"),s=r("3XMw");const i=r.n(s).a.i1801686,c={[a.a.GenericForbidden]:{toast:Object(n.a)()},[a.a.InvalidRequestUrl]:{toast:{text:i,withClearButton:!0}},showToast:!0}},"6M1P":function(e,t,r){"use strict";var a=r("WpDa"),n=r("rJrz"),s=r("ZNT5");t.a=e=>Object(s.a)({timelineId:`retweetersGraphQL-${e}`,getEndpoint:e=>e.TweetActivity.fetchRetweetedBy,getEndpointParams:({count:t,cursor:r})=>({count:t,cursor:"string"==typeof r?r:void 0,tweetId:e}),formatResponse:a.a,context:"FETCH_TWEET_ACTIVITY_RETWEETS",perfKey:"retweetersGraphQL",staleIntervalMs:n.a})},PH3B:function(e,t,r){"use strict";var a=r("ezF+");var n=Object.freeze({Cell:"Cell",PreviewCard:"PreviewCard"}),s=r("XBtf");const i={loader:()=>r.e(337).then(r.bind(null,"a+ad")),loaderKey |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1e3a9727aa406da6_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 22165 |
| Entropy (8bit): | 6.021832134645767 |
| Encrypted: | false |
| SSDEEP: | 384:NSG8xBA5aoAf/wQ5K/rzE4+RcY4rrwBx7lQTa/81hK:NknNf/i8RD4YXUQZM |
| MD5: | FD7AEE494F24AEF137C958D8431CEA5F |
| SHA1: | 65AA1A991F5EB93C07F235F469C8C67735345BF4 |
| SHA-256: | C756EFED0F4DA9757A1601D2FCF6B676A494249AFF5528EA931A77829EEC6508 |
| SHA-512: | 7B8D2083796E2B8AF60A1E9306160D8BA6CE57A13A1481AFC78C8D4FB3ED5425EF435F0E1C1D5B5E773824DD991241476FF9393F0F5DD0849C8061FADE59AFA |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....U...aq8'....https://abs.twimg.com/responsive-web/client-web/bundle.QuoteTweetActivity.6fdbbba5.js.....'.f.....O.....U..#..`.....(S.....`.....dL`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....T..a&.....Qb.....3X8/C..Qb..S.....6M1PC..Qb.....PH3BC..Qb.....SCGqC..Qb.....h2muC..Qb6j3.....i6ORC..Qb...Q....rJrzC..Qb&Y.....u3ZEC..Qb.2<....zgaLC.(S..`.....TL`&....0Rc.....Qb.i.....c...`.....`....Da....x.....Qb..{....d.....M..(S.(.`.....L`.....K`....Dd.....,Rc.....l`....Da.....@.-....dP.....U...https://abs.twimg.com/responsive-web/client-web/bundle.QuoteTweetActivity.6fdbbba5.js...a.....D`....D`p...D`.....`h...&...&..1.&..!.&.(S.P..`Z.... L`.....@Rc.....M...Qb.~d....n.....Qb2.....s...b.....1.`....Da....~.....Qb.[.....WpDa..q...Qb.w.....ZNT5.(S...`..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1eee3b6de180dc19_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 26438 |
| Entropy (8bit): | 5.540051700246954 |
| Encrypted: | false |
| SSDEEP: | 768:6Vsp+MCZbk3rcW3DVP5oOXZ0u2ZE/kh3t9hHWfGrfzV1sjDxAmsHdop2TH:Y9ewrDLzV1sjimsHK6 |
| MD5: | B68AF5C4710D3B662B4FA6B42D7C8E64 |
| SHA1: | 2EB844F06C8203452930B3B42D0909610E39B53B |
| SHA-256: | E637807C8EBD2D0C5E41FB482D19A5F2601411678FAAE7B5C49A4A6779491B4E |
| SHA-512: | 6CD26803FB08FA16FEE3809409EA0DAEE6BD60AB15D66E1BFDBBBA2236F2AB0AA030B095D78B1324493956B06DA971C08733289E95CD75FBB8BB7027746129DC |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....a...."D....https://abs.twimg.com/responsive-web/client-web/shared~loader.DashMenu~bundle.Account.c6a8f0d5.js(window.webpackJsonp=window.webpackJsonp||[]).push([[20],{"45lU":function(e,t,i){"use strict";const l=i("rHpw").a.create((e=>({backgroundArea:{backgroundColor:e.colors.activeBlack},drawer:{maxWidth:"70%"},wrapper:{alignSelf:"flex-start",backgroundColor:e.colors.navigationBackground,boxShadow:e.boxShadows.medium,overflowY:"auto",overscrollBehavior:"contain",WebkitOverflowScrolling:"touch"},header:{flexGrow:0,flexShrink:0},scrollableItems:{overflow:"auto",overscrollBehavior:"contain",WebkitOverflowScrolling:"touch",flexGrow:1,flexShrink:1},scrollableContentPadding:{paddingBottom:"44px"},item:{paddingVertical:e.spaces.space16,paddingHorizontal:e.spaces.space16,flexDirection:"row",flexGrow:1},itemAccount:{paddingBottom:0,paddingTop:e.spaces.space12,backgroundClip:"content-box",backgroundColor:e.colors.navigationBackground,flexDirection:"row",alignItems:"center"},avatarWr |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\1eee3b6de180dc19_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 45585 |
| Entropy (8bit): | 6.367526636202449 |
| Encrypted: | false |
| SSDEEP: | 768:22pD1cMotZX731OaIJQwijGP7NV9h3/HhHWzlFGbkOEYGAzpKAtfkT6WuEMD1QEN:265ratZOaIJTijGP7/nN4KFfMOTHzqZY |
| MD5: | 1E0C057F8C07353B9C90876FDD2FF5C3 |
| SHA1: | 333CDD8185612C988AC32DC66B949A0B2EA8CDE1 |
| SHA-256: | 844A6050B45F2EE567F55611159FA4984D59B0AB7D978FC6B866338F624AC857 |
| SHA-512: | A2E3C5E343F47A6533CA5FCB810E0CA9659BFFB20FAE87263061E714E6CCD6F99134A7712F27DE78A1921D9BFC8846C59543EF2525C5898C1A7E465C360585FF |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....a...."D....https://abs.twimg.com/responsive-web/client-web/shared~loader.DashMenu~bundle.Account.c6a8f0d5.js.....'./c....O.....4.....`.....D.....x.....H.....(S....`.....dL`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....(...`.....T..a&.....Qb.J<_....45lUC..Qb.....45mFC..Qb...8....4BrDC..Qb.0.k....9qNnC..QbZJN-....Drq4C..Qb.....Q3sgC..Qb.bJ.....SNySC..Qb.....VN5nC..Qbn.(.....nV1zC.(S.P.`V.....L`.....QbJ.){....rHpw..M...QcB.5,....create...(S....`,.....L`b.....aV.....Qe..(j....backgroundArea..C..Qc.O.....drawer.....a.....Qcb.0k....maxWidth..Qb.j].....70%...Qc&..N....wrapper.C..Qcz.....header.....a.....Qc.....flexGrow`.....Qd.laR....flexShrink..`.....Qej.b.....scrollableItems..4.a.....Qc.._.....overflow.... Qf.U2....overscrollBehavior....QcJ..0....contain..$Qg.&sb....WebkitOverflowScrolling...Qc.....touch.....1 |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2155d2b7ce818f61_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 17940 |
| Entropy (8bit): | 5.525601752311792 |
| Encrypted: | false |
| SSDEEP: | 384:kUybKz+3Jlkqe0glaaHH5f9HBP8KeOqmfnq19TTbiMshElQj8yj7pDs9:/yboKlk1L3HH5fFByX4nq19HbiMstA8P |
| MD5: | 2279AA2409659269DA010DC16DEE6678 |
| SHA1: | AA71211DD91EB8A4A0D8FED090A9A588DDE7DEC0 |
| SHA-256: | 466A9116F50FA6463224A617C81323D22970AB723798A1FF8463CEA54FD00B97 |
| SHA-512: | 0D5E6CA4A4CA62479D8A6013156A75B567C90333D1BD4725016D13DAB46C782F2BC5F5C09C31032E05B17E4967C2807A6F18B1664DAA7A2CCD09C645F40FA54 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....u....*L;....https://abs.twimg.com/responsive-web/client-web/shared~ondemand.SettingsRevamp~ondemand.SettingsInternals.53e0bf15.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[25],{EPsT:function(e,t,n){"use strict";n.d(t,"a",(function(){return o}));var r=n("KEM+"),a=n.n(r),s=n("ERkP"),c=n("jtO7"),i=n("eb3s");class o extends s.Component{constructor(e){super(e),a()(this,"_handleClick",(e=>{this.setState({showConfirmation:!0})})),a()(this,"_handleCancel",(()=>{this.setState({showConfirmation:!1})})),a()(this,"_handleConfirm",(()=>{this.setState({showConfirmation:!1}),this.props.onConfirmationSheetConfirm()})),this.state={showConfirmation:!1}}render(){const{align:e,color:t,confirmationSheetConfirmButtonLabel:n,confirmationSheetConfirmButtonType:r,confirmationSheetHeadline:a,confirmationSheetText:o,label:l}=this.props;return s.createElement(s.Fragment,null,s.createElement(c.a,{align:e,color:t,label:l,onPress:this._handleClick}),this.state.showConfirmation?s.createElement(i |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2155d2b7ce818f61_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 45437 |
| Entropy (8bit): | 5.9774410054662015 |
| Encrypted: | false |
| SSDEEP: | 768:YXyY8iZ4khDeK62t/na0vfk4OKPpTYqx3884RjU:YX9kkhqUvfsGlh18D2 |
| MD5: | DF735A24782C6B408D8012E0BE1D0FEC |
| SHA1: | B0DC232827C3ED85334EFEE1D38F050C8C59185B |
| SHA-256: | 15CB28DA52CB5EA17266E377626936ED2DFD466CD375A70871632E7E2C184C81 |
| SHA-512: | 784225943EB0DB8AEC2DC92D5C086314DE5611504B0EC4B619F8EB704519F2822DAE040430F421DB5782C267AB48A53FCAD96C864081FF12594432B1E096AB14 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....u....*L;....https://abs.twimg.com/responsive-web/client-web/shared~ondemand.SettingsRevamp~ondemand.SettingsInternals.53e0bf15.js.....'..A....O....`...6ka.....(.....(S....`>....\|L`:.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....2...`....l..a2.....Qbj:lb....EPsTC..Qb2.9.....FDFLC..Qb&7O.....OySiC..Qb.....S/HTC..QbJ'.d....Y3cQC..Qb.....ZvNXC..Qb.....atVNC..Qb...x....dZRFC..Qb.o.>....eM8gC..Qb.[_l....hBohC..Qb.....jtO7C..Qb..E.....uo4SC.(S...`<....DL`.....PRc$.....M...Qb2.....s.....Qb.i.....c.....S...QbV.<.....o...d.....`....Da....&.....Qb..{....d.....(S.(.`.....L`.....K`....Dd.....,Rc.....l`....Da.....@.-.....P.....u...https://abs.twimg.com/responsive-web/client-web/shared~ondemand.SettingsRevamp~ondemand.SettingsInternals.53e0bf15.js...a..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\21c30643f59a0773_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5705 |
| Entropy (8bit): | 5.630542095734853 |
| Encrypted: | false |
| SSDEEP: | 96:yu6f5oPsrXFNrbcyNbX78bLt9UlJyKfFCrQUYM1F24dqD+krxjzFSRspw3h:yu6BKEFOAL02JyaeaMu4crxjw++ |
| MD5: | F71E2F5497B5DB763D4A093F645FCE24 |
| SHA1: | 9B98A49D6A528779D714FED5D67D6E872692E63B |
| SHA-256: | C99B45F8FCA1454E46B3F802D3F0E2FD78AC4DD32CFF431492A5DBDFED1B0FF8 |
| SHA-512: | C2822D4958083A07E9309B85DC52006A71E15044AB297D867C7724DE938FCE1410CA4C77324D0E2A0EEA298C2BDCC5880D71896759E050E41F914E8CBD6E6C0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....T.....3....https://abs.twimg.com/responsive-web/client-web/bundle.KeyboardShortcuts.023210e5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[61],{"5VcM":function(e,t,a){"use strict";a.r(t),a.d(t,"KeyboardShortcutsScreen",(function(){return T}));a("MvUL");var s=a("ERkP"),r=a("v6aA"),i=a("hqKg"),n=a("G6rE"),o=a("oEGd");const c=Object(i.createSelector)(n.e.selectLoggedInUser,(e=>({loggedInUserScreenName:e&&e.screen_name})));var l=Object(o.c)(c),d=a("jHSc"),u=a("ObVQ"),p=a("3XMw"),m=a.n(p),b=a("MWbm"),y=a("7N4s"),g=a("k/OQ"),h=a("6vad"),v=a("t62R"),k=a("rHpw"),f=a("7JQg"),w=a("OrGc");const E=m.a.dfef5ab8,x=m.a.h54e6137,P=m.a.aefd89c7,O=m.a.cafdefb1,R=m.a.add55c97,S=m.a.e95b9448,j=m.a.c106055a,T=({history:e,location:t,loggedInUserScreenName:a})=>{var i,n;const{featureSwitches:o,userClaims:c}=s.useContext(r.a),{isModal:l}=s.useContext(y.b),p=null===(i=t.state)\|\|void 0===i\|\|null===(n=i.previousPath)\|\|void 0===n?void 0:n.includes("/i/moment_maker"),[m,v]=s.useState(!1);s.us |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\21c30643f59a0773_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 12420 |
| Entropy (8bit): | 6.2257471943329845 |
| Encrypted: | false |
| SSDEEP: | 384:y7MLFH60rx6Zq8r8adlwNeTfzL2xQb+q7bSvFkQ:y7MlT6+76bz72F |
| MD5: | AF2C1350F6048D19681DE1AD45538766 |
| SHA1: | D8BB31FE5FEEB0F5A0B563C25B38BE56C82A53A2 |
| SHA-256: | 7095DCCCCB99D6CC23ED2BA6E8B1B8129016FACECEB4C76089E9581228EF3E29 |
| SHA-512: | D0C4509E33769D5A15D892202BBF8115A2669340B5557E5ACDE52070087CB6D1BED78731D0641BFFFD55AF2284128D64C6B6430E7D46950C4D9D6062D128A5A/ |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....T.....3....https://abs.twimg.com/responsive-web/client-web/bundle.KeyboardShortcuts.023210e5.js.....'.O.....O...../.....(S.t..`.....,L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....z...`........a.....Qbr,\|L....5VcMC..Qb..V.....ObVQC.(S....`.....L`V.....Rc`.....(.....Qb2.....s.....Qb..\....r.....Qb..{....d.....R.....O...Qb.....y.....QbR.....h.....Qbj.B.....v.....Qb.G.....w.....Qb...*....E.....Qb.1.2....x.....Qb&..u....P.....Qb..J.....O.....QbF.....R.....Qb..(&....S.....Qb6h.....j.....Qbz.\|.....T.....QbvP4C....I.....Qb..}.....M...s.....Q.`....Da.....$Qg.....KeyboardShortcutsScreen..(S.(..`.....L`.....K`....Dd.....,Rc.....I`....Da....4.....q.....@.-....`P.q.....T...https://abs.twimg.com/responsive-web/client-web/bundl |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\22d523363d792eeb_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 25568 |
| Entropy (8bit): | 5.360336785464234 |
| Encrypted: | false |
| SSDEEP: | 768:/vrhZ9sXKY5N4r2D9XGqmkVvPGWXmmdc6A0N18lnN9m+uEX8l9UFSuE/o:X8M2raUw |
| MD5: | 829AAB1A654DC8BD170C528A8F8A0B17 |
| SHA1: | 77C4B9A5DD6E6209CB6BEB8EB366C90D3C83E72E |
| SHA-256: | DF9C9471839DA0F883DDE95AE74952D8D17EB7B88CC747B3C99E4945263719D9 |
| SHA-512: | 261838AC6DC65AA2C4F0CDEF68F56E216FBAED443E4F044C849975713E2A83BA0CDF482CAAA9EC86A6816DB2F863419CD16A100FFEC7204145006D8FC54E8C0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....X....I.....https://abs.twimg.com/responsive-web/client-web/bundle.SuperFollowsSubscribe.63e9f065.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[95],{"21nk":function(e,r,a){"use strict";var t=a("l9iR"),n=a("3KVO"),l=a("yLYC"),i=a("Ud88"),s=(a("/2Cm"),a("aQQo").useTrackLoadQueryInRender),o=(a("ERkP").useDebugValue,a("K1lQ").__internal),c=o.fetchQueryDeduped,u=o.fetchQuery;e.exports=function(e,r,a){s();var o,d=i(),p=r.fetchKey,m=r.fetchPolicy,g=r.source,y=r.variables,f=r.networkCacheConfig,b=l(e,y,f);if("PreloadedQuery_DEPRECATED"===r.kind)b.request.node.params.name!==r.name&&t(!1),o={componentDisplayName:"usePreloadedQuery()",fetchKey:p,fetchObservable:c(d,b.request.identifier,(function(){return d===r.environment&&null!=g?d.executeWithSource({operation:b,source:g}):d.execute({operation:b})})),fetchPolicy:m,query:b,renderPolicy:null==a?void 0:a.UNSTABLE_renderPolicy};else{var h=u(d,b);o={componentDisplayName:"usePreloadedQuery()",fetchObservable:null!=g&&d===r.environ |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\22d523363d792eeb_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 49416 |
| Entropy (8bit): | 6.170749881408058 |
| Encrypted: | false |
| SSDEEP: | 768:59pk8hWXMnC0ZsAiTNlJnt0dQtE2mRjaq5movTqw5wYBhnuDgpJGx:59dhmGzaBnt0OmHh76l |
| MD5: | AE7E85CB9C3219691F657DF7A1043ED5 |
| SHA1: | 4E2CA198472AC82604319DA68E2D154293AA4360 |
| SHA-256: | 5239AD513C519CD02A47F4A0A464DEBF7CD766E2FFA5067E5ADF1E9A6004BA0F |
| SHA-512: | B72F66C4FF14B32F9207DBDBE5EBF4AF63A9B3E025BB9223A370FDB80691AFBA7B2AEB0B489BF73AD7349CAC12E40B68097007CFD0FBE0683D245F8396A75D12 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....X....I.....https://abs.twimg.com/responsive-web/client-web/bundle.SuperFollowsSubscribe.63e9f065.js.....'.._....O.....L.....x.....H.....(S....`n.....L`F.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....a>.....Qb..I.....21nkC..Qbr..7....23AnC..Qb^.....9RBuC..Qb:9.....9VLyC..Qb6b.....E0ztC..Qb.!.....FEMQC..Qb2.....ID86C..Qb..MK....JWc1C..Qb.....XcCAC..Qb..:.....a2FhC..Qb..\....ahKCC..Qb..:....bCEwC..Qb...P....kbWRC..Qb2.....l62vC..Qb.....n0RlC.(S...`.....HL` ....`Rc,.....QbF!.....t.....Qb.~d....n.....Qb.....l.....S...Qb2.....s.....Qb.i.....c.....R..f.....1.`....Da.....Qb.6 <....l9iR..QbR.Q....3KVO..QbZU.....yLYC..Qb.....Ud88..Qb...T..../2Cm..Qb.j.,....aQQo.(Qh^..[....useTrackLoadQueryInRender.....Qb>..>....ERkP..Qe...J....useDebugValue.....QbRg.....K1lQ..Qd |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\28854cce14dd368d_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 52000 |
| Entropy (8bit): | 5.409036207103873 |
| Encrypted: | false |
| SSDEEP: | 1536:RTsLeNrYEAFW6zXstxt2ekoG4j6Wn7Hqn1FFytWeWLZHf1h01Z6b6m:Tvx2t4w/ |
| MD5: | BF9A675169E1753899C3388C6EFB0152 |
| SHA1: | B2BE43A75562FCDFE37CA297C4ABD2763DC5AA35 |
| SHA-256: | 7D3755AF9D6428B1A5CF4374915E17AF7CC5904CD3D15BE8022F4BDD8BE9918C |
| SHA-512: | 42E16987A4C0E60238E39060232B97A03A5A16642518A8E743183E149478AC92FD5EDCEDC831F095E38658D706C652AC3EE1D6759E85E46B66D7BC368D1B6F4E |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....N.....).....https://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.43eef025.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[108],{"ll/Q":function(e,t,r){"use strict";r.r(t),r.d(t,"UserProfileScreenContainer",(function(){return Nn}));var n=r("97Jx"),a=r.n(n),s=r("ERkP"),o=r("P1r1"),i=r("hqKg"),l=r("zh9S"),c=r("0KEl"),d=r("oEGd"),u=r("RqPl"),m=r("G6rE");const h=(e,t)=>{const{location:r,match:n}=t;return n&&n.params&&n.params.screenName?n.params.screenName:r&&r.query&&r.query.screen_name&&"string"==typeof r.query.screen_name?r.query.screen_name:""},p=(e,t)=>m.e.selectByScreenName(e,h(0,t)),b=Object(m.g)([m.a]),f=Object(i.createSelector)(o.l,((e,t)=>b(e,h(0,t))),u.k,((e,t)=>t.location.pathname.includes("/intent/")),((e,t)=>m.e.selectIsUserNotFound(e,h(0,t))),((e,t)=>{const r=p(e,t);return!!r&&m.e.selectIsLoading(e,r.id_str)}),((e,t)=>m.e.selectIsUserSuspended(e,h(0,t))),((e,t)=>m.e.selectUserSuspendMessage(e,h(0,t))),((e,t)=>m.e.selectIsUserWithheld(e,h(0,t)) |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\28854cce14dd368d_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 107462 |
| Entropy (8bit): | 6.38612239182473 |
| Encrypted: | false |
| SSDEEP: | 3072:k31EupG04EtPqfxZ3T9tn/rSzHcmOlBEB:klEqpiDTnjnEB |
| MD5: | 8A61BAA7AEFB6E1A20E7D4EB69526F7F |
| SHA1: | C6FE25937DDC663866BE5271DA8A2105B3A684BD |
| SHA-256: | E18349F755A904DE211B75862CE931B74145BAB5D0653E5060885053AEF87174 |
| SHA-512: | EDC4EC03C53697A54E578718B9F97EE44A5D2A4B73B8312A1ABC50ADE304FB38BFE47AFB64ABA22817BF5A86BAD754AB513C7E65AD87111CC011A125A469AE7A |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....N.....).....https://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.43eef025.js.....'.K.....O$.....F.....t...l.....<.....<.....($.l..`.....$L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....a.....Qb.L.....ll/QC.(S...m..`.....i.L`.....Rcl.....Qb..\....r.....M...Qb2.....s.....Qb.i.....c.....QbJ!.....m.....QbR.....h.....Qb.....p.....O...Qb...*....E.....Qb.G.....w.....Qb";.....C.....Qb..(&....S.....QbvP4C....I.....Qb&..u....P.....Qb>. .....k.....Qb2.....F.....Qb.1.2....x.....Qb..J.....O.....Qb..#.....N.....Qb.~k.....L.....Qb...}....A.....Qb"r.....U.....QbF.....R.....Qb.....D.....Qb.&U.....H.....Qb.U.E....W.....Qb6h.....j.....Qb.,y.....z.....Qb.?G.....V.....Qb.m.....q.....Qb^L'.....G.....Qb...%....J.....Qbv..^....K.....Qb. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\29e8affa3e7c7b28_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 33545 |
| Entropy (8bit): | 5.423939934113317 |
| Encrypted: | false |
| SSDEEP: | 768:bd8f1d1bsZccogkCWA/a8d2pkJ3wRNeqtMLf1X1uyOp6vf:2eHReRNeq6f1hhf |
| MD5: | 594C2DD1475A5D76313208D8022C8EAA |
| SHA1: | AF878828FC59EF58C7422F6E24B20B42EA1E5D88 |
| SHA-256: | 817678FD698216E72716807B908007F5DF5B385DE8F039961D8C301D22E714F8 |
| SHA-512: | B93433D2F51BA935A7A735A1DC7F941CE4276A16FC80885B52E296DF9FEAB4E9AF12C01FFF7975B5B2D0060FA199E735D6F3F617FA9ADE6E4981BCD1A30109D3 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q....aN.....https://abs.twimg.com/responsive-web/client-web/bundle.AdvancedSearch.6d64f055.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[30],{"3EFP":function(e,t,a){"use strict";a.d(t,"a",(function(){return n})),a.d(t,"b",(function(){return s})),a.d(t,"c",(function(){return r})),a.d(t,"d",(function(){return i})),a.d(t,"e",(function(){return o})),a.d(t,"f",(function(){return l}));const n="ArrowDown",s="ArrowUp",r="Enter",i="Escape",o="ESC",l="Tab"},"5emT":function(e,t,a){"use strict";var n=a("ERkP"),s=a("Lsrn"),r=a("k/Ka");const i=(e={})=>Object(r.a)("svg",{...e,accessibilityHidden:void 0===e.accessibilityLabel,style:[s.a.root,e.style],viewBox:"0 0 24 24"},n.createElement("g",null,n.createElement("path",{d:"M14.548 11.634c-1.207 0-2.188-.98-2.188-2.188 0-.664.302-1.25.77-1.653-.363-.097-.736-.165-1.13-.165-2.416 0-4.375 1.96-4.375 4.376S9.585 16.38 12 16.38c2.418 0 4.377-1.96 4.377-4.376 0-.4-.07-.78-.17-1.146-.402.47-.992.776-1.66.776z"}),n.createElement("path",{d: |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\29e8affa3e7c7b28_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 73017 |
| Entropy (8bit): | 6.199848535640606 |
| Encrypted: | false |
| SSDEEP: | 1536:hjxrU1AnYHGbp2DCU/H8tuFGyXlbI0BWxzWZlZcGs:7sAnhd2D/Ft1M0BWxqZlZcz |
| MD5: | D83450BF7AD09B25633F8B046F82F789 |
| SHA1: | 3A645E0773036D5CA8BA8B1A7E93F7C3A9C7108E |
| SHA-256: | 4401B543FE1C25DC66A373132877481E1B64E74DEEA75AE5FF670CF89661D178 |
| SHA-512: | 3C6D28F95275F3649182A537BBC0AAF5983E423ED29A31F6D171A0426C4E88F58E382210B90BEBA14404770C56D60343CFD93EACCDB460215533A5231062BB47 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q....aN.....https://abs.twimg.com/responsive-web/client-web/bundle.AdvancedSearch.6d64f055.js.....'.....O.... ...t.n.....H..... .....(.....(S....`.....tL`6.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....<...`.....d..a.....Qb.h1)....3EFPC..Qb6 ._.....5emTC..QbB.....6XNvC..Qb..J.....D9cEC..Qb2.9.....FDFLC..Qbjv.....S8srC..Qb.&!.....nS1wC..Qb.....p+r5C..Qb.S.....piX5C..Qb...Z....qYi+C..Qb&Y.....u3ZEC.(S...` .....TL`&....XRc(.....Qb.~d....n.....Qb2.....s.....Qb..\.....r.....S...QbV.<.....o.....Qb.....l...e.....`....Da.....Qb..{....d.....M..(S.(.`.....L`.....K`....Dd..... .....,Rc.....l`....Da.....A.....@.-....`P.q.....Q...https://abs.twimg.com/responsive-web/client-web/bundle.AdvancedSearch.6d64f055.js...a.....D`....D`....D`.....i. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2a70822637a2b394_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 88055 |
| Entropy (8bit): | 5.3739215239119735 |
| Encrypted: | false |
| SSDEEP: | 1536:hAs2SPsccFtYNJRyIvqBmqs2gHPXBLAuaK:as2SPznqs2sj |
| MD5: | 9BC7FB07ADD4EE361CACD42DFA6E96A5 |
| SHA1: | BC5861B22FB4DC05436989BBD38FF680F6E89C21 |
| SHA-256: | 8E8157C3EAD658D9787BE069371305EE1DA9A53FACBBF67C31F7F66AA06237E7 |
| SHA-512: | 0B7FC83BB441EC9896619CC0F417016515A3C2BC148CD53EF83D396341EBBB63D17F7E0B01EB246D521D305F14340B52A09B465C9A88E811D50B6D4CD0003F7 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....K....9P....https://abs.twimg.com/responsive-web/client-web/loader.DMDrawer.a2d2e965.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[166],{"+Bsv":function(e,t,a){"use strict";var n=a("ERkP"),r=a("3XMw"),s=a.n(r),l=a("M2x3"),i="settingsAppBar",o=a("/yvb"),c=a("rHpw");const d=s.a.bb081ea1,u={viewType:"settings_button"},h=n.memo((({onPress:e,pullRight:t,to:a})=>n.createElement(o.a,{accessibilityLabel:d,behavioralEventContext:u,hoverLabel:{label:d},icon:n.createElement(l.a,null),link:a,onPress:e,pullRight:t,style:p.button,testID:i,type:"primaryText"}))),p=c.a.create((e=>({button:{marginVertical:`calc(-${e.spaces.space12})`}})));t.a=h},"3GUV":function(e,t,a){"use strict";var n=a("ERkP"),r=a("rHpw"),s=a("MWbm");class l extends n.Component{shouldComponentUpdate(){return!1}render(){return n.createElement(s.a,{style:i.root})}}const i=r.a.create((e=>({root:{height:5*e.lineHeightsPx.body}})));t.a=l},"5UID":function(e,t,a){"use strict";var n=a("ERkP"),r=a("3XMw"),s=a.n(r),l=a("r |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2a70822637a2b394_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 176803 |
| Entropy (8bit): | 6.2362065656390735 |
| Encrypted: | false |
| SSDEEP: | 1536:lix22Nz39PBJHPk4t+EPZyjGVO1iVWTG4dcy45U2ZN2T5MIkoLvprzqgjde6XHRh:l8hN7XI8ZyVkVgcy4AkoLxrHj4GHKQX |
| MD5: | 333F2EFFA2F62F2EC47C17E0D5298BFA |
| SHA1: | 21B6D03640B9702E6DD0D043729583594AB88DFF |
| SHA-256: | 2A5CB5C98C43FC7898B45E3847991ADB54D2681D6049A044D938469C141559D5 |
| SHA-512: | AEA370433E06C292933DE8BF44286D17D1A534342531CEE681A5A9DCE02EE34F4D740C66A8514E7C07A39EE528EF8431DCDE7A20012F42BBB028144D7CEDEB0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....K....9P....https://abs.twimg.com/responsive-web/client-web/loader.DMDrawer.a2d2e965.js.....'..T....O7... ..."[L..... .....8..... .....d.....D.....X.....,.....(S....`.....tL`6.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\ ....push.....`.....L`.....`.....Ma....L...`.....d..a.....Qb&.....+BsvC..Qb2.%.....3GUVC..QbVS#.....5UIDC..Qbf..P....AvzuC..Qb..w.....BUB3C..Qb..}"....FS1zC..Qb.....TEo OC..Qb..v....fuheC..Qb.}'.....nySHC..Qbr_'.....pXKuC..Qb...E....y59GC.(S...`6....DL`.....`Rc,.....Qb.~d....n.....Qb.....l.....S...QbV.<....o.....Qb..{....d.....R....Qb..... ..p...f.....`....Da....\.....Qb>..>....ERkP..Qb.=%?....3XMw.....QbR..]....M2x3..Qe.,.7....settingsAppBar....Qb..~...../yvb..QbJ.){....rHpw...M...Qc...!....bb081ea1 |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2b3535dd39e20c63_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 56074 |
| Entropy (8bit): | 5.350713298818245 |
| Encrypted: | false |
| SSDEEP: | 768:v76VO7T4eufgErM1dl+tCV8LSJlNXcK/auguJ5NZsNShcpeBSVjl5yDKmmcQzVhb:X5DhNShcPwK5siaPI |
| MD5: | F4701C5F6120DFE5F2CCCA801142E0C2 |
| SHA1: | 05996791816D14ED1CFAFDD4A12777E86D9267A9 |
| SHA-256: | C90202651C0DDA07FBA59E46C9F5A4D31DF7D23F4460DD5081A2B4F8D387C327 |
| SHA-512: | 3B554086EB4EE033A2678D079ACCEB7EA90347DE7901D040957577FC4716A12D9A23C6FF6C1BACE4B988CBCAC0D540BEAEB30CBC1FEF9D59F5E99CD7BD04SBED |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O...n.....https://abs.twimg.com/responsive-web/client-web/bundle.Conversation.545c8775.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[47],{"8BIC":function(e,t,a){"use strict";a.r(t),a.d(t,"ConversationAnalyticsScreen",(function(){return A}));var n=a("KEM+"),r=a.n(n),o=a("ERkP"),c=a("zh9S"),i=a("hqKg"),s=a("XOJV"),l=a("0KEI"),d=a("oEGd");const u=(e,t)=>t.match.params.statusId,m=Object(i.createSelector)(((e,t)=>s.a.selectFetchStatus(e,u(0,t))),u,((e,t)=>s.a.selectHydrated(e,u(0,t))),((e,t,a)=>({fetchStatus:e,statusId:t,tweet:a}))),p={createLocalApiErrorHandler:Object(l.createLocalApiErrorHandlerWithContextFactory)("CONVERSATION_ANALYTICS_SCREEN"),fetchTweetIfNeeded:s.a.fetchOneIfNeeded,scribeAction:c.c};var h=Object(d.g)(m,p),g=a("v//M"),b=a("W5XZ"),y=a("jHSc"),f=a("3XMw"),_=a.n(f),E=a("SrIh"),w=a("Rp9C"),v=a("v6aA"),I=a("7JQg"),T=a("E0cF"),C=a("q9Zt"),S=a("bPFD"),O=a("rHpw"),P=a("yE5w");const k=_.a.g9079b93,L=_.a.a57daeb1,x=_.a.deaf5b15;class A extends o.PureCompon |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2b3535dd39e20c63_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 132151 |
| Entropy (8bit): | 6.19618148381022 |
| Encrypted: | false |
| SSDEEP: | 1536:Yt2CyjR3HVoIb6FYHvf+E7KhsAzbnfNaizV618PCJv3s4ZAUww:YwCyj1HVmYPLqbnfjzErqUww |
| MD5: | E68BF62E3B31D0347125547909CD6EC9 |
| SHA1: | EADC5D1EC5BC16226A29E75DF104CA011B915959 |
| SHA-256: | 47A0296E8A346D555A33AB0ACD9E9E016AB509B11EB9B5265967F5D5CE45A1A2 |
| SHA-512: | 2951D9E55AA73F704819EE4A03BAA165AEB537503F1494305D75A808B53E792E3D60A1F3981797FCB0053B80E86F7A09273ED695F128D007E00535C5780320AD |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O...n.....https://abs.twimg.com/responsive-web/client-web/bundle.Conversation.545c8775.js.....'.....O*.....q@.....\.....p.....\|.....l.....4.....`.....H.....(S....`.....LL`".....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma...^...`.....<..a.....Qb.<G.....8BICC..Qb.+f.....AEu/C..Qb.H9....JilhC..Qb.T.\....aH1VC..Qb...x....kevvC..Qb.}.....z4TAC.(S...`.....L`p.....RcX.....$.....Qb..\.....r.....QbV.<...o.....Qb2.....s.....R.....O...Qb.....y.....Qb...*....E.....Qb.G.....w.....Qbz.\|.....T.....Qb";.....C.....Qb..(&....S.....Qb&..u....P.....Qb>. .....k.....Qb.~k.....L.....Qb.1.2....x.....Qb...}....A.....Qb6h.....j...q.....`....Da....L.....Qb..{....d....(Qh.d.....ConversationAnalyticsScreen..(S. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2c162ea5b7b3e474_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 51915 |
| Entropy (8bit): | 5.348928873862965 |
| Encrypted: | false |
| SSDEEP: | 768:kCPq2z4fVuUNP/bfiMGjg+AFyaMakganJ3lk/2H3FMBmX8Rcy9n0z1lr6K3+fRTZ:kULQITganJf2QXKriUXJzm+F |
| MD5: | D251FA73F039DDA917BF7191C69E4A89 |
| SHA1: | 54B5AF15F8057641BF7F833FD10ECDBF6DDA04B0 |
| SHA-256: | 2BA2C0209CC7BEF51859A5592F8181F0649A3EE66F116381467CBB6219E6E213 |
| SHA-512: | 998EB11838FBE3F3B947CBE07706EC93961650BE721F0452A660ED34DD4D8C99D15A533F82210B9A7C11B435B1A04FD5C3CEE80F65ABB3DD23F4ED9E3D043FBB |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....M.....https://abs.twimg.com/responsive-web/client-web/loader.AppModules.1eb55255.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[161],{"+Aie":function(e,t,n){var i;!function(o,r,s){if(o){for(var a,c={8:"backspace",9:"tab",13:"enter",16:"shift",17:"ctrl",18:"alt",20:"capslock",27:"esc",32:"space",33:"pageup",34:"pagedown",35:"end",36:"home",37:"left",38:"up",39:"right",40:"down",45:"ins",46:"del",91:"meta",93:"meta",224:"meta"},l={106:"*",107:"+",109:"-",110:".",111:"/",186:";",187:"=",188:",",189:"-",190:".",191:"/",192:"`",219:"[",220:"\\",221:"]",222:"'"},u={"~":"`","!":"1","@":"2","#":"3",$:"4","%":"5","^":"6","&":"7","*":"8","(":"9",")":"0",_:"-","+":"=",":":";",'"':"'","<":",",">":".","?":"/","|":"\\"},d={option:"alt",command:"meta",return:"enter",escape:"esc",plus:"+",mod:/Mac\|iPod\|iPhone\|iPad/.test(navigator.platform)?"meta":"ctrl"},h=1;h<20;++h)c[111+h]="f"+h;for(h=0;h<=9;++h)c[h+96]=h.toString();y.prototype.bind=function(e,t,n){var i=this;return e=e in |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2c162ea5b7b3e474_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 139853 |
| Entropy (8bit): | 5.902020756563931 |
| Encrypted: | false |
| SSDEEP: | 3072:Qfdpls9V7zirjNOP4pu30v0q/OWoMqkM2y0oqFt6tZjQp:Ydzs98HwUH76tZUp |
| MD5: | 8EDFC7A1FA0ACBFBAD00D8F40C2A9F7E |
| SHA1: | 32CA8076548A503B718CFEBC147BDF6B52A3C5F5 |
| SHA-256: | 6767067ADABF1C160E7639514EA20EAC9C6DB9C428DFA600799D2B4C470EEDFA |
| SHA-512: | ABF83CD422B695768C36C7F7C52ECFBACB1AFD01E30FC9144F35EFD731C82E3DA9DEB93003921FB35DB471186281A7589AE142AF04841B3C8880303470AAEBA4 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....M.....https://abs.twimg.com/responsive-web/client-web/loader.AppModules.1eb55255.js.....'.....O-.... ...R.....I.....`.....8.....d.....P.....\.....(S....`N.....L`>.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....B...`.....t..a6.....Qb...x....+AieC..QbB.Q.....6oVLC..Qb..n2....AS3pC..Qb.~.g....Chb3C..Qb.....H1k/C..Qb../.....M6MTC..Qb..Z....Pc/xC..Qb.oW.....TpKdC..Qb"..9.. ..UkpfC..Qb.#.....XTymC..Qb.X.....a/eaC..Qbz\|N.....donRC..QbV.<(....rRImC.(S.`.`x.....L`.....HRc .....Qb.~d....n.....QbF!.....t.....Qb.Lh@....e.....S.c$.....$.....q.`.. ..Da.....'...(S....`.....L`V.....RcF.....Qb..\.....r.....M...Qb.i.....c.....Qb.....l.....R....Qb..{....d.....Qb.....p.....QbJ!.....m.....Qb.%.....f.....O...Qb.#....._..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2da8eb89ada8c7fe_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9273 |
| Entropy (8bit): | 5.362765924473128 |
| Encrypted: | false |
| SSDEEP: | 192:XfSRWFKTkT0RXFqMRYXNme8wiacF5oWxM:XaRWIwYRpRhe8wTcj3xM |
| MD5: | 343386343FF3EEE504971455A7B436AC |
| SHA1: | C531CD81377C7C40BEBF5624DA7DF4FE4C8DB1A5 |
| SHA-256: | CC6F657BE659AB4340532863D4491C65E328D3EAC519465BA4561F8F6D7325AE |
| SHA-512: | E0C9FD62BDAEC3B9C1525EC70F0C1583B7820A98573A61D04D3157786BF66B67431C95DCF4A7AFA8DAF4884D1B45973A3AAEBC901D417AEDA6DFDFC277B3BC05 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....E.....$.....https://abs.twimg.com/responsive-web/client-web/polyfills.cad508b5.jswindow.__SCRIPTS_LOADED__.runtime&&((window.webpackJsonp=window.webpackJsonp\|\|[]).push([[346],{Qrtf:function(t,e,n){(function(e){var n;n=function(){"use strict";var t=function(){if("undefined"!=typeof Map)return Map;function t(t,e){var n=-1;return t.some((function(t,r){return t[0]===e&&(n=r,!0)})),n}return function(){function e(){this.__entries__=[]}var n={size:{configurable:!0}};return n.size.get=function(){return this.__entries__.length},e.prototype.get=function(e){var n=t(this.__entries__,e),r=this.__entries__[n];return r&&r[1]},e.prototype.set=function(e,n){var r=t(this.__entries__,e);~r?this.__entries__[r][1]=n:this.__entries__.push([e,n])},e.prototype.delete=function(e){var n=this.__entries__,r=t(n,e);~r&&n.splice(r,1)},e.prototype.has=function(e){return!!~t(this.__entries__,e)},e.prototype.clear=function(){this.__entries__.splice(0)},e.prototype.forEach=function(t,e){void 0===e&&(e=null) |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\2da8eb89ada8c7fe_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 18685 |
| Entropy (8bit): | 5.587431602665727 |
| Encrypted: | false |
| SSDEEP: | 384:vd8YiNiOH5bjWHNQnnGbWKxPYxxi/fW6UR+r82gIRRil:vd81jswnGbNPYO/fW6PRe |
| MD5: | 127E0B343D871C4FB3D4B3CDD396E717 |
| SHA1: | 60D6A000FA0C439CC76890613A92B552E483DD84 |
| SHA-256: | 5BAC941D868CD8B776594C9DBC5628735580811A8656BD8D2B0D59AE7295E06A |
| SHA-512: | 2ED08374E5DD6338BB1A9D26FC4F5970C6841FAFA720FDECC6553132636B4A30280030508C2109E2D8A45ECDCDBBA3FDFBF0DB64A9C99C10C055972289D7C67 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....E.....$.....https://abs.twimg.com/responsive-web/client-web/polyfills.cad508b5.js.....'.y ....O....0H..(..d.....L..... .....(S....`.....@L`.... ..Qcv.I....window... Qf.P%.....__SCRIPTS_LOADED__....QcN.2.....runtime...Qd.W.....webpackJsonp..QbJ.\....push....`.....L`.....`.....Ma.....`.....`.....L`.....`.....M` .....Qb..``....w92O`.....$..a.....Qb.b%.....QrtfC....C..Qbb.j.....yLpjC.(S.L.`N.....L`.....4Rc.....QbF!.....t...a$.....a.`....Da....~<...(S.@.`<.....L`.....4Rc..... Qb.Lh@....e...`$...l`....Da....P<.....(S....`.....L`.....Rcf.....*.....Qb.~d....n.....Qb..\.....r.....S...QbV.<.....o.....Qb2.....s.....Qb.i.....c.....M...QbR.....h.....R....Qb.%.....f.... .Qb..{....d.....Qbj.B.....v.....Qb.....p.....Qb.#....._.....Qb.....l.....O...Qb.G.....w.....Qb.....y.....QbJ!.....m.....Qb..J.....O...t..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\30e07a28cca56a9c_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2920 |
| Entropy (8bit): | 5.746570761137954 |
| Encrypted: | false |
| SSDEEP: | 48:Jpv58wOVAqv7TsaUsMhSuUXUjDIAyk35lWZbmK40/MND3FFen18MwSG:/6v7TsaUsMhP0UvIDk3Xsw6M9FsnLwp |
| MD5: | 5A53FEFB7EEC27FEB1CA5FE53C3823AC |
| SHA1: | F23EC2325A7A4B1DDFD0EEE6754505C01571E3C6 |
| SHA-256: | 9FC8015191466F4DD3E4453CE428C38ECC48C32C948CC9A9A94213E5AC988AD1 |
| SHA-512: | 0684A89FB8D609260B65DA97C698EA9D6C39415A82463145E4D07B2B7B022D3BBBFEA9BB70402B57FE78054F5C7D02FCDEC47A2852E77EF6AC3BD16A0B44A0<br>5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q.....-....https://abs.twimg.com/responsive-web/client-web/bundle.Twitterversary.99db8325.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[102],{yQeU:function(e,t,a){"use strict";a.r(t),a.d(t,"TwitterversaryScreen",(function(){return u}));var n=a("KEM+"),i=a.n(n),s=(a("MvUL"),a("ERkP")),r=a("Hw0q"),c=a("rxPX");const o=(e,t)=>{var a;return!(null===(a=t.location.state)\|\|void 0===a\|\|!a.fromApp)};var p=Object(c.a)().propsFromState(((()=>({title:Object(r.b)("title"),message:Object(r.b)("messa ge"),action:Object(r.b)("action"),text:Object(r.b)("text"),imageAttachment:Object(r.b)("image_attachment"),fromApp:o})))).withAnalytics({page:"twitterversary"}),l=a("jHSc" ),m=a("9Xij"),h=a("t62R"),g=a("/yvb"),b=a("rHpw"),d=a("U+bB"),y=a("MWbm");class u extends s.Component{constructor(...e){super(...e),i()(this,"_handleClick",(()=> {const{analytics:e,history:t,imageAttachment:a,text:n}=this.props;e.scribe({action:"compose"}),n&&t.replace({pathname:"/compose/tweet",state:{defaultText:`${n} |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\30e07a28cca56a9c_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5641 |
| Entropy (8bit): | 6.005350822006961 |
| Encrypted: | false |
| SSDEEP: | 96:BVv4o0tTXJD0qEQQaMbaKG1mfEmejEHjsXpziaWwRrnWN2Wdo/U:BdhCTXt3E/9OAHjepziErnWNPoc |
| MD5: | 816B6E4C2A818C6088700540BE062639 |
| SHA1: | 6DD4EA3CD4D09148F418524D68D969A15CE38621 |
| SHA-256: | 0CD5E26F7CF2AE982D3CAEEB3485521C8DC006EC44CAA959CC821DABA8B7E834 |
| SHA-512: | F518B0FA5A28296E0F09D0D8E73961D90A8FBE6D5DEE99427653CC5C97578FE3ECB4B289CB8D1543A262DA9A7B652A5CFE1F4E8525D0D73660750A413CFB40<br>B |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q.....-....https://abs.twimg.com/responsive-web/client-web/bundle.Twitterversary.99db8325.js.....'.s.....O....@....m.....(S.l..`.....$L`.....Qc v.I....window....Qd.W.....webpackJsonp..QbJ.\....push....`.....L`.....`.....Ma.....`.....a.....Qb.L.....yQeUC.(S.q..`.....L`B.....Rc@.....S...Qb2.....s.....Qb..\.....r .....QbV.<....o.....Qb.....l.....QbJ!.....m.....QbR.....h.....Qb..{....d.....Qb.....y.....R....Qb.G.....w...k.....`....Da.....!...a.. Qf.....Twitterv ersaryScreen.(S.(..`.....L`.....K`....Dd.....,Rc.....l`....Da....,.....@.-....`P.q.....Q...https://abs.twimg.com/responsive-web/client-web/bundle.Twitterve rsary.99db8325.js...a.....D`....D`....D`.....0...`....&...&..1.&....&.(S.@.`6.....L`.....QcR.\|.....location..QcN.....state.....Qc.....fromApp...K`....Dj.....(...&.(.. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\31c15757aff4134e_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 110215 |
| Entropy (8bit): | 5.594668506170634 |
| Encrypted: | false |
| SSDEEP: | 768:xzOtHvK4WwcKvY+XC6P4SZQphPxFMdubPVO/kGXThPJHli0UycAMWpkYRtw5r+0T:RM5wlGYzOvhP0AMHUw5rkgQFVhlDfoD |
| MD5: | 338F9A5D9574EFE7C9D273515C96129B |
| SHA1: | 50E745D0AE4D1B688FF5602A6F889E3C57224A3D |
| SHA-256: | 23F578647F535864A5DCF18B16FAB5C4B68747DDA4A6659F3CA85ED15ECC71DC |
| SHA-512: | D1266D7A8255064DB97279FDB26C1A3FF86B863992ED003F930296DD1E9D2C2886F2847DCC20A93B83C7CBB74BC9DD11F073E95DAF2C0FB5BFB6C5BC140149<br>1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....V....9.....https://abs.twimg.com/responsive-web/client-web/bundle.AccountVerification.0e1907f5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[29],{"5emT":function(e,t,a){"use strict";var i=a("ERkP"),r=a("Lsrn"),l=a("k/Ka");const n=(e={})=>Object(l.a)("svg",{...e,accessibilityHidden:void 0===e.accessibilityLabel,style:[ r.a.root,e.style],viewBox:"0 0 24 24"},i.createElement("g",null,i.createElement("path",{d:"M14.548 11.634c-1.207 0-2.188-.98-2.188-2.188 0-.664.302-1.25.77-1.653-.363-.09 7-.736-.165-1.13-.165-2.416 0-4.375 1.96-4.375 4.376S9.585 16.38 12 16.38c2.418 0 4.377-1.96 4.377-4.376 0-.4-.07-.78-.17-1.146-.402.47-.992.776-1.66.776z"}),i. createElement("path",{d:"M12 19.79c-7.228 0-10.12-6.724-10.24-7.01-.254-.466-.254-1.105.035-1.642C1.88 10.923 4.772 4.2 12 4.2s10.12 6.723 10.24 7.01c.254.465.2 54 1.104-.035 1.64-.085.216-2.977 6.94-10.205 6.94zm0-14c-6.154 0-8.668 5.787-8.772 6.033-.068.135-.068.208-.033.273.137.316 2.65 6.104 8.805 6.104 6.18 0 8.747- 5.973 8. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\31c15757aff4134e_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 238654 |
| Entropy (8bit): | 6.216427625016489 |
| Encrypted: | false |
| SSDEEP: | 3072:up0aqo3FHn8rbLk5SdI91GBId7OeDcHtQRG2jozfEqCiZzIZOWrJCN:O0abFHn8vLPd41skcNf8qCiZzZWMN |
| MD5: | AE79AA4E5EBE769F07BA845E0A9DF0D3 |
| SHA1: | 64A223F8737DACC45B8F938DEA0BA30C192F1130 |
| SHA-256: | 9A63C8C383997A7D31EC838F855C02E6BA4DABD607CCCB0850761CC6B11183A6 |
| SHA-512: | 345992F2B8A60D88A022109390553ED668781C676F0639A53A106D083434A79342D29429926F9ACF88238904C040071A2C45951573D96C087503D55844CF80DA |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....V....9.....https://abs.twimg.com/responsive-web/client-web/bundle.AccountVerification.0e1907f5.js.....'.....O<.....OZ/.....h.....8..... .....x.....T.....(S.m..`.....%.L`.....Qcv.I....window....Qd.W..... webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....:...`.....a.....Qb6._.....5emTC..Qb..X.....5kR0C..Qbn..#....6sfkC..Qb.}.....8Y9HC..Qb.hQ.....FlngC..Qb..kk... .H1lmC..Qb.....IM13C..Qb..9.....IbdMC..Qb.1.....NRlpC..Qbn.....NoO/C..Qb...g....OVD+C..Qb"".....Qp/WC..Qb.~.~....T8pkC..Qb.S.....UmjqC..Qbj.....W7+tC..Qb.u.<....W 9cOC..Qb*X.....WqilC..Qb..^....b1+5C..Qb.....ccgCC..Qbb..(....eWSoC..Qb..`f....fl4iC..QbV.....iQBXC..Qbb.....je27C..Qb.*.,....kAdfC..Qb.....kfbJC..QbJl.}....mmgWC ..Qb.P<.....oAj9C..Qb..... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\32feacfd5c5fbc90_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 29276 |
| Entropy (8bit): | 5.675804117704295 |
| Encrypted: | false |
| SSDEEP: | 768:F9V9DHO5VNmFW48pWM0AwiwbbzRijFD2/Im5ifTurNkN3Nx3jajVN0N0AjdYkc6:/u5aRFMU/Im5ifTurNkN3NljajVN0ki |
| MD5: | C20EC3EEBEB928F7DEABDCBDB78EE880 |
| SHA1: | 12D79632207F27AB127BFD3DC10AD21463F3F1DE |
| SHA-256: | DAD4835121B9ED7778466496B51CCCF0476E3D194A15A806017D300B7F42B326 |
| SHA-512: | 6E3E983DA88B68FE977CD038BEF2649756D6E81C6BA73519F5F8A603A1C495D99E1B48107B27C77D46A2DAE8C4E3C690FAE663ACB8B497F4FEB88573AA06C0D |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....I....w.....https://abs.twimg.com/responsive-web/client-web/bundle.Moment.f0435b65.js(window.webpackJsonp=window.webpackJsonp||[]).push([[66],{CBsz: function(e,t,a){"use strict";a.r(t),a.d(t,"MomentAnalyticsScreen",(function(){return T}));var r=a("ERkP"),n=a("n4jD"),c=a("rxPX"),i=a("0KEI");const o=(e,t)=>t.match.params.momentId,l=e=>(t,a,{api:r})=>{const c=Object(n.c)(a());return r.Moments.analytics({moment_id:e.momentId,teamUserId:c})};var s=Object(c.a)().propsFromState(((()=>({momentId:o})))).propsFromActions(((()=>({createLocalApiErrorHandler:Object(i.createLocalApiErrorHandlerWithContextFactory)("MOMENTS_ANALYTICS_SCREEN"),fetchAnalytics:l})))),u=a("k49u"),d=a("LVU8");var m=a("jHSc"),p=a("MWbm"),b=a("t62R"),f=a("MtXG"),h=a("855f"),E=a("rHpw"),g=a("7JQg"),y=a("3XMw"),S=a.n(y);const v=S.a.e2e35f0d,C=S.a.icfe5fe3,U=S.a.a52a1fb9,_=S.a.if221231;class T extends r.Component{constructor(e){super(e),this.state={}}componentDidMount(){const{createLocalApiErrorHandler:e,fetchAnalytics:t |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\32feacfd5c5fbc90_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 60185 |
| Entropy (8bit): | 6.301199812814281 |
| Encrypted: | false |
| SSDEEP: | 1536:xsqnB+az8XvdR7K7SAGOqypGNWNRNWVCfNt8:CE+a4r7z |
| MD5: | FB081F57BCD5372BAFE98FDD1A19CE6C |
| SHA1: | 1650293F63CCCB101CD5695C2D8F0508C47C889E |
| SHA-256: | 86C82167F77128103FCF111F8DD62A24DDBBA290358E71B945A0054BD0E5E798 |
| SHA-512: | A0F4666FDA7AFCD0F8A265016126EA3D14C1DF2ACC060269FF8246B88EF9B03ADEFDDCBE64E93942A475692926BC329D733C4DE3D2C6D4CC0764501B436B69C |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....I....w.....https://abs.twimg.com/responsive-web/client-web/bundle.Moment.f0435b65.js.....'.un....O.... .....\|.. .....(S....`.....tL`6.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....d..a.....Qb.DF.....CBszC..Qb.....DBIDC..Qbz..k.. ..OzKQC..Qb..<....ShJ/C..QbZL.....XOb8C..Qbnu.....g7RaC..Qb.[_I....hBohC..Qbz.<H....su2VC..Qb.9.....tH6RC..Qb2I.....vFjZC..Qb.....yEpkC.(S....`.....L`T.....Rc\.... .....&.....Qb..\.....r.....Qb.~d....n.....S...QbV.<.....o.....Qb.....I....R....Qb..{....d.....QbJ!.....m.....Qb.....p.....O...Qb.%.....f.....QbR.....h.....Qb..(&....S.....Qbj.B.....v.....Qb";.... ..C.....Qb"r.....U.....Qb.#....._.....Qbz.\|.....T.....QbF.....R...r.....`....Da.....$Qgr.6?....MomentAnalyticsScreen.... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3478fb94447b5440_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7931 |
| Entropy (8bit): | 5.555502403908377 |
| Encrypted: | false |
| SSDEEP: | 192:ETyPGa3d9vD25UQIxHX9Appv4e+Jq1ZU7mXKWp+MSMPt:EOPRd9vq5vIx39Appgi1Mrkt |
| MD5: | D26C5CC9E7ED62024FA2DCDB2F8C8CE2 |
| SHA1: | 8BDABCF746AED75005EF7D7CDDBF6BB567705B76 |
| SHA-256: | BB9BB75D41B68E43C8AB43D8B319D47D39CA9ED7BB18A1C4CC85FE76946344DE |
| SHA-512: | 61B522145BF42A7E3B35E642F94144BAB91B00F8D76C882A30BE4B94DF08AD7104B4313BC58481C4334903D0C6437F7A9B9E5CF2E590E0D4DD1212F782927EE9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q.....%....https://abs.twimg.com/responsive-web/client-web/loader.ExploreSidebar.b5eae565.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[168],{"+Bsv":function(e,t,n){"use strict";var r=n("ERkP"),i=n("3XMw"),o=n.n(i),a=n("M2x3"),s="settingsAppBar",c=n("/yvb"),l=n("rHpw");const d=o.a.bb081ea1,u={viewType:"settings_button"},p=r.memo(((({onPress:e,pullRight:t,to:n})=>r.createElement(c.a,{accessibilityLabel:d,behavioralEventContext:u,hoverLabel:{label:d},icon:r.createElement(a.a,null),link:n,onPress:e,pullRight:t,style:h.button,testID:s,type:"primaryText"}))),h=l.a.create((e=>({button:{marginVertical:`calc(-${e.spaces.space12})`}}))));t.a=p},"+o05":function(e,t,n){"use strict";var r=n("ezF+"),i=Object.freeze({Cell:"Cell",Hero:"Hero",Tile:"Tile"});const o={loader:()=>n.e(224).then(n.bind(null,"QPD4")),loaderKey:"defaultScoreEventSummaryLoader",strategy:n("XBtf").a.Critical};t.a=r.c({selectDisplayType:e=>e.content.displayType,handlers:{[i.Cell]:o}})},"A+RP":function(e,t,n){ |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3478fb94447b5440_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 21657 |
| Entropy (8bit): | 5.919256504088415 |
| Encrypted: | false |
| SSDEEP: | 384:oWgx/AxqPMfQAt4cFl3zf7SjVOSoRoBggFaIsisluPdciIqv:oWOyxfQA2yqfkVOSoRYaIsisluaA |
| MD5: | AA052E2873CC3A7D5505E5C08230F765 |
| SHA1: | BB35B659C968B7811082F11CA657B97B50D0D7B9 |
| SHA-256: | 51773EAA00767059223548B47584F266603893F8E69D57EC22981D59913A8DA5 |
| SHA-512: | EF1656B0F53579B79E775A66183ADC03BD3646AC6AC004B3A7C70CB018B2D868DA2B2670C50021F5D16B7A1CA541878FF39CCDB8A94F2D2569E787C600435F9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q.....%....https://abs.twimg.com/responsive-web/client-web/loader.ExploreSidebar.b5eae565.js.....'.#.....O.....S.....k.....(S....`.....DL`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....P...`.....4..a.....Qb&.....+BsvC..Qb...W....+o05C..Qbv..u....A+RPC..Qb.].....BxsDC..Qb6.F.....XtkEC.(S...`6....DL`.....`Rc,.....Qb..\.....r.....M...Qb2.....s.....Qb.i.....c.....Qb..{....d.....R....QbR.....h...f.....q.`....Da....\.....Qb>..>....ERkP..Qb.=%?....3XMw..Qb.~d....n.....QbR..]....M2x3..Qe.,.7....settingsAppBar....Qb..~...../yvb..QbJ.){....rHpw...Qc...!....bb081ea1...a.....Qc.}L.....viewType..Qe.R.....settings_button...Qb..D!....memo.(S...`<....TL`&.....Qc.....onPress...Qd6.T.....pullRight.....Qb..,}....to....QeZ.....createElement.....\.a*..... Qf.n.....accessibilityLabel..C.$Qgz6.....behavioralEventContext. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\372b5315ca06d87c_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 27373 |
| Entropy (8bit): | 5.483027452114192 |
| Encrypted: | false |
| SSDEEP: | 768:3rluCWhj6ZTGzoPx+VeNCsldfH2PqVaBHEnCiBrerxrvAfM5uSoPa2L4M/B+lb:rWh22de0BknCYKN15Fobsb |
| MD5: | 242F39F49E62C3900834A740E9CD38B9 |
| SHA1: | F3078F87B0B572D6533406CD79EC49E68688B4A4 |
| SHA-256: | 6BA6623708B215AA1A122A01A5AAB5C250C190DF66FDA6092B1EC6A04B2161D5 |
| SHA-512: | 511856DF06E058AB453B72064D1822627E61DD84056CE8A948C17F30F68EA5A68986D078E20F375FA919702F9460433AEA20F1B1C2340647C2BA653CFFE51C4A |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....I...T..@....https://abs.twimg.com/responsive-web/client-web/bundle.Search.dcaa33f5.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[85],{"0E8n":function(e,t,a){"use strict";a.r(t),a.d(t,"SearchScreen",(function(){return Ve}));var r=a("KEM+"),s=a.n(r),c=a("ERkP"),n=a("HPNB"),o=a("es0u"),i=a("zh9S"),l=a("1YZw"),h=a("hqKg"),d=a("3IPs"),u=a("rxPX"),p=a("0KEl"),S=a("v4XE"),m=a("Hw0q");const y=(e,t)=>{const{location:a}=t;return a.query&&a.query.src&&"string"==typeof a.query.src?a.query.src:""},v=(e,t)=>{const{location:a,match:{params:r}}=t;return r&&r.unsafeHashtagQuery&&"string"==typeof r.unsafeHashtagQuery?`#${r.unsafeHashtagQuery}`:a&&a.query&&a.query.q&&Object(m.a)(a.query.q)\|\|""},_=(e,t)=>{const{location:a}=t;return 0===a.pathname.indexOf("/search")?"search":"hashtag"},b=(e,t)=>!!(t.location.state\|\|{}).searchFocused,E=Object(h.createSelector)(Object(m.b)("pf"),Object(m.b)("lf"),((e,t)=>({peopleFilter:e,locationFilter:t})));var g=Object(u.a)().propsFromState(((()=>({sear |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\372b5315ca06d87c_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 64553 |
| Entropy (8bit): | 6.16023356847177 |
| Encrypted: | false |
| SSDEEP: | 768:PxAJe5zgwXJxZmfG8zSJe3YTLskVlsJo59jFOKcP5e+VmQM1SlUqeY:PxAJe5Uw5x8f5zShZr5dFZcP55V81oI |
| MD5: | 50F3B0DE0DDCF0B207A80DC3AE953B04 |
| SHA1: | E072E9ABB6450FECA9E3FF547DF3802F7B2CC781 |
| SHA-256: | 35AF8F1789485C897AE3BF9D41B69CA6D102C239CF12DEAB249B6A58C374561C |
| SHA-512: | 7821BD8DEE2AC9BE1CF5A8B6DEE3D604F1D33CBBFA5A4E9D2E87A3F5484C3082A750CA3A3D1A9128368411AE7E7D4F0B6256A9E3E57BD24B4F7332D07F834019 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....I...T..@....https://abs.twimg.com/responsive-web/client-web/bundle.Search.dcaa33f5.js.....'..g....O....(....P.....`.....(S....`~.....L`J.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma.....`.....aB.....Qb...B....0E8nC..Qb.....3X8/C..Qb".@....4ZbNC..Qb".....Ds5iC..QbJU.....L7toC..Qb.....PH3BC..Qb..F.....g9w/C..Qb.....h2muC..Qb*u.....hiGSC..Qb6j3.....i6ORC..Qb.Jp.....kix0C..Qb.+o.....nmVbC..Qb..._....sYRnC..Qb&Y.....u3ZEC..Qb.>.....v4XEC..Qb.2<....zgaLC.(S.-..`.....=.L`.....RcH.....Qb2.....s.....Qb.i.....c.....Qb.~d....n.....QbV.<.....o.....S...Qb.....l.....QbR....h.....Qb..{....d.....Qb.....p.....Qb..(&....S.....QbJ!.....m.....Qb.....y.....Qbj.B.....v.....Qb.#....._.....O...Qb...*....E.....Qb.%.....f.....Qbz.|.....T.....Qb..J.....O.....Qb>. .....k.....Qb.~k.....L.... |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\37bd520c4b0affcb_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6841 |
| Entropy (8bit): | 5.565826146976729 |
| Encrypted: | false |
| SSDEEP: | 192:Agq1pUX4+TXZ6NMtaTwxczZbxMbfeXVxeh:AbcX4+TX0NMtaTWONtXVxk |
| MD5: | 4B33544CD95739914846408D8E177CD5 |
| SHA1: | BF0DE1CBDA99E7646EB6264F7F20D1AD465E8D4F |
| SHA-256: | 9806D399280298092C2FF6B2DE1ED64710D7F86150C0AA5CA077C29B5AC05987 |
| SHA-512: | 57A087821ED16B04224BE10110F523B2D690B306C477FE4F3E8C74946BDCCBC2931502038180BC6B8B4040F77935831C614A362D7E9A235B71F4F7D65EDD7918 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....]...7.....https://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerEventsUI.d7bfe5e5.js(window.webpackJsonp=window.webpackJsonp||[]).push([[189],{TlAO:function(e,t,a){"use strict";a.d(t,"a",(function(){return w}));var r=a("KEM+"),n=a.n(r),l=a("ERkP"),o=a("t62R"),s=a("/yvb"),p=a("3XMw"),i=a.n(p),c=a("RUwF"),m=a("rHpw"),u=a("Q0n6"),y=a("Wms4");const d=Object.freeze({LIVE_BROADCAST:"liveBroadcast",REPLAY_BROADCAST:"replayBroadcast",VOD:"vod",GIF:"gif",SLATE:"slate"}),E=i.a.j190bf19,f=i.a.f6dc9146;var h=({playbackDurationMs:e,type:t})=>{switch(t){case d.LIVE_BROADCAST:return l.createElement(y.a,{type:"live"},E);case d.REPLAY_BROADCAST:return l.createElement(y.a,{bold:!0},f);case d.VOD:return"number"==typeof e&&l.createElement(y.a,null,Object(u.c)(e))||"";case d.GIF:return l.createElement(y.a,{bold:!0},"GIF");default:return null}},b=a("jV+4"),l=a("mXq/"),v=a("MWbm");const g=i.a.f17dfdb5,S=i.a.e9bd453e,A=i.a.ffeb2fc6;class w extends l.Component{render(){const{hi |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\37bd520c4b0affcb_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 12653 |
| Entropy (8bit): | 6.3535703392570735 |
| Encrypted: | false |
| SSDEEP: | 192:ANXFqjnMNvKU/QSwb615rb28EtWQPgToF+oGHlSIMUEsW+5OujNlRh1a4w:ANI4Kv61528EF+j40Z5OujNlRh1aP |
| MD5: | 2DE5FE2316DC0DD1C6A99591600DB54D |
| SHA1: | 48252569BB8E7C7441ED359CF645E7979AD64E82 |
| SHA-256: | FB77F3E44162415A0C470A823B6E9F7AF0267D5D4D5730C632843D2CD410D570 |
| SHA-512: | 5B72835967FB9AF3BDD937C51BBB2BAF39E4F9332A8A37743D57F167612C17CFF26689D21886DA1CB982A7D8D26BB950969961CE6506B5E9EB213FCD43F8721 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....]...7.....https://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerEventsUI.d7bfe5e5.js.....'.....O.....0...X.i.....(S.t..`.....,L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....z...`.....a.....Qb...,....TlAOC..Qbv..O....wHP+C.(S....`*.....L`J.....Rc\.....&.....Qb.....l.....QbV.<.....o.....Qb2.....s.....Qb.i.....c.....QbJ!.....m.....R....Qb.....y.....Qb..{....d.....Qb...*....E.....Qb.%.....f.....QbR.....h.....O...QbvP4C....I.....Qbj.B.....v.....Qb..(&....S.....Qb...}....A.....Qb.G.....w.....Qb.....D...r.....Q.`....Da.....A....M..(S.(..`.....L`.....A...K`....Dd.....,Rc.....I`....Da.....@.-....IP.....]...https://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerEventsUI.d7bfe5e5.js...a.. |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\396baeb977a25680_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6353 |
| Entropy (8bit): | 5.61554443722947 |
| Encrypted: | false |
| SSDEEP: | 192:hdCJ4NVEaV12HzWVITjJSVMp71Umtwh4BtT5ziz0:h047EaOTNTNSVFhoPiz0 |
| MD5: | 637885FB053C9747D590C94E13732944 |
| SHA1: | 0C5E2BA06F2CD880E033776C610847F2928D637B |
| SHA-256: | 9EB7748ECD39C4B7FAD0CBEC918554ABE54C71D64035BAB085D8F063970A595F |
| SHA-512: | 935DD1376D1AB79D75734615EF9E279C29E60A72DC36E3B3BE23C27BAEBD630E56225BE00F939AF857F6425367DD58496A04B20E5B836B29BF0F3104AB482934 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....P.....2....https://abs.twimg.com/responsive-web/client-web/loader.NewTweetsPill.c9109385.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[174],{WXWl:function(t,e,i){"use strict";var s=i("ERkP"),a=i("Lsrn"),o=i("k/Ka");const n=(t={})=>Object(o.a)("svg",{...t,accessibilityHidden:void 0===t.accessibilityLabel,style:[a.a.root,t.style],viewBox:"0 0 24 24"},s.createElement("g",null,s.createElement("path",{d:"M18.707 10.293l-6-6c-.39-.39-1.023-.39-1.414 0l-6 6c-.39.39-.39 1.023 0 1.414.195.195.45.293.707.293s.512-.098.707-.293L11 7.414V20c0 .553.447 1 1 1s1-.447 1-1V7.414l4.293 4.293c.195.195.45.293.707.293s.512-.098.707-.293c.39-.39.39-1.023 0-1.414z"})));n.metadata={width:24,height:24},e.a=n},o52z:function(t,e,i){"use strict";i.d(e,"a",(function(){return a}));var s=i("VPAj");const a=Object(s.a)([]);Object(s.a)({})},xAHt:function(t,e,i){"use strict";i.r(e),i.d(e,"NewTweetsPill",(function(){return E}));var s=i("KEM+"),a=i.n(s),o=i("ERkP"),n=i("lnti"),r=i("hqKg"),l=i("o52z") |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\396baeb977a25680_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13336 |
| Entropy (8bit): | 6.08727411264418 |
| Encrypted: | false |
| SSDEEP: | 384:bKp8TG9jKubP4O4+gSot3GL8QIBhFuCBeAY5:bKOTYXj4O4YosINF0 |
| MD5: | 7C3EE4F85CAFF5F70F5DD5EA6DD2CD28 |
| SHA1: | C55D5B1120054EFCA19161A55882A1AFE938405E |
| SHA-256: | F0A0A4E7EAB2F10FDE3B1215B3254AA830892B2129625626DC1D0B2B30ED5DBD |
| SHA-512: | 341F9E1F3FCA08BD3B7DBE965479CDDCE46DD67397A1D460564AAB650510B7AC9455CCEFF7E009B693BC07D2CCA46D300B321F97FF3B2A7BC2C3E8E5B9C3DDF8 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....P.....2....https://abs.twimg.com/responsive-web/client-web/loader.NewTweetsPill.c9109385.js.....'.....O....H3..g.....\|.....(S.\|..`.....4L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....\...`.....$..a.....Qb.Ll.....WXWlC..Qb...C....o52zC..Qb...s....xAHtC.(S.\.`r....(L`.....@Rc.....Qb2.....s.....M...QbV.<.....o...b.....`....Da.....Qb>..>....ERkP..Qb*..{....Lsrn..Qb...]....k/Ka.(S..`@....@L`.....Qb.UM.....svg.. Qf.n.....accessibilityLabel...Qf.....accessibilityHidden....`.....Lb.....Qbj..7....root.q...Qdjm.....0 0 24 24.....QcJ.s.....viewBox...QeZ.....createElement.....Qb.....path...a.....Qb..{....d.....Q.....-.....M18.707 10.293l-6-6c-.39-.39-1.023-.39-1.414 0l-6 6c-.39.39-.39 1.023 0 1.414.195.195.45.293.707.293s.512-.098.707-.293L11 7.414V20c0 .553.447 1 1 1s1-.447 1-1V7.414l4.293 4.293c.195.195.45.2 |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3b955fcc770f9cd7_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7151 |
| Entropy (8bit): | 5.664975174711883 |
| Encrypted: | false |
| SSDEEP: | 192:YjT/LQ6dZNcCQ00Y4asjY94QuhIBQgHPHcfTv:YjhNRQ98hBQgHkf7 |
| MD5: | 0FC71E07AE3D44D783DDB8553392C0D3 |
| SHA1: | 8352DAF8501FD827547FF2D215D413477580C8CF |
| SHA-256: | 6C22F76B2DC2ED3E3F0794959A15BA070BBCF76EC5E2D09EC8D8841FB1DF8ED5 |
| SHA-512: | F1622D10ED02BBBA461FCB9CD1A7038C089616567CDEEFB7BDB34C491D190ADDC34EDEA230418A7F84FE8A3066BABF06B2068149ADD5B0F5BF04932EFA4F5DED |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Y.....P&....https://abs.twimg.com/responsive-web/client-web/loader.MediaPickerWithPreview.2c87d025.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[172],{"2Daw":function(e,t,i){"use strict";i.d(t,"a",(function(){return f}));var a=i("KEM+"),r=i.n(a),n=i("ERkP"),s=i("LCtV"),o=i("3XMw"),c=i.n(o),d=i("VPdC"),l=i("pKoL"),p=i("MWbm"),m=i("rFBM"),u=i("/yvb"),h=i("9Xij"),b=i("rHpw"),y=i("hOZg"),M=i("Mbn/"),v=i("T8pk");const E=c.a.b87ca51a,g=c.a.eebff22c;class f extends n.Component{render(){const{borderRadius:e,maskStyle:t,mediaItem:i,onAddMediaFiles:a,onCrop:r,onRemove:s,rootStyle:o,withDragDrop:c}=this.props,d=i&&!i.uploader,l=n.createElement(n.Fragment,null,this._renderPreview(),d?null:n.createElement(n.Fragment,null,n.createElement(p.a,{style:[R.mask,t,C[e]]}),n.createElement(p.a,{style:R.mediaPicker},this._renderMediaEdit(),r?this._renderMediaCrop():null,s?this._renderMediaRemove():null)));return n.createElement(p.a,{style:[R.container,o,C[e]]},c&&a?n.createElement(m.a,{o |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3b955fcc770f9cd7_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13833 |
| Entropy (8bit): | 6.167835803173271 |
| Encrypted: | false |
| SSDEEP: | 384:td8x8hiu5CsQM3aHGpvMI3dWxYp8c4tQHB5UMb5:nViTDsA48tQHD5V |
| MD5: | 92C742A154D7550D23B3E10AA85BD191 |
| SHA1: | 170EAF8CEE53BFB509F9DBC56E176D773DCBF918 |
| SHA-256: | 9F69E36C49D22BBFBD0FF664617AAA63FB35B93F36C0425DB9AE4FE8D9E6B4D3 |
| SHA-512: | DDA86A39AD6A0010DCC056E7E7BD5BC252A47CF369031BA71DEB44D721AC58280249F51183B5A3D74E69CE8ADACAD5372D01EA1B806B0E05953D2DCDDF988A44 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Y.....P&....https://abs.twimg.com/responsive-web/client-web/loader.MediaPickerWithPreview.2c87d025.js.....'.....O....05....d.....(S....`.....<L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push....`.....L`.....`.....Ma....X...`.....,.a.....Qb../.....2DawC..Qb.....Mbn/C..Qb...-....P68UC..Qb.~.~....T8pkC.(S....`.....L`H.....RcL.....Qb.~d....n.....Qb..{....d.....Qb.....l.....Qb.....p.....QbJ!.....m.....R....QbR.....h.....Qb.....y.....Qb..}.....M.....Qbj.B.....v.....Qb...*....E.....Qb.%.....f.....Qb";.....C.....QbF.....R...n.....`....Da.....M..(S.(.`.....L`.....K`....Dd.....,Rc.....I`....Da.....@.-....hP.....Y...https://abs.twimg.com/responsive-web/client-web/loader.MediaPickerWithPreview.2c87d025.js...a.....D`....D`....D`.....I...`2...&...&....& |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3dd68853f8462d0e_0 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 24392 |
| Entropy (8bit): | 5.518050995854306 |
| Encrypted: | false |
| SSDEEP: | 384:HDgETEPAdXZN20aG+VC0qKtEtL1hcaQdpalK+I8ce44MMzrtAT45SZ+38YwL5sKf:HkOEPAdXZN20aG+Q0qKtEtJSaQdoK+z2 |
| MD5: | F2A9B50F9A9AD5499CFF6E75B85FE6C0 |
| SHA1: | 08A6EE1E31637889B2019C97F374F38A86020CBD |
| SHA-256: | 8AC2B0139E265D9774DB01AA7384001E332EB8D44398E380D9A06D89C5A9F75E |
| SHA-512: | 62828BA559314882DD15BE62F105033A46B78EEEC84CAD9B1B890B84582AB68DE83D8D01F06F46B0AEBFE8E4B346376A7937FD3BC11DDF98E7263A63F08D3E44 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O.....https://abs.twimg.com/responsive-web/client-web/bundle.HomeTimeline.d264a675.js(window.webpackJsonp=window.webpackJsonp\|\|[]).push([[60],{"/n9r":function(e,t,n){"use strict";n.r(t);const s={argumentDefinitions:[],kind:"Fragment",metadata:null,name:"TopicPivot_topic",selections:[{alias:null,args:null,kind:"ScalarField",name:"topic_id",storageKey:null},{alias:null,args:null,kind:"ScalarField",name:"name",storageKey:null}],type:"Topic",abstractKey:null,hash:"0572573667f235d11350335060916856"};t.default=s},cOLG:function(e,t,n){"use strict";n.r(t),n.d(t,"HomeTimeline",(function(){return zt}));var s=n("KEM+"),i=n.n(s),a=n("ERkP"),l=n("es0u"),o=n("wM4e"),r=n("kHBp"),c=n("wqZ5"),d=n("rxPX");const u=e=>{const t=Object(c.f)(e);return r.a.selectMany(e,t)\|\|[]};var m=Object(d.a)().propsFromState(((()=>({configurationFetchStatus:o.a,pinnedLists:u,selectedTimelineId:o.c,useLatest:o.d})))).propsFromActions(((()=>({clearLocalPinnedListStorage:c.a,fetchPins:c.c,updateBehavior:o.e})))) |

| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\8f7abdeb3486c1b8780fede76afc20e044eff1b5\b420a012-da80-49b0-9aaa-1f6425dc924b\3dd68853f8462d0e_1 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 50327 |
| Entropy (8bit): | 6.277935146691832 |
| Encrypted: | false |
| SSDEEP: | 768:DkU84416+K911+lzwUeda6Oyf8f1Qpz4gNuLnIOqfhwxJIwmC:Dkh44Qx1Uj37W8tQegLOqfhwxTmC |
| MD5: | FF5E7004C8E7A19CA86FAD1F7F348567 |
| SHA1: | 2FAF5439D9158C4F72A381A180267CDCEACC5196 |
| SHA-256: | 5266D557AEF2DBA3403B076DDA9C9ED27B0DF396BDA63FA3E6F6D264033C78D1 |
| SHA-512: | A2A0C72399EC35DAD3C54B829E38278B15AFC28CE99A6BCCE75AD0D310C693089E38A63A2C81DF8913AEFE04F9E5544A5218B99401336A6871BDF6487D0B1F6F |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....O.....https://abs.twimg.com/responsive-web/client-web/bundle.HomeTimeline.d264a675.js.....'.W[....O.....O.....H.....@.....(S.\|..`.....4L`.....Qcv.I....window....Qd.W.....webpackJsonp..QbJ.\....push.....`.....L`.....`.....Ma....x...`.....$..a.....Qb.j=...../n9rC..QbN.....cOLGC..Qb. .{....yKhEC.(S.<.`2.....L`.....Qb..\.....r....L.a"..... Qf..$.....argumentDefinitions....`....]..Qb.....kind..Qc.T4.....Fragment..QcJ.x.....metadataF.....Qe...B....TopicPivot_topic..Qd.....selections.....`.....L`.....4.a.....Qc.\|9.....alias...F..QbV.....argsF..q...Qd.....ScalarField....Qc.1....topic_id..Qd..+.....storageKey..F.4.a.....a.F....F.....F....Qc"vS:....Topic.....Qd.?.....abstractKey.F..Qb...8....hash.,Qi..% ...0572573667f235d11350335060916856.a...K`....Di.... .....(...&.Y....}...&.%.-.....(Rc.....`....Da....V.....c.. .....0 |

# Static File Info

### No static file info

# Network Behavior

### Network Port Distribution

### TCP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:45:51.829359055 CET | 192.168.2.3 | 8.8.8.8 | 0x9a04 | Standard query (0) | syphilisdating.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:51.846143007 CET | 192.168.2.3 | 8.8.8.8 | 0xa961 | Standard query (0) | clients2.google.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:51.854782104 CET | 192.168.2.3 | 8.8.8.8 | 0x3f9 | Standard query (0) | accounts.google.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.318315029 CET | 192.168.2.3 | 8.8.8.8 | 0x23ab | Standard query (0) | www.theknows.net | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.751454115 CET | 192.168.2.3 | 8.8.8.8 | 0x6d3a | Standard query (0) | uploads-ssl.webflow.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.755397081 CET | 192.168.2.3 | 8.8.8.8 | 0xa296 | Standard query (0) | d3e54v103j8qbb.cloudfront.net | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.344069004 CET | 192.168.2.3 | 8.8.8.8 | 0x19ec | Standard query (0) | uploads-ssl.webflow.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.471080065 CET | 192.168.2.3 | 8.8.8.8 | 0xd010 | Standard query (0) | clients2.googleusercontent.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:01.894984007 CET | 192.168.2.3 | 8.8.8.8 | 0xd01e | Standard query (0) | twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.233084917 CET | 192.168.2.3 | 8.8.8.8 | 0xc9eb | Standard query (0) | abs.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.257603884 CET | 192.168.2.3 | 8.8.8.8 | 0x9310 | Standard query (0) | pbs.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.258335114 CET | 192.168.2.3 | 8.8.8.8 | 0xce2e | Standard query (0) | api.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.547348976 CET | 192.168.2.3 | 8.8.8.8 | 0x79d4 | Standard query (0) | t.co | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.551541090 CET | 192.168.2.3 | 8.8.8.8 | 0x1af7 | Standard query (0) | video.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:06.399866104 CET | 192.168.2.3 | 8.8.8.8 | 0x55c3 | Standard query (0) | abs.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:11.317236900 CET | 192.168.2.3 | 8.8.8.8 | 0x50e0 | Standard query (0) | pbs.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:11.425852060 CET | 192.168.2.3 | 8.8.8.8 | 0x8f96 | Standard query (0) | abs-0.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:16.838130951 CET | 192.168.2.3 | 8.8.8.8 | 0x4321 | Standard query (0) | abs-0.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:28.981399059 CET | 192.168.2.3 | 8.8.8.8 | 0x6ac3 | Standard query (0) | help.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:30.173296928 CET | 192.168.2.3 | 8.8.8.8 | 0x16dd | Standard query (0) | platform.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:31.368887901 CET | 192.168.2.3 | 8.8.8.8 | 0xb08a | Standard query (0) | fonts.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.821285009 CET | 192.168.2.3 | 8.8.8.8 | 0x7513 | Standard query (0) | stats.g.doubleclick.net | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.835850000 CET | 192.168.2.3 | 8.8.8.8 | 0x3f83 | Standard query (0) | syndication.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:33.020572901 CET | 192.168.2.3 | 8.8.8.8 | 0xade2 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:46:53.696703911 CET | 192.168.2.3 | 8.8.8.8 | 0xc2d9 | Standard query (0) | theknows.net | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:54.105703115 CET | 192.168.2.3 | 8.8.8.8 | 0xe8d1 | Standard query (0) | www.theknows.net | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:02.104238033 CET | 192.168.2.3 | 8.8.8.8 | 0xdfef | Standard query (0) | twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.055228949 CET | 192.168.2.3 | 8.8.8.8 | 0x5618 | Standard query (0) | api.twitter.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.224598885 CET | 192.168.2.3 | 8.8.8.8 | 0x6454 | Standard query (0) | video.twimg.com | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:48:05.810547113 CET | 192.168.2.3 | 8.8.8.8 | 0x2324 | Standard query (0) | api.twitter.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:45:51.874398947 CET | 8.8.8.8 | 192.168.2.3 | 0xa961 | No error (0) | clients2.google.com | clients.l.google.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:45:51.874398947 CET | 8.8.8.8 | 192.168.2.3 | 0xa961 | No error (0) | clients.l.google.com | | 142.250.181.238 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:51.882030010 CET | 8.8.8.8 | 192.168.2.3 | 0x3f9 | No error (0) | accounts.google.com | | 142.250.184.205 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:51.942615986 CET | 8.8.8.8 | 192.168.2.3 | 0x9a04 | No error (0) | syphilisdating.com | | 216.70.123.100 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.349898100 CET | 8.8.8.8 | 192.168.2.3 | 0x23ab | No error (0) | www.theknows.net | proxy-ssl.webflow.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:45:52.349898100 CET | 8.8.8.8 | 192.168.2.3 | 0x23ab | No error (0) | proxy-ssl.webflow.com | proxy-ssl-geo.webflow.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:45:52.349898100 CET | 8.8.8.8 | 192.168.2.3 | 0x23ab | No error (0) | proxy-ssl-geo.webflow.com | | 3.248.8.137 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.349898100 CET | 8.8.8.8 | 192.168.2.3 | 0x23ab | No error (0) | proxy-ssl-geo.webflow.com | | 52.212.43.230 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.349898100 CET | 8.8.8.8 | 192.168.2.3 | 0x23ab | No error (0) | proxy-ssl-geo.webflow.com | | 52.49.198.28 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.774988890 CET | 8.8.8.8 | 192.168.2.3 | 0x6d3a | No error (0) | uploads-ssl.webflow.com | | 13.224.96.82 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.774988890 CET | 8.8.8.8 | 192.168.2.3 | 0x6d3a | No error (0) | uploads-ssl.webflow.com | | 13.224.96.104 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.774988890 CET | 8.8.8.8 | 192.168.2.3 | 0x6d3a | No error (0) | uploads-ssl.webflow.com | | 13.224.96.80 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.774988890 CET | 8.8.8.8 | 192.168.2.3 | 0x6d3a | No error (0) | uploads-ssl.webflow.com | | 13.224.96.72 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.779629946 CET | 8.8.8.8 | 192.168.2.3 | 0xa296 | No error (0) | d3e54v103j8qbb.cloudfront.net | | 13.224.98.50 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.779629946 CET | 8.8.8.8 | 192.168.2.3 | 0xa296 | No error (0) | d3e54v103j8qbb.cloudfront.net | | 13.224.98.171 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.779629946 CET | 8.8.8.8 | 192.168.2.3 | 0xa296 | No error (0) | d3e54v103j8qbb.cloudfront.net | | 13.224.98.110 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:52.779629946 CET | 8.8.8.8 | 192.168.2.3 | 0xa296 | No error (0) | d3e54v103j8qbb.cloudfront.net | | 13.224.98.99 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:53.443701982 CET | 8.8.8.8 | 192.168.2.3 | 0xec1a | No error (0) | www-googletagmanager.l.google.com | | 142.250.186.136 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:53.650718927 CET | 8.8.8.8 | 192.168.2.3 | 0xfa73 | No error (0) | gstaticadssl.l.google.com | | 142.250.186.163 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:53.765357018 CET | 8.8.8.8 | 192.168.2.3 | 0xb197 | No error (0) | www-google-analytics.l.google.com | | 142.250.186.78 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:45:55.363598108 CET | 8.8.8.8 | 192.168.2.3 | 0x19ec | No error (0) | uploads-ssl.webflow.com | | 13.224.96.82 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.363598108 CET | 8.8.8.8 | 192.168.2.3 | 0x19ec | No error (0) | uploads-ssl.webflow.com | | 13.224.96.104 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.363598108 CET | 8.8.8.8 | 192.168.2.3 | 0x19ec | No error (0) | uploads-ssl.webflow.com | | 13.224.96.80 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.363598108 CET | 8.8.8.8 | 192.168.2.3 | 0x19ec | No error (0) | uploads-ssl.webflow.com | | 13.224.96.72 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:45:55.498737097 CET | 8.8.8.8 | 192.168.2.3 | 0xd010 | No error (0) | clients2.googleusercontent.com | googlehosted.l.googleusercontent.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:45:55.498737097 CET | 8.8.8.8 | 192.168.2.3 | 0xd010 | No error (0) | googlehosted.l.googleusercontent.com | | 142.250.181.225 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:01.913779974 CET | 8.8.8.8 | 192.168.2.3 | 0xd01e | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:01.913779974 CET | 8.8.8.8 | 192.168.2.3 | 0xd01e | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.254049063 CET | 8.8.8.8 | 192.168.2.3 | 0xc9eb | No error (0) | abs.twimg.com | cs510.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.254049063 CET | 8.8.8.8 | 192.168.2.3 | 0xc9eb | No error (0) | cs510.wpc.edgecastcdn.net | | 152.199.21.141 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.277132034 CET | 8.8.8.8 | 192.168.2.3 | 0xce2e | No error (0) | api.twitter.com | tpop-api.twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.277132034 CET | 8.8.8.8 | 192.168.2.3 | 0xce2e | No error (0) | tpop-api.twitter.com | | 104.244.42.2 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.277132034 CET | 8.8.8.8 | 192.168.2.3 | 0xce2e | No error (0) | tpop-api.twitter.com | | 104.244.42.66 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.277132034 CET | 8.8.8.8 | 192.168.2.3 | 0xce2e | No error (0) | tpop-api.twitter.com | | 104.244.42.194 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.277132034 CET | 8.8.8.8 | 192.168.2.3 | 0xce2e | No error (0) | tpop-api.twitter.com | | 104.244.42.130 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.278831005 CET | 8.8.8.8 | 192.168.2.3 | 0x9310 | No error (0) | pbs.twimg.com | cs196.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.278831005 CET | 8.8.8.8 | 192.168.2.3 | 0x9310 | No error (0) | cs196.wac.edgecastcdn.net | cs2-wac.apr-8315.edgecastdns.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.278831005 CET | 8.8.8.8 | 192.168.2.3 | 0x9310 | No error (0) | cs2-wac-eu.8315.ecdns.net | cs672.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.278831005 CET | 8.8.8.8 | 192.168.2.3 | 0x9310 | No error (0) | cs672.wac.edgecastcdn.net | | 192.229.233.50 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.566250086 CET | 8.8.8.8 | 192.168.2.3 | 0x79d4 | No error (0) | t.co | | 104.244.42.69 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.566250086 CET | 8.8.8.8 | 192.168.2.3 | 0x79d4 | No error (0) | t.co | | 104.244.42.5 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.566250086 CET | 8.8.8.8 | 192.168.2.3 | 0x79d4 | No error (0) | t.co | | 104.244.42.133 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.566250086 CET | 8.8.8.8 | 192.168.2.3 | 0x79d4 | No error (0) | t.co | | 104.244.42.197 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:02.584367037 CET | 8.8.8.8 | 192.168.2.3 | 0x1af7 | No error (0) | video.twimg.com | cs296.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.584367037 CET | 8.8.8.8 | 192.168.2.3 | 0x1af7 | No error (0) | cs296.wpc.edgecastcdn.net | cs2-wpc.apr-8315.edgecastdns.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:02.584367037 CET | 8.8.8.8 | 192.168.2.3 | 0x1af7 | No error (0) | cs2-wpc-eu.8315.ecdns.net | cs189.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:46:02.584367037 CET | 8.8.8.8 | 192.168.2.3 | 0x1af7 | No error (0) | cs189.wpc.edgecastcdn.net | | 68.232.34.217 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:06.418548107 CET | 8.8.8.8 | 192.168.2.3 | 0x55c3 | No error (0) | abs.twimg.com | cs510.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:06.418548107 CET | 8.8.8.8 | 192.168.2.3 | 0x55c3 | No error (0) | cs510.wpc.edgecastcdn.net | | 152.199.21.141 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:11.336865902 CET | 8.8.8.8 | 192.168.2.3 | 0x50e0 | No error (0) | pbs.twimg.com | cs196.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:11.336865902 CET | 8.8.8.8 | 192.168.2.3 | 0x50e0 | No error (0) | cs196.wac.edgecastcdn.net | cs2-wac.apr-8315.edgecastdns.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:11.336865902 CET | 8.8.8.8 | 192.168.2.3 | 0x50e0 | No error (0) | cs2-wac-eu.8315.ecdns.net | cs45.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:11.336865902 CET | 8.8.8.8 | 192.168.2.3 | 0x50e0 | No error (0) | cs45.wac.edgecastcdn.net | | 93.184.220.70 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:11.445400953 CET | 8.8.8.8 | 192.168.2.3 | 0x8f96 | No error (0) | abs-0.twimg.com | abs-zero.twimg.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:11.445400953 CET | 8.8.8.8 | 192.168.2.3 | 0x8f96 | No error (0) | abs-zero.twimg.com | | 104.244.43.131 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:16.854762077 CET | 8.8.8.8 | 192.168.2.3 | 0x4321 | No error (0) | abs-0.twimg.com | abs-zero.twimg.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:16.854762077 CET | 8.8.8.8 | 192.168.2.3 | 0x4321 | No error (0) | abs-zero.twimg.com | | 104.244.43.131 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:29.000910044 CET | 8.8.8.8 | 192.168.2.3 | 0x6ac3 | No error (0) | help.twitter.com | s.twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:29.000910044 CET | 8.8.8.8 | 192.168.2.3 | 0x6ac3 | No error (0) | s.twitter.com | | 104.244.42.195 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:29.000910044 CET | 8.8.8.8 | 192.168.2.3 | 0x6ac3 | No error (0) | s.twitter.com | | 104.244.42.3 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:29.000910044 CET | 8.8.8.8 | 192.168.2.3 | 0x6ac3 | No error (0) | s.twitter.com | | 104.244.42.67 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:29.000910044 CET | 8.8.8.8 | 192.168.2.3 | 0x6ac3 | No error (0) | s.twitter.com | | 104.244.42.131 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:30.196146965 CET | 8.8.8.8 | 192.168.2.3 | 0x16dd | No error (0) | platform.twitter.com | cs472.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:30.196146965 CET | 8.8.8.8 | 192.168.2.3 | 0x16dd | No error (0) | cs472.wac.edgecastcdn.net | cs1-apr-8315.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:30.196146965 CET | 8.8.8.8 | 192.168.2.3 | 0x16dd | No error (0) | cs1-apr-8315.wac.edgecastcdn.net | wac.apr-8315.edgecastdns.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:30.196146965 CET | 8.8.8.8 | 192.168.2.3 | 0x16dd | No error (0) | cs1-lb-eu.8315.ecdns.net | cs41.wac.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:30.196146965 CET | 8.8.8.8 | 192.168.2.3 | 0x16dd | No error (0) | cs41.wac.edgecastcdn.net | | 93.184.220.66 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:31.386688948 CET | 8.8.8.8 | 192.168.2.3 | 0xb08a | No error (0) | fonts.twitter.com | s.twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:31.386688948 CET | 8.8.8.8 | 192.168.2.3 | 0xb08a | No error (0) | s.twitter.com | | 104.244.42.3 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:31.386688948 CET | 8.8.8.8 | 192.168.2.3 | 0xb08a | No error (0) | s.twitter.com | | 104.244.42.131 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:31.386688948 CET | 8.8.8.8 | 192.168.2.3 | 0xb08a | No error (0) | s.twitter.com | | 104.244.42.67 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:31.386688948 CET | 8.8.8.8 | 192.168.2.3 | 0xb08a | No error (0) | s.twitter.com | | 104.244.42.195 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:46:32.852761984 CET | 8.8.8.8 | 192.168.2.3 | 0x3f83 | No error (0) | syndication.twitter.com | | 104.244.42.136 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.852761984 CET | 8.8.8.8 | 192.168.2.3 | 0x3f83 | No error (0) | syndication.twitter.com | | 104.244.42.72 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.852761984 CET | 8.8.8.8 | 192.168.2.3 | 0x3f83 | No error (0) | syndication.twitter.com | | 104.244.42.200 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.852761984 CET | 8.8.8.8 | 192.168.2.3 | 0x3f83 | No error (0) | syndication.twitter.com | | 104.244.42.8 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.861613989 CET | 8.8.8.8 | 192.168.2.3 | 0x7513 | No error (0) | stats.g.doubleclick.net | stats.l.doubleclick.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:32.861613989 CET | 8.8.8.8 | 192.168.2.3 | 0x7513 | No error (0) | stats.l.doubleclick.net | | 74.125.140.155 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.861613989 CET | 8.8.8.8 | 192.168.2.3 | 0x7513 | No error (0) | stats.l.doubleclick.net | | 74.125.140.154 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.861613989 CET | 8.8.8.8 | 192.168.2.3 | 0x7513 | No error (0) | stats.l.doubleclick.net | | 74.125.140.157 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:32.861613989 CET | 8.8.8.8 | 192.168.2.3 | 0x7513 | No error (0) | stats.l.doubleclick.net | | 74.125.140.156 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:33.039962053 CET | 8.8.8.8 | 192.168.2.3 | 0xade2 | No error (0) | www.google.com | | 142.250.185.164 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:53.718411922 CET | 8.8.8.8 | 192.168.2.3 | 0xc2d9 | No error (0) | theknows.net | | 99.83.190.102 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:53.718411922 CET | 8.8.8.8 | 192.168.2.3 | 0xc2d9 | No error (0) | theknows.net | | 75.2.70.75 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:54.131526947 CET | 8.8.8.8 | 192.168.2.3 | 0xe8d1 | No error (0) | www.theknows.net | proxy-ssl.webflow.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:54.131526947 CET | 8.8.8.8 | 192.168.2.3 | 0xe8d1 | No error (0) | proxy-ssl.webflow.com | proxy-ssl-geo.webflow.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:46:54.131526947 CET | 8.8.8.8 | 192.168.2.3 | 0xe8d1 | No error (0) | proxy-ssl-geo.webflow.com | | 52.49.198.28 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:54.131526947 CET | 8.8.8.8 | 192.168.2.3 | 0xe8d1 | No error (0) | proxy-ssl-geo.webflow.com | | 52.212.43.230 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:54.131526947 CET | 8.8.8.8 | 192.168.2.3 | 0xe8d1 | No error (0) | proxy-ssl-geo.webflow.com | | 3.248.8.137 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:46:54.965967894 CET | 8.8.8.8 | 192.168.2.3 | 0x44cf | No error (0) | gstaticadssl.l.google.com | | 142.250.186.163 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:02.122874975 CET | 8.8.8.8 | 192.168.2.3 | 0xdfef | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:02.122874975 CET | 8.8.8.8 | 192.168.2.3 | 0xdfef | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.073988914 CET | 8.8.8.8 | 192.168.2.3 | 0x5618 | No error (0) | api.twitter.com | tpop-api.twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:47:03.073988914 CET | 8.8.8.8 | 192.168.2.3 | 0x5618 | No error (0) | tpop-api.twitter.com | | 104.244.42.130 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.073988914 CET | 8.8.8.8 | 192.168.2.3 | 0x5618 | No error (0) | tpop-api.twitter.com | | 104.244.42.194 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.073988914 CET | 8.8.8.8 | 192.168.2.3 | 0x5618 | No error (0) | tpop-api.twitter.com | | 104.244.42.66 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.073988914 CET | 8.8.8.8 | 192.168.2.3 | 0x5618 | No error (0) | tpop-api.twitter.com | | 104.244.42.2 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:47:03.246315956 CET | 8.8.8.8 | 192.168.2.3 | 0x6454 | No error (0) | video.twimg.com | cs296.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 15, 2022 02:47:03.246315956 CET | 8.8.8.8 | 192.168.2.3 | 0x6454 | No error (0) | cs296.wpc.edgecastcdn.net | cs2-wpc.apr-8315.edgecastdns.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:47:03.246315956 CET | 8.8.8.8 | 192.168.2.3 | 0x6454 | No error (0) | cs2-wpc-eu.8315.ecdns.net | cs189.wpc.edgecastcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:47:03.246315956 CET | 8.8.8.8 | 192.168.2.3 | 0x6454 | No error (0) | cs189.wpc.edgecastcdn.net | | 68.232.34.217 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:48:05.827315092 CET | 8.8.8.8 | 192.168.2.3 | 0x2324 | No error (0) | api.twitter.com | tpop-api.twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Jan 15, 2022 02:48:05.827315092 CET | 8.8.8.8 | 192.168.2.3 | 0x2324 | No error (0) | tpop-api.twitter.com | | 104.244.42.2 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:48:05.827315092 CET | 8.8.8.8 | 192.168.2.3 | 0x2324 | No error (0) | tpop-api.twitter.com | | 104.244.42.130 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:48:05.827315092 CET | 8.8.8.8 | 192.168.2.3 | 0x2324 | No error (0) | tpop-api.twitter.com | | 104.244.42.194 | A (IP address) | IN (0x0001) |
| Jan 15, 2022 02:48:05.827315092 CET | 8.8.8.8 | 192.168.2.3 | 0x2324 | No error (0) | tpop-api.twitter.com | | 104.244.42.66 | A (IP address) | IN (0x0001) |

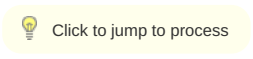
### HTTP Request Dependency Graph

- syphilisdating.com
- https:
  - theknows.net

## Code Manipulations

## Statistics

### Behavior




## System Behavior

### Analysis Process: chrome.exe PID: 3144 Parent PID: 568

#### General

| | |
|---|---|
| Start time: | 02:45:48 |
| Start date: | 15/01/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://Syphilisdating.com |
| Imagebase: | 0x7ff68b0a0000 |
| File size: | 2150896 bytes |
| MD5 hash: | C139654B5C1438A95B321BB01AD63EF6 |

Copyright Joe Security LLC 2022

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

**File Activities** Show Windows behavior

**Registry Activities** Show Windows behavior

**Key Value Modified**

## Analysis Process: chrome.exe PID: 3092 Parent PID: 3144

### General

| | |
|---|---|
| Start time: | 02:45:49 |
| Start date: | 15/01/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1608,3812998973630460944,21257800019593285875,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8 |
| Imagebase: | 0x7ff68b0a0000 |
| File size: | 2150896 bytes |
| MD5 hash: | C139654B5C1438A95B321BB01AD63EF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

**File Activities** Show Windows behavior

## Analysis Process: chrome.exe PID: 7876 Parent PID: 3144

### General

| | |
|---|---|
| Start time: | 02:46:12 |
| Start date: | 15/01/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1608,3812998973630460944,212578001 9593285875,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3636 /prefetch:8 |
| Imagebase: | 0x7ff68b0a0000 |
| File size: | 2150896 bytes |
| MD5 hash: | C139654B5C1438A95B321BB01AD63EF6 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

# Disassembly

## Code Analysis

Copyright Joe Security LLC 2022