ID: 444561
Cookbook: browseurl.jbs
Time: 10:54:53
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

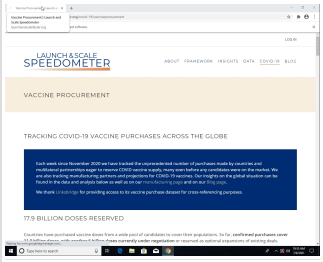
Windows Analysis Report https://launchandscalefaster.…

Overview

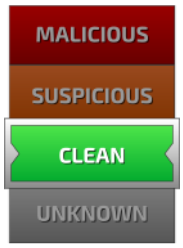
General Information

Sample URL:	http://https://launchandscalefaster.org/covid-19/vaccineprocurement
Analysis ID:	444561
Infos:	

Most interesting Screenshot:



Detection

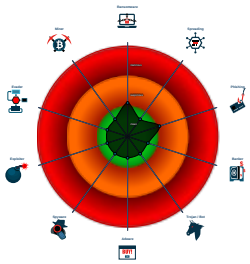


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3504 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://launchandscalefaster.org/covid-19/vaccineprocurement' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4684 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1596,581490905583178796 1,2700687591494063260,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1784 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6844 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1596,581490905583178796 1,2700687591494063260,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5232 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1596,581490905583178796 1,2700687591494063260,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=996 /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

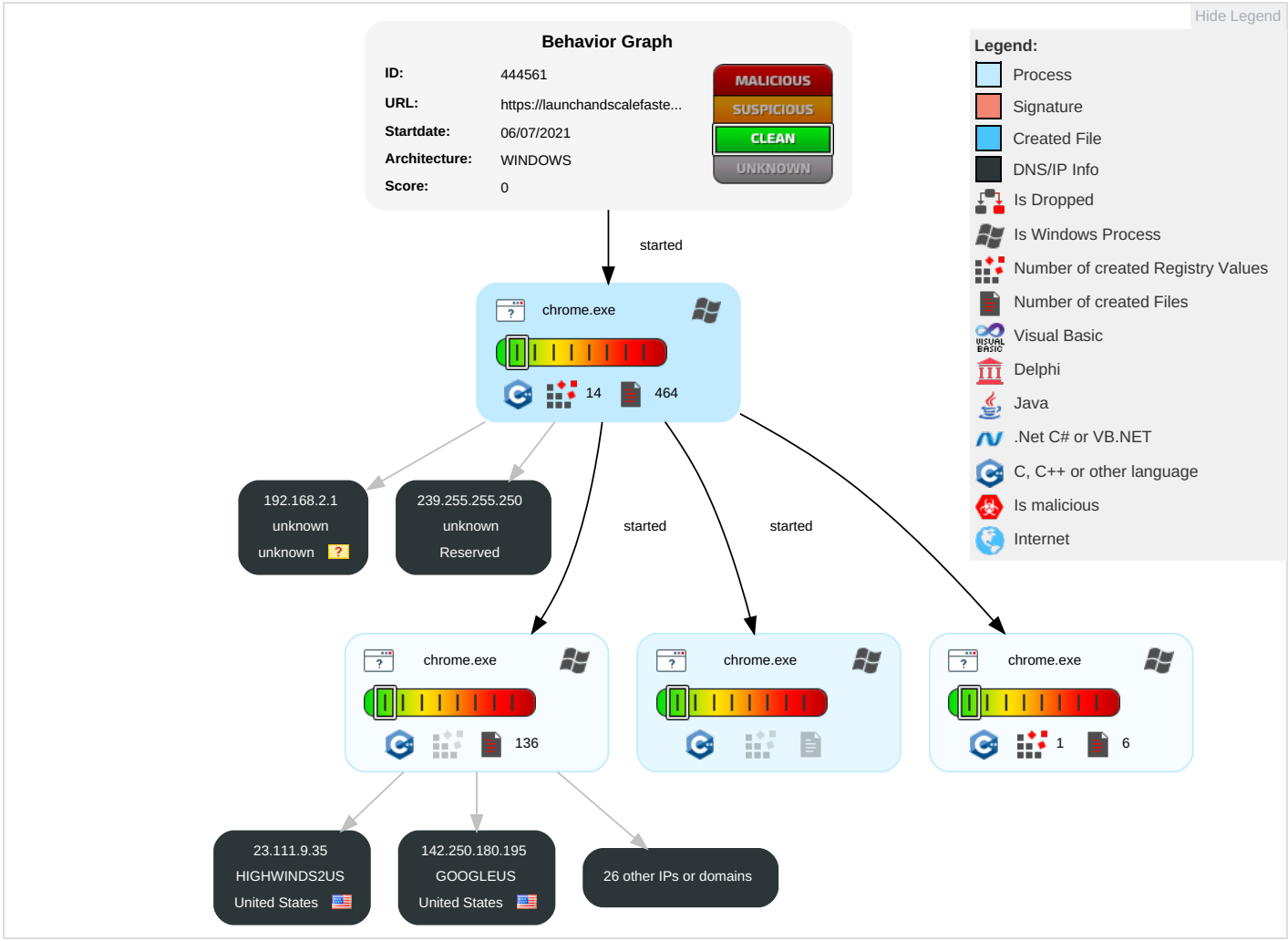
Click to jump to signature section

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	Impact
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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

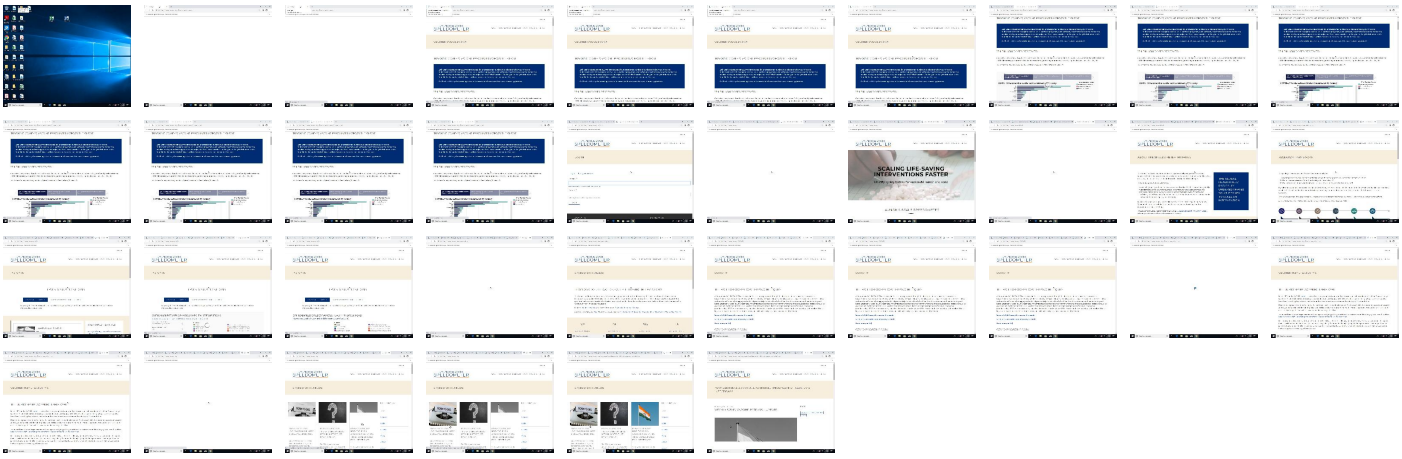
Behavior Graph

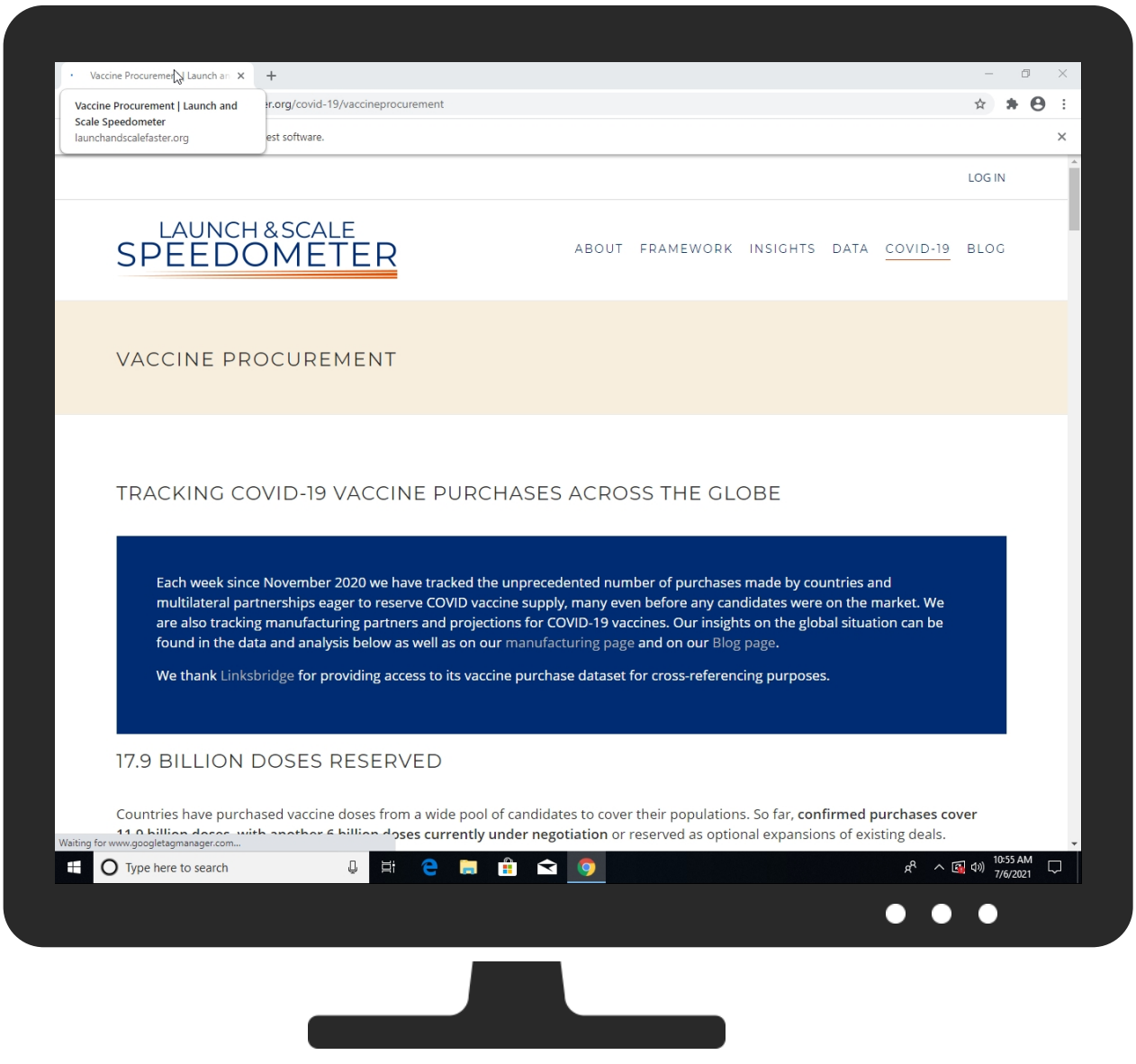


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://launchandscalefaster.org/covid-19/vaccineprocurement	4%	Virustotal		Browse
http://https://launchandscalefaster.org/covid-19/vaccineprocurement	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://launchandscalefaster.org/covid-19/vaccineprocurement%	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-contentVaccine	4%	Virustotal		Browse
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-contentVaccine	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/insights7	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurement2	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurementVaccine	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/speedometer-datau	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccinemanufacturing4Vaccine	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccinemanufacturing-	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-content22Vaccine	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/O	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/sites/default/files/js/js_xls8cObNQq9FQqHFwo2VpyLTkfP3RxVC2C7aT-TuE	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/COVID-19	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/user/login&	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/insights.%Vl	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://launchandscalefaster.org/aboutAbout	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-contentA	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-content2Vaccine	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/COVID-19COVID-19	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org//	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.orgh	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/sites/default/files/favicon.png	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.youtube.com(	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/research-frameworkResearch	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/insightsInsights	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/blog/Speedometer	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/user/loginLog	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://launchandscalefaster.org/speedometer-dataSpeedometer	0%	Avira URL Cloud	safe	
http://https://launchandscalefaster.org/covid-19/vaccinemanufacturingVaccine	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://public.tableau.com/views/ProcurementVisualsnew/Story2?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en&publish=yes&:loadOrderID=3	false		high
http://https://public.tableau.com/views/HealthInterventionTimelineLMICandfilers/InterventionTimeline?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en-US&:loadOrderID=0	false		high
http://https://launchandscalefaster.org/user/login	false		unknown
http://https://public.tableau.com/views/ProcurementVisualsnew/Story1?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en&:loadOrderID=1	false		high
http://https://public.tableau.com/views/DonationCharts/Story1?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en-US&:loadOrderID=2	false		high
http://https://public.tableau.com/views/ApprovalStatusnew/Dashboard22?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en&publish=yes&:loadOrderID=4	false		high
http://https://launchandscalefaster.org/covid-19/vaccinemanufacturing	false		unknown
http://https://public.tableau.com/views/Waterfallchart_16161757876540/WaterfallChart?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:tabs=no&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:language=en&publish=yes&:loadOrderID=0	false		high
http://https://launchandscalefaster.org/insights	false		unknown
http://https://launchandscalefaster.org/covid-19/vaccineprocurement	false		unknown
http://https://launchandscalefaster.org/covid-19/vaccineprocurement#main-content	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.9.35	unknown	United States		33438	HIGHWINDS2US	false
172.217.19.106	unknown	United States		15169	GOOGLEUS	false
143.204.98.119	unknown	United States		16509	AMAZON-02US	false
172.217.16.98	unknown	United States		15169	GOOGLEUS	false
142.250.180.225	unknown	United States		15169	GOOGLEUS	false
142.250.180.206	unknown	United States		15169	GOOGLEUS	false
172.217.19.100	unknown	United States		15169	GOOGLEUS	false
216.58.214.214	unknown	United States		15169	GOOGLEUS	false
172.217.19.102	unknown	United States		15169	GOOGLEUS	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
142.250.201.195	unknown	United States		15169	GOOGLEUS	false
23.185.0.4	unknown	United States		54113	FASTLYUS	false
162.247.243.146	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.1.229	unknown	United States		54113	FASTLYUS	false
142.250.180.238	unknown	United States		15169	GOOGLEUS	false
216.58.214.205	unknown	United States		15169	GOOGLEUS	false
151.101.1.27	unknown	United States		54113	FASTLYUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
172.217.20.1	unknown	United States		15169	GOOGLEUS	false
172.217.20.3	unknown	United States		15169	GOOGLEUS	false
74.125.173.167	unknown	United States		15169	GOOGLEUS	false
172.217.19.99	unknown	United States		15169	GOOGLEUS	false
142.250.180.232	unknown	United States		15169	GOOGLEUS	false
142.250.201.202	unknown	United States		15169	GOOGLEUS	false
74.125.173.166	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.201.206	unknown	United States		15169	GOOGLEUS	false
142.250.180.195	unknown	United States		15169	GOOGLEUS	false
143.204.98.69	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444561
Start date:	06.07.2021
Start time:	10:54:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://launchandscalefaster.org/covid-19/vaccineprocurement
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@44/235@0/30
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://launchandscalefaster.org/covid-19/vaccineprocurement#main-content • Browse: https://launchandscalefaster.org/user/login • Browse: https://launchandscalefaster.org/ • Browse: https://launchandscalefaster.org/about • Browse: https://launchandscalefaster.org/research-framework • Browse: https://launchandscalefaster.org/insights • Browse: https://launchandscalefaster.org/speedometer-data • Browse: https://launchandscalefaster.org/COVID-19 • Browse: https://launchandscalefaster.org/covid-19/vaccinemanufacturing • Browse: https://launchandscalefaster.org/blog
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\22b04098-ea3b-4d42-803d-758947da4ed4.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):	173487
Entropy (8bit):	6.079786759415681
Encrypted:	false
SSDEEP:	3072:AVWORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:mhrDmlMaqfIlUOoSiuRz
MD5:	A1FAE64E615CE2FA9E89F5D0CBDBAEEA
SHA1:	F6D8FE6377B80691177A406BFE56BB350F85F69F
SHA-256:	1127B6EB1D05D128A5FF4A3A4B22A8A639A0A02BC410409AF8A2E1F84219A18D
SHA-512:	3E100552666C8BE17BD41180D93F0C4495FE6FCD1DB538C6E64B7131C4ADB607B7761769229762EEC6BBCEDF0057379F2E9AAA56A4DC9AE334D789F1A8A7715E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\22b04098-ea3b-4d42-803d-758947da4ed4.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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\4845e02c-549a-4f21-af50-4589497254de.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):	165022
Entropy (8bit):	6.049835297652404
Encrypted:	false
SSDEEP:	3072:EORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:HrDmlMaqfIlUOoSiuRz
MD5:	9975FE9CED682426478D99080CEF35A0
SHA1:	E2A8E3EC9AE65607489A60B6CC39D7F471DB4303
SHA-256:	BE8BC886F4B549DC8955AA3F3E9F5656CBC20333348E28A79382C6594FE6A5AD
SHA-512:	D83EB1DD51520E86AFA4719BFC6E42D7EF4346DE045E8333544DB260D3BF9CA6AC93F47B05538597957BFA1707ED190DFFDF3B3E6949AF7176D4C75C8E003CF
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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016432941"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\6452c170-6446-44b8-9ff5-5ed3d5ea9490.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):	173487
Entropy (8bit):	6.079783765231921
Encrypted:	false
SSDEEP:	3072:mBGORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:0xrDmlMaqfIlUOoSiuRz
MD5:	08A4482FA06D759E03167B0DC57E6474
SHA1:	3E979F0FDD7F698A52F143FC54B7BD21FC8F0E39
SHA-256:	B550DF1E9A9C0F3E61AA3CD28BBDCDD713865E92171667393609174 8F120E1C2
SHA-512:	1CB90C7E8DB2A40AD982E5EE8FC97820D8E09D59ECEEA750848A8DCC1C18727237D4B86E230F318EE9E33DD850601772F86828E81DB48EBE206A5E0E40F7F16
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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016432941"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fa7da86-4608-469d-be80-ba40bb6dc284.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):	173487
Entropy (8bit):	6.079783849833142
Encrypted:	false
SSDEEP:	3072:mqJORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:vgrDmlMaqfIlUOoSiuRz
MD5:	35E25AC8A4F832E349B06F253F416D06
SHA1:	39874C7DB4D0F5C96C46FA9033147CE703BA6595
SHA-256:	3D67D022959E0D0E0C1AABB65EBBE520C3967E0E0FC844CFF3DE65EF0CBBD575
SHA-512:	35BEE5B257B330B50EC2F8E000A0123A46033AC8C23FCE6FF226EAFA34ACAAA53CBCE200ACFC10D427BC60E73FC3A2CF2BE1726542621D17C8168D55DD4F1E9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fa7da86-4608-469d-be80-ba40bb6dc284.tmp	
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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016432941"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\7444f60d-44a9-411b-80d7-bc56843ccb5d.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):	173487
Entropy (8bit):	6.079783613332694
Encrypted:	false
SSDEEP:	3072:AoNORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:bErDmlMaqfIlUOoSiuRz
MD5:	48A8CFBF193B8F16EF0197A424335E9B
SHA1:	DF4AD9B3A84DCB3B35969A1E8029DBC575305326
SHA-256:	577C8A5689C0AACDA3349300DF07C72D905F23F3AC13A43BB7A007DAA5E5E913
SHA-512:	3266BE7E8E75A00F361AA0DA7B2F3ACD02BAC3A8A05AED130E64C30344712BC47EAE601EBE36F504939095044E4C9D5BF1052823F8E3600FDDDA7A2769A515A5
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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\7e2663ad-791d-43a4-a0cf-02b48aa707e0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751888524880474
Encrypted:	false
SSDEEP:	384:1DF+K0rlgbUqVjFKtNmrjv6C3JSohHs1G9kr/c68xxgwkTrr+mnTNvsOOytOoMOi:Byi1pyIQ5MerA68Q/DeOKYiKJ8
MD5:	09DECF851DDCFF4F549D8C3DE55FDEB3
SHA1:	C2CA6D927D62CE19983863A7F7AE8F3320E41D06
SHA-256:	DCA4065BBA81743680E3B332C5884BDE7094CD8056209AE88207494CD003B6E7
SHA-512:	D0729C3A394413A1C497356C3C3DEFCC571EC87453B33FD66A7219D42C86F63A4CC3ED1D39D1818B7927D4D8F58CF340FBF87F369720421A109BDA52476D83C
Malicious:	false
Reputation:	low
Preview:	.t.....*...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....>8.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\98725d32-1ee5-4dfa-88ec-104962420c23.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):	173486
Entropy (8bit):	6.079783255843896
Encrypted:	false
SSDEEP:	3072:AZmORJnCD8+CnwlmeMoclFcbXafIB0u1GOJmA3iuRz:2RrDmlMaqfIlUOoSiuRz
MD5:	13AEC8410B3DF6E3D236F9AE9A595C13
SHA1:	9B75661F35355BBC5B97BE77A709248C4CC5D20C
SHA-256:	FBED600E5715CF8D1B65FBF1D217D3EDA96ACF8F0BEDB4D7A4098505390EE092
SHA-512:	0251A324F28CA84587C837267EFAA48601D8F2806A7873A1941CB2CF8FC8BED6AD2476DBC9558B55329D5E64C90201DDCBBA2D98125B6C49AD9AC134C57E16C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\98725d32-1ee5-4dfa-88ec-104962420c23.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":1.625594142528863e+12,"network":1.625561745e+12,"ticks":95505255.0,"uncertainty":4547160.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\11e27509-053b-4834-b0a3-97eeb10fa3d2.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):	1708
Entropy (8bit):	5.582214568585535
Encrypted:	false
SSDEEP:	48:YNOieU86UUh/y0UnUyKUXmsUiSqPeUer2UefPwUQUenw:XieUFUUJy0UnUyKUWsUiZPeU9UE4UQUD
MD5:	990E70AE542C1038021EDBE77492CF5C
SHA1:	0F7C0E9667D7BEC5C4AECCC74F3E2ED9849E289E
SHA-256:	87A0E4C09570212019E6B1B13ACEF603EF90BA193712D031B570114CC3B83AC5
SHA-512:	25E87A3E75422929544BAE9B0C65AC183F280CFFB1D569B919E3CC893464C228941B36B5142AC30525FFD433E92726DE2C01900699BA90AC6C24C3F089347334
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1657130163.621932,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594163.621938},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1625594446.317978,"host":"S2W7UXXjpqs2bEUXrcsE8d6Fc3UTMUueleXK0yq43L0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594146.317982},{"expiry":1636480542.996594,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594142.996601},{"expiry":1657130142.998173,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594142.998178},{"expiry":1657130142.93813,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\144de5f7-3c7c-46f8-a996-e38f93e589c0.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):	5798
Entropy (8bit):	5.179824414818903
Encrypted:	false
SSDEEP:	96:nACrseMRuymHXcKliok0JCKL8Fkk14bOTQVuwn:nACLMRAXcD4KikkQ
MD5:	B6609C297C7C27858888D92FD484F10A
SHA1:	4A50BD5C685A4F2C67BDBF2D4E42D225F957B474
SHA-256:	752AB56FB2115E16A39B2FF24D5E3AFEBED2CDCC8BC0DD41F5BDF26262DF5055
SHA-512:	E367CC0337A26F9C4678932539DB95001C9C37CF095116F77AB2EB9828EAC6C63901B58FB27EC1185C992130952FB7C7F5EBA27CCC966E52C2A593DD3994E26
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\144de5f7-3c7c-46f8-a996-e38f93e589c0.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270067739713297","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1f167f7d-bb27-4338-84ba-0f0e2810fca9.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):	5797
Entropy (8bit):	5.18096497015638
Encrypted:	false
SSDEEP:	96:nACrseMRuymHXcKIdok0JCKL8JkN4jAbOTQVuwn:nACLMRAXc24KCkN4e
MD5:	F206EF5914D77898F0E87F8FE659180A
SHA1:	4216BABA2E6E04DA16AAC1F4B43E33807284F8CD
SHA-256:	FEED0A12A90E284F8029124F388CA376686232530F2F8C7FE2F6EBD4AF70ADCD
SHA-512:	C6EA3581C24779285AE18413FC6F512EAF7532D487EE869B04F2661EE8CB97F159E278EB8288048AEDC68F2562FBA447BFC63C2AAB619C91B34D52DD15AABEE 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270067739713297","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f43967b-fed9-464b-b507-d910d8709e5b.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
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\32f4ac41-0786-4d31-aa62-85f45c1c2cfb.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):	5771
Entropy (8bit):	5.176417735215762
Encrypted:	false
SSDEEP:	96:nACr/eMRuymHXcKITok0JCKL8Fkk1cbOTQVuwn:nACaMRAXck4KikkE
MD5:	E48BAF198CEEB5CE0AA352C05AE9E3AB
SHA1:	80611598F9F21BC25AEDB34A8849B98D0672DBC8
SHA-256:	505407D3D1EA1A7B19363095BF6794F8A055F704144CFC9D77C570C7646989C4
SHA-512:	DDB3E4256E7C3C65F3D80F999D79EF8EA14A67FE9BE9F01D60D4CE5013FD0715085B5FE9085AAF02751A6E7D1600348E34EA30419DD773AED4B7D992AF05D5 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\32f4ac41-0786-4d31-aa62-85f45c1c2cfb.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270067739713297","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4f552847-70e5-4805-a011-343110d9d5e7.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):	1709
Entropy (8bit):	5.586650981649135
Encrypted:	false
SSDEEP:	48:YpieUK6UUhey0U/UyKUXAUUqPeUer2UefPwUQUenw:SieUfUUsy0U/UyKUQUzPeU9UE4UQUD
MD5:	27502E77F30F6FB4918FDEB3FE4EDD4B
SHA1:	57837324881334DB5F4232B89A164AB3B4410B35
SHA-256:	8BAD066D0B514066CD104E41BE27683B4D97C2D9DB132A2184B116E9393DB831
SHA-512:	C8436D3392903C16CB628BE1A7591EA5EB50D0624DFCCC029235B3B766613AD390730C3F844006C8FE93E33067F7B3A6CBF2DCA200A30E8C3EB56D3C31933F2
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1657130189.896308,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594189.896316},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1625594490.388808,"host":"S2W7UXXjpqs2bEUXrcsE8d6Fc3UTMUueleXK0yq43L0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594190.388813},{"expiry":1636480542.996594,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594142.996601},{"expiry":1657130142.998173,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594142.998178},{"expiry":1657130172.451228,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5df2722c-234d-4438-8633-693713c478fc.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):	1877
Entropy (8bit):	5.586955572240945
Encrypted:	false
SSDEEP:	48:YpieUK6UUhcy0UcUbtSUyAKUXAUUqPeUer2UefPwUQUenw:SieUfUUCy0UcUb0U5KUQUzPeU9UE4UQ2
MD5:	6A1644B82DB28DCEF3C8325CE849A137
SHA1:	8142BFBF325F303D26BD87E8E64241D377984B57
SHA-256:	7BD4A2491BCCFEED55BCA814CD1865E699A0D51DBDCB58BDD95BF2B352ADF775
SHA-512:	FEC005EB9675E195F8960BF193F210528BF08D0C64AEF6A56E3757EB8334841EAA0366A176C257D394DEF5EAF146FBD67FC2692FC55F96FC59B0E78B3F164AFF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1657130189.896308,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594189.896316},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1625594495.906382,"host":"S2W7UXXjpqs2bEUXrcsE8d6Fc3UTMUueleXK0yq43L0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594195.906387},{"expiry":1636480542.996594,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1625594142.996601},{"expiry":1657130196.206613,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1625594196.206617},{"expiry":1657130142.998173,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5e8af5f6-30f3-4627-b909-9db7c91bbe67.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):	5797
Entropy (8bit):	5.1798774672754835
Encrypted:	false
SSDEEP:	96:nACrseMRuymHXcKIlok0JCKL8Fkk14bOTQVuwn:nACLMRAXcu4KikkQ
MD5:	988D91F73917414A361291A96036B34C
SHA1:	63013D58B5629E37D6F192927CA4D1D26A084E8D
SHA-256:	A3929551D1C72D69F83110F4467BC2AB618501C24342C0C5DF71D252C66A99B8
SHA-512:	F63BC76E2C4BB3E5F0D08D6C4F4A46E5F76D52636BC49113B80D43F9DFD038E745392842F749A46023551747B70B98868CE1B394196171A0DBC70C66EAE277B1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5e8af5f6-30f3-4627-b909-9db7c91bbe67.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270067739713297","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c72f3cd-59cf-444e-af7c-e8595cfb2cec.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):	16746
Entropy (8bit):	5.577763151443682
Encrypted:	false
SSDEEP:	384:WD4tcLlrSXg1kXqKf/pUZNCgVLH2HfDyrUnbba4LH:6Ll0g1kXqKf/pUZNCgVLH2HfWrUbmE
MD5:	0CA170FDB411FFE47E339099D722BC98
SHA1:	90FDD0F4668C30090422085AD69D3C9260E2C902
SHA-256:	921DE6EBF903317D8FFBD82FCD2CBDC289BE038105854BDFE9D58682F7BCF308
SHA-512:	4E2F8AD44BB71B6299B92DC764C1410B926BF11796DFA4790F2BD76BDC36749D3583AF9DA4499DA21B4ABD9D670EC070B1B3376A46895CF8EE05DFEBF9F7405
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":"13270067739451882","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\73520262-bf98-4da2-97a1-b54f225492c7.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):	5175
Entropy (8bit):	4.980606825095561
Encrypted:	false
SSDEEP:	96:nACrleMpcKISok0JCKL8Fkk1cbOTQVuwn:nACUMpcT4KikkE
MD5:	5354022C63CDE534E69B16F270F2C121
SHA1:	18CEA5AEB19C6E6542CC1EF141E51AD2CC0A37B9
SHA-256:	3B428812FBB5A317E80B956BEFC83D8012F08D17795C4B799D47CBC287B2026E
SHA-512:	31F740DA69934656E02AE317F440681EC3E135D3AEDCC9AF1B42FE11CA751AF40062ACBDE2DC1C95A9A5CA19F17B6AC0895D8185F53DE672A18C36B05111CE5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270067739713297","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.2349114304099995
Encrypted:	false
SSDEEP:	6:m0FOR4q2PWXp+N23iKKdK9RXXTZIFUtppFoRJZmwPpFoRDkwOWXp+N23iKKdK9Rn:zNva5Kk7XT2FUtpjo7/PjoR5f5Kk7XVJ
MD5:	D6A55ABC45EE8313E90B8FED077C4D9E
SHA1:	524B11D5D5D3CA0F327CDB3B45494EC769AA6A95
SHA-256:	7F055D373661211443829E3008F81EB674B14657DC984FE92EBBE6956B19B5F1
SHA-512:	65B914E5E75B7F787685A5D893224D96C9DDCE0BD28B327198F699CD4BD144AF80ECC7FE4F44696FDC268BB2478D1F5DACE9078DB02983BF058E5FAAC63F60D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/07/06-10:56:07.335 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/06-10:56:07.337 554 Recovering log #3.2021/07/06-10:56:07.337 554 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.2242808484540015
Encrypted:	false
SSDEEP:	6:m0FDq2PWXp+N23iKKdKyDZIFUtppFfrLJZmwPpFfrLDkwOWXp+N23iKKdKyJLJ:zDva5Kk02FUtpj3J/Pj3D5f5KkWJ
MD5:	169A1B85DA2B5142E6D1D6B0F970B5A8
SHA1:	DB1012B13C438FE5DFB20FC1DC5953AD63A0DA4F
SHA-256:	F424420E653BB1421223398AF99A694C62363EBAC0217F4B4B398B026AC9D966
SHA-512:	F1BCA3549E26E9A0D5F6F939ADA7FD2E85E3248AB67577CA92D641F02E1D57A8AC5EAC15FAF99DC053C2BF72407F4A46DD80AFD60E9D954716E34DC46DB96C5
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:56:07.328 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/06-10:56:07.330 554 Recovering log #3.2021/07/06-10:56:07.330 554 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02ed5d1d4ea2f0f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	362
Entropy (8bit):	5.895902535083705
Encrypted:	false
SSDEEP:	6:mePY8pMgdKn1oMuiT6HqHVAeK6tor75QxjNRAEuW8sdAhl:j3tK1oMnTfVXciIWbdOl
MD5:	9772E6326F8423BBCFEAC85C9DEC9D5C
SHA1:	643731593D1BB20400BDB8AEFFF85F6D61C35BCA
SHA-256:	600102A68D0937930F2E1A9DA8376D83B89ABEC7D9E1DB02599FB4EE231B3052
SHA-512:	A774FA97EB004B7661CD145010F3ECC0C991FA2E55F0D35F9C5D7DA5301EDBFF2A4C176927AC0055DB22A35194E0A7D4E671C01F59F1EDB43BA86A11AF1747F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.....u....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/vqlweb.js .https://tableau.com/.N.j.%/.....".....C...1.~.[.../k.Y-.z..D2.....A..Eo.....A..Eo.....N.j.%/...Q.F9D13028F156F65B703A0DD0C16A89682BD2DDB2C270C02C5D5D703ACA1B819DC...1.~.[.../k.Y-.z..D2.....A..Eo.....Z.+~L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d665f7499bc5798_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64128
Entropy (8bit):	5.881497092176856
Encrypted:	false
SSDEEP:	768:v9zzdcYfC5Cz3nuHKeLzke9H0tA2uTIeUaOl4eyD3CfLBG/QQb:v9qYjnteLzkG0K2k1UB4UzB2B
MD5:	612C7DBDA739F5AE9D2ADD9F48C8B54F
SHA1:	A8C91B70697C9C5796782B1B5C8C090783263F72
SHA-256:	F241D18920C7FD52EE17CAD3DBF9AE92784A580D605FCAC29BB6C8A7D14B53D9
SHA-512:	185466DCB6E2E6857467AC2A8C96C86275613ADFD3561F2530569F2B949D575C1755DBEB470BC64825E1935CBA75554668A75389467BAAB3309617E229E6F529
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....\q....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/formatters-and-parsers.en_US.js .https://tableau.com/OL.j.%/.....H~....2[>h`.3J..a...a.....&:.I....A..Eo.....n.'.....A..Eo.....'.....O.....T.mi.....C.....(S....`.....@L`.....Q.@.?.....process...Qb.....node..Qc.....release.....$Q...5h.....localizeGlobalNamespace...Q.@.....window....Q.@..q.....Localize....,..a.....Qe.k.....firstDayOfWeek....Qb..e.....sun..$Qg.K.....prefer24HourTimeCycle...H..QeR.MO....narrowDayNames...D.a.....q...Qb.$.:....S.....Qb.).....mon...Qb..~....M.....Qb.._.....tue...Qb.....T.....Qbn..F....wed...Qb.N.O....W.....Qb..S)....thu.....Qb..4f....fri...Qb..|....F.....Qb..[.....sat.....Qd...l....wideDayNames.D.a.....Qc*>.L....Sunday.....Qc"y{v....Monday.....Qcj]....Tuesday.....Qd..@.....Wednesday...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e8eb3848ac7200a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e8eb3848ac7200a_0	
File Type:	data
Category:	dropped
Size (bytes):	119232
Entropy (8bit):	5.780459370111224
Encrypted:	false
SSDEEP:	3072:8JAK+vala04G7qvrH6oWEGm5JLs3GO3GLz/f/oc1zqfg:XK+vWB4GmvrQwZ1Ok/V1zwg
MD5:	68152A40D2AFF898CD32A429A11DA3DC
SHA1:	5B574A1E1662A17190FFC5519C84088E9913D8C1
SHA-256:	15AD550AA964FEC93D6B7CA41C621BAE92FECC71923724B75F7E4F03D413824F
SHA-512:	025C68EDDC2F4B11CA2C75AB60ECC3D3A443634BB6FE26015B44D933BB1D96FB302CF37B88887828F38D8C4BB90B6BBC6B13D7C30A7CED1AEF3D39AE59CD A4C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...ygM ....6A8CE25639234F3CE98061F2FB1F322CC7BC5EC539CA315E9D50A4AC81F281E9.....'.-q....O$...`.....P.....l2..... .....x.....$.....(S.4..`$.....L`.....(S..`F....8L`.....@Rc.....QbvIFM....s.....Qd..n.....replaceAll....Qb..._....key.b.....I` ....Da....D....(S.....lawm...n.....Q..@.-....\P.a.....N...https://public.tableau.com/vizql/v_202122106250039/javascripts/jsstrings_en.js..a.....D`....D`....D`.....$...`....&...&....&.. 1.&.(S.....5.a.....Qb.;.P....tab....a.....a.....Qc.;B....Strings...Pc.....noLoc..agn..|n....Qcrv.....noLoc.....d.....&.(S.....a.....A....a.....a.....!...Pd.. .....getString..a.n...o....Qd..M.....getString.....Q..d.....&.(S.d..`~.....L`.....4Rc.....Qb..Q%....k...`....I`....Da.....Qcf.....{[^}{]+}..Qb*o.*...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10c1981b03a7533d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.570842899383159
Encrypted:	false
SSDEEP:	6:mqQEY8pMgdKn1nVVdu8lkmuy+4dIbK6t:LtK1nVnRDuAk
MD5:	304E860C09B376BCE18D805B5982D7F0
SHA1:	B4F165B57FB16E220CE05B1B4C537C550F5F789B
SHA-256:	77CCCD516286F2ED738F01303F1916F158DCA22B564B3535D74146963E2F25E0
SHA-512:	2C979CC52C37D81B1878DF1C7A4F8F00B32D86C1F2D05FEE5C1A5CAACC5FEC9CB98AF3E3300552E54AEE6C0E37C66EEE9897BBFF82B9FCA950DD09822762D DBE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...}....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/built-dojo/dojo/dojo.js .https://tableau.com/rA.I.%/.....'.....ej..V.A.. .%...3...., .3. ...A..Eo.....[=$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15bfd1d99f9d0eda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	27479
Entropy (8bit):	5.944691091199111
Encrypted:	false
SSDEEP:	384:c6KE5qVo1w62+ABAx5gqMWMihCrepuBrCtMjYhWohh37CJDPg10zrA7E8RXvZGq:c6KL+cenxCr9BS/pVQTHYE4Xxp
MD5:	2D8B4E60C892B18846F1E3839EEA43E9
SHA1:	FD1BD7D8E12E5B3D5450D2919FD8DB4375967F78
SHA-256:	6DF797F06F83223A720D1BB593F19661852B3A5B20FE9AF648B34B98788D1FAA
SHA-512:	BB5FCA23FC9B21E17A423050A0283539C205FD1BD177FAA6CD69908DF1B87C08FE8E1DE90D27C861182027A2193F5C77B4450EE2AD233A8C2007DAB8D034DB A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...y{v....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/require.min.js .https://tableau.com/?..j.%/.....1.....-..N.t.F...~.....- B.A..Eo.....A..Eo.....'.4>....O.....i..e.{u..... ...t.....L.....(S.@..`<.....L`.....L`.....Qdj.....requirejs.....Qc..Av....require... Q.@..".....define...(S....`.....-L`.....Rc.....V.....Qb.46.....ga.....Qb...8....ka....Qb.....K.....Qb.....L.....Qb.....y.....Qb.....X.....Qb...)....x.....Qb.B^J....e.....Qb.....D... ..Qbjj.....Y.....Qb.!W.....z.....Qb..|#....ha....Qb.....ia....Qb..|....F.....Qb:..Q....ma....Qb~Z.....pa.....Qb.q.a....B.....Qb..#.....C.....Qb../.....H.....Qb.....O.....Qb.r.b....I.....Qb.< .F....N.....Qb.Q.....P.....R....Qb.....T.....Qb...f....qa....Qbf..X....ra....Qb.X.....U.....Qb..2.....na....Qb.....Q.....Qb..J....la....Qb.98E....E.....Qb.3.....ja....Qb~.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\165d0443bc543645_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	370
Entropy (8bit):	5.965394096611811
Encrypted:	false
SSDEEP:	6:m7Y8pMgdKn16V/ua6gYVZobDGvgr5DK6tyPDipdXxWsS61PJZobDGvgrr:2tK1ITNYVZuDLbgPDiXw61PJZuDL

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\165d0443bc543645_0	
MD5:	56E0F1069CCCDD5C504E199B07663D8F
SHA1:	65A4AC71EAEE6083A48C1503F0FE1A911FB858F8
SHA-256:	48110E310F694CBE193276AB30173CD9F43CAFD7705FC00D24AD04AE7DED89C5
SHA-512:	5DBC3178AB8A507EA5484D75C9709CF1EBE0B76C3ACD08B1E515394CDA3A2F31FDC9BDB0317D3B8ED1149A25E25302F03957B3ECE328A031911A8FB15187F93
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....\.(...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/messages.en_US.js .https://tableau.com/.<.j.%/.....?~.....~.B}.$.?..!..@.yb.2w,.....U....A..Eo.....Rb.+.....A..Eo.....<.j.%/.....F3783BA59EDE36901A03E821F94664071F4CFBCA81D2FB2D644B63A4F2335AD8~.B}.$.?..!..@.yb.2w,.....U....A..Eo.....e8L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16f52ae7dd8c3a9b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.9544079505000855
Encrypted:	false
SSDEEP:	6:mDKY8pMgdKn1nCdGFPMu16bSt56/5EsK6th4rZ7g456/5EL:86tK1nbOMUSWfPYZ7gJo
MD5:	6A135CBBEB1B6F1157E9AE8D7571F035
SHA1:	165ED590F54D75B5F9F9C2B9E3227ABC3ABE5B29
SHA-256:	8A944984E0486D0CC95B2D26B2615BFAE91BEDFB1522E9190986E2E28E97629A
SHA-512:	2F18704500EE0AD32642327CDB4271DC29724121F68987DD6B4D4ACDA900CF4ADC25D2A91ECE1DDE3D5088D87CFDC8F707A5811164C706EBC73BA105F95DCB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x.....Y...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/built-dojo/tableau/clientweb.js .https://tableau.com/N..l.%/.....'.....}4..4K4..^.T.B..Zj.#b...q...Y...A..Eo.....MP.<.....A..Eo.....N..l.%/.H8..AF95DAC281D40F297343E876104DB4EA76825849A4D79FEABFB76055D1C93D1F}4..4K4..^.T.B..Zj.#b...q...Y...A..Eo.....R.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35f9b71949ab629e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	166160
Entropy (8bit):	5.940046570766601
Encrypted:	false
SSDEEP:	3072:ZsWwxGNUFmMBPYVsDJC1qfpl/EFWIS376M3AePdg:kGGFmoPisDJbMA1hm
MD5:	CD29F03E293ABDAF236D8B9ACBFAA6C1
SHA1:	B386EBE7647E858AB31CD7535C0B5F540CC23B20
SHA-256:	B3FAFA5AF58DC2A67868BE7E12A460EB6BCA47F7FB3F92D30CDC6F662FE14F30
SHA-512:	B44751596676EB97679111EF6D317BBBB4804DD1580CBD24C553F54AC3B2FFBD6BDC4718AE9817607389E6271EC8A12A91FED98931834DA3A42223C9DB296DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....4.....BF678D3B5C971B1E9E17A599B03D0059EC06BC1F6F815C1D516BC29F017D2AB2.....'.h8....O5...h...;^.B.....(....''..<.....|.....(S.D..`@.....L`.....(S.h.`.....L`.....TRc&.....Qb.....w.....e....d.....I`....Daz.....(S.`.`|.....L`.....PRc$.....QbvIFM....s.....dd.....I`.....5.a.....a.....Pd.....<computed>.ea.....K`....DrP.....%...%.....%... ...&...&..&..`&..k&.'..'..'..a=...&.]....b.....@.-....DP.....5...https://www.googletagmanager.com/gtm.js?id=GTM-WP98PN...a.....D`....D`....D`....`....&...&....&..1.&.(S...''..`pE.....=.L`.....Rc.....Qb.0N....data..Qbr6.>....ba....Qb.]*.....ea....Qb..J....la....Qb...f....qa....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37a7f7aa229f83a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	166160
Entropy (8bit):	5.9400334936999
Encrypted:	false
SSDEEP:	3072:4WwxGNUFmMBPYVsDJC1qfpldEFWIS376M3AePdz:6GGFmoPisDJbmA1hx
MD5:	E0437584D7BBF82162BDECBD649636FA
SHA1:	BE4F67443156DC84448CC745526E88ED81691172
SHA-256:	29A92E972B44B6C80DACBB7548444D4F8900CB32ABB33C9C4AEA0378FDBC67F6
SHA-512:	B9816F7AD56F90BF8F9D6753DF11452D07E7FCA0AA036063E5F6B2D75D29E282D9A007E527EF4FAF36B06663657049AF00AC83618C5A31349C9D53E66653C6C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37a7f7aa229f83a8_0	
Preview:	0\r..m.....@.....16EB74E9A6AA5C83CCF431B026AC16B445180983CC605178A3E7F942E10AA565.....'.h8....O5...h...S^.O.....(....''..<.....|.....(S.D..`@.....L`.....(S.h.`.....L`.....TRc&.....Qb.....w.....e....d.....I`....Daz.....(S.`.`|.....L`.....PRc$.....QbvIFM....s.....dd.....I`.....5.a.....a.....Pd.....<computed>.ea.....K`....DrP.....%...%.....%... ...&...&..&..`&..k&.'..'..'..a=...&.]....b.....@.-....DP.....5...https://www.googletagmanager.com/gtm.js?id=GTM-WP98PN...a.....D`....D`....D`.....`....&...&....&..1.&.(S...''..`pE.....=.L`.....Rc.....Qb.0N....data..Qbr6.>....ba....Qb.]*.....ea....Qb..J....la....Qb...f....qa....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\409b9d5c126c3bcb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.987507418660929
Encrypted:	false
SSDEEP:	6:mY6Y8pMgdKn1rClPMuAb6Uke6rm/lB2p64rxtK6tDC0hPMXpBmoWxrm/lB2p64r:XqtK1rClPMXbVke6y/L2pvlHU0hkZQoO
MD5:	42328CF3189C24E2806FD417C832EC3E
SHA1:	27FF15030ED5386D9A79DFA50F04C1D232E2EEE2
SHA-256:	C8360F388C774F7243D7F2923C6FA67CE8157DCFE115F74011633F309F4A1630
SHA-512:	E1787B91E4837544BC543EA07C56BD527C318D3BD0FD4D48BD9CD18BBEE66FE2E91C605CEE463221A7E78AF5860665FC79CB787D08AE83CD13984936B6E0DEB3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....p....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/mscorlib.min.js .https://tableau.com/.3.j.%/.....}.....?.....}2.....f:..A.....A..Eo.....A..Eo.....3.j.%/..G..A1DBE64D6C7C85C5903DFC5BC771C28F51C6120A8D9943CFAC670421D93252DC?.....}2.....f:..A.....A..Eo.....qX.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43369649f28c1d80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.885199300091722
Encrypted:	false
SSDEEP:	6:m7Y8pMgdKn1muKJUK6yF5RCk4aFakAZ0nK6tw1oTf1m6Q75Tyd40Vzqo/Ck4aFaW:utK1mtxYON1ier1r1a0cXONPt
MD5:	F30E43FE06BD7645FC4D5DE2AEB836D9
SHA1:	CF7B5AF2C549290390AA43BC2FCA8A2D872B1470
SHA-256:	5A66F2364F81F372526A35D1A17E32E80689539EF76561D59759E15A3A3BD1EB
SHA-512:	F186CF5D4FA183D1E66DCD96E2A083BE1C203C8E96C8C72647470F460B5C2B54A8D135DCAE10F1C4E6603346B4A958E79B3D2CD821CD5C18A6B6F909D89E5C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/jquery.min.js .https://tableau.com/./.j.%/.....}.....C.f.\.Z..AK.O#..../.S..:.D.Qp.W..A..Eo.....O.....A..Eo...../.j.%/..(..DEDB4A5C003598F823C35C49D2CBCDB6ABD4C3920073504066418F6E7FD05C7EC.f.\.Z..AK.O#..../.S..:.D.Qp.W..A..Eo.....K&L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c1052befeaf4462_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.893497538501661
Encrypted:	false
SSDEEP:	6:mXY8pMgdKn1PGIuZK6ourK8zhMK6tod1Hk2cUGrQfrK8zh:StK1PGIt7urnz4qd1E2cUGOrnz
MD5:	EDA8D0819B1DCA2B169A941C56D57FC5
SHA1:	066C565F5789D0091188D8C62A7D9734079A5F94
SHA-256:	4DE11688BDD943C001A7013AD5D8BF5789E850FACFB9741EAE25952B60AF20BA
SHA-512:	F5F1354AD214A7152FE690166598624564299 2D60398471D849056080D4EEC13C72BE4600E6E2384616F9DA6E9D76DEEACDAB91294141B3DF294AF92E5E95116
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...r3....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/jsstrings_en.js .https://tableau.com/.7.j.%/.....}.....#..1.._.h.y>d....:[..ra+...v..A..Eo.....<.....A..Eo.....7.j.%/.....6A8CE25639234F3CE98061F2FB1F322CC7BC5EC539CA315E9D50A4AC81F281E9.#..1.._.h.y>d....:[..ra+...v..A..Eo.....I...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fcd60dfe698c991_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fcd60dfe698c991_0	
Size (bytes):	166168
Entropy (8bit):	5.940130159453735
Encrypted:	false
SSDEEP:	3072:YWwxGNUFsMBPYVsDJC1qfpl/EFoIS376M3AePd5:aGGFsoPisDJbMO1hL
MD5:	352A5FAFFF29E6ECF3D0AA857CF89162
SHA1:	19636A07EBCD4F39F0191E79C70D5F68FA6AF579
SHA-256:	34BFBF7876FA46F1B0A2142FD1011A89B22DF3E804B404703B82D73D7E5C33D5
SHA-512:	FEDC77991172286578B3FBF010B0EB1274FFFBECB0F99D11ACAA2939FB06CA95032A4FD7B24FBA317295F875F5B0F7F11A11BA09D7111110E7AC02D1009B7C3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....<.....2EE4D0A19BB64D1362DF124FB9F48DBCF575C3073CE941CBA2E843527CFDA365.....'.h8....O5...p....^.....(....''..<.....|.....(S.D..`@.....L`.....(S.h.`.....L`.....TRc&.....Qb.....w.....e....d.....I`....Daz.....(S.`.`|.....L`.....PRc$.....QbvIFM....s.....dd.....I`.....5.a.....a.....Pd.....<computed>.ea.....K`....DrP.....%...%.....%... ...&...&..&..`&..k&.'..'..'..a=...&.]....b.....@.-....DP.....5...https://www.googletagmanager.com/gtm.js?id=GTM-WP98PN...a.....D`....D`....D`.....`....&...&....&..1.&.(S....''..`pE.....=.L`.....Rc.....Qb.0N....data..Qbr6.>....ba....Qb.]*.....ea....Qb..J....la....Qb...f....qa....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ad95937aa4db68a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.874191355430626
Encrypted:	false
SSDEEP:	12:DEvtK1IC2lUkwb/V7105NgTlUwbQl25NgTlUwbQl:DEwgUV/VpJllQhllQ
MD5:	385361F3EA1A78CB62995B5B9804D2DD
SHA1:	A1DE77F76D50C7A908B2777FF23803A7D0726FF4
SHA-256:	9F91D2B895EA89AE13B79A80A6CF81FF6FF63132920428DED3B8A7529D684F72
SHA-512:	431B519D115751299604850251 0E66F57D43AA3F709D006EE74C844F01A52AA97F547B493651AF878AD99B6B54B427EBE8F82E3A9DDCAD0FA36C85966FFA1F94
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...&^=!...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/runtimeanimweb.js .https://tableau.com/\..j.%/.....^.....}.....^O.tm.W....\8.I.PW.L4.A.A..Eo.....A..Eo.....\..j.%/..u..0FF73F0206103D9FEF94EA28AC0D4C638D3115877B61B056363D8E292DB25A8E}.....^O.tm.W....\8.I.PW.L4.A.A..Eo.....].L.....\..j.%/..u..0FF73F0206103D9FEF94EA28AC0D4C638D3115877B61B056363D8E292DB25A8E}.....^O.tm.W....\8.I.PW.L4.A.A..Eo.....].L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ced4db5eee156e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95776
Entropy (8bit):	5.934771432832331
Encrypted:	false
SSDEEP:	1536:SI1np3EOSXgUFAKUSeWyjXu9vw5dBu5bCghe7zGhdFLE0uyP8fZffigkJ+z7Qo7:Si9E9RFk5WEowJfUNJP8fdfid3s
MD5:	12422562CB0793294F6260B654B55E8F
SHA1:	8CA30D00FDBC36258DF0B78487CC606FDF85F926
SHA-256:	9D0468A2A6C22590BADBB5D5091B696BC82616E044AAE26D8A173C770FAB3795
SHA-512:	D6A1E91A3A7F4E30FDDCD0A0F6032A925C11698A4EA909418CF118E71C6B9EE010B691766FB3DA6CD44E35D7351C10BEF1B267FBFDD4E413E41FA0E062659ECC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....c|.....4DAE3DD3E63495FAF0A5B179981CC4C9C7C95BA139A70BA4FFDAE2ED5C83F2C0.....'..6....O''....t...*.O.....l.....d.....(S.0..`.....L`.....(S.....` !.....L`.....Rc>.....Qb..?.....1....Qbz..e...._2....Qb.....3....Qb.....4....Qb.....5....Qb.cp...._6.....S...Qb..=~...._8.....k.....I`....DaN...(I....Q.@..9t....djConfig..Qc.N.....scopeMap..Q.@.....window..I.M...Qb.RU....var ..Qc.b..... = {}; ...Qb..9.... = ...Qb>kJ^....;....Qev6}....._scopeName = '...Qb.B.....';....r..`..... Qf.GV.....dojo._scopeArgs = [...Qb.'':.....];....Qb...8....dojo..Qe>|.m...._scopePrefixArgs..Qd..#.....(function(....Qb..d4....){....QdZ.uG...._scopePrefix..Qb..).....})(...Qbj.:-....).....Qd''P.[...._scopeSuffix..QdJCr....._scopeMap.....QdZ.....`._scopeMapRevb.....(S....` .....L`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e67df9b409b0748_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164312
Entropy (8bit):	5.754864066405747
Encrypted:	false
SSDEEP:	3072:zclYl+vbBU20Tu5ZkWQ+Hw20Tu5ZkWQ+H:u3b0xL+WxL+
MD5:	21962478125594607B5BA1F56481BDC5
SHA1:	A53792CAD42C4040DF76683C052860A8CB8AEBA4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e67df9b409b0748_0	
SHA-256:	B335CDFC7FAA413934448CCB642FCF6DF2327184B2CD9F86FC27D97602A70DA9
SHA-512:	7292458FFC086D96186E4597690007FC4A3985D9FB78E607BC5BFFA406D69354563AC9AEC3446D440EE47D278E0315806C7043046CA094B9490BFDCC8604022B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...a....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://tableau.com/o3,j.%/.....\.....J9g.j8l^....8O.....GG)..0.b....A..Eo.....'.....A..Eo.....0 \r..m.....F...a....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://tableau.com/..[j.%/.....J9g.j8l^....8O.....GG)..0.b....A..Eo.....!.~.....A..Eo.....0\r. .m.....F...a....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://tableau.com/.....'.#z....O....x.....{1.....$.....(S.....`... ..].L`.....(S.h.`.....L`.....HRc .....QbFk"^....n.....Qb.....t.....Qb..B.....r.....Qb*".9....o...c....$.....I`....Da....8....(S...`.....,L`.....4Rc.....Qb.B^J....e...`$.....`....Da6... .....Q...Q.P..]7....__nr_require.... Qf.. .....Cannot find module '..Qb~.....'.....a.....Q.@.].d....exports....a.....Qb...B....call..1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\604b5e7820f6d837_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	113048
Entropy (8bit):	5.640660039949562
Encrypted:	false
SSDEEP:	1536:TbUziPKRIg2jMTJQ3O53WT3NzHmpHCSbY:+1kjP3OszkiOY
MD5:	0D1A18EC58EA2F1476091D5B2CC5F9B1
SHA1:	DCD905F7E1E18DC87D6881FA0932907AC1285EC6
SHA-256:	1A088323ABB7AABC9ACE001B3FFC54F4E9EA6468D89DD4E87F86DA9031D7D11F
SHA-512:	DBAB317D14787F5728C4988C8985F957CB28B0C109D92F47C46E2D82A3271C26FA8BEA0D18AAE81A705714C91CE035E23C83F31D33C203F118D7CD7FEA5622
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....ff....268AF157460686374016BD42338B6176C20161CD9907447FE46500CE2380D289.....'.....O&...0....9N.....d..... .....l.....(S.0..`.....L`.....(S...e..`.>.....1.L`.....Rcd.....*.....O...Qb..-.....c.....Qb.....d.....Qb.B^J....e.....QbR.....f .....Qb.....h.....Qb..>....j.....Qb..Q%....k.....Qb.N.....l.....QbFk"^....n.....Qb*".9....o.....Qb.....p.....Qb.N.....q.....Qb..B.....r.....QbvIFM....s.....Qb.....t.....R....Qb..f.... .v.....Qb.....w.....Qb...)....x...t.....I`....DaD.....Qb.;.P....tab...Qbn}.....ss....Qd.....initAssembly..Q.@.....vqlstory..Qc. .....mkType...,Qi..7K ...tab.FlipboardNavigatorExtensions....a.....$Qgnj.....getViewModelFromStoryId.C.(S.....5.a....l.....a....C.....a....B.....,...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\61c2b1c1755e4a21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211184
Entropy (8bit):	5.8134918618008635
Encrypted:	false
SSDEEP:	3072:ernEOX4RvEwF72G4/icxMmx+O+qBhPSG+MxBvLbgU:dOX+Ew4K0d4VSFfLbgU
MD5:	17F205BCB4FB86CF6FC57D26F055D7F4
SHA1:	D82425BEAA5441DDD4E8547AA10029C318B46919
SHA-256:	323885F563AAFBBBA0C260397D417DC02C811FA6F678A2A6631472A934C6049A
SHA-512:	2F9E0087F9650457A72BE2DF5CB4759F51DEF0F0E5F6F7F459A1D17661656018A24BB57ADFDE00DAB7975D812D573B2C728EE615B2A78C2F730B7B9D2E6B6F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....`.....AF95DAC281D40F297343E876104DB4EA76825849A4D79FEABFB76055D1C93D1F.....'.....O@... 7...h.....(....b..P..... .....p.....t.....p...d.....8.....(S....b..`b.....Q.L`$.....Qb...8....dojo..Q df....._hasResource.,Qi. .....tableau.base.LocalizedStrings.....Qc...]....provide..(Qh.....tableau.nls.clientweb_en-us..,Qi.....tableau.nls.clientmobile_en-us... Qf.G2l....di jit.nls.loading.....Q.@f.....dijit.....Qb6.....nls...Qc...r....loading...Qc....._built...$Qg..!.....dijit.nls.loading.en_us.....a.....Qd..2.....loadingState..Qd.....Loading.....Qd..... ..errorState...$Qg.....Sorry, an error occurred..Qc.N.....en_us.....Qe.U.c....dijit.nls.common..Qc..0.....common...$Qg..f.....dijit.nls.common.en_us...,a.....Qc..4....button

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68228d64aae3374d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1050544
Entropy (8bit):	5.086836851643003
Encrypted:	false
SSDEEP:	12288:ftqiTcRHjti7arTluYXVKgOEBLLhPgjYlT:IvisAm6AU
MD5:	DE0AC28C66898B5B2F26884014129063
SHA1:	449823D735D5BB2A117B9F1280D98DF9C3B7784C
SHA-256:	DE122DC606FE2A0C2ED18591C919B85D51FB9A6BB300F6DC5C8AB9DED35EB324
SHA-512:	05D72203066109E0D2C5F7196882D417B07AED136B69077F7C47814F3FF84AB210008589612198529BE3A3CA86189EE34F1B6779C3EFE125638D3928AB1F38E2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68228d64aae3374d_0	
Preview:	0\r..m.....@...@..H....F3783BA59EDE36901A03E821F94664071F4CFBCA81D2FB2D644B63A4F2335AD8.....'.T.....O....P...e..@.....u.....<....t..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d4fad5aa7dab234_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	52460
Entropy (8bit):	5.623387262605138
Encrypted:	false
SSDEEP:	768:kFdZSQRHf/tRLPZtQVQIGcZyLZQsOT60HZEQOe:kFdwQ//nbnUQIGc4LZNv0HKbe
MD5:	04E879BD2945A0181C498DBCA2A8D13C
SHA1:	6673B845DED7E57B6AD9C6CFA289770DBACA704F
SHA-256:	12C385B2D21D50A06266A25A60437D07A7C8B268700B505C832932572A37A6CF
SHA-512:	1115F962081B81EAF0112BEFCCD6D2BC97DCBFBD84E40292086CA4BC1F5BA7FDC79C4EAA635161F2EB628350630FC0F24BCF3CDFBC2083012D1EC08EA37CF 55
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...%..|...._keyhttps://public.tableau.com/javascripts/api/viz_v1.js .https://launchandscalefaster.org/...i.%/.....x...../.B.!..W...D.z....OvL.....x.A..Eo.....!.. G.....A..Eo.....'..Y....O.....1..g._.....(S...`.....$L`.....(S...`.....LL`"....PRc$.....Qbb.PO....n.....Qb:..m....r.....S...R....Qb6.. .....f...d$.....I`....Da....\....(S.@.`<.....L`.....QcZ.g....iterator. Rc.....a.`.....!...Kd .....y.....Dj.....'.....&.(...PQ.&....&...%.....,Rc.....Qbb..I... .e...`.....a6.....b.....@.-....@P.....4...https://public.tableau.com/javascripts/api/viz_v1.jsa.....D`....D`....D`.....%....`....&...&....&..!.&.(S.....S.a^.....e.....v..... .....(....!...q.d.....D&.(S.....R..a....!.....d.....&.(S.....a,...h.....d.....&.(S.....Qb.T.....o...as..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f1864f44187cfee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2461
Entropy (8bit):	5.8305320627692145
Encrypted:	false
SSDEEP:	48:PLJwtBLCqwRBLewhBL2qwzBLcw8BLbqwvBLWlPw6BLwwbBL+awfBLiImwfBLkwT3:PLuXLo7LPLLcNLhQLvJLilWLl1Lq5Lis
MD5:	B123BBF5DF155A77CA0848A07EDA46D1
SHA1:	D90EAC7CA95819E1C5270A7B85D19F9663A30F97
SHA-256:	D541B7561F29ADCDEB45C126B49FA8614C9CE755107B3EF3C1E7BD4714160072
SHA-512:	1EAB01E1AE7557864489286163F280BAC2DC91FCAAE23403512762E5F63BC9BFA19AB014DED28C94358BC25F8920CCCB54ADAA495DE9B895FA7F104CA7B951 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://tableau.com/..!j.%/.....a.....^Z.h..{$...*..b.....W.r.A..Eo.....710.....A..Eo..... .0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://tableau.com/..!j.%/.....317E62F8620B7F9D1B3FCF97A212C5994FB5A3810FB6BE84C902 DAE15C883234...^Z.h..{$...*..b.....W.r.A..Eo...../..''L.....A..Eo.....0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://tableau.com/h..k. %/.....^Z.h..{$...*..b.....W.r.A..Eo.....A..Eo.....0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://tableau.com/h..k. %/.....317E62F8620B7F9D1B3FCF97A212C5994FB5A3810FB6BE84C902DAE15C883234...^Z.h..{$...*..b.....W.r.A..Eo.....U.F.L.....A..Eo.....0\r..m.....G..... ..._keyhttps://www.google-analytics.com/analytics.js .https://tableau.c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e3fdb283f80ecaf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	81248
Entropy (8bit):	6.081276427774391
Encrypted:	false
SSDEEP:	1536:0tBr7kbcDaE6J8Uh9dLv+lCQnhy/1vF0KdXrvpElvdIkyEzF9dzs0r:CEbQ6fh9t+lRM1vSSbBSaklzF9a0r
MD5:	76F78CA8045EF22B2752B07310A825E7
SHA1:	1646EC15D0532614595F5DC59CFF626E7CDEF0D1
SHA-256:	664B475A52E86074A1B560CDC6EF97AE49A01851C5ED813BB64EB939D500DC7F
SHA-512:	CDB182B31075ADB639D8B6A9C4B43CE40A4E8E9071084A9157D77BD6EAA8636AC45B67BAE61F208012B5C225CFFC99ADB6DDF4201834F61C30559C39AE6B98 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e3fdb283f80ecaf_0	
Preview:	0\r..m.....@...=.....10E238C4067BE3C289982EDA22D171B751FCE2766946BEF1F5CC3FB50A03BE67.....'.....O.... <.....8.....`.....D..... .....|.....h.....(.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.U.#....n.....QbB.....q.....Qb. .....r.....QbF.g....t.....Qb:.....v.....Qb.SU"....x.....QbN ..m....y.....Qb.{.....z.....Qb..P.....A.....QbN!.....B.....Qb..$.....C.....Qb.j.....F.....Qb".....E.....Qb2.k;....D.....Qb...=....G.....Qb2.....H.....Qb..}j....J.....Qb.....I.....Qb...r....K.. ...QbJ~.....aa....Qbvl_.....L.....Qb.*.....N.....Qb.>.....O.....Qb.....P.....Qb.....M.....Qbf.]_....da....Qb*f.....ea....QbR..z....Q.....Qb6h.,....S.....Qb..D....R.....Qb"P.Z....ia....Qb.L... ...U.....Qb.W$.....ha....Qb.....T.....Qb..yh....V.....QbFk`.....W.....Qb.....Z.....QbZMk.....Y.....Qb...u....X.....Qb.-.1....ba....Qb"[.&....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\846fefe5f8157085_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.9502013121829815
Encrypted:	false
SSDEEP:	6:mUzDl/VY8pMgdKn1m0Sue6s27NpvQQDK6tqNUVPzkOnLCl27NpvQd9:pzTtK1m1ne7NpvJ1MNekOl27Npvm
MD5:	3B0DBDFC820F02487F26FA973F7DF3C9
SHA1:	568E0F7637BB2059C4951D226749043535863064
SHA-256:	9D70B82D04828C40BAC6759511E27FD623827DA560C7DD7290B42A7E9FEE51FB
SHA-512:	6B128A86C9FC3797042858B32C56B0F14D4A6C630AA0C57E0DA025500191A62C1EE648DA54B382A5D853155348F7DFBFF999F7756C37850DF61E1ED23FBE1804
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....t@...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/ViewerBootstrap.js .https://tableau.com/.$.j.%/.....}.....x..... .7.....<m.. Ok.&n..%..A..Eo.....e.\|.....A..Eo.....$.j.%/..s..4110675B745CF85D291C578E3DEB97D71CA00B1F341FDC43115E14E835432F73x..... .7.....<m..Ok.&n. .%..A..Eo.....-.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85d2d4a70914e8b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26494
Entropy (8bit):	5.7928037842641595
Encrypted:	false
SSDEEP:	384:yLSc/kj/PHq4O97gnvufbInx5/HLY3tmAlSj3fF7uOmx7KFabU1V3:IEvq40Mx5PM3tlybbUT
MD5:	B424697719CEE24062A0D6453450E6CA
SHA1:	8A0B27F8881F8E9065ECD8DBDA02351574C84769
SHA-256:	0AD676BDFDD04B6C6C7580BB761C385D190A2EFD94335578098E68FD17D4EE31
SHA-512:	3865634C5D1D205C58A2A58BB5B8DE65D8900B6ED2C4710A137321C72BBB0A0A962A42F6FC607444461AAE0E44D46428A34CD37F2FB44CB06828A2C50C59BAE C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~...../...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/typescript-telemetry-forwarder.min.js .https://tableau.com/2Ilj.%/.....eo ..r.&....<...q..o.v.k.X0*V.O.A..Eo.....M e.....A..Eo.....'.US....O.....e.....P..... .....(S.H..`L.....L`.....(S...`.....L`.....Q.@.].d. ...exports...Q.@.....module....Q.@.."....define....Qb.a.|....amd..(Q..~.....TypescriptTelemetryForwarder..K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.|.& .^.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....l`....Da..... ..f.....`...p...0.....@.-....pP.....d...https://public.tableau.com/vizql/v_202122106250039/javascripts /typescript-telemetry-forwarder.min.jsa.....D`....D`....D`.....`....&...&..!.&.(S...`.....4L`.....(S...`.....<L`.....@Rc.....Qb.....t.....Qb.B^J....e.....Qb..B.....r...b$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87bf12eb6f183f6f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	160056
Entropy (8bit):	5.917004724136395
Encrypted:	false
SSDEEP:	1536:FUcXTaTZD9h1HmSY8bsEwf5nWKTYGv8hF4wpRVCQznhAz/Hx3PSsmyUMLdWvQiWQ:STZJtVbPw9WKbvfmjezR3jLdW4iJIEb
MD5:	D8D864E4FDBF3F8DDD8CCB87BDAAD97B
SHA1:	095B2705525B6A015FA24ACC9776802B959313ED
SHA-256:	C29BC9CB8BA867C348910E6F2C714F38A9F539496A0B03030E2D2D98C1652004
SHA-512:	C7475799931F2597ECD68D255467D83A22DB17715B2D811A74A02F9C1909DF9ED1A0E3FA7D40560F657676655354D178A31C687D63E2BF16149C99EC30DC9841
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....c....321C50E0261E99192AAE593DE51E2F62E8319A1473FB0EA973D368248BBF7124.....'.....O5....o...K/.....(...`&..... .....`.....h.....,.....(S.a...`v....tL`6....(S.p.`.....L`.....0Rc.....QbZ.o....t...`....I`.... Da....j.....Q.@fR.....module....Q.@.....exports...Qc.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa..../...l.....@.-....xP.....i... https://launchandscalefaster.org/sites/default/files/js/js_DqE6WkB6R1JtmeQMOa-dpqPyGGrTJ-AXKi-6wu58TI8.js...a.....D`....D`....D`.....`r...&...&....&....&...(S.. .a&..`|L.....L`.....Rcd.....*.....Qb..A.....C.....Qb...6....r.....Qb"LQm....s.....R.....S...Qb2.....n.....Qb. .W....o.....Qb...G....v.....M...Qb.Q.o....l.....Qb>j^..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dbaba7d70f5d669_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	70304
Entropy (8bit):	6.088671563889465
Encrypted:	false
SSDEEP:	1536:yZiDqDos934eib2L+f/nmCwIIR7QpEL6IcSdg8RvF9dzE:ciDtI34eQPGvIIV60hcSZxF9O
MD5:	CC28B356D1C5EA1AC2A4CF0AF8C49F66
SHA1:	971CEF0B9F42161F6A1BDBD8EC4E788FCD64F56C
SHA-256:	659501F7160D31C2160CDE790210B305E7E90DE9CB74AC096927F5068FA03E19
SHA-512:	7522DE2A9C9DD8150BA07348AC19293EA4000AF63ACEB9FF5ED3AAC78DA89B1AD419B9690B46372551EBC848E3E9430DC8F99B18DC85875D175AEFB0EF520C E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...c.....317E62F8620B7F9D1B3FCF97A212C5994FB5A3810FB6BE84C902DAE15C883234.....'.....O....h.....8.....`.....D..... .....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R.....QbFk"^....n.....Qb.N.....q.....Qb..B.....r.....Qb.....t.....Qb..f.....v.....Qb...)....x.....Qb..... y.....Qb.!W.....z.....Qb..!.....A.....Qb.q.a....B.....Qb..#.....C.....Qb..|....F.....Qb.98E....E.....Qb.....D.....Qb.V.....G.....Qb../.....H.....Qb.....J.....Qb.r.b....I.....Qb.....K.....Qb. 1.....aa....Qb.....L.....Qb.<.F....N.....Qb.....O.....Qb.Q.....P.....Qb..~....M.....Qbn..{....da....Qb.]*.....ea....Qb.....Q.....Qb.$.:.....S.....Qb.v.d....R.....Qb.....ia....Qb.X.....U.... .Qb..|#....ha....Qb.....T.....Qb~.....V.....Qb.N.O....W.....Qb&.*.....Z.....Qbjj.....Y.....Qb.....X.....Qbr6.>....ba....Qb.L]G....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dc5309bb07e531e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.425541228854488
Encrypted:	false
SSDEEP:	6:mQR/VYGLUxGBzkwT2mABSguGpiqu/oZ3RGJK4YK6t:nRSGBkw6mkSguGtQsV
MD5:	B45988A5CA8C9650D9AC41F4AAB80561
SHA1:	A08A39504D97BAD02850EDB99D35809ECF4E402F
SHA-256:	23EB4B0B2BCA838D99C71D16AE7D9FB01F8D34F1099BF9350DC5DEAC951A6D19
SHA-512:	192A2D8557EE50FF60D4728EE373F21AD28BB8BD095CAF57D0C19BECF20588F117DAFE341BAF69E18018FF6AB91D0A754A7C0BD0615E39BC48A717E182A9F22 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...s....._keyhttps://www.youtube.com/s/player/7acefd5d/player_ias.vflset/en_US/embed.js .https://youtube.com/.Am.%/.....N.....0.8.....c_e..<...v.*5...r.. ..A..Eo.....s.v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e8a6cf8ca9aeeb7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	6.090670222083417
Encrypted:	false
SSDEEP:	12:l1QyWJaGfsRFQyWJSstzVHkv4QpS8ns1kVHkKE:laPJJkRqPJX7+nn3
MD5:	39CE33FC4B10BC21908826B764B4BF70
SHA1:	B5632958D2CF6E4D86A5A8E19071C053E1220A5B
SHA-256:	003EB836D8FE9D413859D542BF89B5F8A5EA0243655F65E785F42674CBF7FF3D
SHA-512:	0112992ACE2007806E8F2F2ABFD0DF1E50509D54AA1841F078B20396AA52129225A37FA81CCEB07721DC6C559E8BB53B8D1F04D9C1C4BA997E9214101D23F722
Malicious:	false
Reputation:	low
Preview:	0\r..m.....$....._keyhttps://launchandscalefaster.org/sites/default/files/js/js_DqE6WkB6R1JtmeQMOa-dpqPyGGrTJ-AXKi-6wu58TI8.js .https://launchandscalefast er.org/O..i.%/.....x.....q..^Q...!..V.w"9[.L .. H..W.A..Eo.....-F.....A..Eo.....O..i.%/..p..321C50E0261E99192AAE593DE51E2F62E8319A1473FB0E A973D368248BBF7124...q..^Q...!..V.w"9[.L .. H..W.A..Eo.....$..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91fb6960189ffea2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	484288
Entropy (8bit):	5.506724290300842
Encrypted:	false
SSDEEP:	6144:umgznnzCe3nj8bpKfcr/sHYQE7LUlh6yz88RbW:u1HCe3wUeohQ85W
MD5:	5DD22D3DCA8E6E066AE204F3BA90A02A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91fb6960189ffea2_0	
SHA1:	EE9965085A10C6D1E2B4365B60E00CD075F7BA06
SHA-256:	26420A38E98E07D1303ACFE99171E89A556E737D2DD28FE7CFCF5958F515849E
SHA-512:	30F1ABA33175C13D996BBDF9CC73C1E112CB26D5CD26B820FAE15C5653EBDE38FDD1D306CA8788919E07B59FBA302DBEDBBA5374B55CEAF3D480B9B43050E FB1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....6....9AB4CBC288E8B4ED5DB0905FCF6F3FB7F312E33AA530146AFC72637F297A0007.....'..u....O.....`..x.....(+..... .....@..... .....X.....X.....(S.8..`*.....L `.....(S.....`.....)+L`.....Rcx.....QbV..|....ii....Qb.....bi....Qb*".9....o.....QbvIFM....s.....QbJ.....at....Qb6.!....ht....Qb6.7.....ki.....M...QbFp.....vt....Qb.+.4....di....Qbr..m. ...gi....Qb..g.....nr....Qb...@....ri.....R...Qb.F.....ui....Qbbx.q....yt....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98f012075031a98d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2640
Entropy (8bit):	5.684139984252334
Encrypted:	false
SSDEEP:	48:bDLX+OhDLXUEEhDLXqbijhDLXrJhDLXAcLhDLXLWhDLX/LAhDLXoj6mhDLXg6hDK:3LNL+LEeLnL7L+LoL4tLHLrL3L
MD5:	D1D8588F81DA3DCFAF42ED411D543428
SHA1:	EDAAC9354B08D5B9752C6686801C3A662502C895
SHA-256:	66F2A5312B26FBB838225F42B8E15685ABEFA5883DF3BD28DE825D1024D0F0EC
SHA-512:	9425F4677F9EC955D0926B385A941868D77F6BD4AB478850EB43C4E99D43F2E93C5FD93BA32087034E6FBEE7C6EB199C7C9A4D2A9C02E3488DF892431E82A95
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...+:.b...._keyhttps://www.google-analytics.com/analytics.js .https://launchandscalefaster.org/.I.i.%/.....x.....dI.....Xvp!T....."..?*()=+..Se.A..Eo..... .A..Eo.....0\r..m.....T...+:.b...._keyhttps://www.google-analytics.com/analytics.js .https://launchandscalefaster.org/9B~j.%/..... .....dI.....Xvp!T....."..?*()=+..Se .A..Eo.....*v~}.....A..Eo.....0\r..m.....T...+:.b...._keyhttps://www.google-analytics.com/analytics.js .https://launchandscalefaster.org/.]k.%/.....P.....dI..... Xvp!T....."..?*()=+..Se.A..Eo.....9.....A..Eo.....0\r..m.....T...+:.b...._keyhttps://www.google-analytics.com/analytics.js .https://launchandscalefaster.org/...k.%/..... .....dI.....Xvp!T....."..?*()=+..Se.A..Eo.....n.....A..Eo.....0\r..m.....T...+:.b...._keyhttps://www.google-analytics.com/analytics.js .https://launchandscal efaster.org/.E.k.%/.....M.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f53b742e5f8e8cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	160888
Entropy (8bit):	5.773885276816127
Encrypted:	false
SSDEEP:	3072:Ss7n0L85Vd4f10pmS84mP4rwysC5GnY1MmSvNE:l70Sdua7mP4r7/56a
MD5:	79093251C115A5FD582689D08D1361FA
SHA1:	90E65142B45BF795FC33BCE89E99587D6634FF9D
SHA-256:	134B52288749CBD3EA06808B784FB8EF7A8301676268BB5471A6E245EB0BCEBB
SHA-512:	310791F1DCE488BC62C1632276945B47134CE35529DE8B9136EC7078D313D1EBA3C26993CD1514E175D569A1CABD3ADD1C924725933E768D877A55FD03CE05F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....n.....4110675B745CF85D291C578E3DEB97D71CA00B1F341FDC43115E14E835432F73.....'..@....O4....r..Bl.=.....|...p.....t..... .....P.....p.....(S.0..`.....L`.....(S.E..`D.....L`@.....RcP..... .....Qd.....isSupported.. Qf..8(....notSupportedReason....Qd^.).....isBrowser.....Qe..v.....isArraySupported. Qf..1.....isFunctionSupported.. Qf..,.....isObjectSupported.....QeZ.$i....isJSONSupported.. Qfz..(....isWorkerSupported....(Qh~.....isUint8ClampedArraySupported.$Qg..e(....isArrayBufferSupported...,Qi.< .....isCanvasGetImageDataSupported....$Qg...N.. ..isWebGLSupportedCache....$QgR..f....isWebGLSupportedCached....Qe.gk.....getWebGLContext...Qe.O.....isWebGLSupportedo..... ...l`....Da.....(S.....la.t...t.....a..@.-....`P.q..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aaf28abf3fb88937_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.784907136454437
Encrypted:	false
SSDEEP:	6:mm92/lXYGLI6EYtP+3uT0NpguG309AT9HIveJkvP4n1//hK6t:92toQt2eTGguGMEIk1/T
MD5:	92622DD143A3786DC0BA020C6179BE06
SHA1:	CFE4C17645B98C82FDF22508D42C2A11103B888D
SHA-256:	9F87B9ADCD29A7B2DF4D1476C3601F397BE54EAAFA40ACB432E615F95CC988CA
SHA-512:	C1C1F1B18FD4ADFEF3CEE2ED0DE87964833F2EA3ECBA51B8E420F657615C45250163D169770CA72535E6599EFC2ACEBCF04C642C435F6E206F985C6CA451B6 1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aaf28abf3fb88937_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....C....._keyhttps://www.google.com/js/th/HlcVvMpVwt9TcMo1UaoN-mhKNgp-8n-s8HaB4RKa1Go.js .https://youtube.com/.9Dm.%/.....7O.....>$.".r..I.}.*.|1....Qq^..F...A..Eo.....'u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b46b26c8deea13db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.898517048196738
Encrypted:	false
SSDEEP:	6:moullVY8pMgdKn1UtheuWUKyWlA7YuVLeO/ZK6too9TjdSbkREfnvA7YuVLewb:All1tK1UIxULD9rFjhiaD
MD5:	BD5CE3522445FDBCD0A5951FB7D0DF31
SHA1:	8555E2AA844836CFFD314BC313D2ACEBFB87AEA9
SHA-256:	24BB339BFD461654E045E17F381B7200057C958DF55BEEC4AF8B3EB7BEA8F42C
SHA-512:	50301680D6376BD93530C02C3130E56E1DF2A19259B565FA1F030E5AAB9A7B464512B0E825E1F0084D7218BDD6EE1BFFC5B20DC3033A6FFBB3644C27391B3338
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/typescript-endeavour.min.js .https://tableau.com/.=Ij.%/.....a.....O?.....x..Y.I..6...R..p.'.6..A..Eo.....3.....A..Eo.....=Ij.%/..`..D9801C2F906482E802699ED2F3436C69F589907907A67D3CB90352C3788FB66BO?.....x..Y.I..6...R..p.'.6..A..Eo.....PL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b92fb344689cc714_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.4412297313415
Encrypted:	false
SSDEEP:	6:mm9S9YGLUxGBzkwT2buGguG1yrrCgLlOuKyP4WK6t:99GBkw6buGguG1QCglOuKyPr
MD5:	79620FCE475107CB8046A7ECE6302035
SHA1:	6E6373E203566FC0D4932D1D06A6410E2F088329
SHA-256:	4AC8FA51542F41B278AA392CD831617C574724FD89C2BDDF1EF92F1C1AF13BAC
SHA-512:	163AE799F4311850B9148F9F998C4C20EA20B5402A726B66946A6F79923CD0C55AF0A76B8D5CB9CF83B01BD339CEF1D983036071091A9C3A02E0248C4D72F12C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...oC.,...._keyhttps://www.youtube.com/s/player/7acefd5d/player_ias.vflset/en_US/remote.js .https://youtube.com/F.@m.%/.....N.....k.N8O..^I.X^.....S...a.A..Eo.....o!m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b9c6b8fde7c51f10_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5311624
Entropy (8bit):	5.604710228227079
Encrypted:	false
SSDEEP:	24576:+kdslVtBq8qNSlfOAQaMtsIToKffxB7rlcbhDHN2IXxQia+akA3/Y2rMV/akhh4W:t/GOR9f9ffxBHlc/2AQiaWt9/OYzlp/
MD5:	C2B680087C58B7D227BAAFC9EDF11D29
SHA1:	5EC4F18850E36DF3A3038F9C8DEBD94C9C8DAA72
SHA-256:	DE9CF35A41C912D3E23A8479EA2BFEB9F55257444674A673444E3B5A734082FA
SHA-512:	7F2CDD79CC5FB03DFE648D3CD6B640C699C9D5401996ECAC826517178839BE1A9DFBDAE3A2798AE77F235172E6A7AAB854379E5DCBE4F4C82CD639092FBBF8C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....F9D13028F156F65B703A0DD0C16A89682BD2DDB2C270C02C5D5D703ACA1B819D.....'..I@...O....X.P.q$.[.....x.....d.....,.....l}.....l.....D....".....x.....h!.....I...(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb9beabacf12717c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb9beabacf12717c_0	
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.425328913733846
Encrypted:	false
SSDEEP:	6:mUKYGLUxGBzknZk006guGAi/x0Us7dQv+4H4RK6t:pVGBknZf06guGC634r
MD5:	A0FB9F1F9A014BF256A00D54878927F1
SHA1:	FC5A2946520079DEB99751FDDB0035C9476BBC76
SHA-256:	A37F822F3E73F3C5BC360F5BA38FB70CA3A7D33526F74371E83AB652A99F3165
SHA-512:	8555D990975843F1C8BB46BCA03239F97A53E8300EEE379B1B1A3F2D725A6FAC9502CAB4C03FF0589884F3DAB4F3E81179245B9229EB4AC2B2417414525FA9A1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...Z/....._keyhttps://www.youtube.com/s/player/7acefd5d/fetch-polyfill.vflset/fetch-polyfill.js .https://youtube.com/.K+m.%/.....wJ.....2-.H.]C....).E.d.Bu.y .i....d..A..Eo.....&.%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c17c9b219667ada6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	5.845460538291039
Encrypted:	false
SSDEEP:	6:m0tXYcQyWJaNBYDcPOnVXQyWJyWqC3LeBX9k4rK6t:7dQyWJaScPgXQyWJP5yBX9j
MD5:	CFA2CFD9EB34216C180D4BA61567A3A3
SHA1:	4385DCED6D823CF647AD62B2EBF1C76E92303FDE
SHA-256:	2556815A20148675A7891A585D0C80E822FA76E36CA3224337CDFEEC8AE4519D
SHA-512:	06E2CB28526B0884AD51CD42A391CCE173494FD790312875515CF159564E6F039EC03983C87C02EAFEC32A931B5BE09C23C20E06FEA894C0860FBCA710611B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....._keyhttps://launchandscalefaster.org/sites/default/files/js/js_xls8cObNQq9FQqHFwo2VpyLTkfP3RxVC2C7aT-TuEGY.js .https://launchandscalefas ter.org/...m.%/.....{.....S.....CB^.....G$.RRg..)y*`.A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7fcacce44227fc2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	166168
Entropy (8bit):	5.940063815378783
Encrypted:	false
SSDEEP:	3072:lWwxGNUFmMBPYVsDJC1qfpl/EFoIS376M3AePdW:lGGFmoPisDJbMO1hc
MD5:	CC93971439DEEC876CF688DB274FB4BE
SHA1:	7F646FAC32972BD48C1B0178D8D0DF601D5D2411
SHA-256:	513C9C0180AC6514AD690EC7189EA9B66F5D09B65FA3C5946E7B416D034FD337
SHA-512:	C033135DE25BC47BCDF62198663352EC87F1902706D22FC94728856592D46F38609798485BB5AF85E2777D50F8E2BC2E359822E63BE45322B675CF22A1CECC78
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...G.....8A924B2834F6519B952DE6CC8D4EA8261DE0AAB3FE48FA04621F97AD540BA160.....'.h8....O5...p....^.....(....''..<.....|.....(S.D..`@....L`.....(S.h.`.....L`.....TRc&.....Qb.....w.....e....d.....I`....Daz.....(S.`.`|.....L`.....PRc$.....QbvIFM....s.....dd.....I`.....5.a.....a.....Pd.....<computed>.ea.....K`....DrP.....%...%.....%... ...&...&..&..`&..k&.'..'..'..a=...&.].....b.....@.-....DP.....5...https://www.googletagmanager.com/gtm.js?id=GTM-WP98PN...a.....D`....D`....D`....`....&...&....&..1.&.(S...''..`pE.....=.L`.....Rc.....Qb.0N....data..Qbr6.>....ba....Qb.]*.....ea....Qb..J....la....Qb...f....qa....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c98a6a5262c9c182_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.500651622290721
Encrypted:	false
SSDEEP:	6:maXXYGLUxGBzksCj4PY0c71j4GguGxOjoKwf3EWYBbK6t:8GBklsPjcRsGguGuo7/cN
MD5:	1F75FC54136C5A6CF4C40324F14FC84B
SHA1:	7D9ADBB44B5C93033D1C63BDB89BDA599C4AEF4C
SHA-256:	749A435D16034DF7175BE80CA91B915EBA596C7203B5CB46406217F6B4CA8D7D
SHA-512:	E70CEDABC58679555FF7441704600AABB5C540A2A37BF5035B8A6897DE49D6435D8F1B3F26C05A5447AE6001E3FC5505F9202DFC0EDC955D703D01BA30B77AA A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c98a6a5262c9c182_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...s.a...._keyhttps://www.youtube.com/s/player/7acefd5d/www-embed-player.vflset/www-embed-player.js .https://youtube.com/HK+m.%/.....vI.....;..0.. #.....^.Nl...`...2...A..Eo.....A..r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\db598b3b8f31c506_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	549280
Entropy (8bit):	5.651506839327903
Encrypted:	false
SSDEEP:	6144:af/X7hvc+PvmumThlAplhTDhIdz7zQ5JG/fo7D:andvc+Xmu809mxQiC
MD5:	CD94274595D41787EB2E52EFC62565A2
SHA1:	592E8279978C917EBA3C389817E0493DA7B05382
SHA-256:	1A66B013325C3A9EF394826BA17602BEDF84434BE0F5F2A8D9F93529BC29A587
SHA-512:	12DE8CADF86203E5E7B0A0AAE837F4C362F3216C841E3A1F5F75CE8F7612660FC1C623C53B3D6C002714B31137856AEEDCAEA9E0A58AA30F01F61CF01D266B 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....m.....D9801C2F906482E802699ED2F3436C69F589907907A67D3CB90352C3788FB66B.....'.....O....H^..d..I.....3..(....' ...X..... .`..... .h.....x.....(S.<..`4.....L`.....(S...`.....L`.....Q.@.].d....exports...Q.@.....module....Q.@.."....define....Qb.a.|....amd.. Q.p.....TypescriptEndea vour...K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e08840e5a4cee548_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95672
Entropy (8bit):	5.841235427854824
Encrypted:	false
SSDEEP:	1536:g8jMyFnn5WWoxClFWLbOkOoR6+VCvxagYq4sLZ:Jn5ToxaFwMaVCvMvq4I
MD5:	11089D58FE1EB9D7F95A50D0CE341A9F
SHA1:	ABB414BFD25C119EBDE07A776C0A28A886D4E986
SHA-256:	BA913C476E866A22B7F7B27B7117E6758F1E3FA708BF3EC8D7A6D79F69FB9F97
SHA-512:	FBEC5CDD09639D62246C21AB7ED3A3C5AB2A423B373AF7EB664758D7C14A324BC94C08B94FA523CE74E6D746EC83A1F3B7F8D5076DCEB455521AA44DF5460 DB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...z.....0FF73F0206103D9FEF94EA28AC0D4C638D3115877B61B056363D8E292DB25A8E.....'.....O!...`t.....\.....(....,..x.....p..... .....(S....,..`BY.....y.L`8.....=.L`.....y..(S.4.`$.....L`.....Q.@.....module....Q.@.].d....exports...K`....Dg.....s.Q.....&.(..... (Rc.....Qe*.....runningUnderNode`....Da....(.....b.....P..@.-....\P.a.....P...https://public.tableau.com/vizql/v_202122106250039/javascripts/runtimeanimweb.jsa... .....D`....D`....D`.....U....`....&...&....&.(S.....Ia.....8..I,..... IE... d.....D&.(S.....IaA.....Qc.!<#....getNow....Rc.....(`.....d..... .....&.(S.....Pd.....Module.printa....3...I..Q(.d.....&.(S.....5.a.....y...Pd.....printErr...aL.....I..d.....&.(S.....a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e385bddf7cc1e900_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.503479395497687
Encrypted:	false
SSDEEP:	6:moXYGLUxGBzkwT2duguG1b/6vqkP4aK6t:OGBkw6IguGp6ye
MD5:	11FD39EC69D03A6B9F30EA0BC5A46212
SHA1:	13B04067D94FC96DC97E238162103F6FF58839B0
SHA-256:	094E088FC47C5BB4D84C53D82DB368927DD78D26A755C3283EC05109E8929BDA
SHA-512:	72735E4812CA408DEBCEABA3B7E205E6B0C59E1F419E7290BABDC613C073E94284D47BAF19F07A6497A47E72D48FD29887663C31E474FC2B930C752E9F2D328
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...!....._keyhttps://www.youtube.com/s/player/7acefd5d/player_ias.vflset/en_US/base.js .https://youtube.com/.~,m.%/.....vJ.....Y....i<...1...w....B..c.4.. .A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e8cd6301153cab64_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	141720
Entropy (8bit):	5.971256737471811
Encrypted:	false
SSDEEP:	1536:paw+zBK0yKoyH7l25FfKAfOqcmhGWBp8n48HByh4OpP+F+SVgW5yfKfjZbKjjbXl:oDxypyHgFiEqM3rAguJ+S9enyFgkVe
MD5:	E0C548BFFEB161B04251CC9BE4C08EF8
SHA1:	D5EB1F0D1C694D6AD2709DFE69C718ECFB9AF53B
SHA-256:	F03EC26B9C181CAF2D1D818EDCEC16188166127DB294ADF5A329C182F30324C8
SHA-512:	9C32D26A481DB03F28E25F86DF57DC3010027672A01A1589A3209CE961E2FBDF5D46BFCAC6D136D2A98C725F21BE4A2BDB04F7B5361C8BDC368F87F71CE97C9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...I.W....DEDB4A5C003598F823C35C49D2CBCDB6ABD4C3920073504066418F6E7FD05C7E.....'..]....O-....(..y'.....`&.....p.....L.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb.....t...`....I`....Da....j.....Q.@.....module....Q.@.].d....exports...Qc~.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....XP.Q.....L...https://public.tableau.com/vizql/v_202122106250039/javascripts/jquery.min.jsa.....D`....D`....D`.....`....&...&..!.&....&.(S...a&..`|L.....L`.....Rcd.....*.....Qb..#.....C.....Qb..B.....r.....QbvIFM....s.....R.....S...QbFk"^....n.....Qb*".9....o.....Qb..f.....v.....M...Qb.N.....l.....Qb.....y.....Qb..].....m.....Qb...)....x.....Qb.98E....E.....Qb..-.....c.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ec0d52e6c07855c8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2597
Entropy (8bit):	6.014926725691398
Encrypted:	false
SSDEEP:	24:6nUydiu8icn+tUTT7SnpOEcC1UZjvzr3zubbOHCa80BN7XabXONcI:cUyyyqT7epxUHzqHOHCP6WY9
MD5:	6EA4294A16D1F0CCCB4D57FC8E11A2E9
SHA1:	13BA39F64DCF2D99FEC46F9E25A230924C1EDDBA
SHA-256:	EF0E525DC2A1D237687379128F74E2E5A5DB094B97FE29AA2FC6203DDDA17858
SHA-512:	F745019DA54652800D732F53E4A21F14D7E1AA68FE862584E776195FF83BD5C04A8858B66EEDE9736671206FC6212AA5344A3E04DCE981FCDC40E40BC7DFF135
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....,.@...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WP98PN .https://tableau.com/.@.j.%/.....[~.....l..f.t...BO.@.....T,'...A..Eo.....A..Eo.....0\r..m.....O....,.@...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WP98PN .https://tableau.com/v<@j.%/.....l..f.t...BO.@.....T,'...A..Eo.....9..".....A..Eo.....0\r..m.....O....,.@...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WP98PN .https://tableau.com/..ij.%/.....l..f.t...BO.@.....T,'...A..Eo.....A..Eo.....0\r..m.....O....,.@...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WP98PN .https://tableau.com/..ij.%/.h...16EB74E9A6AA5C83CCF431B026AC16B445180983CC605178A3E7F942E10AA565..l..f.t...BO.@.....T,'...A..Eo.....L.....A..Eo.....0\r..m.....O....,.@...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WP98PN .https://tableau.com/fY&k.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f196b0c9c661cfde_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29776
Entropy (8bit):	6.310785208094046
Encrypted:	false
SSDEEP:	384:L8uWzUCn59b45mleU3NUM4i0ZtrOM8Ikau23zfX28YBWpR6ivV2bjPdQAGG14DKy:5Wa8pSOMfzmFBTivVujFQAGq4ODTAZt
MD5:	C59C0B1AF24437D61861F3D021780914
SHA1:	8BD29E6FE1E2B024CA450CBB573DB4439983B559
SHA-256:	34585E6A8BE93A18EFFD29F115C76A2C29615610EAD0025A14CCD7BF84FAB826
SHA-512:	1CBF526B0FEA17E7943603DDBB343EB11751C29D917DB42F7440594EEA969EE6A387AD890CCDEA5B0FA8D7219BD0175A363850E70189291B1C71DB625718A01C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....od....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/platform.min.js .https://tableau.com/..cj.%/.....3...x...2E...O.c.IE".RNxw...A..Eo.....%?.....A..Eo.....'..6....O.....r.....#.....0.....(S.<..`2....L`.....(S....`.....L`>.....Rcb.....(.....Qb.....p.....Qb.....nt.....R...Qb*".9....o.....QbvIFM....s.....Qb.....t.....Qb.....it.....S...Qb..B.....r.....Qb.....w.....Qb.....h.....R.....O...Qb.N.....l.....QbR.....f.....Qb..Q%....k.....Qb.B^J..e.....Qb.....d.....Qb.....y...t.....I`....Da.....m...(S.\.`t.....L`.....q...Qc.I*.....charAt....Qd^.....toUpperCase...Qc..i....slice.....K`....Dq .....&.]...&.(...&..&.Y....&.(...&.X...&.(...&...&.Y....4....,Rc.....Q.`....DaL.....!.....d.....@.-..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2fcf2a1d01a7a40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2fcf2a1d01a7a40_0	
Size (bytes):	364
Entropy (8bit):	5.935071183386518
Encrypted:	false
SSDEEP:	6:mUvXY8pMgdKn1p2VduUEyCorytOS0xpr1cbK6tJTiNbs1lpc2jh6BTeUytOS0xpL:jHtK1p2n/08YHIb+y2F6RwU
MD5:	B3DCEFF7C51093B163BBCA5E8DEE6FFE
SHA1:	21AC688F5C716761999BE7D8A2B31EC7912B6F59
SHA-256:	525126DA67EBC959971F36DED4785BDEFF522E3293B0B4F25A0C1F9047670B3A
SHA-512:	D602912E0A37F3E3CC4C36D9922C8704350854D688F9A9F8C424867235946EDBB65EC68BB1FFA262D10EA89BBE7B1D347A93F7772B51FCA1143372C4C138561
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...wW....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/vqlstory.js .https://tableau.com/.;lj.%/.....{1.z...c....].....aU.....A..Eo.. ....ciQ.....A..Eo.....;lj.%/....268AF157460686374016BD42338B6176C20161CD9907447FE46500CE2380D289.....{1.z...c....].....aU.....A..Eo.....#.?.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f3dc33c8bb989f83_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.955373591798641
Encrypted:	false
SSDEEP:	6:mdY8pMgdKn1yEMunStrMwxW95byATDK6tu9pH5b8aK8AMwxW95byAd/p:ItK1vMsr9gu1Y7H5bnK8Dr9gKh
MD5:	B58D0332B16A3D2BE9C7EEDE7B938FDE
SHA1:	463E1A6A0D36034DE0BD757FD4637EE0B22E07BF
SHA-256:	803A14552523E267792956FC8077F9AE522E231FFACD680158A7A75DE92B9B72
SHA-512:	BAA7460ADBC20BC1889D7ED52CEC426594C2E63ACAD70195B41517E1EDCCD32BBB15EAF22CB44AE93644270803D05F040C967D73B0E870630A58B46DB3EC0 C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....oq....._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/vqllegacydojouiweb.js .https://tableau.com/...l.%/.....;(...../U..%...../*. >..s..N.....A..Eo.....1.....A..Eo.....l.%/..c..9AB4CBC288E8B4ED5DB0905FCF6F3FB7F312E33AA530146AFC72637F297A0007/U..%...../*.>..s..N.....A.. Eo.....U..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f484f7d17eef3c89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	84032
Entropy (8bit):	5.6912128195473075
Encrypted:	false
SSDEEP:	1536:b0w4ev0riQYi5qiW0w748CDocUD1RF/8xF:Aze8WQhqiWP748yoccRF/8P
MD5:	E0C1238E6CA00FCF21E2EA5BD5E8C313
SHA1:	04CC5F0EDAD8003D6E106B27BFC8DB675E50E223
SHA-256:	0B6AE323E2A5979B6AD96C1085EF56EBCCC7BEA56BD9D853350157F596009112
SHA-512:	7D2225C5F7B49EA3D27179A85352C695C8F3603D365EC4E71E2A835AB648A8D0D7E764D01B9BB76A8F1EF297D235D2B67EC2BA3EBE10124C03B2BBB8B81195(5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....J....A1DBE64D6C7C85C5903DFC5BC771C28F51C6120A8D9943CFAC670421D93252DC.....'.j.....O.....F.....,..... .....(S.X..`j.....L`.....Q.@.....window....Qb.7)_....self.(S....,.`<Y.....M.L`.....Rc.....X.....M...Qb.....w.....Qb..B.....r.....Qb.q. a....B.....R....Qb.N.....q.....Qb..Q%....k.....Qb..>.....j.....Qb.B^J....e.....Qb.....p.....Qb.....L.....Qb../.....H.....Qb~.....V.....Qb.....X.....Qb.....T.....Qb&.*.....Z.....Qb.$.:.....S .....QbR.....f.....Qb.X.....U.....Qb..f.....v.....O.....Qb..]....m.....QbFk"^....n.....Qb.!W.....z.....Qb.....y.....Qb..-.....c.....Qb..|....F.....Qb.....D.....Qb.....K.....Qb.....t.....Qb.r.b. ...I.....Qb.V.....G.....Qb.....Q.....Qb.....d.....Qb.N.....l.....Qb.....O.....Qb...)....x.....QbvIFM....s.....Qb.98E....E.....Qb*".9....o.....Qb.Q.....P.....Qb.<.F....N...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\wasm\a4a5b606ed963425_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9953230
Entropy (8bit):	5.650174505399634
Encrypted:	false
SSDEEP:	98304:UWoRUFXTH6ibgNrKete0SJP9WCN9uzVddX:U4tP9WxzVD
MD5:	B5346DF843EB6DD4E5EC58E3FC102122
SHA1:	E603D97C8D1E63A30D3D5D846DBF04ABE27740E2
SHA-256:	B697B5956BCB3150321D6D441F8BAB96682E6CE148B39E451FEC47EF57D19E04
SHA-512:	B8DD82BDBBAC2379F1170C2C0E28D782BD9EF510EAF8D865030110044A968A452F93518BB6C3732989F28B9382A59D195EB5915EC563118F126A41350CE2BC08

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\wasm\a4a5b606ed963425_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....[.=....ECE200CAD33CDF92A54A38A9F060134170C09A82DB7AAC85DAD0CD3657973C37.....'.....O$6.."....I...4...I...I...I.....`.....U H..j.VH...H.^#H;#.....H..].H.E..$...H.E...f.....:fG.....J...(.....UH..j.VH.^#H;#.....H.....H.u..V...H.u..E...H.u..J.....*6..H. u.H...d.....5..H.u.....d.....5..H.u.....d.....5..H.u.....d.....5..H.u.....d....|....d5..H.u.....d.....N...\...H.u.....H...d....<....P5..H.u.....d.....<5..H.u.....d.....N.....H.u .....H...d....~N.....H.u.....H...d....\....n6..H.u.....d....<....>6..H.u.....d.....7..H.u.....d...H.u.H.^..|.....7.....H...d...H.u.H.^.....7.....H...d...H.u.H.^.....p....7..... H...d...H.u.H.^.....p....P....v7.....H...d...H.u.H.^.....P....0....>7.....H...d.....$7..H.u.....d.....6..H.u.....d.....6..H.u.....d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\wasm\af6e3988f4ba23aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	5.782168286463552
Encrypted:	false
SSDEEP:	6:mnY8pMgdKn1TEU/eRtuvAqgXVlKhjWVpWhqo4jBEP212XK6t:itK1IU/eRtCAqSrKhOpWIoAFg
MD5:	7277FF59E819B2FF9D668E0E24ADB90D
SHA1:	E1103A019BD97B8B64F9E0280482EE6EE155B88C
SHA-256:	847DA49F409AA724415245C893A14151657F8F6D87E12BB2CAEED81C5C9B1120
SHA-512:	9896EBA9B51C5959CBD9BE7D2B61C00976E202D9502B98CD10A3FA73E76A7EE4CACCF5C3767A0F781A8374B3A96EC9CC76E638FE24CAAC165E546C88C1BBE 98F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l.....l...._keyhttps://public.tableau.com/vizql/v_202122106250039/javascripts/runtimeanimweb.wasm .https://tableau.com/..j.%/.&..ECE200CAD33CDF92A5 4A38A9F060134170C09A82DB7AAC85DAD0CD3657973C37H. $.C..C.&...!C.}0...C...;O.&c.A..Eo.....O(.HL.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\wasm\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.242585708995671
Encrypted:	false
SSDEEP:	3:q1Z+jq/Gtv/llL0svqlEkYP+tlltwj3pKnyoctAyq/Gtv/llL0svqlEkYf7lltww:q1DOtfteEt+t/twj0y7GOtfteER7/tww
MD5:	C8F177DBB3ADEC849F7CCF65F9243EB6
SHA1:	EFCD6DB70E92D6FC174171A05DCCB0FC733339F2
SHA-256:	E3711F2474A5E0308C015FA04FED9B03C1FF4A2E5AD376786518633E3B62DC03
SHA-512:	21040922B2963A35FDACC7AC98A871335C1D9082BBC1659D616AE190842502B2EB0CD4CBBE98B76A87662A949830CEEC0403F6EAF23DDB78B7137614488301A
Malicious:	false
Reputation:	low
Preview:	X.....<?oy retne.....#..9n.@..k.%/.....%4.....(k.%/.....U..k.%/.X...Xo.$oy retne.....#..9n.@..k.%/.....%4.....m.%/.....U..k.%/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	1.648968482650123
Encrypted:	false
SSDEEP:	96:dNwYpMWNwUsyjsLhgyKyLOyyHzLxM0NweGyjsLhXmTcLnLxM1:duhWuUvs9/Z8M0uehs9WwJM1
MD5:	938FE7F6A2DDCD4F106B42BCA575E240
SHA1:	A1A4F5D2FE0863382AE313110CAEEE00CF8F1D40
SHA-256:	78B2A1B659146E857AB1DE82C7AD7F73C6B918C66CA29F75E1DC779466056BBC
SHA-512:	D367E33A38A40F467C1C58FD6B0F15BF18451CA4B6E8C6DB059EEA53E55B16EC8A4652434BB7FED273E4E5DDCD946B876B4581330609C8D0BF4CFD6ECFB5D EB
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
File Type:	data
Category:	dropped
Size (bytes):	38508
Entropy (8bit):	1.3715586221362284
Encrypted:	false
SSDEEP:	96:zOVcNw0HMoMNwxsyjsLhgyKyLOyy3zLxMg8Nw/:zOVcuVoMuxvs9/Z0Mg8u/
MD5:	5222A4606F41A6A85FB4B4CE20478B66
SHA1:	2934A0DE816D026CA79CAAC1690613CDD2ECF1CD
SHA-256:	FAC1B6D2A8F428ED19A595B9F810A9BDBE69F13DA18ED9EE05F5FBB38A3FEE01
SHA-512:	EA3ADDFC7F579B60E2E2FB5CEFFD5176FB2E1D5EC7C2282FA6F926BB23FF5A953CD7C638BF3D4D4971A4E8E70C92F2B8345B0FE5C6DDCA4C46F9088992611 66
Malicious:	false
Reputation:	low
Preview:	.....R'..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	143159
Entropy (8bit):	3.2512520526561643
Encrypted:	false
SSDEEP:	768:npF9a2S+6l6S/sY0KqKOKsKS/sx1XKsqSKs130S/sx1ylMS/se17LkKs1AEH30/e:Xadn2tR3+l2
MD5:	35B1A3914DA0868D61E2468C92666FC3
SHA1:	962C1105AA703A9633D0A6D239645A9EEE189221
SHA-256:	59E02F982616607C21F7F5EF51F68467AC1DCC174391842E1E6C8B86DF1DDD4D
SHA-512:	CADFB526AA1F04609AEF3CC95454C6D2D40E24EEECB97ECB282B88347C7D01923CD60E9BC47715F98D25A7534CDC86B8A44C89F35B0D4D8E39BCA2E7F5F1D 47
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...47dd556f_57eb_4989_a6fb_6e8cf460990d.....u..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....<...https://launchandscalefaster.org/covid-19/vaccine procurement2...V.a.c.c.i.n.e. .P.r.o.c.u.r.e.m.e.n.t. .|. .L.a.u.n.c.h. .a.n.d. .S.c.a.l.e. .S.p.e.e.d.o.m.e.t.e.r.t...p.....h.....h.....`..... .....9.k!x...:.k!x... .....8.....<...h.t.t.p.s.:././.l.a.u.n.c.h.a.n.d.s.c.a.l.e.f.a.s.t.e.r...o.r.g./.c.o.v.i.d.-.1.9./.v.a.c.c.i.n.e.p.r.o.c.u.r.e.m.e.n.t..... ...8.....0.....8..... .....0.....(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd..............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.27585127270059
Encrypted:	false
SSDEEP:	6:m0vmMN+q2PWXp+N23iKKdK8aPrqIFUtppvmQiFZZmwPpvmQiFNVkwOWXp+N23iKG:YVva5KkL3FUtpoQmZ/PoQmz5f5KkQJ
MD5:	5D0D97CC7FB0D3A352BB6DC3753280C0
SHA1:	55BC2B8B853495CE30271838CFAC097F6C82374D
SHA-256:	D500F8065979B8E104C6B8B3E45B5E0BF3B8707702FC4E9A85CCB8C1F47E7B4C
SHA-512:	6FC0C6E33516A67DEA103F1BF9B873A40194EDC434B27E63B4491006DF3F6CBD0649375D1E4036A9890B65D03F2E0D5C9B87420B041AADAE82779FCE75816D5
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:55:39.748 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/06-10 :55:39.750 5f8 Recovering log #3.2021/07/06-10:55:39.750 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.238733558170139
Encrypted:	false
SSDEEP:	6:m0pF+q2PWXp+N23iKKdK8NIFUtpppzZmwPpp8NVkwOWXp+N23iKKdK8+eLJ:p+va5KkpFUtpn/PUV5f5KkqJ
MD5:	B11C9DA008AED51C15D1D0CAE41CEFC0
SHA1:	8AB7618E6C061026EECC468AEBBF03F8FFAC2A82
SHA-256:	55FDC657E6B588BCEEE410164788B6082862750B3C64797C6E6F103B38E5FCA8
SHA-512:	8904E9C8B0077C0ECF95AF401FC309E1F6C73FAA5CD12793ACA95AEC14F59588E984E901F3959379DDF29A5A3B5FCDAC124C9B34E0448C2506835A7BEFBE19 E
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:55:42.174 16dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/06-1 0:55:42.176 16dc Recovering log #3.2021/07/06-10:55:42.177 16dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

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=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	47104
Entropy (8bit):	1.7359052977090856
Encrypted:	false
SSDEEP:	96:yBCsdwg2Qy7Ha8Jp1Rd/TYwacGIjrT3zNfNPRzANfvRzxCrJfUo:IhJ2QQBLYwNTBNqtvvcxB
MD5:	CCE46F47134C9D6FFB2B197E25902195
SHA1:	D238ED5EC980C79F96A33D5357BDF0D010DB88C4
SHA-256:	A31B9C07B01267C78790D76C340078E1C619E0C1B965EA78ED989B7D30E21F32
SHA-512:	93E6686FF151ABAFDB2AE6D21115D880AFCEE9E215C4DFD96861393574EB73556FAB5B89954AA83C4B617AD5B9CC3215215442714116593 9B4E60CF1F5C9AD9
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50432
Entropy (8bit):	1.013845878248803
Encrypted:	false
SSDEEP:	48:QCdBmw6fUm3zWeOHHiqNiEacu0i7bt9E23+caeqNiEXFkcu0i71taaNGQVKcaeqE:QCdBC9eH6/Td3Tj75fFOz+VcNfAPRz5
MD5:	804FD9E57CB566BD96B0CAA13F422090
SHA1:	3D9A461AD65AA063E888A1AA430EB719FB1FB445
SHA-256:	DCEECE102509016F9EC217C919C4A9F45E7ECFD0178A65FEAA2EBFB0BD02C7C4
SHA-512:	1CF9FA4CA09CCE0E66FC8783E51F248696E589B59AB3A1F9082697239FC854B31CC70680A3760B0A1CF45DE44F17A01C150553B2E24DE48FD763536A6561C3B8
Malicious:	false
Reputation:	low
Preview:	.....t..... ....

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):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.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):	5.281286594176963
Encrypted:	false
SSDEEP:	6:m0FPMq2PWXp+N23iKKdK25+Xqx8chI+IFUtppFhIENJZmwPpFhIENDkwOWXp+N2k:zPMva5KkTXfchI3FUtpjhpJ/PjhpD5fk
MD5:	626799A7B27E976E7F4C2D090487360C
SHA1:	9AEF03217C1153040574B8201AFCDC92DAA8CAF3
SHA-256:	8E42992CCA2B853E65F13C178DE90B0137EC1B84D961216D0C767ABB1062E4F1
SHA-512:	B4375CC3C532B59260209F82CCDC9E1231EECB013E7481E2B780C32227567AC47529776C55966A003352146AA819DD5A69764D920B0CEAF9DF76546E9005E39F
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:56:07.279 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/06-10:56:07.280 554 Recovering log #3.2021/07/06-10:56:07.280 554 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\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.2206756869668265
Encrypted:	false
SSDEEP:	6:m0F5q2PWXp+N23iKKdK25+XuoIFUtppF3JZmwPpFKzkwOWXp+N23iKKdK25+Xuxo:z5va5KkTXYFUtpjZ/PjKz5f5KkTXHJ
MD5:	CCBF4A7812C1C9C947751FAD855D881C
SHA1:	7DD21B2964F7603006B3A276E96A9341E50F3A48
SHA-256:	5EB25D513F46DBE4FF92BD04BBE2C97FA7E1DC37B1DB639E62F08293C90A3CC8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
SHA-512:	C24AD84F267DF0B2BA45080E636707CFAD9E6AE6E642364BE9701A65B9AC70DA36A0CB45D4D7E32351F6358BA2CCF0A8BD0A98411FFC3830407AE6D8C730A5B
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:56:07.274 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/06-10:56:07.275 554 Recovering log #3.2021/07/06-10:56:07.276 554 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.276774794984655
Encrypted:	false
SSDEEP:	6:m0FtgL4q2PWXp+N23iKKdKWT5g1IdqIFUtppFtxZZmwPpFtpokwOWXp+N23iKKd6:ztlva5Kkg5gSRFUtpjtxZ/Pjtpo5f5Kg
MD5:	064B0C8397302D1714871AFD71CED93A
SHA1:	67170AD9FC9384230EBF27D84105A4BDC22D239C
SHA-256:	E35EA99106ED7B7000133A0E747EEF507AB326CFDC9C5769A75E8F5B308963BD
SHA-512:	B65913099B83851E283269079D743021770AE24264AD43D3A1CD4347FDE207A7C90A10A9C647E7E33F62B32569B2A164547913D04BCDEA7B92A7D6B3440FA683
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:56:07.247 554 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/06-10:56:07.248 554 Recovering log #3.2021/07/06-10:56:07.249 554 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	184320
Entropy (8bit):	0.6362951158100334
Encrypted:	false
SSDEEP:	192:xYIaYt0EkYYx0RcYpx09Q6y2Yyx0bUsY3x0uQ2:UyVSP
MD5:	4879844F974C4D4224D840F463238DAD
SHA1:	2EC692BB3D23A0599771E50E416F76C8FE5324C7
SHA-256:	FB473080523297C7732D76C50E9837633F5C00756348FE154B48E235FF1A60EC
SHA-512:	3CE51D2D3F99DD3AABE3DD6F2E709D7F73F809282014D8762F2C9CBB4649C77C9E016AB420DD30CEBB0942BE9095FC4C3E82569D8AA71925491E5F74C28388D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1103
Entropy (8bit):	5.525967787686423
Encrypted:	false
SSDEEP:	24:HZYjGnx+FPq11KOzn/2maqIPJipY057JHPPJiu057VB:HajugFPbOCma3iY057B3057v
MD5:	6A2A3DCD7EF8ECDAFAB1ED3E0C84E3A9
SHA1:	496263845C524EDFAE6CD5CFC1B683F802C5FEFB
SHA-256:	614D96220CF6E923C92DE274301772F8BEF8EC353C38FE9D29BFB528E11EB980
SHA-512:	C2F80967EB0365BD158CEDD2EE72A77605F4AE9C1FAF3755279AE20EE6D2461040406F16DB6FB0685120E87EBA140EECCED06201CB056F32C35DFE9C957FFB3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Preview:	....."....19..and..content..covid..https..launch..launchandscalefaster..main..org..procurement..scale..speedometer..vaccine..vaccineprocurement*.....19.....and.....content.....covid.....https.....launch.....launchandscalefaster.....main.....org.....procurement.....scale.....speedometer.....vaccine.....vaccineprocurement..2.....1.....9.....a.....c.....d.....e.....f.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....:.....B..... .....*lhttps://launchandscalefaster.org/covid-19/vaccineprocurement#main-content22Vaccine Procurement | Launch and Scale Speedometer:..... .....*<https://launchandscalefaster.org/covid-19/vaccineprocurement22Vaccine Pr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	187824
Entropy (8bit):	0.4981748879510206
Encrypted:	false
SSDEEP:	96:m5vYdHlYJ5p0ucBf0lYYFtx0fCfJbVIYoox0yfaIYzdn8x0H:mlYdFYJ5p0uCtY6x0fQAYJx0AXYzCx0H
MD5:	04AB386BDEA2FEC336B5AC49EEEEDE66
SHA1:	8CBA81BF45B7FE40F6372905C7D0F3EBF3FB6E2C
SHA-256:	0DC890842D1DCC97D1C7DE86236E7CBDF87C1F7DFBA7DA4FD1B397552E9ABE85
SHA-512:	2C3C9201D4587A4AE53029995EF9D694FD626D21175EC635502678BFB0B51BEE766B3EB28F8412D6103056E03D1EB8AE926C3C11AFBBDC063626101B9EB1D54
Malicious:	false
Reputation:	low
Preview:	.....fy..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3547
Entropy (8bit):	5.561818292943193
Encrypted:	false
SSDEEP:	48:hS2G8pa7ZM08dbbVl4bQSefgGuJNrS0U9RdiN9uDZwt8jI3:hra7ZMHdbbVl4bQ5fgGerS0qZwt8jI3
MD5:	A5DF0112E7C3319B8E2D6E9046697A93
SHA1:	A0A108F3C8464B477BC7BC87676FC1CFF7A3AB20
SHA-256:	7776F9183590411812868BFAA2E43B13D15D329F9FB0F98452F2D0803B621DE7
SHA-512:	A7CD141880E4D321CBBB5CC7F1F634ACCAA6B74849E4FE3AC659A19D0300B58B715A600952B75993BB9147B7C697AED518335B555E527B2567B2BC118B49DBE0
Malicious:	false
Reputation:	low
Preview:	)......*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..749565000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-06 10:56:08.66][INFO][mr.Init] MR instance ID: 14d2f606-5855-4362-8eba-6e9a7bb2308b\n","[2021-07-06 10:56:08.66][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-06 10:56:08.66][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-06 10:56:08.66][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-06 10:56:08.66][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-06 10:56:08.66][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-06 10:56:08.66][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.204916447147129
Encrypted:	false
SSDEEP:	6:m0vk6UXcq2PWXp+N23iKKdK8a2jMGIFUtppvkUIZmwPpvkUNXPkwOWXp+N23iKKV:Ssva5Kk8EFUtp7l/PdP5f5Kk8bJ
MD5:	172CC3E4A9D46D9BF8E9FA9CE6D46F0A
SHA1:	A3B9143F04F43CCDD26DE5A540E28B3C5956779F
SHA-256:	DE422ED0EDB56A23F6651CAF5AEEFC3662614BD60430C3C469DE82037D062ECB
SHA-512:	E9854946231C1208C2085BDD7068C1549FD6E8CF7C3BD878EBD2E0C76E00E14D60CAC478C502D9030B0107CA70137937B45EE139501F626222F0839D4C664C6E
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:55:39.501 1224 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/06-10:55:39.503 1224 Recovering log #3.2021/07/06-10:55:39.511 1224 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	1.2012823867300633
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOMiOqAuhjspnWOBz7/OqAuhjspnWO7aOqAuhjspnWO+90oAKN6m:HeKbpF0oAKIm
MD5:	D2BAA01FA0ECB871B8AF1792981E9014
SHA1:	FA6D5C223F286F23E292D4AD3E48FC0564B8D2AB
SHA-256:	B988DBFF9FF8F7A39537BB1162E0C071A8ABE1959CC7E0AEFB89E75BF3CA818F
SHA-512:	23D3BA81795E92406A97BEAA9D62AF45F3BE509E993720FBE230937BCFFAF078F1A2C7C2E4C6C81B1EA84F81273F7FA7CBE902961B40714184110297A2B2F18B
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.280987057839446
Encrypted:	false
SSDEEP:	6:m0vmS+3+q2PWXp+N23iKKdKgXz4rRIFUtppvmSDXZmwPpvmSkNVkwOWXp+N23iKj:YBOva5KkgXiuFUtpo8X/PoJ5f5KkgX2J
MD5:	2FA4CDE1F5220DA73C0CFCB4C19E96B2
SHA1:	9B689B3F1558B7C90DECB5E4C3C904C423A77866
SHA-256:	F22808FF492586DD419DD4F783B53CC6BB89B277DCE45AE7E5EF986CAB5148A4
SHA-512:	2D4A39651FBA981B8D19BA0FDE40756C2867A08D974DC6C28C6A6DE8C3E396B84B8E4A3C61D14AF7EF1F8AE4A601880A965FBB273E440355E537377EFAFAF43 0
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:55:39.774 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/06-10:55:39.775 5f8 Recovering log #3.2021/07/06-10:55:39.776 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.010904475240455
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAo/:wIElwQF8mpcSJ2YL1
MD5:	32874A48ABC006ABF1387DBC1B268AFF
SHA1:	1C58D0BE735D3FE75B77FE5DE51A27BF1E886404
SHA-256:	49912198EDF5EDF40ECEE93901BC8F8872F3B91D17E236702A37DB0C9A4EB602
SHA-512:	92FE785D329CD76D2D16292E263D3D20DACC07E55A80E9373ACE5CFC07B4BDEAFCB71EB52B04CBE1D47A410A8F6895BB3FF29DDCE87A251D5CA46EF5FE64 4DC
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8250397245269779
Encrypted:	false
SSDEEP:	48:GsqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUQ6:GshIElwQF8mpcSZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
MD5:	7679BA4A61AC53C8ED789C5BDA7BB4BF
SHA1:	C0CFCF03C1814293B4569AD0A04014061AE82D21
SHA-256:	885AC82EDC38C06E09D856C801652B61A475ABC348F221E36621B2DC4193864F
SHA-512:	95BA7111F57F74BAB07DB35A520CB932109D520D936298FB6E0BCA1F7E11CDAAF4DAA2852E4E7361C3E0D3A78C72F3053686791273DFBCD0AD29E37696801E9D
Malicious:	false
Reputation:	low
Preview:	.....lh.>..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1295
Entropy (8bit):	4.828920210076539
Encrypted:	false
SSDEEP:	24:7mzAtuvsGw1XLmf+bwPt4Htxg3lwQAR4hZwQllowQPwQyR3lwQ2zNwQj/XG:7m8Erw17jbLt23lwQARqZwQHowQPwQyv
MD5:	83E610344155B5FDC7400773A739151E
SHA1:	CBEFC0B9721FDEE74DFFB85C5967CAF2A5497A55
SHA-256:	600BA5800DFF511BF37B257426A4E3B9BF6B0C600E4BE0EDB32F58754D126EC9
SHA-512:	3B947B5E2FE11C5F8070B8FA55F805F3765C6F7F1C17D82BC9E59F5BE80B32DE16D6763C0D433E2901CE270AD16F5907AA70F91A4C18F8F9A9646A7C2F744F77
Malicious:	false
Reputation:	low
Preview:	..&f.....B".i.....next-map-id.1.Jnamespace-47dd556f_57eb_4989_a6fb_6e8cf460990d-https://public.tableau.com/.0V.e.....V.e.....V.e.....p$ .i.....next-map-id.2.Jnamespace-355d09da_21cb_47b7_864b_fd8f2083ec11-https://public.tableau.com/.1. .....d%..i.....next-map-id.3.Jnamespace-42ef4ba1_56c6_484b_94ba_153983e8bc4c-https://public.tableau.com/.2bW._f.....next-map-id.4.Gnamespace-3face54e_8138_4d41_b009_4f4e909eb025-https://www.youtube.com/.3....|.....map-3-yt-remote-cast-availableR{.".d.a.t.a.".:.".f.a.l.s.e.".,.".c.r.e.a.t.i.o.n.".:.1.6.2.5.5.9.4.1.9.8.5.2.9.}...map-3-yt-remote-cast-installedP{.".d.a.t.a.".:.".t.r.u.e.".,.".c.r.e.a.t.i.o.n.".:.1.6.2.5.5.9.4.1.9.8.5.2.7.}..!map-3-yt-remote-fast-check-periodb{.".d.a.t.a.".:.".1.6.2.5.5.9.4.4.9.8.2.1.1.".,.".c.r.e.a.t.i.o.n.".:.1.6.2.5.5.9.4.1.9.8.2.1.1.}...map-3-yt-remote-session-appf{.".d.a.t.a.".:.".y.o.u.t.u.b.e.-.d.e.s.k.t.o.p."

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.236356425591806
Encrypted:	false
SSDEEP:	6:m0vO+q2PWXp+N23iKKdKrQMxIFUtppvfHZZmwPpvfHNVkwOWXp+N23iKKdKrQMFd:xva5KkCFUtpX/PF5f5KktJ
MD5:	CD0D67BD6038E58041B856643642E36D
SHA1:	52583E0A1F7448C9578CBBE9F7982FF69C0ED05F
SHA-256:	01F81ECE4C5BAD69FAF06F5C6F0CC9D0C5ED8FF9383DF16EAF7C5E1CD9716891
SHA-512:	A6E8242EF076BDF8DFDC8372147948455563789 1EF26DFB1365B5C672FAB167FC10F41FFA85AB866B8AA110655920C69477E3444129C68970BD1A5E57CD27951
Malicious:	false
Reputation:	low
Preview:	2021/07/06-10:55:39.691 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/06-10:55:39.692 5f8 Recovering log #3.2021/07/06-10:55:39.692 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.244513623195657
Encrypted:	false
SSDEEP:	6:m0v9+q2PWXp+N23iKKdK7Uh2ghZIFUtppvRZmwPpvX8VkwOWXp+N23iKKdK7Uh2w:Kva5KkIhHh2FUtpH/PV85f5KkIhHLJ
MD5:	FA5EE7FA1B7F343674AD8A294319B211
SHA1:	D75686AEBC5EAA332483BBA635AE6AC55D464CA8
SHA-256:	F1B3121F823F0F557477E6F413B71489B92F9A828DA2401C1B606D3D6F3D3050
SHA-512:	3CD91DE219BBB9BDE04AB1E4A089DB347029573529AE1AEC897176EE1709E830A0ED81BBA2C4B6BCC073AE1D8B2A131AB00C77DF25DAD804DEA977F6D253C466
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Preview:	2021/07/06-10:55:39.429 5f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/07/06-10:55:39.432 5f8 Recovering log #3.2021/07/06-10:55:39.433 5f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

Static File Info

No static file info

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3504 Parent PID: 2128

General

Start time:	10:55:38
Start date:	06/07/2021
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 'https://launchandscalefaster.org/covid-19/vaccineprocurement'
Imagebase:	0x7ff77b960000
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

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4684 Parent PID: 3504

General

Start time:	10:55:40
Start date:	06/07/2021
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=1596,5814909055831787961,2700687591494063260,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1784 /prefetch:8
Imagebase:	0x7ff77b960000
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

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6844 Parent PID: 3504

General

Start time:	10:56:40
Start date:	06/07/2021
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=1596,5814909055831787961,2700687591494063260,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=736 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 5232 Parent PID: 3504

General

Start time:	10:56:42
Start date:	06/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1596,5814909055831787961,2700687591494063260,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=996 /prefetch:8
Imagebase:	0x7ff77b960000
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

Registry Activities Show Windows behavior

Disassembly