ID: 458981
Cookbook: browseurl.jbs
Time: 00:14:42
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

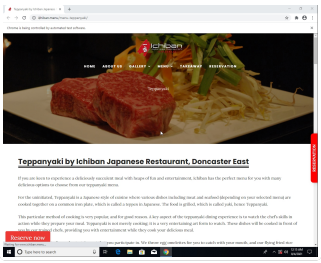
Windows Analysis Report http://www.ichiban.menu/men…

Overview

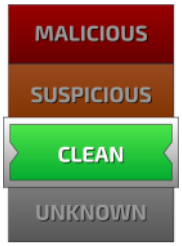
General Information

Sample URL:	http://www.ichiban.menu/menu-teppanyaki/
Analysis ID:	458981
Infos:	

Most interesting Screenshot:



Detection

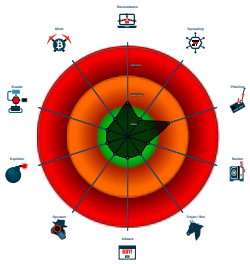


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- No HTML title found
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 752 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://www.ichiban.menu/menu-teppanyaki/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4720 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,16433198126318794357,6094034236782199136,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /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

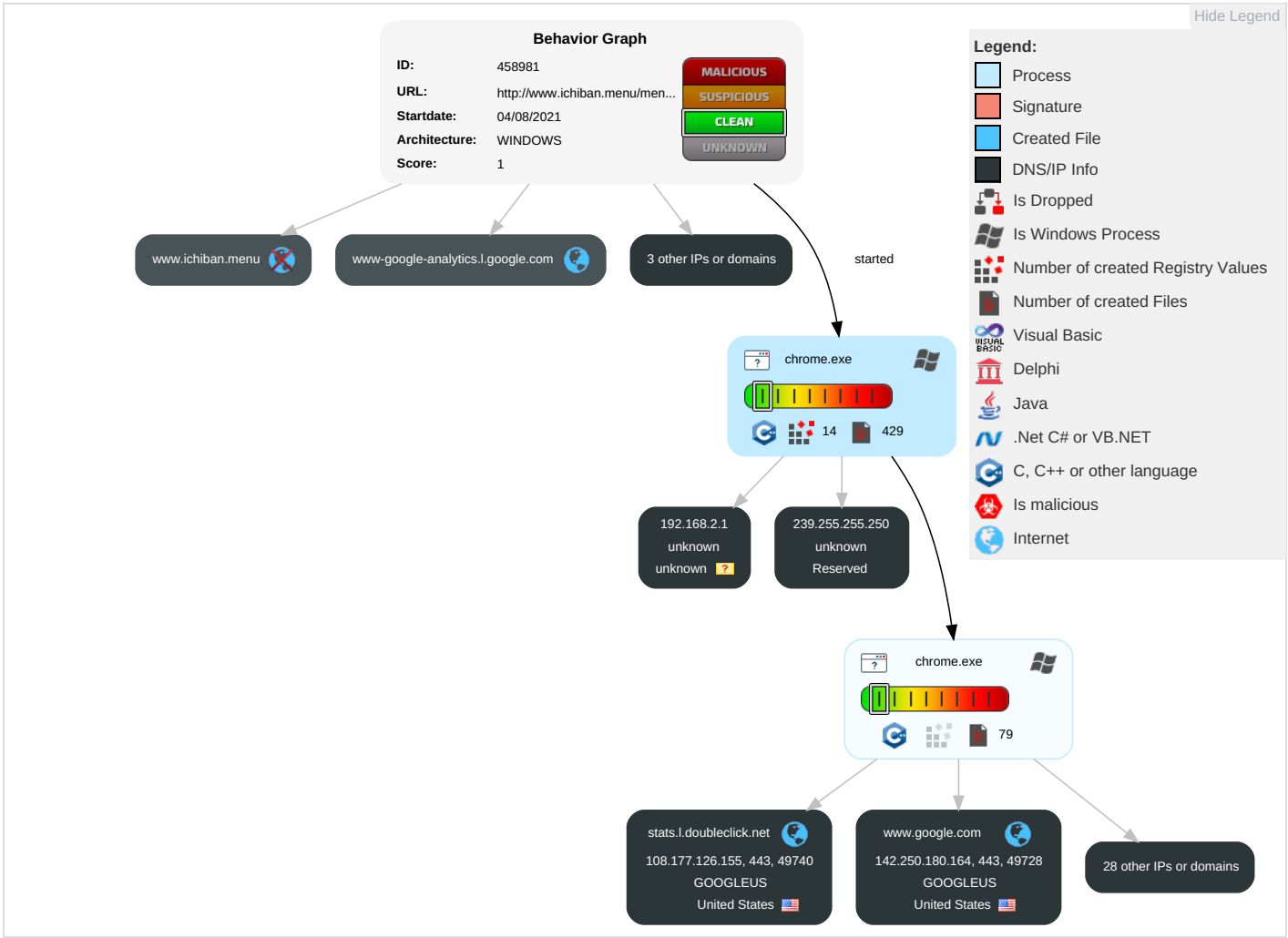
Click to jump to signature section

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap	

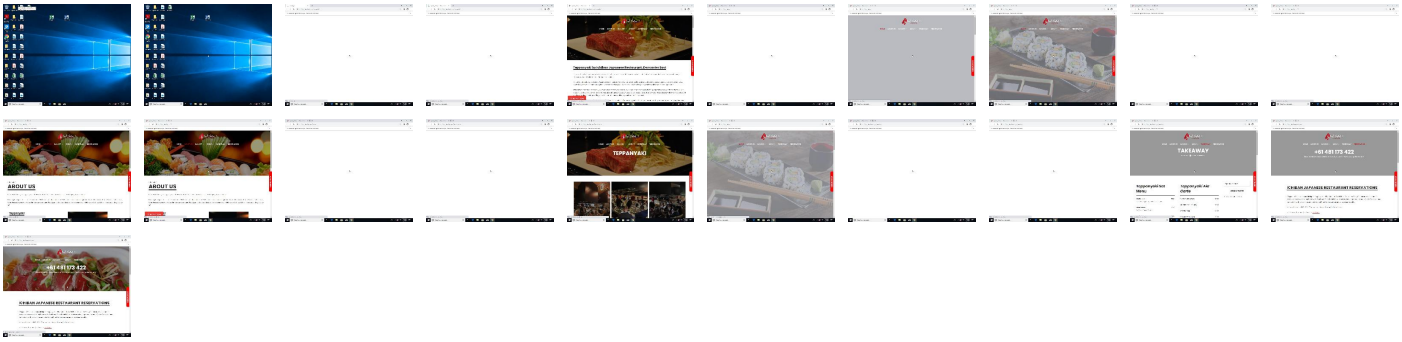
Behavior Graph

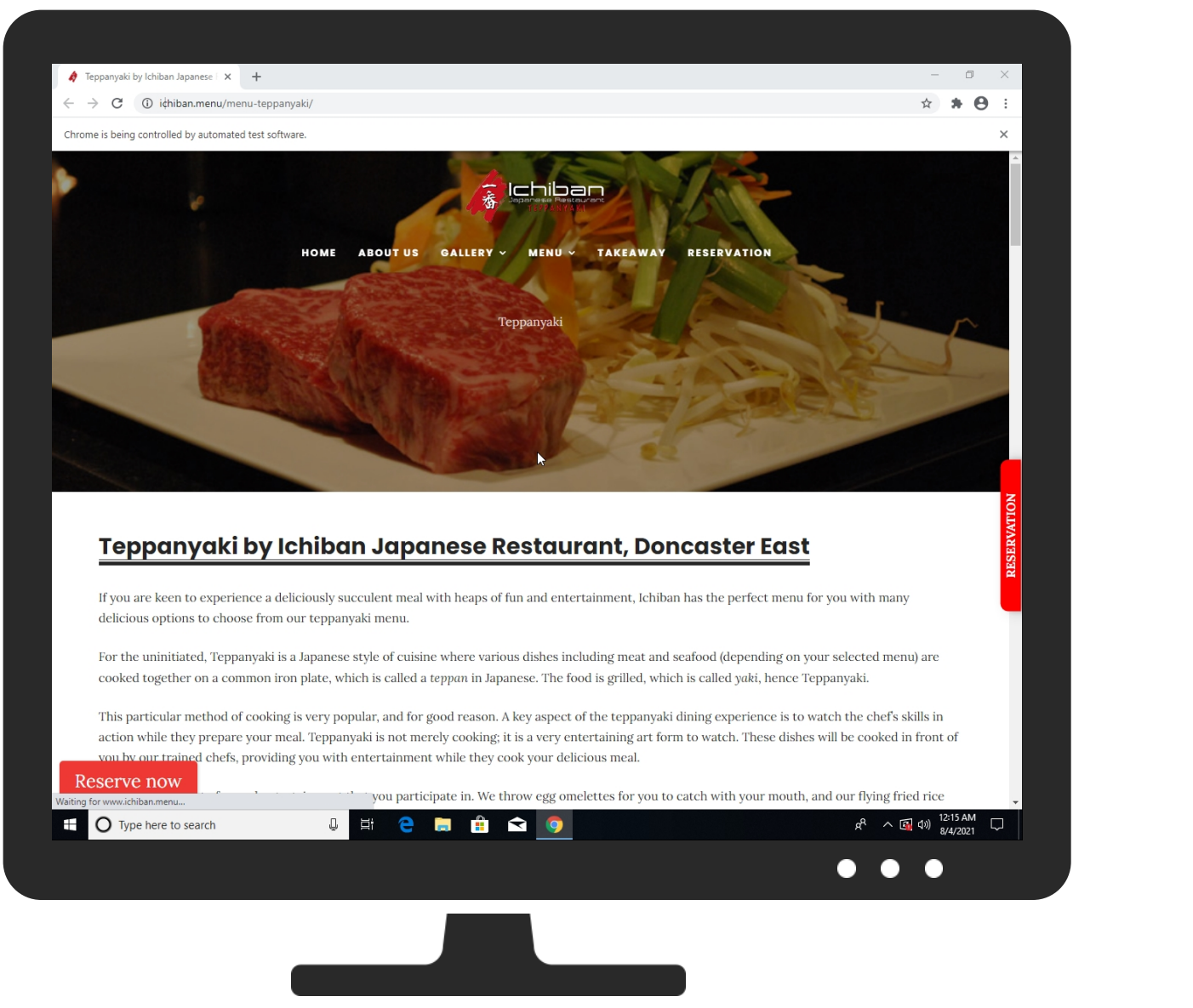


Screenshots

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://www.ichiban.menu/menu-teppanyaki/	0%	Virustotal		Browse
http://www.ichiban.menu/menu-teppanyaki/	0%	Avira URL Cloud	safe	

Dropped Files

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.quandoo.com.au	0%	Virustotal		Browse
ichiban.menu	0%	Virustotal		Browse
booking-widget.quandoo.com.au	0%	Virustotal		Browse
www.ichiban.menu	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ichiban.menu/	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/transparent.png)	0%	URL Reputation	safe	
http://www.ichiban.menu/wp-content/cache/minify/9af47.js	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-teppanyaki/Y	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-teppanyaki/2:Teppanyaki	0%	Avira URL Cloud	safe	
http://ichiban.menu/:U	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-admin/admin-ajax.php	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/themes/dina/css/fontawesome/fonts/fontawesome-webfont.woff2?v=4.7.0	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-teppanyaki/J	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/cache/minify/37e61.js	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1963_1-squashed.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/cache/minify/c7035.js	0%	Avira URL Cloud	safe	
http://ichiban.menu/B	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-teppanyaki/:	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2024_1-squashed.jpg	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6_hdpi.png	0%	URL Reputation	safe	
http://www.ichiban.menu/menu-teppanyaki/2	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IchibanFrontDoor.jpg	0%	Avira URL Cloud	safe	
http://ichiban.menu/tdD	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/06/738370-1920x1280.jpg	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/24899790_2187483284599017_7338923987939449924_n.jpg	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://www.ichiban.menu/wp-content/uploads/2017/06/japanese_food-t2.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/06/sushi-backgrounds_112713348_82.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/06/410666-1920x1280.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1922-squashed.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu/takeaway/&	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/about/sl	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/cache/minify/37e61.jsaD	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu/takeaway/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1991-squashed-e1502606036564.jpg	0%	Avira URL Cloud	safe	
http://ichiban.menu/0K	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/reservations/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://www.ichiban.menu//	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn	0%	URL Reputation	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/Screen-Shot-8-1.png	0%	Avira URL Cloud	safe	
http://ichiban.menu/t	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-teppanyaki/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2014_1.jpg	0%	Avira URL Cloud	safe	
http://ichiban.menu/h	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2018/04/ichiban_horizontal_teppan_small.png	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://www.ichiban.menu	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.ichiban.menu/menu-teppanyaki/:Teppanyaki	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/Ichiban	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/gallery/ayce/Teppanyaki	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/24293862_2175673712446641_5670291794321811786_n.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/gallery/teppanyaki/(Teppanyaki	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/about/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-ayce/3	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IchibanFrontDoor-768x1002.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-ayce//	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-includes/js/wp-emoji-release.min.js?ver=4.9.8	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2014_1-squashed.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/cache/minify/fbbf4.js	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/gallery/teppanyaki/Teppanyaki	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2023_1-squashed.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/menu-ayce/	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/gallery/teppanyaki/#rainmaker_form_2109	0%	Avira URL Cloud	safe	
http://ichiban.menu/gk	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/wp-content/uploads/2017/08/niseko-pirka-teppanyaki-02.jpg	0%	Avira URL Cloud	safe	
http://www.ichiban.menu/gallery/ayce/&	0%	Avira URL Cloud	safe	
http://https://www.google.comh	0%	URL Reputation	safe	
http://www.ichiban.menu/menu-teppanyaki/zw	0%	Avira URL Cloud	safe	
http://www.ichiban.menuh	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.35	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
s3-eu-west-1.amazonaws.com	52.218.20.156	true	false		high
1.gravatar.com	192.0.73.2	true	false		high
accounts.google.com	216.58.205.77	true	false		high
www-google-analytics.l.google.com	142.250.184.78	true	false		high
stats.l.doubleclick.net	108.177.126.155	true	false		high
www-googletagmanager.l.google.com	142.250.184.72	true	false		high
booking-widget.quandoo.com	143.204.207.60	true	false		high
www.quandoo.com.au	176.34.109.148	true	false	• 0%, Virustotal, Browse	unknown
ichiban.menu	166.62.28.94	true	false	• 0%, Virustotal, Browse	unknown
booking-widget.quandoo.com.au	13.32.22.7	true	false	• 0%, Virustotal, Browse	unknown
youtube-ui.l.google.com	216.58.208.174	true	false		high
www.google.com	142.250.180.164	true	false		high
api.segment.io	35.167.90.204	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
z-p42-instagram.c10r.facebook.com	157.240.17.174	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high
9110-api.quandoo.com	52.213.64.175	true	false		high
static-cdn.hotjar.com	13.32.22.92	true	false		high
www.facebook.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.instagram.com	unknown	unknown	false		high
www.ichiban.menu	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
static.hotjar.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ichiban.menu/wp-content/cache/minify/9af47.js	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/themes/dina/css/fontawesome/fonts/fontawesome-webfont.woff2?v=4.7.0	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/reservations/	false		unknown
http://www.ichiban.menu/wp-content/cache/minify/37e61.js	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1963_1-squashed.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/cache/minify/c7035.js	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2024_1-squashed.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IchibanFrontDoor.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/06/738370-1920x1280.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/24899790_2187483284599017_7338923987939449924_n.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/	false		unknown
http://www.ichiban.menu/wp-content/uploads/2017/06/japanese_food-t2.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/06/sushi-backgrounds_112713348_82.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/06/410666-1920x1280.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1922-squashed.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_1991-squashed-e1502606036564.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/menu-teppanyaki/	false		unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/Screen-Shot-8-1.png	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2014_1.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/gallery/teppanyaki/	false		unknown
http://www.ichiban.menu/menu/takeaway/	false		unknown
http://www.ichiban.menu/wp-content/uploads/2018/04/ichiban_horizontal_teppan_small.png	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/	false		unknown
http://www.ichiban.menu/reservations/	false		unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/24293862_2175673712446641_5670291794321811786_n.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IchibanFrontDoor-768x1002.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-includes/js/wp-emoji-release.min.js?ver=4.9.8	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2014_1-squashed.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/cache/minify/fbbf4.js	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/about/	false		unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/IMG_2023_1-squashed.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/about/	false		unknown
http://www.ichiban.menu/menu-ayce/	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/wp-content/uploads/2017/08/niseko-pirka-teppanyaki-02.jpg	false	• Avira URL Cloud: safe	unknown
http://www.ichiban.menu/menu/takeaway/	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.218.20.156	s3-eu-west-1.amazonaws.com	United States		16509	AMAZON-02US	false
216.58.208.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
52.213.64.175	9110-api.quandoo.com	United States		16509	AMAZON-02US	false
35.167.90.204	api.segment.io	United States		16509	AMAZON-02US	false
108.177.126.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
13.32.22.92	static-cdn.hotjar.com	United States		7018	ATT-INTERNET4US	false
13.32.22.7	booking-widget.quandoo.com.au	United States		7018	ATT-INTERNET4US	false
142.250.184.72	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
142.250.180.164	www.google.com	United States		15169	GOOGLEUS	false
142.250.186.35	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.58.208.174	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.78	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.207.60	booking-widget.quandoo.com	United States		16509	AMAZON-02US	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
192.0.73.2	1.gravatar.com	United States		2635	AUTOMATTICUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
166.62.28.94	ichiban.menu	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458981
Start date:	04.08.2021
Start time:	00:14:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.ichiban.menu/menu-teppanyaki/
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:	21
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:	clean1.win@38/250@26/19
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: http://www.ichiban.menu/ • Browse: http://www.ichiban.menu/about/ • Browse: http://www.ichiban.menu/gallery/ayce/ • Browse: http://www.ichiban.menu/menu-ayce/ • Browse: http://www.ichiban.menu/menu/takeaway/ • Browse: http://www.ichiban.menu/reservations/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:16:39	API Interceptor	1x Sleep call for process: chrome.exe modified

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 GM DS.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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2A0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.117636708753809
Encrypted:	false
SSDEEP:	6:kKr8CdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:jr5kPlE99SNxAhUe0et
MD5:	AF08AE8CD082EC572D18E91AB98C27D4
SHA1:	E08CDF00B1A720EF2D835E3D5324CBA69EC431FE
SHA-256:	07847D598DDC132D09CA271F009919BAE24557C110BD6DE6CC8F55DCA30A846D
SHA-512:	80A0CC73F3315EF1E191282113519BAAA3C4EF42FAE6F0846355840B14320BB76EA84BF4990E3EC508BE55AE8DA09920D863343AAC970AD158087129FF9A8C85
Malicious:	false
Reputation:	low
Preview:	p..... .....(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\4e660f93-3ca7-40f6-8af5-7eed649b90b2.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):	165870
Entropy (8bit):	6.049556176026057
Encrypted:	false
SSDEEP:	3072:9GaYTJQE+mugy9+QV1T7IRwdfLSNPOFcbXafIB0u1GOJmA3iuR5:4xaV+QfT7GSmhEaqfllUOoSiuR5
MD5:	C057AF0D4D958150A1050BA0D386C2AF
SHA1:	25A447AC133C3CC80C6A05B8AF8D44FD66DE87CF
SHA-256:	8534E090D163E19ED896F427BA60302790D50A31192B7B57849B855853968A60
SHA-512:	A897FE499C933478E8DC146EAD448371657503CE6FF0C8FE0E26FB7C4F56AFDAF2A33B3271519985FB3B05560B59CD8CA79503DB039782EA49295F111694000C
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":1.628061332406819e+12,"network":1.628028934e+12,"ticks":4483065250.0,"uncertainty":4367825.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016321227"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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\0003996a-5449-4d1d-ba52-5cef383641cc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0003996a-5449-4d1d-ba52-5cef383641cc.tmp	
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\4db253b3-c9f6-49ea-8793-560fa8ce710c.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):	22595
Entropy (8bit):	5.535872250505424
Encrypted:	false
SSDEEP:	384:2/htBLlmmXI1kXqKf/pUZNCgVLH2HfDErU8HGqnT8+km4l:GLl7I1kXqKf/pUZNCgVLH2HfYrUwGqnA
MD5:	83BC8D7A974A0522CFD7C16143C44592
SHA1:	8D5CD79D6EDF65D266C65A960E1E1B084B8C0D17
SHA-256:	C6D55E3BFF826D0E0BF4F2F7B7EC978F0DB7FD47848C3E49C4DE9D917606A46D
SHA-512:	6FB0EA72FC2E66AD30D1B59B5A9B3AAF13A244E585E54C1EA6A1D24BA114D95F04298BB466C2602AC31B37CE3F4C736912DA6C24236C55A73A746E2FF8D6E9A4
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":"13272534929324348","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\519b6273-2d33-47ac-8936-fa6149ce560d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5f195c04-b565-406a-93b4-7c645131fb3a.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):	1539
Entropy (8bit):	5.593778945655415
Encrypted:	false
SSDEEP:	48:YEeUAieU46UUhlU1KUZqPeUer2UefPwU5Uenw:zeUAieURUUrU1KUUPeU9UE4U5UD
MD5:	F687BF9CEC970A00ABA26FCD7CCE17B2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5f195c04-b565-406a-93b4-7c645131fb3a.tmp	
SHA1:	44CBF3263D02ED4851972999A2F22B1283609F3E
SHA-256:	C056876E4638546404E434A232C1E3B1D4CFA6F312C50B96D8296142FB8EBE4B
SHA-512:	54531194DB3135AD151EFCC9F3BC679F7A906AA05F3B250C7552919BAE80237E7592BE3CA26473DA5EDE90E1478DAE86201B5624363F54DCC1CF95E7D9B98C3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1638947735.746837,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061335.746843},{"expiry":1659597335.043785,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061335.043791},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1638947735.304174,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061335.30418},{"expiry":1659597333.402484,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628061333.40249},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\69246233-5046-4f1d-9e2c-76dc9c9c6634.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1539
Entropy (8bit):	5.597689725012484
Encrypted:	false
SSDEEP:	48:YbeUWieUu6UUhlU1KUZqPeUer2UefPwU5Uenw:MeUWieUzUUrU1KUUPeU9UE4U5UD
MD5:	1C2D7ABE5767821CC5CB16CA1A17E969
SHA1:	465799648921A8CF2DE2D803C9C14B74D6CBB520
SHA-256:	3F6EFCCA7652324564B546010460C43CFDFD9B0FF791A6CCF9FF4AFF6BAFD842
SHA-512:	4AED9288778908C9DB070FBA3C05B2C369330D5D46E891B0620A37D4C01919DE78303283370301A344E8C0F5081153C828C5D475739605E693D29DF52EB5A6D7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1638947795.698289,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061395.698294},{"expiry":1659597398.148832,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061398.148839},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1638947735.304174,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628061335.30418},{"expiry":1659597333.402484,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628061333.40249},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6eec1960-4fc4-4231-9567-8e4eb9e3515e.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):	5783
Entropy (8bit):	5.188622326290684
Encrypted:	false
SSDEEP:	96:nRCfkn9SwxXRcKIXok0JCKL8hkk1IbOTQVuwn:nRCq9rhcA4KykkQ
MD5:	CE47936928842D721C6D3ADDAAE7841C
SHA1:	E3B1836670EA7CECE2FE8C31AB1A02DD9ACBAE75
SHA-256:	3AA5CE647CC21F309EE588DFC0E9BAB64341416B1904E4984F4C11D623094843
SHA-512:	73FBE9D0DEC635ED97113F99D3F7932D7B936DD2570FD199C933876D09181D41AC734C2013EED622137DF470CCE12C60A114E10FEF4151F91F808E5DB7271AD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534929626370","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\70d8e68d-654b-4bd3-a574-7b6422efd888.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):	5809
Entropy (8bit):	5.191173759512403
Encrypted:	false
SSDEEP:	96:nRCfzn9SwxXRcKITok0JCKL8hkk15bOTQVuwn:nRCL9rhcE4KykkP
MD5:	07CA9118F6C64E14A2EDCDBD2E207923
SHA1:	E21D5AA18A58B9DA64B4D81678999E79E9A50EE5
SHA-256:	1BE1881FA85AB86C3476730C5CCC2B3636C9AA9A77B07809714031A0D9F03092

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\70d8e68d-654b-4bd3-a574-7b6422efd888.tmp	
SHA-512:	40D36513099D3E1F7AE4276993C5C251E51029B9AAD3F0404EF4C815C507FF5ABA829A52B1DD118D8304C6E964CF9C2A9B09744DAAD95FC34C20ADE5AA784F 8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534929626370","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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\766a81c8-70dc-4e7f-a659-38ccea56616c.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):	4122
Entropy (8bit):	4.894981539348123
Encrypted:	false
SSDEEP:	96:JTOXGDHzhlzes6VM2erNsSGuGpT5j6l5KzFGdw5GbIH:JTOXGDHzhFes6VM2eruSD4T5j6l5KFP/
MD5:	16C55AF035F5826766FEF328F81C9E7A
SHA1:	1EC194710ED060DBC390F21BF6B0479F2E6982C8
SHA-256:	F903070491FE3105E48FA5F9E3214A9CB75018841C57FB4D37B357329A7E6BE0
SHA-512:	6020928D129C1E2E43490825FB488E522B2B9ED9194D5CA29BBE88B38CDFE88143BDCDE4FC54251D0DEF0D03F5D00FF55A74D42F98BBC55D89E73F9CE36BD3 EB
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932510936","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932511847","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932697074","port":443,"protocol_str":"quic"},{"advertised

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):	334
Entropy (8bit):	5.221428881628009
Encrypted:	false
SSDEEP:	6:m4o+M+q2PWXp+N23iKKdK9RXXTZIFUtpldyZmwPl1MMVkwOWXp+N23iKKdK9RXXH:S+va5Kk7XT2FUtpu/P/NV5f5Kk7XVJ
MD5:	078C8BA5A09319C95F547264689E9F47
SHA1:	815A490BCE2DA65661FEA558095357DFF7659B07
SHA-256:	17FB9138CEF4AD5BB6C0FE4292BE52AA450118421BD8B275200B6952C7DC08CC
SHA-512:	23E023E9A7B46FA03E83DCEA23D206DCFF24CED2A01A15CC689E9CD104E213A4C041EF6426B759D4E3FCBB5B079EA66B628C35C675D5B9A368D1D64B5714E 32
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.897 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:15:40.912 1b1c Recovering log #3.2021/08/04-00:15:40.913 1b1c 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\AutofillStrikeDatabase\LOG.old=& (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.221428881628009
Encrypted:	false
SSDEEP:	6:m4o+M+q2PWXp+N23iKKdK9RXXTZIFUtpldyZmwPl1MMVkwOWXp+N23iKKdK9RXXH:S+va5Kk7XT2FUtpu/P/NV5f5Kk7XVJ
MD5:	078C8BA5A09319C95F547264689E9F47
SHA1:	815A490BCE2DA65661FEA558095357DFF7659B07
SHA-256:	17FB9138CEF4AD5BB6C0FE4292BE52AA450118421BD8B275200B6952C7DC08CC
SHA-512:	23E023E9A7B46FA03E83DCEA23D206DCFF24CED2A01A15CC689E9CD104E213A4C041EF6426B759D4E3FCBB5B079EA66B628C35C675D5B9A368D1D64B5714E 32
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old=& (copy)	
Preview:	2021/08/04-00:15:40.897 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:15:40.912 1b1c Recovering log #3.2021/08/04-00:15:40.913 1b1c 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):	318
Entropy (8bit):	5.198154860355162
Encrypted:	false
SSDEEP:	6:m4JM+q2PWXp+N23iKKdKyDZIFUtplUfZmwPlwMVkwOWXp+N23iKKdKyJLJ:Y+va5Kk02FUtpef/PPV5f5KkWJ
MD5:	33BE0FF6E651AD2780875B450E85BA61
SHA1:	FC1B72FA14CF20A405E3F44B851E8A8EE3680D32
SHA-256:	5A8B540F0866EBEBAF5DFE4E2D557BC953D1AA6EC18ADBCCC3A563343969508E
SHA-512:	C5625086640CF1E7AA5C1BEA8F943AE624FED4ADFAE6F32C65EF84CC68D98AEC6B2A9C0D92C63771B1F0FEC198BB672E73CDC2C858680DD8CFC3ACE32EA7DBC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.882 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:15:40.886 1b1c Recovering log #3.2021/08/04-00:15:40.887 1b1c 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\BudgetDatabase\LOG.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.198154860355162
Encrypted:	false
SSDEEP:	6:m4JM+q2PWXp+N23iKKdKyDZIFUtplUfZmwPlwMVkwOWXp+N23iKKdKyJLJ:Y+va5Kk02FUtpef/PPV5f5KkWJ
MD5:	33BE0FF6E651AD2780875B450E85BA61
SHA1:	FC1B72FA14CF20A405E3F44B851E8A8EE3680D32
SHA-256:	5A8B540F0866EBEBAF5DFE4E2D557BC953D1AA6EC18ADBCCC3A563343969508E
SHA-512:	C5625086640CF1E7AA5C1BEA8F943AE624FED4ADFAE6F32C65EF84CC68D98AEC6B2A9C0D92C63771B1F0FEC198BB672E73CDC2C858680DD8CFC3ACE32EA7DBC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.882 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:15:40.886 1b1c Recovering log #3.2021/08/04-00:15:40.887 1b1c 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\0fcc6d437574cf25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14466
Entropy (8bit):	5.826478110281821
Encrypted:	false
SSDEEP:	384:XoA8VrbTfpMo0EtDSpy7ZuYW+TJr3J//bEI+XgA5U6e:43HWnEtDcy7ZlBlr3J//YfXgAC6e
MD5:	A39784FD942DFF8A3387C40514EAD6A4
SHA1:	A785FB9E4BAA6A4E83C3D98AF944C0AE6653A5D1
SHA-256:	9FFFB8CEA260BF33C34F02984A428484DBE8E507209D6A195D05F8F01D43D77A
SHA-512:	494499DE57DEDC28553A4B3FCC2A53A096F0BAECD54C5C719CCEECC19F1CC6191B73F93F26ADA8B24BC3FF85DA31D4B6CC7E06F4C20995EF29AB40CD45910F6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.../^%...._keyhttp://www.ichiban.menu/wp-includes/js/wp-emoji-release.min.js?ver=4.9.8 .http://ichiban.menu/...L'/.....E..g...D.v..Itr&y.I(|E..SJ.A..Eo.....3RF.....A..Eo.....'.....O.....6..\. -.....x..... .....(S.\..`n.... L`.....L`.....Qc>.....twemoji..(S....`.....L`B.....Rc`.....(.....M....O...Qb.P.7....c.....QbV.....d.....Qb.M.....e.....Qbz..~....f.....Qb>.}.....h.....S...QbR9.....j.....Qbn9.+....m.....Qb.UN.....o.....Qb..t....p.....Qb.r'H....q.....Qbj.....r.....Qb.....s..Qb.#L.....t.....R....Qb.....v.....Qbz.....w...s.....l`....Daz....G...(S.....IaW.....@.-....TP.A.....H...http://www.ichiban.menu/wp-includes/js/wp-emoji-release.min.js?ver=4.9.8a.....D`....D`....D`.....|...`:...&...&....&....&.(S...Ia.....O.....d.....@.....&.(S.....Ia.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2927575d9fcb27ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2927575d9fcb27ca_0	
File Type:	data
Category:	dropped
Size (bytes):	105784
Entropy (8bit):	5.804471270344644
Encrypted:	false
SSDEEP:	1536:MCez8UvxRxisbiszH3eH326x/7vkXLgVFbmdmh4h4nCtlO/:MZlFbigeGmveLgfbmmh4hlw
MD5:	4C2190F4CAD4A2C4DD718DA94B9514C4
SHA1:	3EA34FEFAC43CD799DBD9FAE3BBE8E41E76C594E
SHA-256:	0059C26BEFCBD443FCD0A2A3BE462B0E1DEC8FA89CA2B0A0643CC53A8C190FA3
SHA-512:	28359856D7E2AFDA2DC476E7A719F618EBF8446AE32E3261716B45E3C6CF1348F7F6A03D816D3D00E34B95861CC61E0A87A717C18F3B45E4B3FF3C996E0A293
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....B....671C25995607767730D65CBCEA8500D9C97FDBBAD6C5DA42D603EB474C2C7139.....'..{....O$.....w.....4'.....x.....d..... .....D.....(S.X..`h.... L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da...,....Q.@./`....module....Qc..\%....exports...Qc~. PU....document.(S.....5.a.....a.....a.....a....a.....a.....Pc.....exportsa.....I..Q..@.-....DP.....8...http://www.ichiban.menu/wp-content/cache/minify/ c7035.jsa.....D`....D`....D`.....`....&...&....&....&.(S...5'..`"N.....L`P.....Q.Rc.....J.....M...Qb.P.7....c.....QbV.....d.....Qb.M.....e....Qbz..~....f.....Qb>.}.....h... ...S...QbR9.....j.....Qbr.....k.....QbZ..g....l.....Qb..&.....n.....Qb.UN.....o.....Qb..t...p.....Qb.r'H....q.....Qbj.....r.....Qb.....s.....R....Qb.....v.....Qbz.....w.....QbRt....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e06fb361c0b40d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	102816
Entropy (8bit):	5.916246925607827
Encrypted:	false
SSDEEP:	1536:oq7alBOreIQ6I+JbwvrZEdgl7SKTmKbfHFHgBuBV23/bxVUG15cKZEl/9:vSIreyIg4rZEaumH2Bu+3kec+k9
MD5:	4C7E058E0E02835FD273ECFFB0263953
SHA1:	707907AB07D32FFC5CD9B5E8983B05AA5E2BF61A
SHA-256:	A74FED669425B4003C859679AF7B9D0F02EC5CD2CA0889F02A14D6799C7D578B
SHA-512:	428C7B431B041348DFD79DD05E8ABD70BC76F1ACB57F726CA4FFAEF49F877B391EB7FEFF07157806BBB350FFDC6CFB1DA7918C6D001576CEFD0C82950C7D9 19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...S.....C5DA1F7A90AA7902D89C292054BABC51773665111A64F74FD6FBC0D7210A463A.....'.r.....O#...@.....i..... ...h.....D.....L.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t....__gjsload__...Qb.X.g....map..(S.....`.$.....L`. ....E.Rc.....F.....Qb...p...._.....Qb2.4.....ns....Qb..._....Fia...Qbr.#.....os....Qb.j.....ps....QbJ.c.....Gia...Qb. .^....qs....Qb...-....Hia...Qb.....Iia...Qbz}i.....rs....Qb...3.. ..Jia...Qb.ZN.....Kia...Qb.....Lia...Qb&.T<....Mia...Qb.....Nia...Qb.....Oia...Qb..u.....Pia...Qb.....Qia...Qb.....ss....Qb..hP....Ria...Qb..W.....ts....Qb.n.....Sia...Qb.... ....us....Qb.w.....Tia...Qb6."....Via...Qb.o]....Wia...Qb6.Je....Xia...Qb.....Yia...Qbjo;.....Zia...Qb.....vs....Qb*.r.....ws....Qb..|f....$ia...Qb.+p.....xs....Qb.....ys....Qb.amZ. ...zs....Qb.:.....aja...Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\362e18053d8cbdb4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	145240
Entropy (8bit):	5.851719246549156
Encrypted:	false
SSDEEP:	3072:3HnHHUOZDLYSLrPXSaCcP4o5XzPKq+KatYP2R8HpwRU3xXqGXiSF:3HUMYmWohNF
MD5:	0F0470CF39863084E8AD0595352C5412
SHA1:	02A670F61F14019E165A4E39E3297BF4299B0189
SHA-256:	8E08CAE1EFE64F84692ED7F5FAEB1D0783849A6BF5DE039FD86EAE457D1B45EA
SHA-512:	96E637453DA7E15F3321904F72E66FBF6824AE5E425CBA4DDE5AB5166D5E235E1D13CFB28834BF10453E9BBA8D46EA8EE05280D0DA72CB1811458A74ADD4BE 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....:|.....16903FC3C734C924C597C57257528BB3DA5BC5DEC9AC2699C0AEF217C4E55EC7.....'.....O1....5...5.....4.....t..... .....@..... .....\.....<.....d.....p.....(S.....`,.....L`R.....L`.....Qd..b>....bap_object....Qc.h.....ajaxurl..$Qg..... .es_widget_page_notices....Qb..n.....ES....Qd.(.x....Rainmaker....(S..`P....DL`.....Qb*.....push....a.....Qd...0....gtm.start...C..Qc6.....event.....Qc.....gtm.js...Y...Qc.....g etTime..... QfF.....getElementsByTagName..Qe.....createElement.....Q.PN.....dataLayer.....Qb.....&l=.I....8Ql&.4.+...https://www.googletagmanager.com/gtm.js?id =...Qb.C.g....src...Qd...,....parentNode....Qd.....insertBefore..K`....D...@...0.....%.*..'..'....|.0...%.*..&.(...&.}..)&....&.e....&.(...&.X.../...Y....(...&.Y....&..*..&.(...&.Y....&...g. .. ..&.%.4.!....&..-.."..&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3beb4f631bd2117c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3beb4f631bd2117c_0	
Entropy (8bit):	5.897885926053165
Encrypted:	false
SSDEEP:	6:m9lPD4FEYAILvnN2aXiSUKy+siXVKDBOMHw3DK6tmT7Y7V3QJTymQ2bod7KDBOMy:II7nN1DUKs0VKDBj2gT7Y7VQlDBjy
MD5:	7D3C7CAA36A4770C0695CF30380C7BD7
SHA1:	12479A2970492B2C7A4562386F2CD25FA170BA1E
SHA-256:	441E71A047B23846AA6BE478444463C302F9ED8B7C82BC9036E084723A76707B
SHA-512:	29904B805FAC21BFABAEF58E3B2036FF4B953994342E2A659BDA05D0856579A944AFB617D6C3B26157B77C6BDC08BF94301FAAFE77B33177BFBF9A8707C21AE E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....Vq....._keyhttp://www.ichiban.menu/wp-content/cache/minify/fbbf4.js .http://ichiban.menu/h...L'/.....i..MA|.....^9.(k6.)"O?.?..H..A..Eo...../.....A. .Eo.....h...L'/..6..16903FC3C734C924C597C57257528BB3DA5BC5DEC9AC2699C0AEF217C4E55EC7..i..MA|.....^9.(k6.)"O?.?..H..A..Eo.....f_.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e81a720e5335a28_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	330888
Entropy (8bit):	6.093095395089364
Encrypted:	false
SSDEEP:	6144:HOprnCbkPZbncB7ZduJmhKCLR0BT8ohfbXTulB:uprnPZE14sjKNiv
MD5:	57C61CBF5C648278651F7BB74237B023
SHA1:	8B6D05D4DAE0DA01FA7539DA5F1D2B4EA2B1F423
SHA-256:	C2C2CAE2F073709F6BA196AC89E5A89E9CEDD063354905DD64BAD27256FC61F2
SHA-512:	F3145A3EDEB9F149A47E1634A469D7018DDB22B45498F5BCF8253E83383B070BD742B49A7C2DBDA90DB02B25C0BAB80F601959388C8440B7C6B639E9844A45F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...)L.3....5C126F5C1AA97CED4EC65B186D5F60018EBA48E319FBC252952F9D202447F7FC.....'.....Oa...0...|..b.....a..(....!.....@..... .....h.....`.....(.....X..... .h.....(.....8.....4.....(S.<..`2....L`.....(S....a.`.....).L`.....!Rc.....:.....Qb.c;&....aa....QbF.....ba....Qb6..c....ca....Qb.P.....da....Qb.=..... p.....QbN|.)....ea....Qb...p....fa....Qbf.....ha....Qb~W3.....ia....Qb...J....q.....QbF.J.....ja....Qb..X.....ka....Qb.. .....la....Qb.qC.....ma....Qb..e.....na....Qb.\.....pa....Qb..[.....qa....Qb "o.....ra....Qb.$.....sa....Qb.....ta....Qb.....ua....QbvK.m....va....Qb>.d.....wa....Qb&.....xa....Qb.....r.....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f2d48f104e12204_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.479977751220825
Encrypted:	false
SSDEEP:	6:mcVD4FEYAILG2vCXi/h6/m24LoAgPK6t:jIi2vW0b24ux
MD5:	69979ED0112F47E0ACBB83B106A7D6E3
SHA1:	8D193245CFF3B6A1EB0124840DEBD2ED3DA3805B
SHA-256:	1D07D2EA12EBD043588599AC6D4842B9409AF8831C64823F2471262CD0AEC5D6
SHA-512:	62A950FAC1E22673A7A45829520F696E49E3ACD2FF695390CBCFD95313EB8195CABF289CF9BFD3030BCE09407035C6A26C849AAB958D9B75295CB5C3C144FF8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...I....._keyhttp://www.ichiban.menu/wp-content/cache/minify/9af47.js .http://ichiban.menu/tdD.L'/.....@.....".4...{EBq.v.-.Eh.<...SE3.9B.A..Eo..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3fe29dc3ee4dedc6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	155080
Entropy (8bit):	5.88278036435692
Encrypted:	false
SSDEEP:	3072:6T93mITbTmVWJQE3RW4CF5P+QnmaKatYP2R8HpwRU3ML9WG:2baEJfhW4ImtG
MD5:	AA82DAC0025586BF127E48E302BDE1C7
SHA1:	57AA8AEAE16D181E79F439CF44208563E9587145
SHA-256:	F45DA9E777000F997092A6AE8B503B85AA1A407003488C168BAE32C55C64F8C3
SHA-512:	3EC3DBBE29079D34155E88E05E43685CFCFF260BCBDC7397754CF5DB39E3EBBD6ABB15515D1CCA115E35A4009845BE7EAD3085B56D9DE5A0A3A2AAC61CE9 837
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3fe29dc3ee4dedc6_0	
Reputation:	low
Preview:	0\r..m.....@....k.....DCDE908F43C012E4194CE988ED6E315DDD156A3AD5048CB25CED2034B3767664.....'.....O3...(\...U`.....p.....(S.....`.....L`V.....L`.....Qd...R....bap_object....Qc...B....ajaxurl..$Qg.A.....es_widget_page_notices....Qb.....ES....Qd.<.....Rainmaker....(S..`P....DL`.....Qbb..v....push....a.....Qd.~.`....gtm.start...C..Qc6J.....event.....Qc.!.'....gtm.js...Y...Qc.<`(....getTime..../. Qf..A....getElementsByTagName..Qe.....createElement.....Q.P.x.....dataLayer.....Qb.k.....&l=.I....8Ql.W}.+...https://www.googletagmanager.com/gtm.js?id=...Qbbh~^....src...Qd.n.....parentNode....Qd..}l....insertBefore..K`....D...@...0.....%.*..'..'....|.0...%.*..&.(...&.}..)&....&.e....&.(...&.X../...Y....(...&.Y....&..*..&.(...&.Y....&...g. ....&.%.4.!....&.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\49c8f33c87de4fa9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1421
Entropy (8bit):	5.531548774139003
Encrypted:	false
SSDEEP:	24:MIQ3iFde/mV2IQ3ue/mbC2IQ3pwie/meT2IQ3He/mQ2IQ39Ne/mQ2IQ3SDCe/mNJ:ML3ifV2L3uu2L3pdeT2L3HQ2L3LQ2L3d
MD5:	FA3DB6711928004DFC8507FB2D83DB27
SHA1:	43860E6B335829BE7FA76C652506A4554651C891
SHA-256:	15AB3CEE37D977D2230ACAF88BA28F05452F0DEBC39531EAEEBCF818C546B701
SHA-512:	9BDAD6F0AA01A83A2BF4CD6DF14CC2076630961B07F83DB21BE702FEA0BB11BBD9205B5079800413BCA4E5086E85168742ABDD64736F109D1AD10DF42C187C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...u....._keyhttps://www.google-analytics.com/analytics.js .http://ichiban.menu/.n..L'/.....?...s6a.....Cwa3C..A6.T...N..A..Eo.....53.....A..Eo.....0\r..m.....G...u....._keyhttps://www.google-analytics.com/analytics.js .http://ichiban.menu/....L'/.....?...s6a.....Cwa3C..A6.T...N..A..Eo.....2..o.....A..Eo.....0\r..m.....G...u....._keyhttps://www.google-analytics.com/analytics.js .http://ichiban.menu/....L'/.....0.....?...s6a.....Cwa3C..A6.T...N..A..Eo.....)....A..Eo.....0\r..m.....G...u....._keyhttps://www.google-analytics.com/analytics.js .http://ichiban.menu/.hK.L'/.....?...s6a.....Cwa3C..A6.T...N..A..Eo.....A..Eo.....0\r..m.....G...u....._keyhttps://www.google-analytics.com/analytics.js .http://ichiban.menu/.7.L'/.....U.....?...s6a.....Cwa3C..A6.T...N..A..Eo....._.....A..Eo...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\62809a1915858607_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2191
Entropy (8bit):	5.688336581902472
Encrypted:	false
SSDEEP:	48:D5rmT955rm755rmfS55rmS55rm9SN55rmQ55rmtL:G5J
MD5:	A96DAB35030BD82E71989555C50235A6
SHA1:	FC51D508BC6F21F9F8EFC30700B5A79B2946B34A
SHA-256:	BAF3FE062A98DD2354BDE03547935DE0E309D1E13B858E84323D4493749D190C
SHA-512:	A325A096C73F9B8C2F887BB7FA279B81CBD4BE68D0C27AE48DEA1FE64FAE76C239FE502286527BB7671EF9133D04A5B1820A18DF71E56D7CED83F5AFD0D2B313
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8....._keyhttps://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en_US&region=au&callback=onApiLoad .https://google.com/f...L'/.....}G..0.6|.U...;....>...T,.Rc..A..Eo.....A..Eo.....0\r..m.....8....._keyhttps://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en_US&region=au&callback=onApiLoad .https://google.com/...L'/.....Z.....}G..0.6|.U...;....>...T,.Rc..A..Eo.....$.....A..Eo.....0\r..m.....8....._keyhttps://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en_US&region=au&callback=onApiLoad .https://google.com/:...L'/.....8.....}G..0.6|.U...;....>...T,.Rc..A..Eo.....X3b.....A..Eo.....0\r..m.....8....._keyhttps://maps.googleapis.com/maps/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6cb099d4e0f055ee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6143
Entropy (8bit):	5.530682103710191
Encrypted:	false
SSDEEP:	96:7yiwPsvQG3wmwraFoJVR9hvrTkoZmhNKvx+RbQPeD4bNUfl:uiwrlmwrAoJ9hIymhNKvx+RbQW0NUw
MD5:	C2C8C6339E9F04511ED56973EB8713AA
SHA1:	7EC29D1512A20F55C3DCC696AF944D846989D8FF
SHA-256:	1AC3DBE0B09F00498221F485BB619B9780572CD2290C322D0FD5A860111DA74C
SHA-512:	B51B9EC24E990AAE45825E2684AEB1D9A1B30F1A84139D563A7678386CC8BA33EE6C87B475F4FA5E95914A43648D72EB743BC55EACD3D7EA3F6772ACF47D59B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6cb099d4e0f055ee_0	
Preview:	0\r..m.....W....d)....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/overlay.js .https://google.com/|...L'/.....?.....>.&H..F.....T.$...s..Y..Y,..r..[.A..Eo.....A..Eo.....'.i.....O.....Bs.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t.....\_\_gjsload\_\_...Qcr%T.....overlay..(S.}..`..L`L.....RcH.....Qb...p...\_.....Qb.....jt....Qb.....Jka...Qb.....kt....QbJ.].....Kka...Qb6d.....Lka...Qbno.....Pka...Qb^-.....Oka...QbRTi.....Mka...Qb..t.....Nka..QbFh83....Qka...QbFvI.....lt....Qb.....mt....QbJB.Y....nt..m$.....I`....DaV.....(S.....!.a>...K.....@.-....LP.!.....>...https://maps.google.com/maps-api-v3/api/js/45/8/overlay.js..a.....D`....D`....D`.....`B...&...&..q.&..a.&.(S.$..`....]..K`....Dc.....,Rc.....a.`.....a.....A.d.....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\779cdb7592da434b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.8521352639925315
Encrypted:	false
SSDEEP:	6:mZllXYZHfY7t/guL6Bikt/CNvnyl+1t4Z+qRK6tDx8kceXTn+326vnyl+1t4Li/:All+/ix+iktKlnykPartTcej+3jnykPd
MD5:	6DEDA4D1058330742A48DA2A7467B6F8
SHA1:	DC991943CCB67B717B53EBA8400E9B43D9CC40E4
SHA-256:	D9596837A9A26C42FA4D6E628A8EB7488301440D3714EDA031F0CDE78A5FCFC9
SHA-512:	41E737F708D8BDD2F64AD96A626F2AAF14D167933026B2CE1DEDF70A4576618038D7004197FE68B54E4613D74FB0C94A2301C12F99BAFDA7D9530D90572A0E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...H.m....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/util.js .https://google.com/X...L'/.....F.y..d..lJ....Ni.3..}-^..k.-[.y.A..Eo.....A..Eo.....X...L'/..0..A280A94EA610005A02E9627B317177629B3F95A3242CF39B051BA33C57C82812.F.y..d..lJ....Ni.3..}-^..k.-[.y.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83b514cbc0a57437_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.870015757431693
Encrypted:	false
SSDEEP:	6:mcxYZHfY7tOSuKLv64XlF6Uwf/yP4DlDK6tU37D0TtanLUPqeMUwf/yP4pl:PQ/tKzve6P8l1rqUhe6P
MD5:	28D5C75EA9A75A749380C7DAEBD101FC
SHA1:	7DAFB82CD749B7F6E7230151E39D54475C994923
SHA-256:	B33C0D15C82EC0C3D959F9E61863D4F564A483A3A2EF59D1501EAB940E45B0D6
SHA-512:	A4157D370FB872D987FB6539C1CF1BFB84233F15D301D15AC90F69B32ABA4610099909BC7426ABDBB093356F34F1B0BE1D1EDE4CFA5E301696B442429DA6971
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/common.js .https://google.com/...L'/.....g).%.8.Qt>.,g...2\..?Z...\Y..A..Eo.....9u.....A..Eo.....L'/.H...4C69F8ED662C10B8B9E5176B0EFEA22B7E451CEA5E3011185F39D573F420C2A4g).%.8.Qt>.,g...2\..?Z...\Y..A..Eo.....6..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89199a962e76065d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3080
Entropy (8bit):	5.842026986056491
Encrypted:	false
SSDEEP:	48:fVa5rEP7tVa5rQtVa5rY/7tVa5rQtVa5rL8tVa5rftVa5r/:ff9FZBNi
MD5:	271F7D480E5CA2287E2DD105B71DF029
SHA1:	127D05810C3D84CCA07100BA07EF6F2272C85654
SHA-256:	DFDFE011A79C96740D001DCBAAB840E6BABA0BC6C9BC5298CB0F5F326D4377CF
SHA-512:	EE579DFF8DC56414643AAB879901666FBDD82C55F0B6242B98E23ECB135A701F189C941FAC50FD4985FE51FB4263CA2748267717D9CD46BCF84FD15547405EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4...N..G..._keyhttps://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewportInfo?1m6&1m2&1d-37.77987813852119&2d145.15647795731974&2m2&1d-37.77199153617042&2d145.17606725993295&2u16&4sen-US&5e0&6sm%40566000000&7b0&8e0&11e289&12e2&callback=_xdc_._l28xeh&client=google-maps-embed&token=4805 .https://google.com/.>#.L'/.....g.....p.5....._...E.}.l!.~S.S...".PT.A..Eo.....7.....A..Eo.....0\r..m.....4...N..G..._keyhttps://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewportInfo?1m6&1m2&1d-37.77987813852119&2d145.156477957319742&2m2&1d-37.77199153617042&2d145.17606725993295&2u16&4sen-US&5e0&6sm%40566000000&7b0&8e0&11e289&12e2&callback=_xdc_._l28xeh&client=google-maps-embed&token=4805 .https://google.com/D...L'/.....\.....p.5....._...E.}.l!.~S.S...".PT.A..Eo.....5m.....A..Eo.....0\r..m.....4...N..G..._keyhttps://maps.googleapis.com/maps/api/js/ViewportInfoService.GetViewportInfo?1m6&1m2&1d-37.77

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8faa0d8de0d24714_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\8faa0d8de0d24714_0	
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.945460431883082
Encrypted:	false
SSDEEP:	6:melD4FEYAILe4sNwXiNv6gkl/ulRMAMsLhTkhK6tn/rfVZV8QwlRMAMsLh:LfIC4J+vhs8MSeBf/6MS
MD5:	0337E68CD92EBB2F5ACB21F98246354C
SHA1:	6B7434348A37B7E6A811E6DD5C04AFB2E6564A12
SHA-256:	6872F0C13C06EA842977510E02A2891E12A2DBBB4AE349B833616817C8A8D65D
SHA-512:	C1DFA6DC05C0AF288AC75CAA4D1DE29B9584E3D875BD9C70BF666295F82DF9B5325BADB40642180D5E1B148FFDDD5D723B85E817FD29B1C76A2EE86B23D8F09
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....%E...._keyhttp://www.ichiban.menu/wp-content/cache/minify/37e61.js .http://ichiban.menu/!...L'/.....B.....L..@....(..b....@=.._..W>%....A..Eo.....A..Eo.....!...L'/.]..DCDE908F43C012E4194CE988ED6E315DDD156A3AD5048CB25CED2034B3767664.L..@....(..b....@=.._..W>%....A..Eo.....5hL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\93f52fb938ee1996_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.517631285851526
Encrypted:	false
SSDEEP:	6:mDD4FEYAILRiCXiDs6NF2pdy4lxhZK6t:wIcWdAF2TpXT
MD5:	AC277ED29775006BDE1706C6CC19B106
SHA1:	8DA270E567E95C6D97CCA34D1722D7A3C0BE0012
SHA-256:	1897DA128B038564D5184A89F496C5F5F83F2AA8BF43BA1F50BBF5FCD2BF0CD7
SHA-512:	6ADF234CC877041BE680366ECB72C318DD9EB1EF1ACEDA618CE589139D222DDA0F2D55F0DDE93957915F43BE0B05BB8FF85C83F19BE6AC2D4FCF8959F1D274C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...\.%...._keyhttp://www.ichiban.menu/wp-content/cache/minify/853a9.js .http://ichiban.menu/.@..L'/.....q.....nG.*...d^.....(.o....)...X1...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\997643720c860f01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4027
Entropy (8bit):	5.784502049724419
Encrypted:	false
SSDEEP:	48:PWH+yUZ9QIsUD0Zkm5xEe9lwbocTjyj6yvf+bmDgVeGe7CqFz5EoQUg:OaAIDs1bwbocTu1HBUk1CqFz5bg
MD5:	B39D7F4AC9A2A85479E79F73AB1057DB
SHA1:	D28D4B08C130560D3B8935BD03E25C4544031555
SHA-256:	86056F0AAA7E84FDE1A185DD04BC7375C1555CE6C5C568BCCD764ABB393C07D8
SHA-512:	32A939FDA40CABE29AC50BDD5B3057ADE860AB147F559A243C8C7CE1872536CB086749DCBFD9AF11EC75E6443DC7A6859C0AB49241D5A1C13478E485C3346A8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/search_impl.js .https://google.com/^=#.L'/.....F.....i.w.]..A0..bE.1u...+S.X..d..|..A..Eo.....A..Eo.....^=#.L'/.....'.....O....P...G_9.....|.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t...__gjsload__...Qd.....search_impl..(S.-..`.....xL`8.....Rc<.....Qb...p...._.....QbVc.....Dcb...Qb~).'....Fcb...Qb..q.....Gcb...QbN.....Hcb...Qb.P&.....X$....Qb.i.?....Icb...Qb..7.....Lcb...Qb.m.....Jcb...Qb.....Kcb...QbN.a.....Ecb.j$.....I`....Da^.....(S.....aC...U.....@.-....PP.1.....B...https://maps.googleapis.com/maps-api-v3/api/js/45/8/search_impl.js..a.....D`....D`"...D`....\...`*...&...&....&..q.&.(S.....1.ab.....Q.d.....&.(S.....q.a.....d.....&.(S.....a.....d.....&.(S.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9a6c0cc2dc7afa9b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	130800
Entropy (8bit):	5.687134933748195
Encrypted:	false
SSDEEP:	3072:MMkjTS3CrlMGENx2YubZE7pLFp5oWAb0QtKUliEgCPvdq0Vlh7tB+YpisgBosj8d:GMNxr7pLFp5oWAb0QtKUliEgCPlH7tBR
MD5:	03B61A1882FDD072DA302590B96787CB
SHA1:	3281266197DB373119188FF3B78962E7A378E3F1
SHA-256:	F2CEFBB7EA3A63708068934A8A921CDC1AD5D1B54DD39EF1A79FEFD9D21E1A68

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9a6c0cc2dc7afa9b_0	
SHA-512:	AE07A4DDFDEFF88625164DEB68902C7C76331E08499BFC055A7AB6B29338EA88821A61533640417B604AF81B71D892AB3FD52695074288B1D5FA8394326F5D4B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....j0....4C69F8ED662C10B8B9E5176B0EFEA22B7E451CEA5E3011185F39D573F420C2A4.....'..Z....O(.....c).!.....I.....,.....x.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t....__gjsload__...Qc.k(.....common...(S....I.`|.....L`.....a.Rc.....N.....Qb...p...._....Qb>.....ofa...Qb.?.....nfa...QbR.A.....pfa...Qb.@.....rfa...Qb.BK.....Mk....Qb.I.....Ok....Qb.x=.....vfa...QbF.....wfa...Qb..v.....Tk....Qb.....xfa...Qb...z....yfa...Qb..7.....Afa...Qb.D.n....pl....Qbfgk7....Kfa...Qb.....Mfa...Qb."....Nfa...Qbr.v(....Ofa...Qb.s.....Pfa...Qb.U.....Rfa...Qb.C.F....qfa...Qb>.....Sfa...Qb..~....Ml....Qb.u....Ql....Qb...r....Vfa...Qb.....Yfa...Qb.e.....Xfa...Qb..F....$fa...Qb.n.....cm....Qbr.....cga...Qb.<.....ega...Qb^.....mm....Qbz.k.....fga...Qb...J....gga...Qb.r0}....tm....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4927b8e8b6e8e49_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	36221
Entropy (8bit):	5.624850224274241
Encrypted:	false
SSDEEP:	768:fJfGOYK4pni/dOdA2x5cdQJsZF4JxjUJ5:hfMBn7Z5cdAOFYjUv
MD5:	38ED791E7BB87FD26F094296CCC9F0CF
SHA1:	D71DC2A544EEBF7F40363C937556EECADD183E1E
SHA-256:	2B6DB9CA4B5E7D6C84ACE63AF2888E69DD8D263169922F2E9B3FFC6C08EACDC4
SHA-512:	85E506A849FC5299C8E8691089D33CEAEC7D2EDADCA57FB65B2BE6ED9FDAB611AA01D9FCFCED0540708E84CFC62C5293E3E4EC98A1EF443C354FA54BB0690903
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....}....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/onion.js .https://google.com/.t..L'/.....i.....DV.Fv(|.pJ.....3,..X$4..&Q.wC..A..Eo.....A..Eo.....'..c....O.....:+r.....H.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t....__gjsload__...Qc.....onion....(S.%..`.....!.L`.....1.Rc.....Qb...p...._....Qb..!.....RG....Qb.g. ....EBa...Qb.h.....FBa...Qb.....TG....Qbn..Z....GBa...Qb...H....HBa...Qb...P....eH....Qb..d...fH....Qb..g.....gH....Qb2@.4....IBa...QbB).....hH....Qb..4.....JBa...QbF.Z.....KBa...Qb..V.....LBa...Qb.....MBa...Qb..^.....NBa...Qb...N....OBa...Qb~.....QBa...Qb.....RBa...Qbv.W.....UBa...QbZ.....jH....Qb:.~....WBa...Qb.y6.....YBa...Qbz.V.....aCa...Qb>.....XBa...Qb..u.....ZBa...Qb2..P....bCa...Qb.<.-....$Ba...Qb.....cCa...Qb.....kH....Qb.U.....mH....Qb.n.....nH....Qb.m

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\acfe1214994be3e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1484
Entropy (8bit):	5.700818666952989
Encrypted:	false
SSDEEP:	24:YwEIa3HtSwrH3HXSwf/S3HgrSwY3HxSwC83HmjSwD/U3HXSww3HX:LEIa91jn13Swr1YB1C8Wj17Un1wn
MD5:	39A99C7D66A13603B4823C1A71231BCE
SHA1:	8DA56D34A2C0CFD389CD213274B9FDFBB778F5B3
SHA-256:	1673004F1671C26087DD6881FA04736E9B38B28C3AD6DBAAD6FE3D692F9F472D
SHA-512:	A64092C7B59AB1F4068184B003A462C8FC11A42898B9CE816FF0A3D54364C4A3839935554D43DD6A985B2BB018305DB30A0932713C0A407272BC522C37D00030
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....v....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-M4B3WHH .http://ichiban.menu/gk..L'/.....?#M.-....:..k,..l.%..o.>&.....k.A..Eo.....y.....A..Eo.....0\r..m.....P....v....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-M4B3WHH .http://ichiban.menu/....L'/.....?#M.-....:..k,..l.%..o.>&.....k.A..Eo.....T.....A..Eo.....0\r..m.....P....v....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-M4B3WHH .http://ichiban.menu/....L'/.....?#M.-....:..k,..l.%..o.>&.....k.A..Eo.....!i.....A..Eo.....0\r..m.....P....v....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-M4B3WHH .http://ichiban.menu/..I.L'/.....`.....?#M.-....:..k,..l.%..o.>&.....k.A..Eo.....stI.....A..Eo.....0\r..m.....P....v....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-M4B3WHH .http://ichiban.menu/..3.L'/.....T.....?#M.-....:..k,..l.%.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c82a6d17667a3b4e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.518019773866926
Encrypted:	false
SSDEEP:	3:m+ltt1A8RzYK6oKfKLBsDmXniR73lHCvnCkiIsVxYkH5m3FQlpK5kt:mGnYKxKfaBFXiavCkrsVxJH43FKK6t
MD5:	C2AEFE7D0DA3E1E844F2BA38870F5B22
SHA1:	5712F74031BE23B5A8279EDF6457BAB0004D1B21
SHA-256:	0B780455EDE36C6BD1F7129211D7A2BF9D879EEE530640F01142BB567F030863
SHA-512:	42A1AD691CF6CA0918696557E34F288B944655B8109957B8240D5D697B1FAC5B664561B2C43E731A1988F22D5F4012930395AA4641FA0C4CB63365A7A89704F0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c82a6d17667a3b4e_0	
Preview:	0\r..m.....E....I....._keyhttps://booking-widget.quandoo.com/index.js .http://ichiban.menu/B...L'/.....|.....;(\<`..|..l.....<V.....A..Eo.....] .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dbf0ad74f36c4d17_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98048
Entropy (8bit):	5.806847685174559
Encrypted:	false
SSDEEP:	1536:CY0hqOo71nTTW11VNXi34LDBvGjiTu8ozYpk30+K3:WM7xzQPa2eE+K3
MD5:	9F94AD91EC5CE991F6BC7B08652BB95B
SHA1:	5EA780E02CC03F6C290B998A568E813AB3382B88
SHA-256:	33D7D08014D42AFD6227C6037CBCB81EF122D905489FCD05CC158D82426C64B9
SHA-512:	F31511EF3A8B20D306DB8FFB50127FA571EB0E9F889610D64F9CE556A14D010C808B67EF7981DBA0A83BEFB9A20A01811B0A4E74C660D6E987609A7BD7B89F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....>*K....013793D1F1FE6AAC21BE7247376C5796657B46E656CE6CCD58B17A4E2B973FE0.....'..m....O#....}....2.....<$.....L.....l.....(S.4..`$.....L`.....(S...=$.`0H.....L`.....Rc.....8.....Qb.;.....t.....Qb..e.....e.....Qb.-Y....._.....Qb.....H.....Qb....B.....Qb.....et.....R...QbV.....ut....Qb.k.....at....Qbb.....ft....Qb..<.....lt....Qb.G.s....Lt....Qb&.J.....At....QbN.....Ot....Qb..ar....Mt....Qb.u+....._t....Qb.....Qt....QbVt.H....Gt....Qb..IT....Yt....Qb.j.....Zt....Qb.....en....Qb..G.....tn....Qb^X'.....nn....Qb.....fn....Qb^.x....kn....Qb..1.....Ln....Qb...W....An....Qb.p.....On....Qbn.....Fn....Qbz.....In....Qb..>6....$n....QbB.....Jn....Qb".4.....Kn....Qbb.....Qn....Qb2.+.....Yn....Qb..U.....Zn....Qb^.5.....tr....QbJ..e....n.....Qb.....r.....S...Qbzp.9....o.....R.....M...Qb.l.7....f...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e0c377885a89094b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.819969480998976
Encrypted:	false
SSDEEP:	6:m4eXD4FEYAILNXijC+YOitdzzlz6gK4kZK6tpREVl0dwt9oIvnRUAzzlz6gK4eL:4llVfzzlm3ZldwHNnqAzzlmvL
MD5:	740472C09A2658416CC916E53B223A5E
SHA1:	FC7BB9C9443CB4D59ED7E04A87A6FEF877F89397
SHA-256:	0068A4E4A3D3BFA757F6D7C22FA8AD6001A70F23FC33A69C852CD533E6C171A5
SHA-512:	D778F6ED0F6F53B4412FE70AC5391968418A74E2CAD4A74D4627E691C83832A568D0DBE83A08A8A9FF69CC54B0BD6B2415DBCD08D5C758263C12B336AC64CC8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...-k...._keyhttp://www.ichiban.menu/wp-content/cache/minify/c7035.js .http://ichiban.menu/0K..L'/.....\....'@26".....g..b.N.../...A..Eo.....t..k.....A..Eo.....0K..L'/.....671C25995607767730D65CBCEA8500D9C97FDBBAD6C5DA42D603EB474C2C7139.\....'@26".....g..b.N.../...A..Eo.....{RB~L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7745fb0fb323f3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.925873342688047
Encrypted:	false
SSDEEP:	6:mau/PYzdv3IeDugQO61/ES/HhIh/hK6tiTm1GxTcCK7fES/Hhr7l:5tf6ztn/mTam4oV/N7
MD5:	DE03635CCF3D8837DF6495E39F01B7D9
SHA1:	5CE28DD6C50D1DCC61ACA7FD7B5703D151A828E8
SHA-256:	599B0D9DB77307C06991A736027F4CBD9F5720B60FFED6192F8CF9EAC2A598EC
SHA-512:	01271E48E2BFC36505E043C3F51208F6E05DCF5534497A9FFDC8BFEB31F7D75EB11596814E5458F0A74F9E7936BB74056E9A7659B3FF5E9E362256C6B9F20271
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.../.6...._keyhttps://maps.gstatic.com/maps-api-v3/embed/js/45/8/init_embed.js .https://google.com/c...L'/.....`.Fq..iY.)A.n....{(Z....>.W.....A..Eo.....Th.....A..Eo.....c...L'/.....5C126F5C1AA97CED4EC65B186D5F60018EBA48E319FBC252952F9D202447F7FC`.Fq..iY.)A.n....{(Z....>.W.....A..Eo.....j...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed62acd94547fee5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274728
Entropy (8bit):	5.874760394982651
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed62acd94547fee5_0	
SSDEEP:	3072:v4Hi6WcoCI6UMmTRmPtQ9JGogJGo/CG4ba5ZW7tvci0nu7SlKfT:vX9coCI1MmYa+wSCGn5g7th0n/lKr
MD5:	9AEF2A77C7E8D79A0D9B7F559E0DA632
SHA1:	27AF64DD21C078788A1C095B13B6ED76B95C1559
SHA-256:	1994E121AC3EEF3909E30E1E707E73C7A5147D1B1DA252BCD5E82DDFE404CE0A
SHA-512:	04C7D740821EF4CE1C8490D3E83DCD464AD19BEAB77FC1786B8C80D0935076F44502AEF96954F829A0E98729E2833C63A68ADC09367B3723164C8E17C6B34E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....A280A94EA610005A02E9627B317177629B3F95A3242CF39B051BA33C57C82812.....'.P.....OR..../.....~.....o.....|.....0.....<.....0.....D...4...$.....$... .....$...D...$...t... ....0... ....<... ....(...8.....<.....x.....(S.H..`H.....L`.....Q.@...4....google....QbB..k....maps..Qd*.t....__gjsload__...Qb.7.d....util.(S....o.`.....L`v.....}.Rc.....Qb...p...._.....Qb.....Rka...QbF.}.....Tka...Qb..L.....Uka...Qb.akX....Vka....R...Qb.M.)....$ka...QbFC.....ala...Qb..7v....cla...QbvB=.....dla...Qb..Y.....At....Qb.b.....Bt....Qb...q....sla...Qb:U.....Gt. ...Qb.6.%....yla...Qb.C.C....zla...Qb.S.....It....Qb.....Ala...Qb...t....Jt....Qb.(.,....Kt....Qb2le.....Lt....Qb..b.....Dla...Qb..xR....Cla...Qb~.....Mt....Qb..(.....Fla...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\edcb47dfafe4384e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.627509783793103
Encrypted:	false
SSDEEP:	3:m+llIplta8RzYK6oKfKWLV9WXEYvDmXniRVFelHCSK/lwhvfmpiD+l/Zme/tlpK+:miI5XYKxKfNLXQETXi91ecp2de/ZK6t
MD5:	4936499A0EE4A08651CD6286DDD8153F
SHA1:	338E0F5E6781CC378F934D5BB4ACBC0FEDFD6157
SHA-256:	4C369ED590280B3B46FC887F73062819982DBF01C0BF4A07653AD276E674180A
SHA-512:	F9B578B59271A85D2729B377AE4AC6201B0A4D869F412EF5C56EB341361C73076574478D9B9A7D7B58A655CF001891B10BFD9914EB4D519C116144FF18881B80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....._keyhttps://booking-widget.quandoo.com/3.0.1620734422/bootstrap.js .http://ichiban.menu/.*..L'/.....}...../W...%..C.KQ.Hy....T.U...6.A..Eo.....{ =a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ee81135c03c7b5b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3357
Entropy (8bit):	6.0829279271701795
Encrypted:	false
SSDEEP:	48:yCWcVAl+fvK9qcHozqITNPRwYx7OM2cpmfOViUsiP+Qr9+LTo5:ywAMfKqcozq6PmYNOMwfch+i
MD5:	74677C065BA90D4964D92A22A178DC0F
SHA1:	6190182449A5217436BC55690EF2B075EF103714
SHA-256:	4998742EAEC14D09E8A145A140FA65C755A7D899220D80DFB4E029B7D96929A9
SHA-512:	9FB51B936EDB8EAF47AD866BD259BD55803637BD605A01602B7DCD5D5975332544A690DCDCE33111C1F0DCA22A68F40C717485F9CBA36F95E10B9EECE90888A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u...c.>}...._keyhttps://s3-eu-west-1.amazonaws.com/quandoo-website/widget-builder/quandoo-widget-builder.js .http://ichiban.menu/....L'/..... .Y.p...#a... ,y8.+.....M.n.8...A..Eo.....(,.....A..Eo.....L'/.....'..X....O....._.....t.....(S.4..`$.....L`.....(S.i..`.....L`F....xRc8.....Qb..?....w.....Q.@ ..6.....jQuery....Qe.....segmentAPIKey.....QdZ.-.....scriptHost....Qc.lq....images....Qc..CC....loadCss...QdB..n....deferQuandoo..Qd...=....loadWidget... Qf..b.....getD ataFromClasses....Qb.W.e....maini$.....I`....Da.....(S...`.....HL` ....4Rc.....Qc.....onLoad..`.....Qdr.$.....loadScript..`....Da.....A...QcF. dU....document..Qe.....createElement....9...Qd.^.....setAttribute.....Q.`..(6....text/javascript...Qb.C.g....src...Qd&:.4....readyState...(S.....5.a.....Qd..e.....script_tag..... a..... Qf.. .....onread

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f8a71b102e62ffe6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.81701148591848
Encrypted:	false
SSDEEP:	6:msTYZHfY7t+uN6ZGwSIxg/4UhL4lbK6t/bqkgmjCuglR3AMIxg/4UhK:Bq/ukGogz1oNZpjy2gz
MD5:	BB6184CAB4B8DD231737092844840CCB
SHA1:	B09C56E68AB51ADFD7DAAD9346A7132179001805
SHA-256:	147E44F39F12C63F7E9CE512525D8657481A27CC1611DF868B685576C8FC3F88
SHA-512:	D2A0675EBD18933A0D96B402785B51CB9AAA24031F0402F476EF3ED8A3947334362D6E2C569A001AE730CC1BDC8ADF83742A4396E2631EF481D73F8F1E92A89
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f8a71b102e62ffe6_0	
Reputation:	low
Preview:	0\r..m.....S.....y...._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/map.js .https://google.com/.}..L'/.....<..... Ir.v)...u.~.j.E)aR..6...K4.c..A..Eo.....N1)..... .A..Eo.....}..L'/.....C5DA1F7A90AA7902D89C292054BABC51773665111A64F74FD6FBC0D7210A463A. Ir.v)...u.~.j.E)aR..6...K4.c..A..Eo.....4..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9a9992f840ec712_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.9354434016834405
Encrypted:	false
SSDEEP:	6:mb/VYSHT8NWQA2A2XiIs15qbwnK6t2aTkGPZkqheXAINb5:Wz8NWQduPlpqGqqAv
MD5:	DA78334F6D4C7484CF9C28AF3DB4D934
SHA1:	DBF364F0554E87B3643E95977E319DB3B92F1EEC
SHA-256:	A888FA12C924CBC3319E466C5486995EB222302BEA83EB4F0C30BBE719A2BA61
SHA-512:	17ADF112046970AE86D519D23C176EF044EE4BEBB2DB02E3A642DF7F00BC3DF945293DE91CF7DC54F8A1705969CB4F98FCA03FF276179D8C105C11535CE593C F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....p]...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js .http://ichiban.menu/...L'/.....3[9!|P"Q...-..*j..-'...r.h...n..A..Eo....._0.....A..E o.....L'/.X~..013793D1F1FE6AAC21BE7247376C5796657B46E656CE6CCD58B17A4E2B973FE0.3[9!|P"Q...-..*j..-'...r.h...n..A..Eo.....\(IL.....

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):	1.195832753957213
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U12JPdCOxZLLOpEO5J/Kn7Uo1L26hpLLOpEO5J/Kn7Us1tu8q:dNwEhDNwMxrNwgTfPsZ
MD5:	970BC4E38F00462AC5CEC391326F3AC7
SHA1:	4DC0C3B19CA63B4AEC2B59D71F9574F39F19F302
SHA-256:	936316FCBC9F69444634711ABE0BD2A01EDAF4873EFA6FC0989709280E9C4002
SHA-512:	0950CC3A6217E57E66292ABB2E602422C8E1E8987920A49881459A7581AF91969D56CD55533C93313D83C68FED80C7DC3EE9927C5B88A4664D33749C742BEE79
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
File Type:	data
Category:	dropped
Size (bytes):	38508
Entropy (8bit):	1.0995332098971424
Encrypted:	false
SSDEEP:	48:t8NOZHpq5LLOpEO5J/Kn7U/gCOs/JPyqekLLOpEO5J/Kn7Ur51LtX6tWqZLLOpEL:aOHpcNwv/hyMNwpxoW8Nwm
MD5:	3389ABC826B88F736AF43FAE729B6CD1
SHA1:	B7C7877227B426FD565C4F37F6ED2BB70D740B0B
SHA-256:	FEF9B0E76BDAE9C78BFFE9E2705B06A9674B4AB32A2EDDAE27EFF373B4599998
SHA-512:	7D8B874455A805FF9C497124B41B0AE404A885B311FA633E3FA438F54B46E3A8B41DDA6D39AE4B1E9C0F01BFC1EA05ED9F07254ADCD0030116E6131ECFAA95F B
Malicious:	false
Reputation:	low
Preview:	.....*..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Category:	dropped
Size (bytes):	39693
Entropy (8bit):	3.1161771455889373
Encrypted:	false
SSDEEP:	384:sQ9JbQFbLypHdrigVwYeLAhgOd4gOz4zA4cq:sApSCbtVwSa67cX2
MD5:	B818151E3B3FFB1099F9EC98A05A7A5C
SHA1:	FF8482B7017672AF05944BF2CC07E59FCFF41325
SHA-256:	8707CD646DC9E7F663E155CBD9E1683332859941F12A8599C23FCFC9DB002AA3
SHA-512:	B8C7A00B90212671B036847379762642A1B731941277FCC383AAB5123EDECE363BFEBFBCF7DAAAAC631235959A8FA3E9D040C5C361BC40D019B1B93C1162A48
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...bcfb9cc0_596e_4ef4_a9af_5448c29d755a.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....5..0.....(...http://www.ichiban.menu/menu-teppanyaki/:...T.e.p.p.a.n.y.a.k.i. .b.y. .I.c.h.i.b.a.n. .J.a.p.a.n.e.s.e. .R.e.s.t.a.u.r.a.n.t. .|. .D.o.n.c.a.s.t.e.r. .E.a.s.t.....h.....`.....`.....d.....d....`.....x.....X...(...h.t.t.p.:././.w.w.w...i.c.h.i.b.a.n...m.e.n.u./.m.e.n.u.-.t.e.p.p.a.n.y.a.k.i./.....P.....H.....h.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....

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
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
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):	320
Entropy (8bit):	5.1874673704249705
Encrypted:	false
SSDEEP:	6:m+Nyq2PWXp+N23iKKdK8aPrqIFUtpjX1ZmwPjMRkwOWXp+N23iKKdK8amLJ:zNyva5KkL3FUtpjl/PjMR5f5KkQJ
MD5:	F4001BCD3E48E6FC497968D7004FAC45
SHA1:	E74A93DFF545F55731DFA46C0A506682E6C864B9
SHA-256:	94B2E21421406AE79A28738418ED3A7516733C40207667D910ADF3F61CD3315C
SHA-512:	AE57551E90D798F06B64E54D8AC036A6A2568D53CCDF8C558BFEC15D77B0AEA2FE79EC92F351BD4739FEA0D362F572F53F48CAB1D6C757E6FC8F6B04CD2AC21
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Reputation:	low
Preview:	2021/08/04-00:15:29.658 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:15:29.661 1010 Recovering log #3.2021/08/04-00:15:29.662 1010 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 Rules\LOG.oldF (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.1874673704249705
Encrypted:	false
SSDEEP:	6:m+Nyq2PWXp+N23iKKdK8aPrqIFUtpjX1ZmwPjMRkwOWXp+N23iKKdK8amLJ:zNyva5KkL3FUtpjl/PjMR5f5KkQJ
MD5:	F4001BCD3E48E6FC497968D7004FAC45
SHA1:	E74A93DFF545F55731DFA46C0A506682E6C864B9
SHA-256:	94B2E21421406AE79A28738418ED3A7516733C40207667D910ADF3F61CD3315C
SHA-512:	AE57551E90D798F06B64E54D8AC036A6A2568D53CCDF8C558BFEC15D77B0AEA2FE79EC92F351BD4739FEA0D362F572F53F48CAB1D6C757E6FC8F6B04CD2AC21
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.658 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:15:29.661 1010 Recovering log #3.2021/08/04-00:15:29.662 1010 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	5.16753318022203
Encrypted:	false
SSDEEP:	6:mu08q2PWXp+N23iKKdK8NIFUtpOAhZmwPaNyzkwOWXp+N23iKKdK8+eLJ:f08va5KkpFUtpB/PLz5f5KkqJ
MD5:	CE26011036A6510CCA2E9A2B7874D61C
SHA1:	23F7DD84EB645FBD99F7E95B983490D94A9C34E4
SHA-256:	707B53518D66A87FE6B15BF3DD56F7354D190A54E586583AAD772112DB03A9F4
SHA-512:	12EDC4885E6C2EFEA76BBED6EABF400DACDC323A94DD7BC2FC66F921E92EECDA54495D450ACB26AD6C7824A4B3AA11E7BCBD360981B0C651BDD81E43E55A17DE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:32.308 1170 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:15:32.310 1170 Recovering log #3.2021/08/04-00:15:32.314 1170 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\Extension State\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.16753318022203
Encrypted:	false
SSDEEP:	6:mu08q2PWXp+N23iKKdK8NIFUtpOAhZmwPaNyzkwOWXp+N23iKKdK8+eLJ:f08va5KkpFUtpB/PLz5f5KkqJ
MD5:	CE26011036A6510CCA2E9A2B7874D61C
SHA1:	23F7DD84EB645FBD99F7E95B983490D94A9C34E4
SHA-256:	707B53518D66A87FE6B15BF3DD56F7354D190A54E586583AAD772112DB03A9F4
SHA-512:	12EDC4885E6C2EFEA76BBED6EABF400DACDC323A94DD7BC2FC66F921E92EECDA54495D450ACB26AD6C7824A4B3AA11E7BCBD360981B0C651BDD81E43E55A17DE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:32.308 1170 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:15:32.310 1170 Recovering log #3.2021/08/04-00:15:32.314 1170 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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	1.4652289349035788
Encrypted:	false
SSDEEP:	192:mm+Uq88dIYAg/ZRKTD7sVfWV8VJqJYVJqbYB:1+UAuqhRWvsJWV8zqJYzqbYB
MD5:	3A1248771992038DD309B7B3D9196431
SHA1:	3D66664CC7BD7193DEA7EB11D71A3BBFD90E8C6B
SHA-256:	2984C36DE5EB7AC1284DDEB72BD34284CC984930803100E583CA6F3FAD9DED09
SHA-512:	27F5E6F23EE7D00016E4F55AAAAA663ED8097479052744A0DBD3DAC59094A2E6D02A4C755BBEA4706A88203E1C5B4CC1F67CF6FBC780553A7EB95F4EB558D3D3
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):	43740
Entropy (8bit):	0.6434789676502546
Encrypted:	false
SSDEEP:	24:E/OUZRyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwKKyLyt3hzby+ub6YFhBKVz0YzC:odBmw6fUcV3hzG+u5gVAY5nfBofJc8
MD5:	D61257193751375F34376B6C1C8648E8
SHA1:	983273B55F4A7812354A2B9E2FE11DCECEC0AF56
SHA-256:	9103356F15828B94A0302F0DA5DEF8F08121BF8308FC4F6C908812D0AB3E9568
SHA-512:	758C04BC220BC74C76EA720E1D3AD4959BB63916858EFCE9B052F05174DB0EBCF3CCAA886D8A88699FE6FF856AC0CD02BA12A04125990849D600F4D1B74F183C
Malicious:	false
Reputation:	low
Preview:	.....*.`..... ....

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):	372
Entropy (8bit):	5.221741913853241
Encrypted:	false
SSDEEP:	6:m4A/qM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtplnZZmwPlRMMVkwOWXp+N23iKKN:c3+va5KkTXfchI3FUtpZZ/PvNV5f5KkI
MD5:	4E58E55D528408F5F0A998E62510D358
SHA1:	549D64B94B4AD773DB85C15AC79578BF4964A8F1
SHA-256:	4837965EA04FA0BEF303B46D5FD182285E8F590674BC808C7AA73378A0862BE9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
SHA-512:	897525983138CDFA62878122F3EB9F7785FB5F0C124B17EE24265B707D0EEC92CE452E52EC9A61B62FBD22B9AFAF454829C3077337580735951B9044C17282E7
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.820 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:15:40.821 1b1c Recovering log #3.2021/08/04-00:15:40.823 1b1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.221741913853241
Encrypted:	false
SSDEEP:	6:m4A/qM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtplnZZmwPlRMMVkwOWXp+N23iKKN:c3+va5KkTXfchI3FUtpZZ/PvNV5f5KkI
MD5:	4E58E55D528408F5F0A998E62510D358
SHA1:	549D64B94B4AD773DB85C15AC79578BF4964A8F1
SHA-256:	4837965EA04FA0BEF303B46D5FD182285E8F590674BC808C7AA73378A0862BE9
SHA-512:	897525983138CDFA62878122F3EB9F7785FB5F0C124B17EE24265B707D0EEC92CE452E52EC9A61B62FBD22B9AFAF454829C3077337580735951B9044C17282E7
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.820 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:15:40.821 1b1c Recovering log #3.2021/08/04-00:15:40.823 1b1c 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):	358
Entropy (8bit):	5.202112573587329
Encrypted:	false
SSDEEP:	6:m4gRoqM+q2PWXp+N23iKKdK25+XuoIFUtplgBZmwPlgTfMVkwOWXp+N23iKKdK28:z+va5KkTXYFUtpl/PgkV5f5KkTXHJ
MD5:	C92B1CBC8069CB4A55A3696DF7C5D68B
SHA1:	CF33D0ED098380C783623E2A34AAD7FFF19A49F2
SHA-256:	D0767FFECBA39FEE2DA4A500328B08B6B3A66AACD270E853B21753A63DD5850F
SHA-512:	1E953F7074FE028CFF7987D9EA13AE414DF70ED41FA1E007F607FD4253515EAA2BCAD64C637B2F11F5180120A34835E13E22EA196906CCDF31434BED9CB95B4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.814 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:15:40.815 1b1c Recovering log #3.2021/08/04-00:15:40.816 1b1c 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.202112573587329
Encrypted:	false
SSDEEP:	6:m4gRoqM+q2PWXp+N23iKKdK25+XuoIFUtplgBZmwPlgTfMVkwOWXp+N23iKKdK28:z+va5KkTXYFUtpl/PgkV5f5KkTXHJ
MD5:	C92B1CBC8069CB4A55A3696DF7C5D68B
SHA1:	CF33D0ED098380C783623E2A34AAD7FFF19A49F2
SHA-256:	D0767FFECBA39FEE2DA4A500328B08B6B3A66AACD270E853B21753A63DD5850F
SHA-512:	1E953F7074FE028CFF7987D9EA13AE414DF70ED41FA1E007F607FD4253515EAA2BCAD64C637B2F11F5180120A34835E13E22EA196906CCDF31434BED9CB95B4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.814 1b1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:15:40.815 1b1c Recovering log #3.2021/08/04-00:15:40.816 1b1c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.21175770225398
Encrypted:	false
SSDEEP:	6:m4oq2PWXp+N23iKKdKWT5g1IdqIFUtploU9ZmwPlCUERFkwOWXp+N23iKKdKWT5i:Ova5Kkg5gSRFUtph/PU75f5Kkg5gS3SJ
MD5:	0585438E80A367075E67842C4B856BF8
SHA1:	54C3DEB2B2D8CBA001E158F35517F2412EC888C4
SHA-256:	3478F3E6E0E6FE327794A1CB62DCAEC20A0E3AACDA0DDFC5EAD1EC1D9D98D5A8
SHA-512:	71A54D7C0CBDAA4AF02E7EB91C20B5093FDEAD1D129BC65B316F72E3BEA10EA392978B61542C281E638BAF54461A4B9F5365CADE6414E054462AD121F880101 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.680 1214 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /04-00:15:40.682 1214 Recovering log #3.2021/08/04-00:15:40.683 1214 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old= (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.21175770225398
Encrypted:	false
SSDEEP:	6:m4oq2PWXp+N23iKKdKWT5g1IdqIFUtploU9ZmwPlCUERFkwOWXp+N23iKKdKWT5i:Ova5Kkg5gSRFUtph/PU75f5Kkg5gS3SJ
MD5:	0585438E80A367075E67842C4B856BF8
SHA1:	54C3DEB2B2D8CBA001E158F35517F2412EC888C4
SHA-256:	3478F3E6E0E6FE327794A1CB62DCAEC20A0E3AACDA0DDFC5EAD1EC1D9D98D5A8
SHA-512:	71A54D7C0CBDAA4AF02E7EB91C20B5093FDEAD1D129BC65B316F72E3BEA10EA392978B61542C281E638BAF54461A4B9F5365CADE6414E054462AD121F880101 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:40.680 1214 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /04-00:15:40.682 1214 Recovering log #3.2021/08/04-00:15:40.683 1214 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\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):	155648
Entropy (8bit):	0.394865471597977
Encrypted:	false
SSDEEP:	96:Wmo2UcO/DqUgFjwxe4CdUlnwxH4x8lUn2:Wmo2UZ/DqUgZwc4CdUlnw94x8lUn2
MD5:	9E5E58B3A8A8C2F9BCEE3FF33AD016F6
SHA1:	D8A7A7230492FFE1317527E283125962CC4CF1C7
SHA-256:	449A129C032CDC0D23C34E519F2B47CE999FB3316B13CC6BF2E25A63E5586611
SHA-512:	BB62A3A42D49E4E652B901C16CD7C71FBC9286CF63F6EFDD593B2D3DA8E8725E946D5086ED6BB400775384BA99525A4984CDA9291D100D50C715A607ED2A60 9
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):	691
Entropy (8bit):	5.2596866068102734
Encrypted:	false
SSDEEP:	12:ToW1Q/0XhSDfVIvruPjqJCSwVTG7W3XDs13uGfvYMBk778B/xgskZBa9sdukWk3/:TouQcxSDk6LZhVqWXDs13u+Q2Y78BJg3
MD5:	83E1ABF41C413310F0A9DB562D1F710C
SHA1:	813CB712EA283C1E2CADAB9DB9183DF0C66E10F3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
SHA-256:	38D574C28EF494A75F781CC0C680270D2A280D18EDFEC905BDD0B5D9B91A231B
SHA-512:	30BA8D04AB8FB617D3435C6FF7A33EBBB7B04515141E2C7D092245696C75DABE59F3626A8AC22333378960321576EB8907BFAF29267D579874F9C701DDF9CB88
Malicious:	false
Reputation:	low
Preview:	....."S....by..doncaster..east..http..ichiban..japanese..menu..restaurant..teppanyaki..www*{.....by.....doncaster.....east.....http.....ichiban.....japanese.....menu. .....restaurant.....teppanyaki.....www..2.....a.....b.....c.....d.....e.....h.....i.....j.....k.....m.....n.....o.....p.....r.....s.....t.....u.... .....w.....y....:\.....B..... .....*(http://www.ichiban.menu/menu-teppanyaki/2:Teppanyaki by Ichiban Japanese Restaurant | Doncaster East:.....J.....,6

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):	158572
Entropy (8bit):	0.2960967897145685
Encrypted:	false
SSDEEP:	48:Sqa3kaZX1AUUyARAnuOnUUj6U6/rylLjwx1UcAybHDU+4:SdlAUYMuOnUUP5Fwx1U1a4p
MD5:	302B5B5A833FA22756141A746E694060
SHA1:	0830CD34B0392E487F905D6C94AD763775E007DE
SHA-256:	FC515AC46CCB1CF8B99BEFEE2F321D697B3C959A3839C4E8EFE94ABA5BA0410A
SHA-512:	B1EF4902461A12DF6BCD5F1F6793BA8D119A9D69B32808E156A412CFADE3641AAEA833CE3E4DAAA485FA90A48CF94BF7DE2D132E952217B6403EA569397E43 2
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessionn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	39693
Entropy (8bit):	3.1161771455889373
Encrypted:	false
SSDEEP:	384:sQ9JbQFbLypHdrigVwYeLAhgOd4gOz4zA4cq:sApSCbtVwSa67cX2
MD5:	B818151E3B3FFB1099F9EC98A05A7A5C
SHA1:	FF8482B7017672AF05944BF2CC07E59FCFF41325
SHA-256:	8707CD646DC9E7F663E155CBD9E1683332859941F12A8599C23FCFC9DB002AA3
SHA-512:	B8C7A00B90212671B036847379762642A1B731941277FCC383AAB5123EDECE363BFEBFBCF7DAAAAC631235959A8FA3E9D040C5C361BC40D019B1B93C1162A48
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...bcfb9cc0_596e_4ef4_a9af_5448c29d755a..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....5..0.....(...http://www.ichiban.menu/menu-teppanyaki/:...T.e.p.p.a.n.y.a.k.i. .b.y. .l.c.h.i.b.a.n. .J.a.p.a.n.e.s.e. .R.e.s.t.a.u.r.a.n.t. .|. .D.o.n.c.a.s.t.e.r. .E.a.s.t.....h.....`..... ..... .....d.....d.....`.....x..... .....X...(...h.t.t.p.:././.w.w.w...i.c.h.i.b.a.n...m.e.n.u./.m.e.n.u.-.t.e.p.p.a.n.y.a.k.i./.....P.....H.....h..... h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
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\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.462926841229076
Encrypted:	false
SSDEEP:	48:dyG0yva7+M98dbw05k5MbQSefgGlNrS0U9RdiN977+:Fa7+MWdbwu+MbQ5fgGXrS0Vy
MD5:	EA3C11C8F35322588F389A32B6DF2B38
SHA1:	C10A34FAD59BD09F467412B33C1F7FE27A507877
SHA-256:	EEFFF9E63CA355F5A5C87A11B8D2EBBA068808552741D3DBD172245282921A24
SHA-512:	6F396D182A48370C2E29A4C1E10A453366E9353DC495AE50D76D6B1BAC4CDAAEF58D89AF47F1AFDFC33F224B27FBC3A202F4CE3576AACB309A93AEF24DE8F 21
Malicious:	false
Reputation:	low
Preview:	-@....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.Hangout SinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast .RequestIdGenerator..192663000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 00:15:42.24][INFO][mr.Init] MR instance ID: e634bf7b-42bd-4278-8f26-50d0b2576700\n","[2021-08-04 00:15:42.24][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 00:15:42.24][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 00:15:42.24][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 00:15:42.24][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 00:15:42.24][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 00:15:42.24][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):	329
Entropy (8bit):	5.184626848267575
Encrypted:	false
SSDEEP:	6:m+fq2PWXp+N23iKKdK8a2jMGIFUtpjcXZmwPjeQRNDkwOWXp+N23iKKdK8a2jMmd:zfva5Kk8EFUtpjI/Pj35f5Kk8bJ
MD5:	F8CDA82D93223A07C9D8C8AA0A9F07D4
SHA1:	425AA6424D77693CDF96030BA648B437EF199EE9
SHA-256:	2C8498F0C31DF76AAB3A319CBF7F5A68828777B22EA35B9883D872B50AC5B0D4
SHA-512:	47D8A25E68C034D7876695083B2D6B68A1B6BA3B8377F8F1A62095D37ACBA6A811E11B56C8F217D701575567D8FE074D3E2AB329177F2F912005E49ADF2250A2
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.380 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:15:29.382 d14 Recovering log #3.2021/08/04-00:15:29.383 d14 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\Local Storage\leveldb\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.184626848267575
Encrypted:	false
SSDEEP:	6:m+fq2PWXp+N23iKKdK8a2jMGIFUtpjcXZmwPjeQRNDkwOWXp+N23iKKdK8a2jMmd:zfva5Kk8EFUtpjI/Pj35f5Kk8bJ
MD5:	F8CDA82D93223A07C9D8C8AA0A9F07D4
SHA1:	425AA6424D77693CDF96030BA648B437EF199EE9
SHA-256:	2C8498F0C31DF76AAB3A319CBF7F5A68828777B22EA35B9883D872B50AC5B0D4
SHA-512:	47D8A25E68C034D7876695083B2D6B68A1B6BA3B8377F8F1A62095D37ACBA6A811E11B56C8F217D701575567D8FE074D3E2AB329177F2F912005E49ADF2250A2
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.380 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:15:29.382 d14 Recovering log #3.2021/08/04-00:15:29.383 d14 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):	24576
Entropy (8bit):	1.1993314343159756
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
SSDEEP:	96:vOqAuhjspnWO4DM5OqAuhjspnWOM5s868:HvDMt5
MD5:	F4CCF9D8A1FF8D3BC41650E4E87A1D31
SHA1:	B7C61D3365FCDE6A7E7B7E9BB3B292F4B4FBA239
SHA-256:	577573071A1E781236312A63980AFB9939AE53CAD3D0652FF7CB3671612523D4
SHA-512:	97E2288F15D2A0F6000316C30A7980D9DC98D3421C8EFD9A10495D9DDAB268E809D638FBC0D57DC60A367D5E044B8AC01D9E41F6FC1D7E4EAD85A03E242B8E2
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0195193840797179
Encrypted:	false
SSDEEP:	48:coq7w/qALihje9kqL42WOT/jKqrw/qALihje9kqL42WOT//8:coUOqAuhjspnWOCkOqAuhjspnWOg
MD5:	3D3CF783F5373AAE569CA0B256555380
SHA1:	64777FAEF9EF443DBFC8ADDD6FA164571939ED8C
SHA-256:	F5FBDD8A38E9B741CBBE8F2E248E878EB87A527932898BFD3BB160E5C4B623DE
SHA-512:	F4A0E4F2668FC65C396A2584CA4B3B939BF8EB10255A49238384A8929CE019822814E117DD8D0BB4FCA694D22FD3E9F2C8551EFFD297F27EEED40A1C3B876E2E
Malicious:	false
Reputation:	low
Preview:	.....M.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
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\Network Persistent State8 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4122
Entropy (8bit):	4.894981539348123
Encrypted:	false
SSDEEP:	96:JTOXGDHzhlzes6VM2erNsSGuGpT5j6l5KzFGdw5GbIH:JTOXGDHzhFes6VM2eruSD4T5j6l5KFP/
MD5:	16C55AF035F5826766FEF328F81C9E7A
SHA1:	1EC194710ED060DBC390F21BF6B0479F2E6982C8
SHA-256:	F903070491FE3105E48FA5F9E3214A9CB75018841C57FB4D37B357329A7E6BE0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State8 (copy)	
SHA-512:	6020928D129C1E2E43490825FB488E522B2B9ED9194D5CA29BBE88B38CDFE88143BDCDE4FC54251D0DEF0D03F5D00FF55A74D42F98BBC55D89E73F9CE36BD3EB
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932510936","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932511847","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275126932697074","port":443,"protocol_str":"quic"},{"advertised

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):	334
Entropy (8bit):	5.244177612196206
Encrypted:	false
SSDEEP:	6:m+iIq2PWXp+N23iKKdKgXz4rRIFUtpj4tZmwPjvmFkwOWXp+N23iKKdKgXz4q8LJ:ziIva5KkgXiuFUtpj4t/PjS5f5KkgX2J
MD5:	4C439A5D3A976B531C139E493868203F
SHA1:	52C599AEEC59203AE2DDDD51CBB8E600A2E76ADC
SHA-256:	3EB03D3F485AF07765F2804A512BC1D385EEC77BFD16E141DB14CB1F219587D2
SHA-512:	993F5C968D3696E6A6F853CFCAF577BEAC948653690DDE8E74DE184293EFCFA9AE7E168367678C95E0ACA1BD61A4FB3CDC0F80863FDDE1182095DE457352545
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.676 1170 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:15:29.681 1170 Recovering log #3.2021/08/04-00:15:29.683 1170 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.244177612196206
Encrypted:	false
SSDEEP:	6:m+iIq2PWXp+N23iKKdKgXz4rRIFUtpj4tZmwPjvmFkwOWXp+N23iKKdKgXz4q8LJ:ziIva5KkgXiuFUtpj4t/PjS5f5KkgX2J
MD5:	4C439A5D3A976B531C139E493868203F
SHA1:	52C599AEEC59203AE2DDDD51CBB8E600A2E76ADC
SHA-256:	3EB03D3F485AF07765F2804A512BC1D385EEC77BFD16E141DB14CB1F219587D2
SHA-512:	993F5C968D3696E6A6F853CFCAF577BEAC948653690DDE8E74DE184293EFCFA9AE7E168367678C95E0ACA1BD61A4FB3CDC0F80863FDDE1182095DE457352545
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.676 1170 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:15:29.681 1170 Recovering log #3.2021/08/04-00:15:29.683 1170 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\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5809
Entropy (8bit):	5.191173759512403
Encrypted:	false
SSDEEP:	96:nRCfzn9SwxXRcKITok0JCKL8hkk15bOTQVuwn:nRCL9rhcE4KykkP
MD5:	07CA9118F6C64E14A2EDCDBD2E207923
SHA1:	E21D5AA18A58B9DA64B4D81678999E79E9A50EE5
SHA-256:	1BE1881FA85AB86C3476730C5CCC2B3636C9AA9A77B07809714031A0D9F03092
SHA-512:	40D36513099D3E1F7AE4276993C5C251E51029B9AAD3F0404EF4C815C507FF5ABA829A52B1DD118D8304C6E964CF9C2A9B09744DAAD95FC34C20ADE5AA784F8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534929626370","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","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\PreferencesTM (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5783
Entropy (8bit):	5.1885579163192554
Encrypted:	false
SSDEEP:	96:nRCfkn9SwxXRcKIQok0JCKL8hkk1IbOTQVuwn:nRCq9rhch4KykkQ
MD5:	E3DB35D6F23F893F24DA78EDE1FD88EC
SHA1:	42BD70CE06226B900B1A1A4CA44DF0C5C409D52E
SHA-256:	29505DFF88C98B29BA1ECE318CCE06172C6945FD6E27A38A54BBD5FE7C99BA70
SHA-512:	65C253CBC85DF948117F3C0CEDBB70D7D3C67EE5521EED80913D4B7789C46FB9461543A70A5D7887C9645479BEB2D26469344CD9810BE053CAD5717FAB5D915
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534929626370","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","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\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):	1.0030668581546078
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGURTO:wIElwQF8mpcSdy
MD5:	F637F7B845AB8F8DC1FFA9E837008D3B
SHA1:	614977A4444420547F2F9D3EE9928A7E70243C04
SHA-256:	F574AFC6E572B6BB8EDDBA867BF7D4E6FEE4EBB76FA8B2AD012C830B6F39B4ED
SHA-512:	A62788FD348175B8B1BCD6B700757B9E09F803D7A1585728A13F847F636BAE8D1ED1CA8275BD0D1C933E25FE0F4000BE3EF3020C922945F8D8861C9CB324B74
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):	0.8268285005338882
Encrypted:	false
SSDEEP:	48:qwqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU06:qwhIElwQF8mpcSd
MD5:	3BA8682970B95A96AEB30AEDCEB3AD1D
SHA1:	0F5B5E46654126A0B9132F651B1500E4578F271C
SHA-256:	55E35C1AD5A4DC04330B341A42714176456CAD07FB8E201D860E7943DCFDDF1C
SHA-512:	91DC8A3CEAD2B0E99EE8EADAC34499F131CAC1D7693881928EFC51A53F16BFF788276A82D7489366625904E6669F1E971D4D73F014FBF31C9725B5CE35E6862
Malicious:	false
Reputation:	low
Preview:	..............+..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences3d (copy)	
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):	22595
Entropy (8bit):	5.535872250505424
Encrypted:	false
SSDEEP:	384:2/htBLlmmXI1kXqKf/pUZNCgVLH2HfDErU8HGqnT8+km4l:GLl7I1kXqKf/pUZNCgVLH2HfYrUwGqnA
MD5:	83BC8D7A974A0522CFD7C16143C44592
SHA1:	8D5CD79D6EDF65D266C65A960E1E1B084B8C0D17
SHA-256:	C6D55E3BFF826D0E0BF4F2F7B7EC978F0DB7FD47848C3E49C4DE9D917606A46D
SHA-512:	6FB0EA72FC2E66AD30D1B59B5A9B3AAF13A244E585E54C1EA6A1D24BA114D95F04298BB466C2602AC31B37CE3F4C736912DA6C24236C55A73A746E2FF8D6E9A4
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":"13272534929324348","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences5d (copy)	
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):	22596
Entropy (8bit):	5.535776875249774
Encrypted:	false
SSDEEP:	384:2/htBLlmmXI1kXqKf/pUZNCgVLH2HfDErU8HGBnT8+Om43:GLl7I1kXqKf/pUZNCgVLH2HfYrUwGBnE
MD5:	A0219BE62A910D9C1D5E3AF33259B6C6
SHA1:	D4ACE3ED1389C6834F1191B13FC013E2EB5F8480
SHA-256:	EE25F5F0DA163F9F84AA09EFAF1439ECF41EAE696D59F0F5C63BF9F9C2AC38D2
SHA-512:	163E02220001508187A33BB8F174D29439165DB49586D8A0B173CE3F8296278FBD2C09147EB38C8CBB2663DE54E05741CBF0DAEE0E4579B1179304637518C707
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":"13272534929324348","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferenceseo (copy)	
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):	16745
Entropy (8bit):	5.577118838687711
Encrypted:	false
SSDEEP:	384:2/htMLlmmXI1kXqKf/pUZNCgVLH2HfDErUEK2m4F:9Ll7I1kXqKf/pUZNCgVLH2HfYrUUm2
MD5:	4293C47769B30CE3233497B99EB68B8B
SHA1:	A3925AC8E2E060BBDC56C3F142694CAAC217C2C7
SHA-256:	B124D5D0026AD8A1CC6A3C4B38D4A4A8A0F15C53B92F9DACD686433816353E7A
SHA-512:	2A2B00AACCB305EE05817DA6EF7697E1B9EFBB97BFE82E9B5D0CBE1EBA08B80359859FD6686BEB9995E78DC4748658D0B477C3197779EE7DAF2F146F9D39D708
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":"13272534929324348","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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):	851
Entropy (8bit):	5.179785208089463
Encrypted:	false
SSDEEP:	12:5lpnq6ICAGs+BBC3A/X2Q0lc1CKlXwwECbC5YBAkf0CpolLAKCllK4h6FkmCT:7pnq6M+BX27qlXwrpYJfdolLArlK4hjB
MD5:	53B6638CA711AEF630D34EB5A2D50A15
SHA1:	E649B42653752C8171353942A265A20BCE718FA7
SHA-256:	50251925C09DCA6D9B834C4F5D8EB07252625E4CC0CD89485BB261046002E1BF
SHA-512:	A00515F92A138D2640798DA188B3B90D3A7CD83AA55A6699CAA2BF6CD07C4269B986B0D7AF9F1841407516B9D1BC29A59C11DAE0770CED967856F95528782BB
Malicious:	false
Reputation:	low
Preview:	..&f.....K[e.....next-map-id.1.Fnamespace-bcfb9cc0_596e_4ef4_a9af_5448c29d755a-https://www.google.com/.0V.e.....V.e.....V.e..... ....U.Dve.....next-map-id.2.Fnamespace-6003f412_ca6a_4d60_9632_121bd93e7ffc-https://www.google.com/.1. .....g*.e.....next-map-id.3.Fnamespace-bda5dedd_3059_468a_a16c_7f66256b88ff-https://www.google.com/.2.&..e.....next-map-id.4.Fnamespace-c7c4eded_30c1_431b_8ffc_c4d83ba6ce24-https://www.google.com/.3.r..e.....next-map-id.5.Fnamespace-434d094d_7a25_4eb3_867e_ddf3aa87c857-https://www.google.com/.4..UOe.....next-map-id.6.Fnamespace-9650b281_3c90_45a2_9d8a_bc16dc31c485-https://www.google.com/.5....e.....next-map-id.7.Fnamespace-bbabeb9f_7131_476e_81b4_b0bb792fed65-https://www.google.com/.6

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):	320
Entropy (8bit):	5.158118451260149
Encrypted:	false
SSDEEP:	6:m+WEyq2PWXp+N23iKKdKrQMxIFUtpjk+r1ZmwPjEVjRkwOWXp+N23iKKdKrQMFLJ:zWEyva5KkCFUtpjP/PjoR5f5KktJ
MD5:	8420B9411DD7F4A41D54E000F14155F3
SHA1:	62B5BCFFAD835D360600929770D9720680AED6FD
SHA-256:	8975E292012607F9725E2A35BCEB7ADE025A8D0CE0AD18AE11C0C82843A2D749
SHA-512:	3212D05FB0B39C531C91B2D55925F5613E92E8F08FBF5D3F83FFF044E3A099C481E966D5F1E77027559099C2EF8DBFD851869CAE0E00996C4FD296D674E6FE81
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.575 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:15:29.586 1010 Recovering log #3.2021/08/04-00:15:29.587 1010 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.158118451260149
Encrypted:	false
SSDEEP:	6:m+WEyq2PWXp+N23iKKdKrQMxIFUtpjk+r1ZmwPjEVjRkwOWXp+N23iKKdKrQMFLJ:zWEyva5KkCFUtpjP/PjoR5f5KktJ
MD5:	8420B9411DD7F4A41D54E000F14155F3
SHA1:	62B5BCFFAD835D360600929770D9720680AED6FD
SHA-256:	8975E292012607F9725E2A35BCEB7ADE025A8D0CE0AD18AE11C0C82843A2D749
SHA-512:	3212D05FB0B39C531C91B2D55925F5613E92E8F08FBF5D3F83FFF044E3A099C481E966D5F1E77027559099C2EF8DBFD851869CAE0E00996C4FD296D674E6FE81
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.575 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:15:29.586 1010 Recovering log #3.2021/08/04-00:15:29.587 1010 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):	5.1746036776402216
Encrypted:	false
SSDEEP:	6:m+8IYQyq2PWXp+N23iKKdK7Uh2ghZIFUtpjy0MAG1ZmwPj8SQRkwOWXp+N23iKKF:z8IAva5KkIhHh2FUtpjy0Mj1/Pjw5f5m
MD5:	E74C923C67F0BAA8B31105BE70673A71

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA1:	F52DF62CFF722DF35FFD730394E4B5A24D78A7B4
SHA-256:	2A325592CFBC3C22159E0271B51A484629ACA7023DEEB5330863C913307ACEFB
SHA-512:	3835C17C92C5BA9B396FCF5AB5F9A41C36B0542FC06D3401712FCB9EBFC9E661869363DFA17CE43AE1D051D39930E959B1253CCB14BD98757A41F5242F1B5C3
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.345 f30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/04-00:15:29.359 f30 Recovering log #3.2021/08/04-00:15:29.360 f30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.1746036776402216
Encrypted:	false
SSDEEP:	6:m+8IYQyq2PWXp+N23iKKdK7Uh2ghZIFUtpjy0MAG1ZmwPj8SQRkwOWXp+N23iKKF:z8IAva5KkIhHh2FUtpjy0Mj1/Pjw5f5m
MD5:	E74C923C67F0BAA8B31105BE70673A71
SHA1:	F52DF62CFF722DF35FFD730394E4B5A24D78A7B4
SHA-256:	2A325592CFBC3C22159E0271B51A484629ACA7023DEEB5330863C913307ACEFB
SHA-512:	3835C17C92C5BA9B396FCF5AB5F9A41C36B0542FC06D3401712FCB9EBFC9E661869363DFA17CE43AE1D051D39930E959B1253CCB14BD98757A41F5242F1B5C3
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.345 f30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/04-00:15:29.359 f30 Recovering log #3.2021/08/04-00:15:29.360 f30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.277056541701496
Encrypted:	false
SSDEEP:	6:m+lq2PWXp+N23iKKdKusNpV/2jMGIFUtpjAJZmwPjBkwOWXp+N23iKKdKusNpV/s:zlva5KkFFUtpjC/PjB5f5KkOJ
MD5:	4583E9696EB7F57F614AEF35670A06BF
SHA1:	3F1575C11FF112FFE2FAA605E7EA87F7E80F65BE
SHA-256:	83839520869C4C785F389C31E63B16772DEC0361C7B8CC72032F5847CC7C47CC
SHA-512:	FDDBE58183AD2D77FA7C1280406F160655D31B950B83796A8F984B01449033EB3C84E8AF1AE0D1AE1F2C26BB131041507AAE21F03ECEF77270AC39705AC71C4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.609 834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:15:29.610 834 Recovering log #3.2021/08/04-00:15:29.611 834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.277056541701496
Encrypted:	false
SSDEEP:	6:m+lq2PWXp+N23iKKdKusNpV/2jMGIFUtpjAJZmwPjBkwOWXp+N23iKKdKusNpV/s:zlva5KkFFUtpjC/PjB5f5KkOJ
MD5:	4583E9696EB7F57F614AEF35670A06BF
SHA1:	3F1575C11FF112FFE2FAA605E7EA87F7E80F65BE
SHA-256:	83839520869C4C785F389C31E63B16772DEC0361C7B8CC72032F5847CC7C47CC
SHA-512:	FDDBE58183AD2D77FA7C1280406F160655D31B950B83796A8F984B01449033EB3C84E8AF1AE0D1AE1F2C26BB131041507AAE21F03ECEF77270AC39705AC71C4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.609 834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:15:29.610 834 Recovering log #3.2021/08/04-00:15:29.611 834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.303723065724325
Encrypted:	false
SSDEEP:	6:m+Gq2PWXp+N23iKKdKusNpqz4rRIFUtpjiZmwPjpfkwOWXp+N23iKKdKusNpqz4n:zGva5KkmiuFUtpji/Pjpf5f5Kkm2J
MD5:	B74EF9974B8087844C63F84BABC9AA56
SHA1:	21053EDB8E5208E4E77A9E0BE216E6390691F76E
SHA-256:	B9C6AE5A332315527BF523D0591C69312C3D8F96D6EA83AF70FE0807542AE1BE
SHA-512:	D285EA94C5CC9DFBAF8EE497F17EFD9E75D41A465D205E600A3FE099FB229E61FE438E2EB5D248F73813E07CE0174213CAAE621C2B6758288AC1AF90BB0179(1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.683 444 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:15:29.686 444 Recovering log #3.2021/08/04-00:15:29.690 444 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.303723065724325
Encrypted:	false
SSDEEP:	6:m+Gq2PWXp+N23iKKdKusNpqz4rRIFUtpjiZmwPjpfkwOWXp+N23iKKdKusNpqz4n:zGva5KkmiuFUtpji/Pjpf5f5Kkm2J
MD5:	B74EF9974B8087844C63F84BABC9AA56

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)

SHA1:	21053EDB8E5208E4E77A9E0BE216E6390691F76E
SHA-256:	B9C6AE5A332315527BF523D0591C69312C3D8F96D6EA83AF70FE0807542AE1BE
SHA-512:	D285EA94C5CC9DFBAF8EE497F17EFD9E75D41A465D205E600A3FE099FB229E61FE438E2EB5D248F73813E07CE0174213CAAE621C2B6758288AC1AF90BB0179(1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:15:29.683 444 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:15:29.686 444 Recovering log #3.2021/08/04-00:15:29.690 444 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:15:32.778825998 CEST	192.168.2.3	8.8.8.8	0x2103	Standard query (0)	www.ichiban.menu	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:32.795274019 CEST	192.168.2.3	8.8.8.8	0xcd1d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:32.802877903 CEST	192.168.2.3	8.8.8.8	0x988c	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.127536058 CEST	192.168.2.3	8.8.8.8	0xfea3	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.331661940 CEST	192.168.2.3	8.8.8.8	0x3b9b	Standard query (0)	s3-eu-west-1.amazonaws.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.916996956 CEST	192.168.2.3	8.8.8.8	0x823	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.976445913 CEST	192.168.2.3	8.8.8.8	0x4885	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:15:34.976490974 CEST	192.168.2.3	8.8.8.8	0x1b4d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.981867075 CEST	192.168.2.3	8.8.8.8	0x1f63	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.964498997 CEST	192.168.2.3	8.8.8.8	0x48b	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.025564909 CEST	192.168.2.3	8.8.8.8	0xa037	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.507069111 CEST	192.168.2.3	8.8.8.8	0x629	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.961869001 CEST	192.168.2.3	8.8.8.8	0x5479	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.961915016 CEST	192.168.2.3	8.8.8.8	0x780d	Standard query (0)	www.ichiban.menu	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:41.534362078 CEST	192.168.2.3	8.8.8.8	0x3aa2	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:33.594248056 CEST	192.168.2.3	8.8.8.8	0xe699	Standard query (0)	www.ichiban.menu	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:34.091085911 CEST	192.168.2.3	8.8.8.8	0x46e	Standard query (0)	1.gravatar.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:34.260344028 CEST	192.168.2.3	8.8.8.8	0x4c1a	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:37.795916080 CEST	192.168.2.3	8.8.8.8	0xab7a	Standard query (0)	1.gravatar.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:38.708877087 CEST	192.168.2.3	8.8.8.8	0xacd0	Standard query (0)	booking-widget.quandoo.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.185419083 CEST	192.168.2.3	8.8.8.8	0x852e	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.187473059 CEST	192.168.2.3	8.8.8.8	0x7bd	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.189631939 CEST	192.168.2.3	8.8.8.8	0x741b	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.312515974 CEST	192.168.2.3	8.8.8.8	0xe997	Standard query (0)	9110-api.quandoo.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.738996983 CEST	192.168.2.3	8.8.8.8	0x45dc	Standard query (0)	www.quandoo.com.au	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.741797924 CEST	192.168.2.3	8.8.8.8	0x44bc	Standard query (0)	booking-widget.quandoo.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:15:32.814940929 CEST	8.8.8.8	192.168.2.3	0x2103	No error (0)	www.ichiban.menu	ichiban.menu		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:32.814940929 CEST	8.8.8.8	192.168.2.3	0x2103	No error (0)	ichiban.menu		166.62.28.94	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:32.827931881 CEST	8.8.8.8	192.168.2.3	0xcd1d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:32.827931881 CEST	8.8.8.8	192.168.2.3	0xcd1d	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:32.838119984 CEST	8.8.8.8	192.168.2.3	0x988c	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.156738043 CEST	8.8.8.8	192.168.2.3	0xfea3	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.354269981 CEST	8.8.8.8	192.168.2.3	0x93c4	No error (0)	gstaticadssl.l.google.com		142.250.186.35	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.366014004 CEST	8.8.8.8	192.168.2.3	0x3b9b	No error (0)	s3-eu-west-1.amazonaws.com		52.218.20.156	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:34.952222109 CEST	8.8.8.8	192.168.2.3	0x823	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.010150909 CEST	8.8.8.8	192.168.2.3	0x1b4d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:15:35.010150909 CEST	8.8.8.8	192.168.2.3	0x1b4d	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.010399103 CEST	8.8.8.8	192.168.2.3	0x4885	No error (0)	www.instagram.com	z-p42-instagram.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:35.010399103 CEST	8.8.8.8	192.168.2.3	0x4885	No error (0)	z-p42-instagram.c10r.facebook.com		157.240.17.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.209.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.184.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.184.110	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.198.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		172.217.21.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.180.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.180.110	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.180.142	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.206.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.206.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.023297071 CEST	8.8.8.8	192.168.2.3	0x1f63	No error (0)	youtube-ui.l.google.com		216.58.208.142	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.745809078 CEST	8.8.8.8	192.168.2.3	0xb12f	No error (0)	www-google tagmanager.l.google.com		142.250.184.72	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		35.167.90.204	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		52.43.10.86	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		52.10.17.224	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		52.39.143.152	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		52.89.95.104	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		52.39.24.11	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		54.68.253.11	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:15:35.988867044 CEST	8.8.8.8	192.168.2.3	0x48b	No error (0)	api.segment.io		54.190.208.247	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.067531109 CEST	8.8.8.8	192.168.2.3	0x7db	No error (0)	www-google-analytics.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.069538116 CEST	8.8.8.8	192.168.2.3	0xa037	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:36.069538116 CEST	8.8.8.8	192.168.2.3	0xa037	No error (0)	static-cdn.hotjar.com		13.32.22.92	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.069538116 CEST	8.8.8.8	192.168.2.3	0xa037	No error (0)	static-cdn.hotjar.com		13.32.22.41	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.069538116 CEST	8.8.8.8	192.168.2.3	0xa037	No error (0)	static-cdn.hotjar.com		13.32.22.75	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.069538116 CEST	8.8.8.8	192.168.2.3	0xa037	No error (0)	static-cdn.hotjar.com		13.32.22.91	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.550403118 CEST	8.8.8.8	192.168.2.3	0x629	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:36.550403118 CEST	8.8.8.8	192.168.2.3	0x629	No error (0)	stats.l.doubleclick.net		108.177.126.155	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.550403118 CEST	8.8.8.8	192.168.2.3	0x629	No error (0)	stats.l.doubleclick.net		108.177.126.156	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.550403118 CEST	8.8.8.8	192.168.2.3	0x629	No error (0)	stats.l.doubleclick.net		108.177.126.157	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:36.550403118 CEST	8.8.8.8	192.168.2.3	0x629	No error (0)	stats.l.doubleclick.net		108.177.126.154	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		35.167.90.204	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		52.43.10.86	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		52.10.17.224	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		52.39.143.152	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		52.89.95.104	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		52.39.24.11	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		54.68.253.11	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.995172977 CEST	8.8.8.8	192.168.2.3	0x5479	No error (0)	api.segment.io		54.190.208.247	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:38.998425007 CEST	8.8.8.8	192.168.2.3	0x780d	No error (0)	www.ichiban.menu	ichiban.menu		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:38.998425007 CEST	8.8.8.8	192.168.2.3	0x780d	No error (0)	ichiban.menu		166.62.28.94	A (IP address)	IN (0x0001)
Aug 4, 2021 00:15:41.567867041 CEST	8.8.8.8	192.168.2.3	0x3aa2	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:15:41.567867041 CEST	8.8.8.8	192.168.2.3	0x3aa2	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.161	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:33.626610994 CEST	8.8.8.8	192.168.2.3	0xe699	No error (0)	www.ichiban.menu	ichiban.menu		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:16:33.626610994 CEST	8.8.8.8	192.168.2.3	0xe699	No error (0)	ichiban.menu		166.62.28.94	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:16:34.125076056 CEST	8.8.8.8	192.168.2.3	0x46e	No error (0)	1.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:34.285154104 CEST	8.8.8.8	192.168.2.3	0x4c1a	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:37.828176022 CEST	8.8.8.8	192.168.2.3	0xab7a	No error (0)	1.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:37.922597885 CEST	8.8.8.8	192.168.2.3	0x1ad5	No error (0)	gstaticadssl.l.google.com		216.58.198.3	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:38.753567934 CEST	8.8.8.8	192.168.2.3	0xacd0	No error (0)	booking-widget.quandoo.com		143.204.207.60	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:38.753567934 CEST	8.8.8.8	192.168.2.3	0xacd0	No error (0)	booking-widget.quandoo.com		143.204.207.124	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:38.753567934 CEST	8.8.8.8	192.168.2.3	0xacd0	No error (0)	booking-widget.quandoo.com		143.204.207.63	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:38.753567934 CEST	8.8.8.8	192.168.2.3	0xacd0	No error (0)	booking-widget.quandoo.com		143.204.207.107	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.221286058 CEST	8.8.8.8	192.168.2.3	0x852e	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:16:39.221286058 CEST	8.8.8.8	192.168.2.3	0x852e	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.209.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.184.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.184.110	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.198.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		172.217.21.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.180.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.180.110	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.180.142	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.206.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.206.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.224025011 CEST	8.8.8.8	192.168.2.3	0x741b	No error (0)	youtube-ui.l.google.com		216.58.208.142	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.226793051 CEST	8.8.8.8	192.168.2.3	0x7bd	No error (0)	www.instagram.com	z-p42-instagram.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:16:39.226793051 CEST	8.8.8.8	192.168.2.3	0x7bd	No error (0)	z-p42-instagram.c10r.facebook.com		157.240.17.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.347829103 CEST	8.8.8.8	192.168.2.3	0xe997	No error (0)	9110-api.quandoo.com		52.213.64.175	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.347829103 CEST	8.8.8.8	192.168.2.3	0xe997	No error (0)	9110-api.quandoo.com		52.214.46.190	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.347829103 CEST	8.8.8.8	192.168.2.3	0xe997	No error (0)	9110-api.quandoo.com		3.248.134.122	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.811969042 CEST	8.8.8.8	192.168.2.3	0x44bc	No error (0)	booking-widget.quandoo.com.au		13.32.22.7	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.811969042 CEST	8.8.8.8	192.168.2.3	0x44bc	No error (0)	booking-widget.quandoo.com.au		13.32.22.46	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.811969042 CEST	8.8.8.8	192.168.2.3	0x44bc	No error (0)	booking-widget.quandoo.com.au		13.32.22.59	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.811969042 CEST	8.8.8.8	192.168.2.3	0x44bc	No error (0)	booking-widget.quandoo.com.au		13.32.22.65	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.864726067 CEST	8.8.8.8	192.168.2.3	0x45dc	No error (0)	www.quandoo.com.au		176.34.109.148	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:39.864726067 CEST	8.8.8.8	192.168.2.3	0x45dc	No error (0)	www.quandoo.com.au		54.217.223.212	A (IP address)	IN (0x0001)
Aug 4, 2021 00:16:41.663414001 CEST	8.8.8.8	192.168.2.3	0x5f40	No error (0)	www-google-analytics.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)

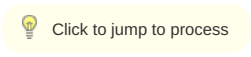
HTTP Request Dependency Graph

- www.ichiban.menu
  - 1.gravatar.com

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 752 Parent PID: 968

General

Start time:	00:15:28
Start date:	04/08/2021
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 'http://www.ichiban.menu/menu-teppanyaki/'
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: 4720 Parent PID: 752

General

Start time:	00:15:30
Start date:	04/08/2021
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=1556,16433198126318794357,6094034236782199136,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /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

Disassembly