ID: 458990
Cookbook: browseurl.jbs
Time: 01:07:21
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

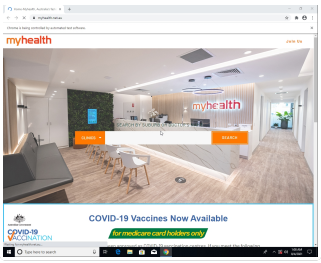
Windows Analysis Report https://myhealth.net.au

Overview

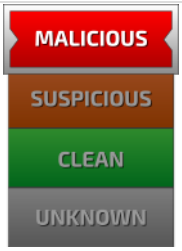
General Information

Sample URL:	http://https://myhealth.net.au
Analysis ID:	458990
Infos:	

Most interesting Screenshot:



Detection

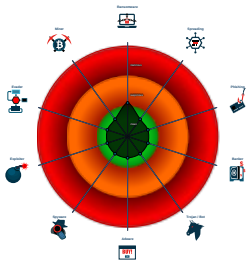


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4088 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://myhealth.net.au' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5624 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,17615188742813691833,8383625610936018057,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /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

AV Detection:

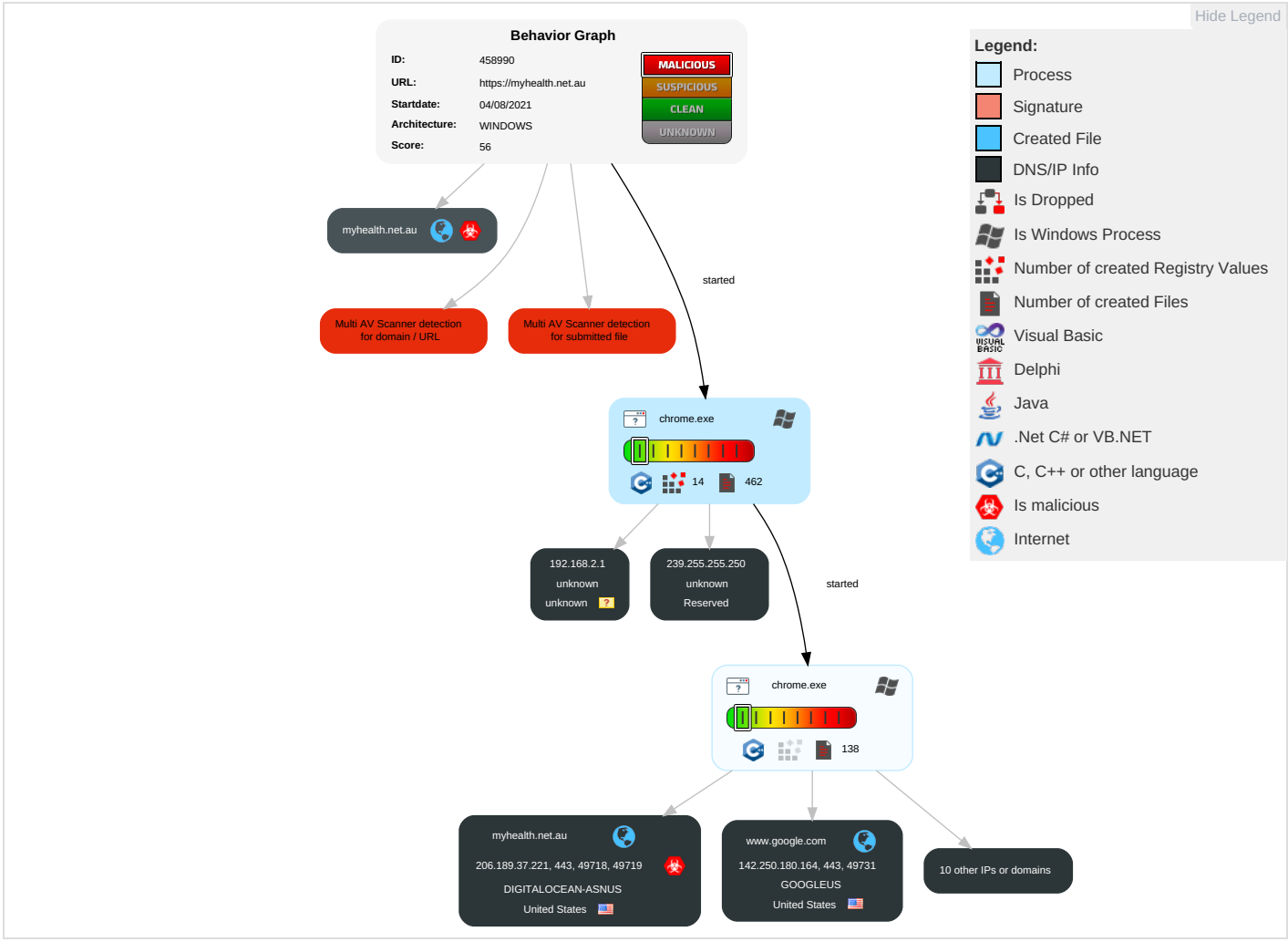
Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

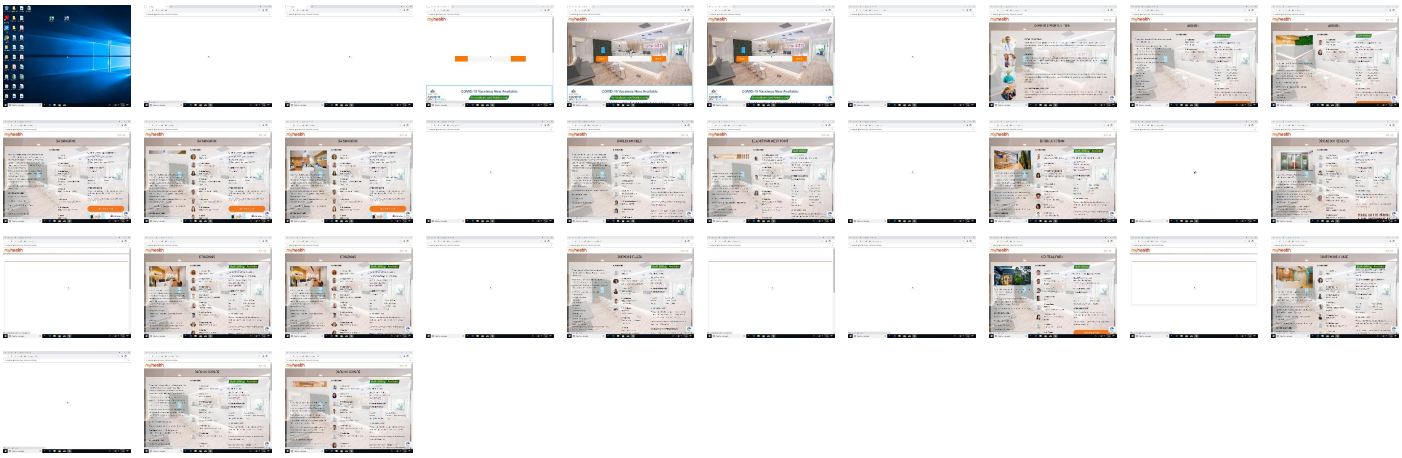
Behavior Graph

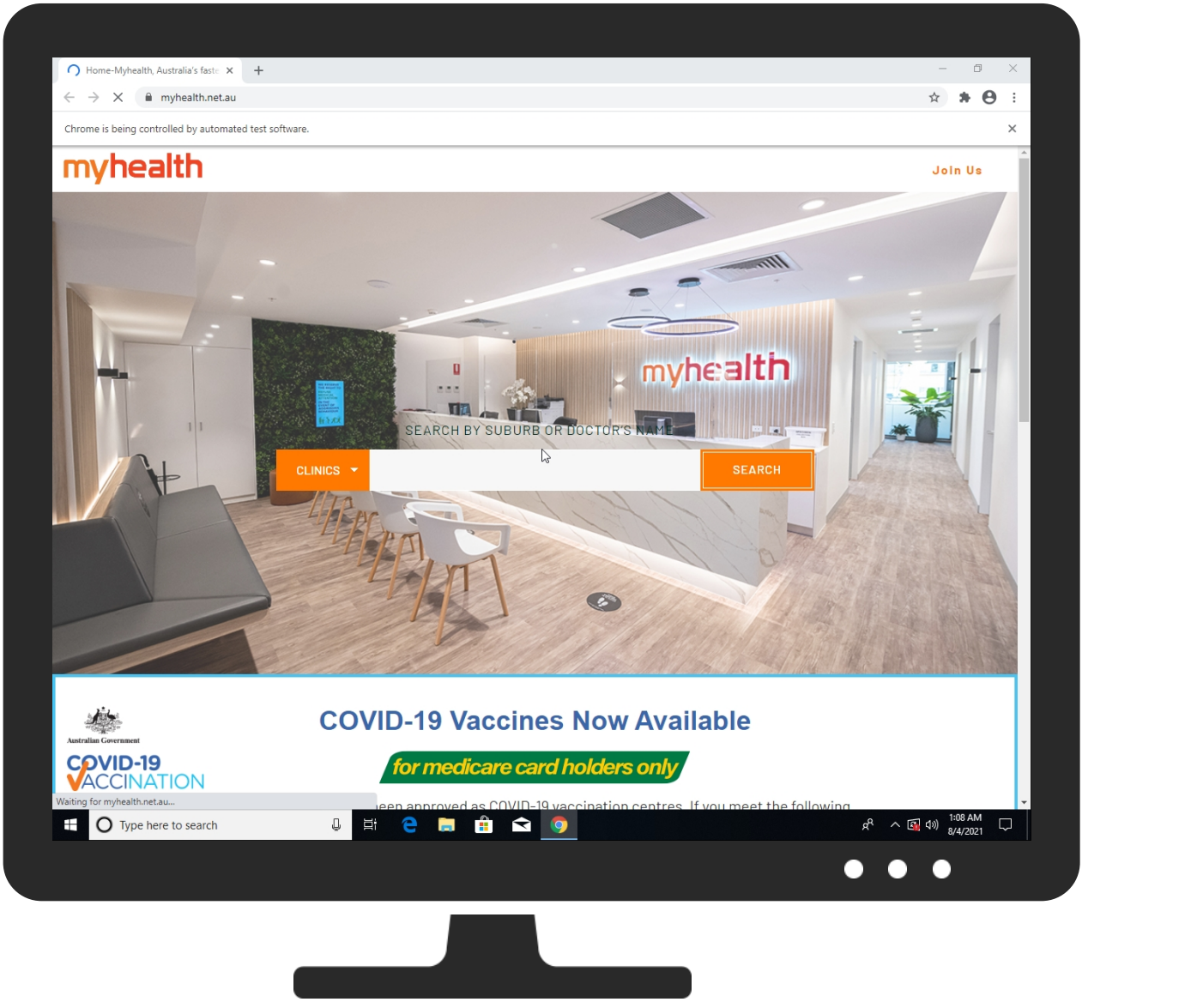


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://myhealth.net.au	7%	Virustotal		Browse
http://https://myhealth.net.au	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
myhealth.net.au	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://myhealth.net.au/central-park/S	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/custom.js?ver=5.8aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/wp-embed.min.js?ver=5.8	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/Home-Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4.2	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/burwood-plaza/%	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20170530	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/darling-square/&Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/wp-emoji-release.min.js?ver=5.8aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap-select.js?ver=5.8	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/KV	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/castle-towers/%Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/custom.js?ver=5.8a	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/bondi-junction/&Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/custom.js?ver=5.8	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/darling-square/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/owl.carousel.min.js?ver=5.8aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20170530aD	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://myhealth.net.au/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=5.4.2aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0a	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://myhealth.net.au/3	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/career-opportunities/Career	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/9	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/:	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/7	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/plugins/google-analytics-dashboard-for-wp/assets/js/frontend-gtag	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap.min.js?ver=5.8aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/twentysixteen/js/functions.js?ver=20181217	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/B	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/chatswood-chase/)	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/C	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/J	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/baulkham-hills/&Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/owl.carousel.min.js?ver=5.8	0%	Avira URL Cloud	safe	
http://https://myhealth.net.auh	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/L	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/Q	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/auburn/1	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/jquery/jquery.min.js?ver=3.6.0aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/O	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/U	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/broadway/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/chatswood-chase/Myhealth	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://myhealth.net.au/brigadoon-revesby/)Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.7aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.7	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/barangaroo/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/burwood-plaza/Y	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap-select.js?ver=5.8aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/f	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/i	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/blacktown-west-point/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/k	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/r	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap.min.js?ver=5.8	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/bondi-junction/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/castle-towers/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4.2aD	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/brigadoon-revesby/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/burwood-plaza/Myhealth	0%	Avira URL Cloud	safe	
http://https://myhealth.net.au/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.7a	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.184.99	true	false		high
myhealth.net.au	206.189.37.221	true	true	• 7%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
www-google-analytics.l.google.com	142.250.184.78	true	false		high
www-googletagmanager.l.google.com	142.250.184.72	true	false		high
www.google.com	142.250.180.164	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://myhealth.net.au/broadway/	true		unknown
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf7qc4ZAAAAAHC1nx_vfVaxGg9awmlhdu6Ad1NV&co=aHR0cHM6Ly9teWhlYWx0aC5uZXQuYXU6NDQz&hl=en&v=ecapuzyywmdXQ5gJHS3JQiXe&size=invisible&cb=x81jhulwnvnt	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf7qc4ZAAAAAHC1nx_vfVaxGg9awmlhdu6Ad1NV&co=aHR0cHM6Ly9teWhlYWx0aC5uZXQuYXU6NDQz&hl=en&v=ecapuzyywmdXQ5gJHS3JQiXe&size=invisible&cb=wjpv8a92ktbc	false		high
http://https://myhealth.net.au/brigadoon-revesby/	true		unknown
http://https://myhealth.net.au/auburn/	true		unknown
http://https://myhealth.net.au/career-opportunities/	true		unknown
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf7qc4ZAAAAAHC1nx_vfVaxGg9awmlhdu6Ad1NV&co=aHR0cHM6Ly9teWhlYWx0aC5uZXQuYXU6NDQz&hl=en&v=ecapuzyywmdXQ5gJHS3JQiXe&size=invisible&cb=lwu5077k3r09	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf7qc4ZAAAAAHC1nx_vfVaxGg9awmlhdu6Ad1NV&co=aHR0cHM6Ly9teWhlYWx0aC5uZXQuYXU6NDQz&hl=en&v=ecapuzyywmdXQ5gJHS3JQiXe&size=invisible&cb=qnz7o5xxh0or	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf7qc4ZAAAAAHC1nx_vfVaxGg9awmlhdu6Ad1NV&co=aHR0cHM6Ly9teWhlYWx0aC5uZXQuYXU6NDQz&hl=en&v=ecapuzyywmdXQ5gJHS3JQiXe&size=invisible&cb=k2luqpy7rx32	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.99	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
206.189.37.221	myhealth.net.au	United States		14061	DIGITALOCEAN-ASNUS	true
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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458990
Start date:	04.08.2021
Start time:	01:07:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://myhealth.net.au
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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@44/274@10/10

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://myhealth.net.au/career-opportunities/ • Browse: https://myhealth.net.au/auburn/ • Browse: https://myhealth.net.au/barangaroo/ • Browse: https://myhealth.net.au/baulkham-hills/ • Browse: https://myhealth.net.au/blacktown-west-point/ • Browse: https://myhealth.net.au/bondi-junction/ • Browse: https://myhealth.net.au/brigadoon-revesby/ • Browse: https://myhealth.net.au/broadway/ • Browse: https://myhealth.net.au/burwood-plaza/ • Browse: https://myhealth.net.au/castle-towers/ • Browse: https://myhealth.net.au/central-park/ • Browse: https://myhealth.net.au/chatswood-chase/ • Browse: https://myhealth.net.au/darling-square/
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\Local\Google\Chrome\User Data\0db9da00-8fcb-4800-b7df-10d80d459f0b.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):	174336
Entropy (8bit):	6.079356632268102
Encrypted:	false
SSDEEP:	3072:caQGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuR7:JRxaV+QfT7GSmhhaqfIlUOoSiuR7
MD5:	49101D611CEDAF0AD73095AC422D92FE
SHA1:	6F5ADC7906B99820A0364EE2C8E628A9A55A6368
SHA-256:	D86631734E6DA893C012D8A89328A0A57A99327AD1C22F08BC8EC521ABFDED49
SHA-512:	3BE062F20E265136D323DD3C512F1A8B0FD2DB9278D7250C18EFBD22719DF9C0C0EF8FC1E253CA3F3EE492DCE9F151955DB53A47D27E382C8C47A7190D2F3C6
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":1.628064491157753e+12,"network":1.628032094e+12,"ticks":6341605087.0,"uncertainty":4489850.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\4a4e2d9b-e959-43e8-b667-0b2d2d6012f2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7493079716874647
Encrypted:	false
SSDEEP:	384:RPRumYbdgTw+VTV65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzHNf8eKCZOkIKy:laeZRKok5AenAiocvjGaKACKJs
MD5:	A68BE2558FE9EAE03AD7C42AB626F71B
SHA1:	098BEBD46DE77FD965E4DA3E5D00F75C695ED70A
SHA-256:	1DD4752E64463AEDFF0117928B34E88EA04635FE2B78D389B43B2000204FEFE0
SHA-512:	B4DEE9084BDB556893FBEDD46ACF864BB98244842B8F44BB6011C8EEB08ED4A0B84329406491C1953E2036159760593193567AF716C434E598BD6BAB012BD27E
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\5336cdc0-9540-4930-b44b-e695f13f7afa.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):	174337
Entropy (8bit):	6.079358044811794
Encrypted:	false
SSDEEP:	3072:QjxGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuR7:48xaV+QfT7GSmhhaqfIlUOoSiuR7
MD5:	2402AF44CFE74F5A838E052E708F66D1
SHA1:	7B568A69A6FFABFE388D51A437BFA9EECF000BF0
SHA-256:	9427D5CBA40082F04A17D5A7D26A774E6A0D054E138AD93867E06072CF3C8111
SHA-512:	CF1D59D09D7256CE67BE45EB23FF95D9C9091D5B1C4F7817E92C20EFBF2C50AFA095A405798F4D3A24F93B7C77238AB69D766360B4827FEC5E5522341B843EB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\5336cdc0-9540-4930-b44b-e695f13f7afa.tmp

Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628064491157753e+12,"network":1.628032094e+12,"ticks":6341605087.0,"uncertainty":4489850.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016175992"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\62dba8f9-b965-4f90-b61d-9f6c7a78ec47.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7489538170141197
Encrypted:	false
SSDEEP:	384:nPRumYbdEwf65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzQf8eKCZOkIKNH1OPA:LeZRKoJ5AenAiocvjGaKACKJz
MD5:	402A499FC2C8AAD06C9827650C0838A3
SHA1:	9D0A487664DE108EC93700C68756A5E574025579
SHA-256:	E20B05DDD4BF4B8F12548DCA269D9086C1EE5D86433348AF22AB7BD28B5D033C
SHA-512:	4CD23341C39ABF0B219A827623D1E50F49B829A274759CB7B265F2D59E0AC69A85C4B5455FDBF62ABA63791147305F568B38B4EBAECD4A634A1C1ACD88A5E3F5
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f9542e4-6cc0-4ecd-bc0b-061a314a4bb3.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):	165872
Entropy (8bit):	6.049552117436366
Encrypted:	false
SSDEEP:	3072:i0GaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuR7:IxaV+QfT7GSmhhaqfIlUOoSiuR7
MD5:	88F28E05E37DA4EE54F8E1996DEE4FD8
SHA1:	C0DC49D991692FC188333F9D9B58DBBB3F093E72
SHA-256:	257B581F960CF240E1305033ED53B641DE408D8B2CFE1263AB02044CED0403FF
SHA-512:	3215DC40A218DC25C9026AAB7BB8F703D9A4C55C209CAB77E372AD25708B61724C5056860524DD033C41CA2D5C9A5BBBC650716E642081BFCBDD6ABA39D126
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":1.628064491157753e+12,"network":1.628032094e+12,"ticks":6341605087.0,"uncertainty":4489850.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016175992"},"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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

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\02de18d9-0839-4b93-8540-78175e240d4b.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):	1372
Entropy (8bit):	5.580723555154478
Encrypted:	false
SSDEEP:	24:YEeNo9RAeU616H0UhVrfwUjRjQG1KUgKSACkq/HeUeXby2qUeXvtJ7wUgOiRUenw:Y1+ieU616UUhuUjlKUg+qPeUer2Uefrb
MD5:	111F3BF7BD20017D37A64EF1807A4723
SHA1:	E65A9D2DB8BB43077B5A225F7D9AC61B72FF3812
SHA-256:	1113C1C91947EE46F78F575D8013E2363EAA4BBCA74EBFF0C2B29A082822B56F
SHA-512:	88550EB00C2C7D05B9C7B8BB48BD2C06D1FD9F8600E3DBD248DE2679B4A7920F47CE9F8B1F4DCA14FDBA42B33BE3C6C44DE6F8515FDF1B124769A41BFF8DC DF7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659600515.085407,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064515.085413},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1638950894.0541,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064494.054106},{"expiry":1659600492.932569,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2Okg A=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628064492.932574},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1S shXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YU Y9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0517c12b-90a8-482c-8e8e-de91ffe286a3.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):	3792
Entropy (8bit):	4.886307108356222
Encrypted:	false
SSDEEP:	96:JOXGDHz6bB5szm5GpG15KWlkQG+G60mhH:JOXGDHz6bB5szm5UO5DlkQ5D06
MD5:	E56BF24A4E43925E0EF47BA758920CAB
SHA1:	E3AAA37D0DA5507A899BBB030655C0FC629B1D77
SHA-256:	2A248CB88CA62C42E892D0B056B1DF089B45CD734BC15809C468E6515D97EC2A
SHA-512:	98B6E0653E7379ADB949BF30326D53AAB393FF18A61D7353084722A2C42709E5A776B8E7A16619F184C07106A9CDCC20F90C8DF460D7916E1129C29B8858A679
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"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":"13275130091315287","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275130091358364","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275130 091539754","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13275130091539758","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\07aaefe0-b4e9-46a5-8b94-af8fd61f2b9e.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):	16745
Entropy (8bit):	5.578046357896868
Encrypted:	false
SSDEEP:	384:x4f/ts9LlLrXE1kXqKf/pUZNCgVLH2HfD3rURVErpu4U:N9LlPE1kXqKf/pUZNCgVLH2Hf7rURVw8
MD5:	0EE56F69EAD3F977FAE26F3B20DCA2B6
SHA1:	1620A6D0D7CC30575EBEDD36433270D3B0C582C2
SHA-256:	A6F955EB0AC6F72820415B8DD48AD6BE318332172AC22B91193E47A0CA942148
SHA-512:	238DF6B5247DC7345AE4F2596D3D6D1CE62923158A073C13520F80ED7770F04383BFEFE241253EDBF1C181DFC6A0EBF135F43ACAB628243240865A8BCB1713D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\07aaefe0-b4e9-46a5-8b94-af8fd61f2b9e.tmp	
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":"13272538088150368","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15621bae-85aa-4ec4-997b-62cbba9da036.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):	5.5365274222511225
Encrypted:	false
SSDEEP:	384:x4f/t59LlLrXE1kXqKf/pUZNCgVLH2HfD3rUEHG5nTTVEHpu4b:S9LlPE1kXqKf/pUZNCgVLH2Hf7rUIG5s
MD5:	E480886F6922C5EC99CAC5A881D3CC4B
SHA1:	C7704E59DA1A7801B04805686D8395ED5F786148
SHA-256:	FDF3AB31994CCFD106CFA6EAA62C4A4D94FA9CFA82359FE8CB02706294F23CF8
SHA-512:	780ED74811E1303DD46A57ABF3F3BB92311436DBF4E131F956227D482507FD575A62FA935335502BE9B92669B3D15878E5B2D29411335D0CEACA9F42229FAFA2
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":"13272538088150368","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2da81252-10b0-4cd0-b9d8-bb6e4d66dad7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5175
Entropy (8bit):	4.982944979644311
Encrypted:	false
SSDEEP:	96:nGSCmXX9pcKIdok0JCKL84kK41/bOTQVuwn:nGSCw9pcu4KlkK4Z
MD5:	2B55E62BE58934DA63AD04D339DE7F3C
SHA1:	09E973145FC43599B719A1AFCB852D4C7C479F35
SHA-256:	0BB466CB23CA5E6E8969C6CF5DD7208A9833A91C39315B340F1E7E60763BA94E
SHA-512:	7AEE6566082FFCB5A238262C46A3B355BA37E6A06779B37BC2D104DC47D9151CBD0A59FB63D1B778EE114FEC7564229D8F1BFF75C5314872A12C8CC3D7B6F5: 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538088418067","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\33aa13ff-0770-43a7-a30f-6ad79a39ce7f.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):	1372
Entropy (8bit):	5.58325228008032
Encrypted:	false
SSDEEP:	24:YEF9RAeUx6H0UhVrfwUjRjQG1KUgKSACkq/HeUeXby2qUeXvtJ7wUgOiRUenHQ:YYieUx6UUhuUjlKUg+qPeUer2UefrwUP
MD5:	53B2503F2888DD883ED9A4823A95E3D6
SHA1:	1DE740AF4359FC105D502EA005AF4738A16664F8
SHA-256:	01F5196B6229B4EEC63B7F560676F1BEBBD94D0F16A839DE210E18D233C8FA49
SHA-512:	20482C45EA289A2213589A2A58A5F362DCEF72C75C0CCCB3A17E80D7B9AD7B09ED5248CC6539B75EF1A6C8BCEB9C664AA6A90EDFC0CB52219FFA8372B67EE F3C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33aa13ff-0770-43a7-a30f-6ad79a39ce7f.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659600538.387089,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064538.387094},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1638950894.0541,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064494.054106},{"expiry":1659600492.932569,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628064492.932574},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ed574a4-e6e9-4a3f-8f5b-ead68f0fb1db.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42827917-d390-4f01-8dec-dd0d64de8a7c.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):	5785
Entropy (8bit):	5.189199364116199
Encrypted:	false
SSDEEP:	96:nGSC6kac916Wa9cKI1ok0JCKL84kK41/bOTQVuwn:nGSCt9QWa9cG4KlkK4Z
MD5:	8F8654970BF5D660C3463E39575CAC39
SHA1:	3C7CABAE526DB3AFCEC3606AD412A7844CC3217C
SHA-256:	0853D529AA75D221972E16A9C67D925EFE920A79303ADEC915C376FCF30140CF
SHA-512:	723BE33411A9C220B5682B23D10975D745529C0CCD0EF09A50E793DC2C278593878B755A874AFF218028CB648783BD36EA382D8D4F2677A362D410B1FCD3C83F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538088418067","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\4db147fe-274a-4810-83b1-d63c74b407a5.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):	1372
Entropy (8bit):	5.582468088463157
Encrypted:	false
SSDEEP:	24:YEU9RAeUWF6H0UhVrfwUjRjQG1KUgKSACkq/HeUeXby2qUeXvtJ7wUgOiRUenHQ:YLieUw6UUhuUjlKUg+qPeUer2UefrwUP
MD5:	F0D4B87A775685CA41A503C152AFFAFE
SHA1:	78302F7AF8F6A58CEAA4A9FED4037474218F4B68
SHA-256:	388530EA7497097686524B0976C41E94DC8BABEE28E1DCBB7B1C74B63F572D31
SHA-512:	D55B2F48166CEFBD07086C7BD6EDD967BDDA4BD9B2C948CAC253B4229DC6354E10E7C6E5988944F383A12C3EC151AA970824AA1570479A9E7CFFDDF7A04CF 24
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4db147fe-274a-4810-83b1-d63c74b407a5.tmp

Preview:

{"expect_ct":[],"sts":[{"expiry":1659600554.855356,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064554.855361},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1638950894.0541,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628064494.054106},{"expiry":1659600492.932569,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628064492.932574},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5211c6c4-87cf-40f5-b9e6-b22ccfd8ce4c.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):	5785
Entropy (8bit):	5.189099271901682
Encrypted:	false
SSDEEP:	96:nGSC6kac916Wa9cKIiok0JCKL84kK41/bOTQVuwn:nGSCt9QWa9cb4KlkK4Z
MD5:	5FA4053605D456EA9865A01266ED870C
SHA1:	A5F32D8402E1AC0015D0ED7899C43EC935D4AA2D
SHA-256:	6E31FB3AEF8155B605C6981A4BF130BA1C7E24E21BCDE16BE3B1A852B4007A06
SHA-512:	96995B3C5DA83E28C50CDC67A45C61A754DE79B41BF2F5C8EB791C9CDE4B21DF02E85D2D04CB4631874E74E6D39FBCE64EAB533A65DF3FF0C637E2DAD2EC/0F6
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538088418067","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7561d46d-29e3-4ca2-b148-cd39ac1de154.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):	5812
Entropy (8bit):	5.191193494221688
Encrypted:	false
SSDEEP:	96:nGSC6zac916Wa9cKIzok0JCKL84kK41xbOTQVuwn:nGSCQ9QWa9cs4KlkK4X
MD5:	F32C7F6FFAED464294FA1722E3414045
SHA1:	030148B012432A6C57F95FB43576E53A2E8702A4
SHA-256:	81214DCB4C7B0FB40D05B089067407D64D008A6E11621CA1CE257CE87EC7C6FD
SHA-512:	CD3F49B47A4D9BC5BDE9D0D2D2ED08F0180B438521958F06379E56DE84FA04058618E1AF3A06C21DD2DC28191F0D1CDCD4445A1E979ED327A5E87AA7240A28A
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538088418067","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.1674134636576365
Encrypted:	false
SSDEEP:	6:mbhq2PWXp+N23iKKdK9RXXTZIFUtp2RFHvZZmwP2RFHvzkwOWXp+N23iKKdK9RX3:Ghva5Kk7XT2FUtp2RFB/P2RFb5f5Kk73
MD5:	4CA6323D992BF0D9CA17BAAB3AA0422E
SHA1:	FB9465E21268D269AC95AF27D98FD6A099D058F9
SHA-256:	29CF1CE64A400E5D6E88EC0EFE5F8A9BF13B95FEB88711DEA470B3CD45971FCA
SHA-512:	888852BE33D15ED336B233AC4371DDA224158615088B98B8B9400BEF2E7FC28D4488BCE9AC59F9559508CA786848B7871C4A292922736A3A684C9AB502D09486
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/08/04-01:08:24.313 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:08:24.316 3e0 Recovering log #3.2021/08/04-01:08:24.316 3e0 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.oldNT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.1674134636576365
Encrypted:	false
SSDEEP:	6:mbhq2PWXp+N23iKKdK9RXXTZIFUtp2RFHvZZmwP2RFHvzkwOWXp+N23iKKdK9RX3:Ghva5Kk7XT2FUtp2RFB/P2RFb5f5Kk73
MD5:	4CA6323D992BF0D9CA17BAAB3AA0422E
SHA1:	FB9465E21268D269AC95AF27D98FD6A099D058F9
SHA-256:	29CF1CE64A400E5D6E88EC0EFE5F8A9BF13B95FEB88711DEA470B3CD45971FCA
SHA-512:	888852BE33D15ED336B233AC4371DDA224158615088B98B8B9400BEF2E7FC28D4488BCE9AC59F9559508CA786848B7871C4A292922736A3A684C9AB502D09486
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.313 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:08:24.316 3e0 Recovering log #3.2021/08/04-01:08:24.316 3e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.1253857757842525
Encrypted:	false
SSDEEP:	6:mbcp34q2PWXp+N23iKKdKyDZIFUtp2cCNJZmwP2cvzkwOWXp+N23iKKdKyJLJ:Gcp34va5Kk02FUtp2cCX/P2c75f5KkWJ
MD5:	CE8804F6448542D964F975F80FEF0814
SHA1:	8728A16447DB5824296142014E4B4BD8D60A00BB
SHA-256:	5D77617F4E30064D9326ECF097DC4B36A6C2CA8C9617351E5A318D8F06F8860B
SHA-512:	03F79D00E48CD45311F074D823546C8D18B0BF571B6B3ACAE2B112D0229EAA291B8EFB74D7BFD5FBB7C9D9FBD8A4A5973BA3402211803F192F3EE879A4EAF85
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.302 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:08:24.307 3e0 Recovering log #3.2021/08/04-01:08:24.308 3e0 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.oldle (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.1253857757842525
Encrypted:	false
SSDEEP:	6:mbcp34q2PWXp+N23iKKdKyDZIFUtp2cCNJZmwP2cvzkwOWXp+N23iKKdKyJLJ:Gcp34va5Kk02FUtp2cCX/P2c75f5KkWJ
MD5:	CE8804F6448542D964F975F80FEF0814
SHA1:	8728A16447DB5824296142014E4B4BD8D60A00BB
SHA-256:	5D77617F4E30064D9326ECF097DC4B36A6C2CA8C9617351E5A318D8F06F8860B
SHA-512:	03F79D00E48CD45311F074D823546C8D18B0BF571B6B3ACAE2B112D0229EAA291B8EFB74D7BFD5FBB7C9D9FBD8A4A5973BA3402211803F192F3EE879A4EAF85
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.302 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:08:24.307 3e0 Recovering log #3.2021/08/04-01:08:24.308 3e0 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\06b6f943fece6826_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\06b6f943fece6826_0	
Size (bytes):	78088
Entropy (8bit):	6.076234722697117
Encrypted:	false
SSDEEP:	1536:xlmdPDb+KsGR+sLGzjYiq2Bvkj8B6TMUjHdPe6+Ik44vOgeF9dzrL:jmduVGRyjYGBvu8BRUjd26tp4FeF9d
MD5:	EFE02F71694B55BFDCAB0D98532CD62D
SHA1:	AF43D1A49C37F3EF08BF39FD152407BCC778F280
SHA-256:	6D379D3625EA59F2A3E365493898915E5E9DAE0970AFC0634ED2797499608919
SHA-512:	D3EBCAE4287DEA013D0BBCCEC84CF2CC8CC2BB8ED2A3120870CFB68796FFCE64C25540BA27C766FE52FF3A4BEE62382C40938259D23572580184DD9ACF38A98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....>....3B19DA429CE3F7F7BE4174E858B655F9A70EE664C6272A813A58C2F61FFD033C.....'.....O..../..,5.....8.....`.....D.....(.....<.....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R....Qb.....n.....Qb.D8.....q.....Qb.....r.....Qbr.....t....Qbv..<....v.....Qb.....x.....Qb.3.....y.....Qb.E.X....z.....QbV.y.....A.....Qb"R__....B.....Qbz.(....C.....Qb.....F.....Qb.$.H....E.....Qb.w.....D.....Qb.6.....G.....QbZDcX....H.....Qb..B.....J.....Qb&].d....I.....Qb.q.....K.....Qb.....aa....Qb..Qx....L.....Qb.....N.....Qb.\.d....O.....Qbb.r+....P.....Qb..F.....M.....Qb...s....da....Qb...k....ea....Qb..43....Q.....Qb>.e....S.....Qb&.X.....R.....Qb2..a....ia....Qb.#.....U.....Qb.....ha....QbJ0kN....T.....Qb".....V.....Qb.....W.....Qb..=z....Z.....Qbnhx.....Y.....Qb.[.....X.....Qb~.....ba....Qb:..K....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\071f894f5a947705_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.077954872981968
Encrypted:	false
SSDEEP:	1536:43WUVcDcnY7zkwL2W+i5/A793VW4U8tHLqpaIFu+EqvF9dzr3:TUV3Y7z4W+8AxDUsLaB4+RvF9R
MD5:	6E24CD3BDE0A30C830713BEC375F5C65
SHA1:	D055B6F7AE7E6A768615B7DA398903573D049B8D
SHA-256:	99513030808B160D6A16FB1604A0B8558E67CEFE3B950E14934BC79CC7F4883A
SHA-512:	542FC721E46108F77FD3E441C05E1B7ADDD71B751BF9D793E4A9BCD2C0BE27B56C3E2824B18B2ECD4DC2632381F60D909608BDE40E68F22F3047D6E2B055F10
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...w.....8B719A251B1BE4A715EC7A27450A02E5261F8931DB99C1B13D5AC499AC695E74.....'.....O...../.....8.....`.....D.....(.....<.....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R....Qb.2l.....n.....Qb..[~....q.....Qb...G....r.....Qb..U.....t.....Qbr.B\....v.....QbN./.....x.....QbV**....y.....QbF.....z.....Qb.D(.....A.....Qb...`....B.....QbF!.....C.....Qb...<....F.....Qb.....E.....Qb6.....D.....Qb..i.....G.....Qb.n03....H.....Qb.....J.....Qb.....I.....Qb.pW.....K...QbfNF.....aa....Qb..M.....L.....Qb6.\f....N.....Qb.G?.....O.....Qb.#.....P.....Qb.bD-....M.....Qb6l^.....da....Qb..K\....ea....Qb.&.....Q.....Qb.....S.....Qb.....R.....Qb..26....ia....Qb.....U.....Qb&.#.....ha....Qb.~.....T.....QbBl^2....V.....Qbj..h....W.....Qb..'....Z.....Qb.~A.....Y.....Qb27.....X.....Qb...S....ba....Qb2.Lw....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0796d99e6cc73b39_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.416845260671873
Encrypted:	false
SSDEEP:	6:m+YZHfY7tOlopMri6x0l/rhsyH4jZK6t:G/9mac/FsqIT
MD5:	CA29DF386A574D7703602A81ABC6E683
SHA1:	74BB9FA37BDB1FD5977CA91271031E55AC870BD2
SHA-256:	4EE515BB629872F9873337BF2CA220DD858191A9E45D3DA55D06DC711AEB5FE5
SHA-512:	1DD1A02F37B352348A18C342C74E71AFBC4BED29C795EBA22BD5ECAB0320C4D54FAD37B9B425F3DA6B8BB46C4850425FBB6279084161382D2D0698B2DDC287B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]..........._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/controls.js .https://myhealth.net.au/....M'/.....37t.".y-... 1.S.....|..i:.....A..Eo.....&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08b5d8213844f29c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.0758284123629025
Encrypted:	false
SSDEEP:	1536:lLwZ/DtK2eyok2ALe+a9I3QQ6pS7BUBPHBJquIfmJaEqhF9dzrs1:dwZA2foky+aOQpkUBvBc98aVhF9u
MD5:	C8A3E49819755B32D87F53105F07106F
SHA1:	38F567D93397C7ECA068BE3118676A2C98F2CDFD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08b5d8213844f29c_0	
SHA-256:	8B081EEF6BD2A77CCBD7AE435EDFC817BD5E03135E5E4EF268FD4093A72E447C
SHA-512:	BDD1A14A48A75A32FE521022126A998D4BD225F4865F6ADE092DFD4AB3B6577FA54018EC185B416371E27AD6A08D7A23D12EE4FA0CAAE5E722F6F1612F2C5BI 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...')q.....ED2F94566E8636A2A42E4B5C33625CEC9356198BFDE2329BD4C1957C03BBD7D7.....'.....O...../....q.....8.....`.....D.....(..... .....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....QbR..<....n.....Qbz,.j....q.....Qb.....r.....Qb..u$....t.....Qb.Co.....v.....Qb.AM.....x.....Qb. .sB....y.....Qb.%~g....z.....Qb...F....A.....Qb.l.....B.....Qb.....C.....Qb.5a.....F.....Qb:..)....E.....Qbb..d....D.....Qb>W.....G.....Qb.....H.....Qb&..F....J.....Qb.s.....l.....Qb.ab.....K. ....Qb2.)u....aa....Qb.V.....L.....Qb~.'+....N.....QbV*.....O.....Qb.\n.....P.....QbJ=.....M.....Qb.\b.....da....Qb.....ea....Qb.....Q.....Qb..1G....S.....Qb6C.....R.....QbR`.8....ia ....Qbz.....U.....Qb&..H....ha....Qb..D`....T.....Qbj9!.....V.....Qb..V.....W.....Qb.....Z.....Qb..."....Y.....Qb.....X.....QbRd.7....ba....Qb.K.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d3ab7c0ddcf0d50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78088
Entropy (8bit):	6.075742623959917
Encrypted:	false
SSDEEP:	1536:PPSowDsk3pZ9SeLog061wWunDBNxeU8JH2c/IIRJvF9CF9dzri:HSoLaZ9N06HunDBiU852OrDvLCF9o
MD5:	CE9D3FE61D525433B6CB894D84E32D03
SHA1:	379C25FB7E802E3CBDB3974CD12345AD757FB013
SHA-256:	CCB4CF026C712A0353A96FB050C48C1D4C947D69E3ABF3C21100282361BEA107
SHA-512:	002F59EDE14CD36F4EE969E62CF00D702A055E62C504F0748608A6538EBF85B01CBB5539417DD47185EE95A7059B7A8E941706CB7EC333366E9EC571B4D3EC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....._....5DAA2B241B15563FBB3DE67441AE4923B0F62B320462633610AE02648BE5F048.....'.....O...../.....m.....8.....`.....D.....(..... .....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb..n.....n.....Qb...2....q.....Qb:7.....r.....Qb...6....t.....QbR.$....v.....Qb.....x.....Qb.m .j....y.....Qb.. ....z.....Qb.>.....A.....Qb.....B.....Qbf..?....C.....Qb.nlj....F.....Qb..#....E.....Qb...{....D.....Qb*.....G.....Qb:X`.....H.....Qb.73O....J.....Qb..H.....l.....Qb..Ou....K.... .Qb.....aa....QbND.....L.....Qb.kwh....N.....Qb.....O.....Qb.=l.....P.....Qb.../....M.....Qb.7.W....da....Qbf.r.....ea....Qbn.Z.....Q.....Qb.U.....S.....Qbz!aC....R.....Qb>!/.....ia.... Qb"J.W....U.....Qb.D.....ha....Qb.....T.....Qb.....V.....Qb.n.....W.....Qb..%.....Z.....Qb...3....Y.....Qbf.....X.....QbJ.r.....ba....Qb.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fa01bd6516f6f3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4027
Entropy (8bit):	5.496024949680522
Encrypted:	false
SSDEEP:	96:sBHH5JOeindgI+oikUvfeVq16BLydhNlsH:2BIqkGeFByjeH
MD5:	0BB522356ECC43E7BB936F70B0B21CF2
SHA1:	DD4C93705653C65052D01B2C118F90590C90927F
SHA-256:	CD6763AB547DF0A29390A0E08ACBAAB671CB09722512D1BDF1D9F396778C0473
SHA-512:	FA766AC372E83E95503758B3EF0875BEC85E7E00596492788E429E877F559C7888E1CE18990ACBECF5C1D568E7948D19436574CEED6A144FA73230F4ADDD36F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://myhealth.net.au/wp-content/plugins/google-analytics-dashboard-for-wp/assets/js/frontend-gtag.min.js?ver=6.8.0 .https://myhealth.net.au/ .]Q.M'/.....t.....'B....d}lA....":>.f.L....A..Eo.....A..Eo.....]Q.M'/.`.....'..#....O.....7.....(.....(S.D..`D.....L`.....L`.....Qd..i....Exac tMetrics. Qfj'.....ExactMetricsObject...(S....`8.....L`d.....Rcf.....*.....Qb.AS.....e.....M...Qb..b.....o.....R....Qb.2T.....t.....QbBN.....n.....S...Qb>kr.....l.....Qb.nL.....c.....Qb..ER. ...d.....O...Qb...1....h.....Qb.c.....y.....QbJy."....w.....Qb..v.....x.....Qb..?.....v.....QbJ.x.....k.....Qbf#.w....p.....QbN3x.....f.....Qb.Gw.....s...u..... .....Q.`.....a4....G...(S.....Ia.....@.-.....P.....u...https://myhealth.net.au/wp-content/plugins/google-analytics-dashboard-for-wp/ass

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2354ee022fd0e895_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	356064
Entropy (8bit):	6.111297703324335
Encrypted:	false
SSDEEP:	6144:XGprz6R+tSQG8acu2Gvgp0K1hXbQ6bV7553t53zy:WrnMcujvgpprx5e
MD5:	E156D2DF1ABEB7950955D9FF05B0FB79
SHA1:	E532D26396EEA88948A0EA2073D0870E65C84DCD
SHA-256:	9FCAF58B55A450D8D842F5DE37F09F11336B1E4D549071977AC736E5F962F24E
SHA-512:	54DDF9460D3A7DF777CC64432673F2DCC079EEB6792DFCDF0C90E0126A90290C3E943BE2F3E6C1CAA1824DBE456A39EB8116A3090946C4D01C56121886EF91
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2354ee022fd0e895_0	
Preview:	0\r..m.....@.....6.....85E41C21FA369FDBBB387695CBE54A8C535001EB81D57C4E745058F62C12B9D2.....'..X....Oa....I..''..z.....D.....,..... .....I.....|.....|.....0.....<...|.....H.....p.....I..... .....(S.<..`2.....L`.....(S.....`jO.....L`.....E.Rc.....QbBN.....n.....QbF.<.....A.....Qb..ER....d.....Qb.2T.....t.....Q b.W.....P.....QbF!.v....X.....Qb.H4.....Vx....Qb.....Em....Qb.x.0....z3....Qb.6.6....iv....QbR../....UQ....Qbf.....dr....Qb..}.....dL....Qb.....Cy....QbR.....aT....Qb.....K5....Qb .....IY....Qb..~....cY....Qb...:....X1....Qb.@.....Ms....Qb"?.....Ck....QbZ.~!....Vz....Qb._.....SK....Qb..{|....OS....Qb.$E.....i7....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a4e046e36fb3782_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3080
Entropy (8bit):	5.717817220389283
Encrypted:	false
SSDEEP:	24:/tBb+ptBbNZtBbqNWztBbWiePtBbW4utBbGHOtBbLftBbzstBbX9/+tBbE2tBbTz:H+BNR2mnkW3GHqLnzwX9yEiT00fQbsH
MD5:	E19CD9AFC9E8BA9C58B140A81CAA1E64
SHA1:	3E1D1BA2FE062452B387222906BBE49FEDA0B6BA
SHA-256:	633CD40EDEBAC7D907182283554ECFF5D35E15CB4D8EF1C128238FD58FFB87B8
SHA-512:	13C7D4CF0B31F715BB449ADB827EE49797DE9E1E96D6F16642E59EBA6E41C427478A29726453DD98DDCCF767F8EF4E41C5937758E01BC032708A8529373DC85
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....1....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-64917910-13 .https://myhealth.net.au/O.L.M'/.....n.i|..%.?....]".....h....e..A..Eo.....)..,.....A..Eo.....0\r..m.....X.....1....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-64917910-13 .https://myhealth.net.au/Zq%.M'/.....k.....n.i|..%.?....] ".....h....e..A..Eo....._.....A..Eo.....0\r..m.....X.....1....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-64917910-13 .https://myhealth.net.au/..^.M'/..... .....n.i|..%.?....]".....h....e..A..Eo.....h.....A..Eo.....0\r..m.....X.....1....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-64917910-13 .https://myhe alth.net.au/f.M'/.....n.i|..%.?....]".....h....e..A..Eo.....s.....A..Eo.....0\r..m.....X.....1....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-6 4917910-13 .https://myhealth.net.au/i...M'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2af32d91d4628217_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	363
Entropy (8bit):	5.94413371515373
Encrypted:	false
SSDEEP:	6:mhPYmIfIQKDTcpLilA5sDEdXK6ttlEUdgGBn5DE6/:vfIQKDTcp7kAinGRx/
MD5:	075D64FE8C9E4B36F2FD59103B9F7066
SHA1:	8C33B59F29784E30AC46A2B85AAD40F81D39468C
SHA-256:	423A60A079E9EC865E167CFDB65C9E4F8796B3976098D0945927DC69690E2886
SHA-512:	E4CCBB74452DB134B7F7C923DE0992281E076DC4A114926B5C1C729FA3E90A99672B4D7BE4B2E5D457BC1832175A5C22AB0B75A9E6CE005E036E92B838FBBA D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...i....._keyhttps://myhealth.net.au/wp-includes/js/jquery/jquery.min.js?ver=3.6.0 .https://myhealth.net.au/.]Q.M'/.....P..\..`.#....p.4t."..''C.A..Eo.... ....h.....A..Eo.....]Q.M'/..~..03C4F06D54903379235FDF81130364791A04C41822244093FF514EB449D099EE.....P..\..`.#....p.4t."..''C.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b94473d5686c857_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15819
Entropy (8bit):	6.045834253244999
Encrypted:	false
SSDEEP:	384:Vv23AR1vmObR7FrRlHP9UOinCIypFoxXUauzJvhVhG8iCF:JUOdlHPzgt4G8B
MD5:	4D29722C7FC684FD755ADE9B3D6CFA72
SHA1:	0F591DEE923533046BB3E0F52EF5191D59F3449F
SHA-256:	2110B89F9D83DB36D5723ACAAF95030A65EC4DCDEB09E8081790E65F0580A24C
SHA-512:	86FCC665396BE30B5EF71ADA7F63DCA8D55ADAFD2BC70D5BB6405EA48EC7838CC7367D6B4BD45E46469931F767C4F3EE20BED338CF4C7DC695259FAB7606B C14
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://myhealth.net.au/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 .https://myhealth.net.au/.]Q.M'/.....]ud~...0..2.z.%g.].:w,...{. A..Eo.....r.....A..Eo.....'..+....O....0<..]x+T.....T.....8.....(S.P..`\.....L`.....Q.@.....jQuery....Qd^.....migrateMute..(S...`.....4L`.....0Rc..... .....Qb.2T.....t...`$...I`....DaR.....Q.@.Ij.....define....Qb.....amd.....`.....M`.....Qc...\|....jquery...(S.....Ia.....I.....@.-....\P.a.....M...https://myhealth.net.au/wp-includes/j s/jquery/jquery-migrate.min.js?ver=3.3.2...a.....D`....D`$...D`.....!....`....&...&....&..A.&.(S.....`.....L`n....Y.Rc.....L.....QbBN.....n.....Qb.Gw.....s.....Qb:.....r.....R....Qb.. b.....o.....M...Qb.nL.....c.....Qb..ER....d.....Qb>kr.....I.....Qbf#.w....p.....QbN3x.....f.....Qb.c.....y.....Qb../T....m.....Qb...1....h.....Qb..?.....v.....Qbf.....j.....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c7acdd10ffafea6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	373
Entropy (8bit):	6.045660603633504
Encrypted:	false
SSDEEP:	6:mpDl9YGLKdXNQKVQGHtiKQGjRuxA5gmdu34p4inK6tS+hV8KVkHAamdu34p4X6:e2hNQKLtiKQGj8xsgIu347o+T8KunIuG
MD5:	B4698F8ED441042A44C7EF910D45E214
SHA1:	81C642387577A646DB69A861D64BE93C458ABB2A
SHA-256:	1907D10BB7E0287977241CB292B7BAEDE137F9382A2944A12917F0AA6AF52C04
SHA-512:	4119BF42152B2F85ADD2C69060AA3841D5844DDA0F9550541AC8A65B1AC6CF6A0350759FFF563E26E755EC9D0B7AA6019E5E96EC204D608AF1D23AA836B2550
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m.....O...._keyhttps://www.gstatic.com/recaptcha/releases/ecapuzyywmdXQ5gJHS3JQiXe/recaptcha__en.js .https://google.com/.H..M'/.....=k...5.....>...(...;.R.].T.K.v.A..Eo.....4.....A..Eo.....H..M'/.....2C8528466CAC216B4AD9164027B14F2F9E4D96A373854C8C3BA2E328CFE8FA42.=k...5.....>...(...;.R.] .T.K.v.A..Eo.....>.h%L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\466c3b9f699ea0fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	79664
Entropy (8bit):	6.07810286564282
Encrypted:	false
SSDEEP:	1536:UHIUpDE6qQwK+LMc9KB5D5A1iiv+8uxUZaIVUmaOF9dzKE:YIUqnQwKhcu5Desiv+bxkBVUbOF9N
MD5:	488FCA5EF005DD92848176F45AD12C63
SHA1:	2974E7CA72F17E75ABB6643565FF71B03D839826
SHA-256:	5403F2AC6E1EF218A1DDBAC52ED6B5A072B521E26350F4A589679577DD275990
SHA-512:	7B6A2E39090D5A9166C8BB37622CF66FC5DBC05ED75352D4E8C7907ECF9918D8922C804EC1554A0D127486C75F5DEFD859485B6C28BBC0EEEC2535888D095A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....9A13C37DBDBAE6D813D636A066D317CB170688632A9ED9D8D387726C7B4108DB.....'.....O.....5..7.....8.....`.....D.....|.....(.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.....n.....QbB;.....q.....Qb2.....r.....Qb.....t.....QbzM.....v.....QbfpDq....x.....Qb....y.....Qb.>U.....z.....Qb...B....A.....Qbr.l.....B.....Qb.7/.....C.....Qb.Y.f....F.....Qbb.....E.....Qb.....D.....Qb~.f.....G.....Qb*.....H.....Qb.}.w....J.....Qb..s0....I.....Qb..zz....K... ..Qb.3.P....aa....Qbv.....L.....Qb.5.T....N.....Qb.y.u....O.....Qb~.....P.....QbN.....M.....Qb.M.....da....Qb.....ea....Qbfy.....Q.....Qb...B....S.....Qb..w.....R.....Qb.=.....ia.. ..Qb.6.....U.....Qb...Q....ha....Qb.....T.....QbN.U.....V.....Qb.($M....W.....QbN{.....Z.....Qb.....Y.....Qb.....X.....Qb.!.D....ba....Qbz..%....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\493250e010a29c82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16612
Entropy (8bit):	4.9176002072506
Encrypted:	false
SSDEEP:	192:V07F5Ib9jF8lPV4yTr3gH5PmJnj23tqFHGqsP7q7JUqCfhfuPTb9Uh31//bEvXbo:Vi5IZSxV4VuPTb9Uh31//bEP+XgA3b
MD5:	616E2C7FE79846B6EE66FA10F8F95CCD
SHA1:	B074A7B6078EC4B279F3897DAA7F6D60DD157F47
SHA-256:	944487FC398A83EA0402BDC6A4E4BD15755C2718076F24A74BBA2E55013E9B53
SHA-512:	8E7C618A25C4E462E33A97BD9A4B5A0F23367683106175668AC06A18742749FE7BA7BCF0070A312B362B31273B83AF6A826E907EF519842E8F8684BCAA6B14CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://myhealth.net.au/wp-includes/js/wp-emoji-release.min.js?ver=5.8 .https://myhealth.net.au/ZEb.M'/.....=.....m..-._.$.....=..u.-{.s.d. 3...A..Eo.....y.....A..Eo.....'..G....O....X?.....1.. .....(S.\..`n.... L`.....L`.....Qc..5.....twemoji..(S..`j....xL`8.....RcL.....QbN3x..... f.....R....Qb../T....m.....Qb.nL.....c.....Qb.AS.....e.....Qb.2T.....t.....Qb...1....h.....O.....M...Qb..v.....x.....QbBN.....n.....Qb:.....r.....Qb..b.....o.....S.n..... .....I`....Da.....w...(S.....Ia.9..!:.....@.-....TP.A.....F...https://myhealth.net.au/wp-includes/js/wp-emoji-release.min.js?ver=5.8..a.....D`....D`....D`.....|..`:...&...&.. ..&.(S.....5.a.....q....a.....a.....Qc.....convert....a.....Qe..\.....fromCodePoint...a....].....d.....@.....&.(S.....Pd.....f.onerror

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53d8e1befd8facb4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9700
Entropy (8bit):	5.715488874176358
Encrypted:	false
SSDEEP:	192:Qbfa5aXaWS/EaPVSmRe8xv/VuHAPKg6Py8BEwPHEP:afyaXPS8SS8e8ZM2Ky5wPa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53d8e1befd8facb4_0	
MD5:	56FD7CF3FBC2B9384CC97D658D628DFD
SHA1:	D84F5CBFF689CFF1202FE460C96FB1ADAAFE3256
SHA-256:	2D7A3DB1A2AAAB29B08A94BE51E1C7257189D8350EA3B633255F67E5725DC0DF
SHA-512:	8DF25BCAA99982D2522CC0F5D0C05EDF77BD39CDA8745BFF289CCEF293473AB464FC8214DF7735DC1A02BD1BC6FB66B09E3634F4CCD027D762162CC4140058
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...b8....._keyhttps://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap-select.js?ver=5.8 .https://myhealth.net.au/.^Q.M'/.....hc.. ..7^^.2...x$V.w..Q.....A..Eo.....A..Eo.....'.....O....@$..w..x.....(S.4..`$.....L`.....(S....`x.....L`.....XRc(.....Qe.^e.... .normalizeToBase...QdV. "....htmlEscape....Qd.;.....Selectpicker..Qc...W....Plugin....Qb...t....old.e$.....I`....Da.....(S.....Ia....$.....d.....+.,..@.0.....@.-.... IP.....^...https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap-select.js?ver=5.8..a.....D`....D`....D`.....i....`....&...&....&.(S....`.....4L`.....<Rc..... .....Qcb}.....indexOf.a.....I`....Da.....(S.\.`r.....L`.....e.. Rc....J.....Qc...8....error...`.....$..Kd .....%...9.....Dq@.....'..~&....&.(...&.'..'.'..[.....%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d0a4b3fe700e127_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3786
Entropy (8bit):	5.882721467310435
Encrypted:	false
SSDEEP:	96:5KO0zw3LM0xqj/NgFOqDXI6FyuvsKv+ekOn/l:5p8ww0xIGOqD4WyysKGOnt
MD5:	AB0B2D8ABB947C1791D5C522CA8444FF
SHA1:	E28A0D697EEA0D4FEDC378DBD4FED67CDDC9B475
SHA-256:	74960DC33FC8FB9D70814D8CC098F95D18C34E12D708BA48B4C4BCD2AC9C5A20
SHA-512:	5B7DCFD6F485D97E6BA51BF99B2865A559401EA677045FF3CA217FBF3B912EF840530B47FCBDD31293BE32F8763DAAFFC32E186075ADBDCB37ABB8B0C2CDECBF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r.....a...._keyhttps://myhealth.net.au/wp-content/themes/twentysixteen/js/functions.js?ver=20181217 .https://myhealth.net.au/..^.M'/.....F.....W....2.!.jKj. ..U."`..f.t..A..Eo.....F.;.....A..Eo.....^.M'/.....'.....O....P...^v.....8.....(S.4..`$.....L`.....(S..`f....HL` ....pRc4.....Qb...7....body..Qd.n.U ....menuToggle....Qe.iU^....siteNavigation....Qe..@.....socialNavigation..Qe.1?.....siteHeaderMenu....Qd.....resizeTimer...Qd.~.....onResizeARIA. Qf.eP.....belowEntry MetaClass.h$.....I`....Da....J9...(S....`.....dL`.....Qdv.....<button />.....a.....Q.@f.....class.....Q.`B-.....dropdown-toggle...Q.`.#.....aria-expanded...H. .Qc.....append....Qc.`........a..... Q.p.g .....screen-reader-text....Qb.~W.....textC..Qe..E.....screenReaderText..Qc.H.....expand.....Qb*;.....find.(Qh... i.....menu-item-has-children > a...Qc...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\65824dcf8e361a4f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98104
Entropy (8bit):	5.815655583256716
Encrypted:	false
SSDEEP:	1536:DWx3pGQRQAX6iwmakgpIIZpnRuWAb71p2m3Aw9PwpBMqU/:AIwn5PaHPU3913A64g
MD5:	E08D6ACA1078525CE26FCBD3AD4C4712
SHA1:	22C51BF2B22F4821D968C1840C9E9F743D2DC49F
SHA-256:	17BDE64DAD361ACB90097A32CCA905536CE80EA7698444C489B5BA9C3EE2C3FC
SHA-512:	99D5F6488FFC8DF0F7C4F801073112F8F59B8F50F6760DE0C4674CDA9354B50068825FAB3645B240D67E9CC8B9C8E90890340364C077F415C2E0EEF5A387BD61
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...1.....03C4F06D54903379235FDF81130364791A04C41822244093FF514EB449D099EE.....'..]....O!....}....]]..@&..... .....(S.X..`h.... L`.....(S.p.`.....L`.....0Rc.....Qb.2T.....t...`....I`....Da....r.....Q.@.[.....module....Qc2.8.....exports. ..Qc...H....document.(S.....5.a.....Q....a.....a.....a.....a.....Pc.....exportsa....3...I..Q..@.-....TP.A.....E...https://myhealth.net.au/wp-includes/js/jquery/jquery.min.js?ver=3.6.0...a.....D`....D`....D`.....`....&...&....&..A.&.(S...A&..`:L.....L`.....Rc\.....&.....Qb...5....C.....Qb:.....r.....Qb.Gw.....s.....R.....S.. .QbBN.....n.....Qb..b.....o.....Qb..?.....v.....M...Qb>kr.....l.....Qb.c.....y.....Qb../T....m.....Qb..v.....x.....Qb.....E.....Qb.nL.....c.....O...QbJy."....w.....Qb.....S.....Qbf#.w....p.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b8b2ac2453f0389_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78088
Entropy (8bit):	6.076458107437041
Encrypted:	false
SSDEEP:	1536:Z1vdv4DACGIYBhxkLWMMhW5pHHHgBbU1AH6XMLsIZ9CHWpF9dzrh:zdv2GbBhPMMapHHGUUqWHPC2pF9X
MD5:	0C25031DE8FE09B4AA297EE6AB8B5177
SHA1:	D803A1DCD1077940476956BBBC3A8D70430D594D
SHA-256:	273A69E998F47B64DB7FEC4E9B22FE21ABAD4A8D3E8E6649B48E29AB156207DB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b8b2ac2453f0389_0	
SHA-512:	12B03195D4A12B1FFA3BCC65BC3AFD63F53A3A34336D9EF83A9B2E2195ADD9C352FDB1D44EC77E5AF49DA28441257655F04E1E66FF8C215768EFEC762C81B5B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....r2.....D015435DC9309DA7C299AA2E49FCC78305AA72EBB65067108DF8910C11E27B3A.....'.....O..../..#.....8.....`.....D.....(.....<.....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R.....Qb"..._....n.....Qb.A\....q....Qb>.....r.....Qb.>.!....t.....Qbr,.....v.....QbRw.>....x.....Qb>.....y.....Qb..A.....z.....Qb2.....A.....QbF~ .....B.....QbV.)I....C.....Qbj./F....F.....Qb.(x....E.....Qb..O.....D.....Qb..Cm....G.....QbF.....H.....Qb..J.....J.....Qb.....I.....Qb.02.....K.....Qb6qr5....aa....QbR..J....L.....Qb.%.....N.....QbZx.....O.....Qb..o....P.....QbvSI,....M.....Qb.....da....Qb.+.....ea....Qb..su....Q.....Qb^.$.....S.....Qb.v.=....R.....Qb.1U.....ia.....Qb...q....U.....Qb.....ha....Qb.....T.....Qbb."....V.....Qb..6.....W.....QbnL.(....Z.....Qb.:.....Y.....Qb.Dn.....X.....Qb.....ba....Qb...Z....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c65571643f71d1b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6174
Entropy (8bit):	5.713753030398343
Encrypted:	false
SSDEEP:	96:LjjE4OvW792vXL99mhDvPfXnZHQH1XZtlZC2D7y19KymGhmGH:gZO7svW9vPfXSH1XBOLrmGH
MD5:	C5D7CE5738C70C51ECFC1E5A2D60B0D9
SHA1:	30C123933EA320F353E03FE9335FCC0D035125E8
SHA-256:	11A9BF3024566F8F2A5C312F53D5BF255C9EE111A7E390AEC424FE18727E52ED
SHA-512:	36DC99BDD4576734A79905536300B020CDE4655DF57B5AC4721CC521E4F816839EC002A7FFBF6AF9285B24CC35FFB41A1D8300CB4FC9680709C32F59BCA6D91
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...Z.{....._keyhttps://myhealth.net.au/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.7 .https://myhealth.net.au/C.^.M'/.....8.....C.#....(.S.G.K]:...#...p.....A..Eo.....z.....A..Eo.....'.....O.....(S....`.....0L`.....L`.....Qc.=n....runtime..(S....`:....-.L`.....Rcl.....M...R....Qb...1....h.....QbBN.....n.....Qb..b.....o.....S...Qb.nL.....c.....QbN3x.....f.....Qb>kr.....l.....Qb.Gw.....s.....Qbf#.w....p.....Qb.c.....y.....Qb..?.....v.....Qb..ER....d.....Qb../T...m.....Qb..a-....L.....O...Qb.....E.....Qb>..K....._.....Qbf.....j.....Qb2.`.....O.....QbJ.x.....k...v$.....l`....Da(....1...(S.L.`P.....L`.....e.,..a.....C...G.E.G...G...K`....Dm(... .....&.(...&.}..)&.%./...'..'..W....%.*.....,Rc.....S.`....Da.....q...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d34ed706fadbee2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78088
Entropy (8bit):	6.078592903168657
Encrypted:	false
SSDEEP:	1536:sSPX8Dj5lXlEMVLcULpxvYdNFUUOHdP5w+IwqvhMfF9dzrb:FPXyllEXULnYdkU8dxGzvifF9h
MD5:	791AA35AA3C733D9377B2988FDBD0EF5
SHA1:	4FCFF883ACB33334B53A33C1F57C63C9DEE3131D
SHA-256:	C6D6C3A0E1C082733DDCC6071A75EF487276CB3A29BEB2B975F83547F488256E
SHA-512:	FE8DC1B1753E0E385497D1AB6CA34DC55E33B9D51E49D53E52A7CA78BD3FF49AE527438E4C8561FA23E645021AA65DB6930D3CF8DF25466000F45ECB20F5DD4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....N.b....13D8233A820276D98F41C1AA996BE135E385FC2F8C5F39BACDFBEA50D303DD81.....'.....O...../..b.....8.....`.....D.....(.....<.....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R.....Qb...I....n.....Qb.....q.....Qb.X.j....r.....Qb.....t.....Qb.....v.....Qb.....x.....QbnT.g....y.....Qb...!....z.....Qbv.4....A.....Qb.:.....B.....QbR.o.....C.....Qb.4.....F.....Qb..\.....E.....Qb.!CO....D.....Qb.J.c....G.....Qb..-....H.....Qb.-.....J.....Qb.....I.....Qb.'5R....K.....QbV5F.....aa....Qb.....L.....Qb.K.c....N.....Qb...*....O.....Qb.i .....P.....Qb.5.....M.....Qbr:.....da....Qb.....ea....Qb.....Q.....Qb~..6....S.....Qb.Y.j....R.....Qb.....ia....QbJ.....U.....Qb.Q.0....ha....QbR}.....T.....Qbv..G....V.....Qb&.p.....W.....Qbz.4....Z.....Qb._-n....Y.....Qbj7.....X.....Qbr._.....ba....Qb.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71663acbf944c615_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.407782554639262
Encrypted:	false
SSDEEP:	6:mn/lVYZHfY7tU78ewh16CXZLrcTCXKnK6t:KtE/byXXZHc4C
MD5:	A78457593751EEE78F8960A0D94030DC
SHA1:	248C7D4C5C03C281958522C9608F962394A143D5
SHA-256:	53013E871C67B3E5040F62EE7045689319DAAE7441C3553D77D9849F06A1C99C
SHA-512:	77C87F54DE167B75798586E8D6A906DF0EE873DE095615CD0C84E73E40D8EE50BD6D405DD81D9ACB0FF3DCC414523753FE66E87446BDF067BA69D4D271CCC9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71663acbf944c615_0	
Preview:	0\r..m.....`...G}tN...._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/places_impl.js .https://myhealth.net.au/`...M'/.....Ay.21.Q.Y.Q.wu..y...d.....D4.r...A ..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71b254c1e13c2448_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22289
Entropy (8bit):	5.701670974785768
Encrypted:	false
SSDEEP:	384:RyxjPeHWZgTZGwkxCkx02GPyt4UDasiiKT5GLoZLJ:8xm2oZKxC60X8usir5cc
MD5:	751E9B02379D693CEAB274240B82F329
SHA1:	6556A0E5D6C50E6AFA6B23D59844123EF481507A
SHA-256:	8BB9318476CEF79BD03AA5BD7698FDC0AD7BC5B2E403F9DDB32783EA41FFA3A6
SHA-512:	D87E53BC8F1A227ABE75286C259FA445310525950F09F87C003848A44BF78675BA3590B50295A5F67554AF1A931CEC293F27E4669027BE4920C9DDE384C56245
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....)....._keyhttps://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap.min.js?ver=5.8 .https://myhealth.net.au/.^Q.M'/.....i.....%. |..VN6..`..f...y.f.`....A..Eo.....A..Eo.....'.....O....`U...*.*.....L.....(S....`.....HL` .....Q.@.....jQuery.....4Qk>...&...Bootstrap's JavaScript requires jQuery...(S...`0....$L`.....Qb..\....fn....Qc...\....jquery....QcZ[.d....split.....K.....dQwV.V:X...Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4..K`....D...(.....(...&.(...&...(...&..Y....&..*..&.(...&...&.Y....&..*..&...i.....*..&...i..8..&..*..g.....&...*..g.....*..&...i.....*..&...j..... &...&.%.e..."".....(R c.....I`....Da....t....$..g$.....P.. P.. ..."..."....@..@.-....hP.....[...https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/bootstrap.min.js?ver=5.8.a.....D`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b3833bf046cbf73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78088
Entropy (8bit):	6.078891012616598
Encrypted:	false
SSDEEP:	1536:6ZKkgDcg6rEmpcL+IoSE54XfyKUfSHoBNLhIgbzXQRRF9dzry:IKki6EmTIoz4XnUooHuezXqRF9c
MD5:	36ECAAA7EC520AC6600203E9551CB483
SHA1:	A059BD543B98C7E4EDF1D4E55BCC162CF9A3D1C3
SHA-256:	1962F5C73CC68F509E6BAF9C140368206EE4985DA9B146AF2F9715E3753951EE
SHA-512:	2F81F1F1A2987A6D57DC94710276D6F3E2BE8F2A25D3476398D47FA0CF8067AA02F40A601CEDAF40616FF91CA69B224B4FFB15FD0151070BEDDBB7C16D95342
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...%.X.....8411F56708FE13A53AA7B5CB2323B6F5831F7DBC3D7E5AD67D0C8C4A2628B5B3.....'.....O...../....e.....8.....`.....D.....(..... .....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....QbBN.....n.....Qb..!.....q.....Qb:.....r.....Qb.2T.....t.....Qb..?.....v.....Qb..v.....x.....Qb .c.....y.....Qb..iL....z.....QbF.<.....A.....Qb.._9....B.....Qb...5....C.....Qb*{T.....F.....Qb.....E.....Qb.....D.....Qb.i.....G.....QbR.mY....H.....QbN.l.....J.....QbZSq.....I.....Qb..Fo....K .....Qb..a.....aa....Qb..a-....L.....Qb.....N.....Qb2.`.....O.....Qb.W.....P.....Qb.}Q$....M.....Qb~D.6....da....Qb..Sk....ea....QbF..L....Q.....Qb.....S.....Qb.....R.....Qb.x^.... .ia....Qb..CU....U.....QbJ.....ha....Qb.kf.....T.....QbbL.....V.....Qb.V.....W.....QbZ.....Z.....Qb.....Y.....QbF!.v....X.....QbJ..J....ba....Qbr<.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\805d5db99720f502_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	79176
Entropy (8bit):	6.075184637362282
Encrypted:	false
SSDEEP:	1536:UZaTwqDXRtD+lLrkNgNruj8jn9l6VhlyIWbUkhF9dzYRk:uaTw+nDCkNWuj8j9QVH5WbzhF9Si
MD5:	239E5987F64ADFE83CE6820C524FC346
SHA1:	AA38F01AFFE3F0D67B7E2E1C5137F055E48076BA
SHA-256:	D7A04C9DC7DF3C23357A72E116B6D618485985E3A55A4CF8DA13FC9017B60FAC
SHA-512:	C8749735648088F15C3AC6B3B81C3301DB36F2A3FE4D63E3C378CAE487649011D6F6872CE0F351EF48B60F0CBECFDA468D4420254DDC09C1A17646B7231ADB7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...G..{....2969C745EA878B1D7E6CA8566B4BEB7D2ACFEE2BF5A9942982F72E7C21CB13A0.....'.....O.....4..U.&.....8.....`.....D..... .....,.....|.....(.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.....n.....Qb.....q.....Qb..[....r.....QbRN.-....t.....Qb6.....v.....Qb.;.$....x.....Qb. >.....y.....Qb.W.....z.....Qb..'\....A.....Qb..).....B.....Qb.....C.....Qb...g....F.....Qb2.....E.....Qb..h.....D.....Qb.r.?....G.....Qb.....H.....Qb".7P....J.....QbZ.Ur....I.....Qb.>.&....K.. ...QbJ.....aa....Qb:.....L.....QbNeF.....N.....Qb..kP....O.....Qb..,.....P.....Qb*.....M.....Qb...G....da....Qb>.wl....ea....QbboT.....Q.....Qb>IA+....S.....Qb...s....R.....Qbz.~.....i a....Qb>.....U.....Qb..Wk....ha....Qb...S....T.....Qb.....V.....QbJa`.....W.....Qb.....Z.....Qb..(.....Y.....QbBS_0....X.....Qb..D.....ba....QbF..E....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88ffe91f0b68a64f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88ffe91f0b68a64f_0	
File Type:	data
Category:	dropped
Size (bytes):	22724
Entropy (8bit):	5.670931842562697
Encrypted:	false
SSDEEP:	384:sJ1rfP4eq14/QeJgGEcbBjTNArm22xK7jc0OipFLemNv1/ZSwZK8G:KIeq14/QeJgGEcb9BArm22xK7nlh91/Q
MD5:	949D8A7A7B3EF4DBCDC7C0B10EAE41E8
SHA1:	F2C0EE25AB6461C65ACC0C0A66A28842C3E81648
SHA-256:	8CEBB55C845B149F7717995A26934C2B85114910BE1875483FF3E485C1882480
SHA-512:	22B06779F617344A337744D769AA2936CA4C7743E8C1CD8253BA60D8F9C37CEBB90E24FCCB680EA4B9FF50667D1508639852AB2366ABC7799C4F26DFD0C8D8F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....2.U...._keyhttps://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/owl.carousel.min.js?ver=5.8 .https://myhealth.net.au/.^Q.M'/.....xO6..S.?>o].tw..:..w.$...lu..A..Eo.....e.....A..Eo.....'.6.....O.....W...5e.....(S.....`b....@L`.....(S....`.....i.L`0....PRc$.....Qb..ER....d.....Qb.nL.....c.....O....M...Qb.AS.....e...d....$.....$.....I`....Da`.....(S.....Ia....6....$..g.....+...*.@.-.....IP.....^...https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/owl.carousel.min.js?ver=5.8..a.....D`....D`....D`.....M....`....&...&....&....,.D&.(S.....5.a.....+..Pd.....Workers.runap.....Qb.8.V....run....*...-d.....&.(S.....a.....Pd.....Workers.runa.....>..d.....&.(S.....a.....Pd.....Workers.runa8...d.....d.....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f0bd0e67c5758f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3080
Entropy (8bit):	5.692155127298148
Encrypted:	false
SSDEEP:	48:13ypz8zVPzRwxzuCzczZ0Kzb4z6KzfzUzh7zbz9:vrJ
MD5:	3197C6385F1C54CADCCF067DE2131E49
SHA1:	410F09D6D1BF1B70EBDED4FF6B8807541D67B122
SHA-256:	B859A59CFB607A6F55DF767714C93548F8CEEA4FB63548802721136F10FA8AF1
SHA-512:	FF768B6779C6544EC5B59C34E6DA2472B043827C26BD34E852E029260A0FA87B3238474ED342AC7B4717129D42F3D576FCBE5D1A01AAADE2FAD548CD7FC455(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...+N6....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1 .https://myhealth.net.au/.2\.M'/.....3 ...zn.....J..qF5.....*.A..Eo.....P9.....A..Eo.....0\r..m.....X...+N6....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1 .https://myhealth.net.au/..).M'/.....3 ...zn.....J..qF5.....*.A..Eo.....*T.....A..Eo.....0\r..m.....X...+N6....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1 .https://myhealth.net.au/..a.M'/.....3 ...zn.....J..qF5.....*.A..Eo.....+.....A..Eo.....0\r..m.....X...+N6....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1 .https://myhealth.net.au/0...M'/.....3 ...zn.....J..qF5.....*.A..Eo.....v.\.....A..Eo.....0\r..m.....X...+N6....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1 .https://myhealth.net.au/....M'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fc8f3536e4d4cff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.078204522274884
Encrypted:	false
SSDEEP:	1536:NkBWxDDKEAViIXa5LOWb1v0GQfNOeUIHcj1uIflbgh2F9dzrO:OBWFKE6iIXeb1dQf9UmcZ9gby2F90
MD5:	A6C6C8345E5ACAD5272C4F4C48ED93B1
SHA1:	38D0E745026F140DC974507293D333545414C3F2
SHA-256:	26D593EC9C89513351227B80066DA428B88F6CA776741DDBF08C8753F8431347
SHA-512:	E5716BE51BEC39560A9AF4D915B405C35A04614C9A284B527F04BBCAD82DABCCCF1FF1E06287C3C787F4460C6A4599DC0857BF9E2CBB3CD7FBBFFFBA8BE7E668
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...%.....E7576EEBC4B6D068707D7DEB1CC583FB0020A2C435EFB204B5BEED3EBE40FEA6.....'.....O...../..v..x.....8.....`.....D.....(.....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.....n.....Qbv..S....q.....Qb..>....r.....Qb*Z.v....t.....Qb.....v.....Qb.t).....x.....Qb.:.....y.....Qb.Y.v....z.....Qb..9....A.....Qb.K4o....B.....Qb.....C.....Qb...I....F.....QbV.c$....E.....Qbb$i.....D.....Qb:.....G.....Qb*..G....H.....QbF.`.....J.....Qb.o.....I.....QbrHvm....K.....QbVz.....aa....Qb..."....L.....Qb.:.....N.....Qb...K....O.....Qb~Hpm....P.....Qbf!.....M.....Qb~.U*....da....Qb.98l....ea....Qb..ID....Q.....QbB.R.....S.....QbJ.....R.....Qb..J.....ia..Qb..9.....U.....Qb.~m/....ha....Qb...X....T.....Qb"c.....V.....Qb..,.....W.....Qb.%.\....Z.....QbzC.j....Y.....Qb.....X.....Qb.....ba....Qbr.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99be34e0a00c26f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.488322553396402

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99be34e0a00c26f4_0	
Encrypted:	false
SSDEEP:	3:m+lzFOA8RzYCJhmHfor7Rf/Rz2QIzfK1lHCp3sXPZbEYim6gk1lpK5kt:maFEYZHfY7t/pYrK6p8fZbLkRK6t
MD5:	3AD299E9FACC9EED0549355D91796024
SHA1:	288A52E905336B88E40EEC677A672AD1FD5C742A
SHA-256:	3FB0FBA9246A26493656EBF349145C1452E429CA8FFFFFD9C63A36ADC24F2658
SHA-512:	C87AFE02D5B242BFB8522E1D0E75D148A649016E525317951FD6B70358ABE6E5325C6721A83604819B2889DA3C881FF0D29F969C1A209485F511AD6E6332D3BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...7....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/util.js .https://myhealth.net.au/.#..M'/.....v.g;..3.....).8E.P...V.j....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a0da0ebbeb01bd01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	5.831150253036404
Encrypted:	false
SSDEEP:	24:pT/rMutNWw0w55R5lyufPS7X+FTtpUyXc9zLDevwq84BeNn:pT/rfbWlE5D4GPScTls5LDevxoNn
MD5:	3F06216E0D5CCF80C712B5CACB286171
SHA1:	6591C25D63983A3BC5C623DD60B78E64777A20B4
SHA-256:	F0DAEE4BB4C931422CCA869AD9C59C50823420C3EA75A7773B97F3C9A4705CE2
SHA-512:	C34660D34477899611FD744FA678075680FB97961A2DD7D3419EFA1AD71C739EA96EE5743857E2986C8AA60A69969B7ED761FCBFAA5C14057CC693031143FBCE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|.....6...._keyhttps://myhealth.net.au/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20170530 .https://myhealth.net.au/9.^.M'/.....B.....PD.K S.._<...I.....q..._(...A..Eo.....^.....A..Eo.....9.^.M'/.....'.#.....O.....c.....P.....(S.0..`.....L`.....(S..`.....<L`.....Qd^v.....navigator.....Qd.y... ...userAgent.....Qd...h....toLowerCase...Qcb}.....indexOf...Qc.ck?....webkit....QcZ1x.....opera.....Qb"5.K....msie..Qc...H....document..Qen..x....getElementById....Qcf.. .....window....QeR.....addEventListener..Q.P.qn.....hashchange...(S.....laB.....IE.@.-....lP.....^...https://myhealth.net.au/wp-content/themes/twentysixteen/js/skip-link-focu s-fix.js?ver=20170530..a.....D`....D`4...D`.....`....&...&....&....`....DI]d.....K`....D.q.@.....&.(...&.(...&.X...&.(...&...&.Y....&...j..&....&.(...&.(...&.X...&.(...&...&.Y ....&...j..&....&.(...&.(...&.X...&.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a749b9cfd775b6cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3318
Entropy (8bit):	5.756641495448361
Encrypted:	false
SSDEEP:	96:7J4fK4MV94a54O94exP4014Xp4jj4EE4oo4SL4J345L4:7J4fK4MV94a54O94exP4014Xp4jj4EEb
MD5:	17F8B51F2E9980DE67D3BF2FBDFA671F
SHA1:	BB3E284E89DAAE3DA6D9CAE70D60AF62BE781F11
SHA-256:	971B92081FB666E29869ADA6E8AD9E01C11C772D7ECCCCCDFB1851F724F755C1
SHA-512:	DC9FE45D4EAE050E06C24AF7F254D1520006AD3F975C6497C2C8383D7F80397C04BE94B8F43B83A413C2AA81A5D54DAEC17F6999BD2025D9848566FF9ED082F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1&l=dataLayer&cx=c .https://myhealth.net.au/.;\.M'/.....O..,i..'*...wB...,..{.. ?.....A..Eo.....a.....A..Eo.....0\r..m.....i....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192-1&l=dataLayer&cx=c .https://myhealth.net. au/'i,.M'/.....b.....O..,i..'*...wB...,..{..?.....A..Eo.....sX.....A..Eo.....0\r..m.....i....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-119135192- 1&l=dataLayer&cx=c .https://myhealth.net.au/."e.M'/.....O..,i..'*...wB...,..{..?.....A..Eo.....\.....A..Eo.....0\r..m.....i....._keyhttps://www.goog letagmanager.com/gtag/js?id=UA-119135192-1&l=dataLayer&cx=c .https://myhealth.net.au/r..M'/.....w.....O..,i..'*...wB...,..{..?.....A..Eo.....^O.....A..Eo..... ..0\r..m.....i....._keyhttps://www.googletagman

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7fb7466c5830dba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	507432
Entropy (8bit):	6.123085253924776
Encrypted:	false
SSDEEP:	12288:3MhxuHmpwaPHo/stuwZLg7w7u0zCyPR0lyv6pg:or57uAR/P
MD5:	EC5B72B9B6B0EC4FF4D33211381B6C5E
SHA1:	F1701BC4BD75BC106135F33CE80223F50A282E1D
SHA-256:	7DD7CF0C89C8A6C07EF890777932CAA2BDB7E63792C5321A102D45779506DE2F
SHA-512:	89873B601368AF19735C0D2CDA4AB508F746549A1AFC3759CBA8DEBAA60A97558F8FF123ACA736A897E365A2B223E06EEE3CF7809FAC4658C9D943C67206144

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7fb7466c5830dba_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....C.....2C8528466CAC216B4AD9164027B14F2F9E4D96A373854C8C3BA2E328CFE8FA42.....'..X....O....0...C.....D.....I...,..... ....L.....L.....d.....4.....p.....X..... .....$.....$..... .....$.....L.....d...X...$.....p.....T.....(S.<..`2.....L`.....(S.....`jO.....L`.....E.Rc.....Qb.T.W....n.....Qb".n1....A.....Qb.....d.....Qb&.L.....t.....Qbb({.....P.....QbF&f@....X.....Qb.....Vx....QbZ.....Em....Qb.I.....z3....Q bV*.W....iv....Qb.....UQ....Qbr..q....dr....Qb>..F....dL....QbJ.....Cy....Qb.....aT....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a9404d251cc895eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.077135803046631
Encrypted:	false
SSDEEP:	1536:B0lYSDyJymQrDDLZlqjQ5Aig9ohnUrH1wpowlqZp1CkSEF9dzr8:WIYlJbQrdlq2Ai0mUL1wWTUC9EF9S
MD5:	DA1EDC8DA4ECA5876E5F07C475A02FFD
SHA1:	A86EFCF4F6F89234BCF0D6AAFB03DCB308F59E6B
SHA-256:	D8E792D845490B5619E1CF55A6EE9887EAEE847A29F7C17BF0E39F7C58F310E4
SHA-512:	5C784CD820CC4627BE3264B9AC84AB0AEC277A7BD67F07376CA8A87E7510F25F80C7946FF663777B0E56C236DF9B10BFFC8BB6476AA720787C857574CEABD8E 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....=.k....8653FEF670DFCDBBB11DFDD887BB2EE35F62A98D3DCDC87634889BAE083FFE44.....'.....O...../..a.....8.....`.....D.....(..... .....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qbf..0....n.....Qb.....q.....Qb*.P$....r.....Qb.....t.....Qb.....v.....Qb.....x.....Qbn'uD. ...y.....Qb..B.....z.....Qb:.....A.....Qb..E.....B.....Qb.DH.....C.....Qb.bUb....F.....Qb.c.b....E.....Qb".)....D.....QbB.....G.....Qb.....H.....Qbv.-8....J.....Qb.(.E....I.....QbF.....K..... Qb...T....aa....QbZ+.....L.....Qb.....N.....Qb.GyT....O.....Qbr.-.....P.....Qbb.....M.....Qb...<....da....Qb.\.o....ea....Qb..N.....Q.....Qb./.H....S.....Qb.....R.....Qb.....ia....Qb .D.....U.....Qb..R.....ha....Qb..9.....T.....Qb.G.....V.....Qb..)....W.....Qb.....Z.....Qb..Z.....Y.....Qb.7~....X.....Qb..[.....ba....Qb.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae5a3f401015520f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.50720421470639
Encrypted:	false
SSDEEP:	6:m//XYZHfY7tOD3ebr16YsI8Lj21DYz/Qzra9bK6t:OG/Neb/sIo2tYz/7N
MD5:	A592D54B9394768236DC03DFF4CA4D57
SHA1:	590BCC853BF3D7B49565098504640EEAC08C6C09
SHA-256:	4F1F3296BC299C200996C11E4065538A5B3F550B6E2BA5F43D271F0633A7CBA8
SHA-512:	6714ECF6123D5E1ED8878436812CA39F77835C5CB5FBBAC5DEC315A5AA9BB70239A706D60A4CDB4E4ECE59F6721A19106A8A8977416C6E646F5C9E2BFF5941E D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[....{....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/8/common.js .https://myhealth.net.au/....M'/.....k.....U..u.h..q..AK.)....q.....A..Eo.....b... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\afa4c45b95634b06_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.9217009223201735
Encrypted:	false
SSDEEP:	6:mbYGLKdXNQKVQGHtiKQGjsyo6Am1ehAXflFYK6tS+0ddnWQkt2mlChAXfljo:DhNQKLtiKQGjE649o+0XWBt2mlZ
MD5:	26E0CEA2EF8EB0B3A2048D836D81B670
SHA1:	5A28F8C580870B22D9B62F9212DD2A4C9A29463B
SHA-256:	E39796C78C6AA4CF7CF885AFF05393FE8BC8DAA00F54E3EDDC5A303A618DA5CE
SHA-512:	91AD1415FDA4C49BCDB8D05CFC8EE9170EF41CDEA4210AACC4059C50427B6BB1DB99C8BFA22EB7D2B7F1EA9FA3539A216E530F2E26702E371B128326A62A2A E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...:....._keyhttps://www.gstatic.com/recaptcha/releases/ecapuzyywmdXQ5gJHS3JQiXe/recaptcha__en.js .https://myhealth.net.au/.H..M'/.....'...0.]R..e.. .+..d.jSbz.YE...A..Eo.....z..9.....A..Eo.....H..M'/.8n..85E41C21FA369FDBBB387695CBE54A8C535001EB81D57C4E745058F62C12B9D2...'...0.]R..e...+..d .jSbz.YE...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0ec7561a4011265_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.078148879456705
Encrypted:	false
SSDEEP:	1536:0NcljVDiZ/irYAZY7LStYh5xiPEwLUGHIA62ITnrKWCF9dzrt:0cljgZ/yYAZbtYRiPzUUILl7r/CF9v
MD5:	6F658EEA76F2E65C8FBCDF5D48D99565
SHA1:	D9642C39127B22CAFEAB5B77FBEE38C94285D15E
SHA-256:	94352B40463DD251F862C3F51BA3BCA229AB6EB679D3940715D34B2FDBE1F654
SHA-512:	F38154BB6C3DB6275E42C54ED5312126553E2A8BB812A16CD59BCC459C86EFEBB5879F3C63D7577881CCD5EE9D446620B5B6534392599D1C1FBB53EA41FDCCA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....\.....2B5242A9F10B57F951CA25F3D4FD430786C23C59E4DD48EA37752E526D2AB8CE.....'.....O..../..o.....8.....`.....D.....(.....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb..\c....n.....QbVQ.....q.....Qb...N....r.....Qb..;....t.....Qb..2;....v.....Qb.y.)....x.....Qb..7.....y.....QbVr.....z.....Qb..Be....A.....Qb.e.....B.....Qb..[.....C.....QbN,g.....F.....Qb..L....E.....Qb.A6.....D.....Qb.....G.....Qb.....H.....Qb.`.....J.....Qb.....I.....Qb~. Y....K.....QbBE.....aa....Qb*E.....L.....Qb.7L.....N.....Qb.B;....O.....Qb..It....P.....Qb.M.....M.....Qb..-.....da....Qb.....ea....Qb.M.....Q.....Qb...>....S.....Qb&..I....R.....Qb...g....ia....QbN.....U.....Qb.....ha....Qb.....T.....Qbz.&1....V.....QbZj.....W.....QbrN.....Z.....Qb..:\....Y.....Qb".u.....X.....Qb.....ba....Qb.m.?....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4555d1fc49a4d02_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	5.784627863647316
Encrypted:	false
SSDEEP:	6:mfVYZHf/VpEV7LB7WaGfKMRxrLikleHKVYm4xnJhK6t:gE/I7waGpOmoJ7
MD5:	02E132DD6B8C479F99994581357F6346
SHA1:	899089DF2FF9550D7CD30BBA4D5732C930E84AA7
SHA-256:	283C23E001FFBFD837356FD65BFF28EA913B6D326ACB8419BEC91D5975488E5D
SHA-512:	E3BD4573D30C9E1411AAA732956CAFA16D268BCF97EC81827280F9319EE37B38BDE12A89FC3239A3B65D6F778DA983E25759C9D22EB16B5E6D2EAC1E7FD3C74
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://maps.googleapis.com/maps/api/js?key=AIzaSyC-iv26QNUzpWZB0ysmYo16PBZSBqS6hSk&libraries=places&callback=initAutocomplete .https://myhealth.net.au/$.].M'/.....\|...QN.J$.E..%.....}.A.?..A..Eo.....A.%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c46eaa73f56bb611_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35326
Entropy (8bit):	5.451355579926915
Encrypted:	false
SSDEEP:	768:0i1cDxtN3+MhvMMulNVW5IhE6SvFB6BcMfwXYsB:0PtvhkjHhE4B7wIsB
MD5:	273E91A5608DB4FDBF83CD33F975385F
SHA1:	CBEC444030B91A93887910C03791E0E558272A66
SHA-256:	41872F72C19D2BCB5061BE5B10820ADEAF739D1BFBE2E574A1A19A394F9A5EC3
SHA-512:	D4C2774ABC864F2A2A8EB2AA0D353A8B906768E09FE9F01409E346D57DDD91CEA626558CEBF9CE47DCB6D73D033F0052F3CA4E7FF71749B0A1E7885A34BF68E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....._keyhttps://myhealth.net.au/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0 .https://myhealth.net.au/ .^.M'/.....@.....X...^t....j.].v...y...X..A..Eo.....@.....A..Eo.....'.T@....O....H....O'.....(S.0..`.....L`.....(S.Q..`\.....L`....HRc .....Qb.....S....Qb:.....r.....Qb.AS....e.....Qb..b.....o...c$.....l`....Da4.....(S...`.....L`.....Qc2.8.....exports..$..a.....S.C..Qb>kr....l...H.....a.....QbJ..y....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....q.`.....a.....e..... P.....`....@.-....\P.a.....P...https://myhealth.net.au/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0a.....D`....D`....D`.....`....&...&....&....&.(S.H..`L.....L`.....K`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d082d0b2b96339fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78088
Entropy (8bit):	6.079585071193409
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d082d0b2b96339fb_0

SSDEEP:	1536:c5HFAID4WdLXbWL4HTdRM2lYa1ygrU4HC3jmIbo20TAF9dzrh:+FALgLXRHTd7lYvoUWCT102IAF9r
MD5:	E3C116489CBE488076709C10FEFB5ED3
SHA1:	75A8C95A213090326746F9D1D260890A5C3C85BC
SHA-256:	42A85A683FA6B2E90FB20B6CBFB66B0EE391ED8A1E1672E62D0684CBB28C9B31
SHA-512:	7306C11133CD0A9782E241997AC0D22CB80C508659560730287D31E7EE73D4B8388AB74793163345178584910F22C21223F8B5E38EEEA1AF023AC5B40D48F247
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....08A6340CDFB8705E1B0D1EC93DC5234C869921DC4C3F5C163C665AFB865AE709.....'.....O...../..s!.z.....8.....`.....D.....(.....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.....n.....Qb~.\....q.....Qb.Nu.....r.....QbVD1.....t.....Qb~XB.....v.....Qb.2I.....x. ....Qb.}5....y.....Qb&..~....z.....Qb...M....A.....Qb..Pw....B.....Qb..X....C.....Qb.....F.....Qb.....E.....Qb.p~.....D.....QbF.]<....G.....QbV8d.....H.....Qb._....J.....Qb*.N.....I... ..Qb.T.....K.....Qb.9.>....aa....Qb..Z....L.....Qb.....N.....Qb.....O.....Qbf..6....P.....Qb&.....M.....Qb*:.....da....Qb2.....ea....Qb.14.....Q.....Qb.....S.....Qb..:.....R.....Qb..... .ia....Qb:.?8....U.....Qb..}.....ha....QbF.....T.....Qb*86.....V.....Qb:XA!....W.....Qbb.....Z.....QbV.....Y.....Qb..+Z....X.....Qb& V.....ba....Qb.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d58eeb8fddecbf1f_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2172
Entropy (8bit):	5.416068575188562
Encrypted:	false
SSDEEP:	48:LrEnHg+gAOtRuro1VFUSD4JoeqgZ0szlb4hzRQt:WHnOtRurOLUlig/BbQq
MD5:	01677052E320BA57C80D101465A05C63
SHA1:	3DEB33481B188171B2F7C5419F29526378AF63B4
SHA-256:	368B58F8AB324E9516ADDAF4DCF483E8D13DE5551B0FA8983E0C6ED0CF7A5B2D
SHA-512:	DAC8124977B96751DAD916A3D958DBA72291D346AC48B70DB76FB4CB7A8A765DB1F7B748626867CFFBF8038484BD8B0E6145CE4679D50F53378714B877CFAF4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...n.S....._keyhttps://myhealth.net.au/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=5.4.2 .https://myhealth.net.au/..^.M'/.....G.....#. ./ks..!.)K4.....#.....[1.A..Eo.....A..Eo.....^.M'/.8.....'.9....O.....Py.....d.....(S.D..`>....L`.....(S...`....LL`'....@Rc.....Qb.AS..... e.....Qb.2T.....t....QbBN.....n...b$.....l`....Da.....(S...`.....L`.....Qc2.8.....exports..$..a.....S.C..Qb>kr.....l...H..a....a.....QbJ..y....call..A...K`....D}8.....&.%.*.. ....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da@...8.....a.....e..... P.....@....@.-....IP.....^...https://myhealth.net. au/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=5.4.2..a.....D`....D`F...D`.....\...`*...&...&....&..!.&.(S.....Pb.....n.d.a.....l...1.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dcf1121eb35a5dd7_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78096
Entropy (8bit):	6.076638662572611
Encrypted:	false
SSDEEP:	1536:7CJoYIDRgVrGE3LAr5UuXTmJGbzUQsH+LBs4zxI2eFMnuFF9dzrY:GJoYuGrGxr5RTmkUL+LG4zepFKuFF9S
MD5:	F26F07DC15C9AA2B683DE7E6FD2EAFDD
SHA1:	E7B1905FAC9A711D6B84D5DAAE2083E665C56B44
SHA-256:	86EF21686179A89B3AA3930A9923969DF51AAEEF18191C28F0617D4908781147
SHA-512:	21529A17337CF166CAD879F5DA372633D21B6814BE31BCF5CC6920C7AC989E08AFFD578482A5CD9C56C41435CC3FACE892B5B1F07975AC82D5016849166F663
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...3u.....49C1AF94EC583387831C0833AE5C99CE52A2B9D51826FED9098726AEBD30DCF5.....'.....O...../.....3.....8.....`.....D.....(..... .....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qbj.....n.....Qbv.Q.....q.....Qb..`)...r....Qb.....t....Qb.G.F....v.....Qb.%|5....x.....Qb.K .....y.....Qb~.5"....z.....Qb.....A.....Qb.h.....B.....Qb.d.....C.....QbN.3.....F....Qb.CzD....E.....Qb.....D.....Qb.f.U....G....QbR.....H.....Qb.....J.....QbjC;....I.....Qb.+.8....K... ..Qb&d.X....aa....Qb*.....L.....Qb.bo....N.....QbZ.....O.....Qb.i.....P.....QbR.....M.....Qb>.....da....Qb.Z.....ea....Qb.....Q.....QbRD.D....S.....Qb.F.E....R.....Qb..uY....ia... .Qb.f.....U.....Qb.o.....ha....QbF.....T.....Qb6..'....V.....Qb.h&W....W.....Qb../....Z.....Qbb.....Y.....Qb..bp....X.....Qb2OYU....ba....Qb~[.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de03e5645c6a3a52_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5702
Entropy (8bit):	5.370963766914045
Encrypted:	false
SSDEEP:	96:2RnOtXg4houMo1lfzpJTlpj5V6U8KV15OF9lgLz1s4n1IrDlCHFoWpAtxR:Q+XBMefzpTpjj6U801YFMX1s4n1IrhiO
MD5:	B1712717172E08B9F220D8E6E1BD42DF
SHA1:	748626D7F0064DF944F28B48B2665596785F957A
SHA-256:	11A7FED9A64B59AE99D65E95E07524CFC02414A7CF65D5B13893CD49A902D64A
SHA-512:	E33D8E5F3276F3E113163D1F0C0B915670210028F9D2826D711CCAA7C52B0E0A6F66C9BBD816CC652D51DAB728FAB827EA6589458349D7268892692E84FD594E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de03e5645c6a3a52_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...g>+...._keyhttps://myhealth.net.au/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4.2 .https://myhealth.net.au/..^.M'/.....B....._.....AY.....:..4.....>..A..Eo.....x.W.....A..Eo.....'..2...O.....(.....(S.h..`..... L`.....(S...`.....LL`"....@Rc.....Qb.AS.....e.....Qb.2T.....t.....QbBN.....n...b$.....I`....Da.....(S...`.....L`.....Qc2.8.....exports..$..a.....S.C..Qb>kr....I...H..!....a.....QbJ..y....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da@...8.....!.....e..... P.....@....@.-....dP.....X...https://myhealth.net.au/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4.2a.....D`....D`2...D`.....`....&...&....&....&.(S.X..`l.....L`.....Qb..b.....o.....e.....a.....G...C...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eebba20cd63ca78b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1412
Entropy (8bit):	5.693859039932752
Encrypted:	false
SSDEEP:	24:HBCrkNqAdtn3l98uLexDBCrI3Mbz78fuRgAonYkWGJjkXTJv:hCokAdt3v8RzC0WgUlkWGCXTJv
MD5:	D7E0AE172B094894BD6A5943F529770D
SHA1:	0C8E80797E7AAAC5EF6275B273FEC46EDA669526
SHA-256:	0F48E97DF72D96626BBF6DF9E75D1EF66D66FD24FCA94FE447CD50DCB9DEEA4D
SHA-512:	ADA45F8043EFFA208E3536DFAEA811D651803EAEDAE1AD6F2605C101A95269DD333C8D0DE53AA73051744B78036ECE6953209BF0BE4F8EC633321577099BEA9E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...w....._keyhttps://myhealth.net.au/wp-includes/js/wp-embed.min.js?ver=5.8 .https://myhealth.net.au/..^.M'/.....H.....Xq..cZP.bWYe...q....g..&.+[u..A..Eo.....\.....A..Eo.....^.M'/.`.....'.....O.... .....(S.<..`2.....L`.....(S..`.....0L`.....@Rc.....Qb..ER....d.....Qb.nL.....c.....QbBN.....n...b....$.....I`....DaX.....(S.....Ia.....Qb.2T.....t.....@.-....LP.!.....>...https://myhealth.net.au/wp-includes/js/wp-embed.min.js?ver=5.8..a.....D`....D`H...D`.....`....&...&....&.(S.....5.a.....!...a.....a.....Qb..c.....wp....a..... Qf..|....receiveEmbedMessage.a....H...I....d.....@.....&....`....DI]d.....@.....QeJ.....querySelector.....QeR.....addEventListener..!.....Q..m...Q.`.}.]....DOMContentLoaded..Qbj.Lh....load..K`....D.Q.@.....%...%.....&..&.....&.(.....&.(.....&...&...&.(.....~-.....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f169562cfa59e125_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	5.975734814638894
Encrypted:	false
SSDEEP:	96:UL4CpiL0ZSLs13DCLCKhbLd/8lLOkePLjOKL1knyGLhoZSLQmUBLbo7Lglw9M5LG:XCpxZt13D/Khd/84keHOYOykoZF/hoAy
MD5:	BCDA5EC84C126A85101B5CF95F89B11A
SHA1:	52CBF1EA80685F3F42C0AAE9D65B6EEDB7B605A7
SHA-256:	D3CFC5B5837D42A88C9070696EAEB6EBA7D106B5637FB52842FE8FFC2C1B5120
SHA-512:	E360DC0A86485C5BA99FD080F6D361113A50DA5C224939B07C43CC652309193FC270280212361C4A6D676240DF6C68F9464F8F939A5D8FCB2BF3B35E244E2ADF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....<....._keyhttps://www.google-analytics.com/analytics.js .https://myhealth.net.au/.$].M'/.....>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.....A..Eo.....$].M'/..6..9A13C37DBDBAE6D813D636A066D317CB170688632A9ED9D8D387726C7B4108DB>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.....j.L.....0\r..m.....K.....<.....,_keyhttps://www.google-analytics.com/analytics.js .https://myhealth.net.au/.,,M'/.....].....>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.....A..Eo.....,M'/.`0..8411F56708FE13A53AA7B5CB2323B6F5831F7DBC3D7E5AD67D0C8C4A2628B5B3>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.....L.....0\r..m.....K.....<.....,_keyhttps://www.google-analytics.com/analytics.js .https://myhealth.net.au/3.d.M'/.....>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.....A..Eo.....3.d.M'/.h0..49C1AF94EC583387831C0833AE5C99CE52A2B9D51826FED9098726AEBD30DCF5>oW.N...d...hpTC.AMF...Fo.iJ.A..Eo.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fb29d5ffb08354e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1666
Entropy (8bit):	5.639045936086817
Encrypted:	false
SSDEEP:	24:alZwN2Qb3NrTDOUP4FlZqKPcToRW1he6NfKGRM/hK8K3fXXm8XVajgVGTdCpoKQz:aEAGNr2JVuow+jGeZK3vXAldCWKwou33
MD5:	D220EF1EC11FAF62A9A3666FFC034987
SHA1:	4BFB439FDD96098ABF2C4AF69D347A0640BDB81D
SHA-256:	3CE8AF7F8D6C38982D5AFFF51289AB3CCCAE5FA1479980E5E027D5994636B5D7
SHA-512:	70B4188889738C1BD5400C831C5F0465FB1C3B9B2F7DBE04C6A6BAD6AD2A6CAE8E21BE108ADF0CDDBFD17CC01206FB73E2EB40B93B3428968082622EEE4225D9D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fb29d5ffb08354e9_0	
Preview:	0\r..m.....r....A....._keyhttps://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/custom.js?ver=5.8 .https://myhealth.net.au/i^Q.M'/.....^.....&.. .(."....@..r.....A..Eo.....v.|j.....A..Eo.....i^Q.M'/.H.....'.....O.....2.....(S....`&....@L`..... L`.....(S.....Ia....U.....Qe~.....resizeGridItem..E.@.-.... `P.q.....T...https://myhealth.net.au/wp-content/themes/myhealth-child/assets/js/custom.js?ver=5.8a.....D`....D`(...D`.....(...`....&...&.(S.....Ia!.....c.....W.....IE..Q.d..... .....D&....&.(S.t..`.....$L`.....Qc...H....document.$Qg.`.....getElementsByClassName....Q.@>{.....towers....Q.@..8....allItems..Qb..v.....x....M.....K`....Dw.....&. (...&...&.Y.....&....&.(...i...#...&....&....*..&.].....L.....1.....(Rc..... Qf..X/....resizeAllGridItems..`....Da.....e.....@..`.....d.....&.(S.....Ia....\..

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):	24576
Entropy (8bit):	1.466280995179176
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7UEuxkOFIkWnIkIlk9J2YcZLLOpEO5J/Kn7UEwYk1fIkWnIkIW:dNwYx0CqNwYmi0KV
MD5:	C5A782F0161041C0B1BE809E738ACADD
SHA1:	A6BCEC91A4BBFBBFCEAE91072DCA85C60754983A
SHA-256:	A822AB16D6A2968A2CF557E78589425018004F35913ED2B83FFE664457318787
SHA-512:	37C0149F4E5B7E08AB5BF7280718DDF518C22522463387903987CD55470D90F699D9132582CCB77A8D0C5EC80C8C0331EFBECD4FB6D6302390B12639A4BEA20
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):	25672
Entropy (8bit):	1.2142849226370795
Encrypted:	false
SSDEEP:	48:D8NOZ/q5LLOpEO5J/Kn7UCnxkOFIkWnIkIlk9J2YgqekLLOpEO5J/Kn7U08:YO/cNwl0CAMNw7
MD5:	2EEAF0C141C84CE1568C1987A156933F
SHA1:	CBC5824882C7BC21149CA7C9DB6C962B1F8F818F
SHA-256:	E5B97FEFBF69458E2C578A4DFE6CE96547A0F28AD6FB271164E511CA628F6B8B
SHA-512:	6976596793E8D691056D760576FFF18998C4D75CCFDEEF68EDB04F09271EBD5F0E535EFE189D77ACE87A7975D299D2BCBD5E1C232E12BD12432C75774F8C7D
Malicious:	false
Reputation:	low
Preview:	.....1Z..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85725
Entropy (8bit):	3.3243356478999835
Encrypted:	false
SSDEEP:	768:Ud+o0vb0cf47OF4UrV30fOIhBZEV3LxOdLRNixRNpexeaB8jyf:Nlvo7Il0FKooK
MD5:	7B3A3023AD10D1875B4C41FC0A1447D9
SHA1:	CCC0FC444F7B38391024D179C9703AD609FB2223
SHA-256:	B8EBEA1B3B974EAF33EBEE781E4D2FD0F68FB8B4F0C5EE7DDF6C890FFCB2F5BC
SHA-512:	FC74E723C10131EB57B4D4D376BA7CA09302F94C26A4648F09243185DBB4064FAA901681E28959FCCBC50021A0C6AEDCB6A6F410055B145E8C162BF11C0A46F
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...abaff71f_70e4_4dab_ae96_b190a8786f2a.....:..y..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://myhealth.net.au/:...H.o.m.e.-.M.y.h.e.a.l.t.h.,. .A .u.s.t.r.a.l.i.a.. s. .f.a.s.t.e.s.t. .g.r.o.w.i.n.g. .m.e.d.i.c.a.l. .c.e.n.t.r.e.!.....h.....`.....Zv.M....[v.M..... ..... .....8.....h.t.t.p.s.:.//.m.y.h.e.a.l.t.h...n.e.t...a.u./.....P.....8.....`.....x..... .....8.....H.....`.... ...p.....(.....8.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	5.166729040304998
Encrypted:	false
SSDEEP:	6:mZSv4q2PWXp+N23iKKdK8aPrqIFUtp0KJZmwP0KDkwOWXp+N23iKKdK8amLJ:HAva5KkL3FUtpv/P95f5KkQJ
MD5:	B9A076FBC7F6D1281116C9FBF5DE29EE
SHA1:	F3C91C33700C44563AD6589D9492708F79A90CA2
SHA-256:	7E5673C4B32A250F1E008838E1A9DD2BD800FFE6A3FB10039B311685EDF4B47D
SHA-512:	C1EF4477B7EF4F94154990F0FD6E8DE1FD057DB6D9A87727004F74C04DE6DDFBFBF4CF164BC2E915676BD27B7402DFC2C74917BCFDAF9766BD4111BE9E5295A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:08.455 1280 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:08:08.457 1280 Recovering log #3.2021/08/04-01:08:08.457 1280 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.166729040304998
Encrypted:	false
SSDEEP:	6:mZSv4q2PWXp+N23iKKdK8aPrqIFUtp0KJZmwP0KDkwOWXp+N23iKKdK8amLJ:HAva5KkL3FUtpv/P95f5KkQJ
MD5:	B9A076FBC7F6D1281116C9FBF5DE29EE
SHA1:	F3C91C33700C44563AD6589D9492708F79A90CA2
SHA-256:	7E5673C4B32A250F1E008838E1A9DD2BD800FFE6A3FB10039B311685EDF4B47D
SHA-512:	C1EF4477B7EF4F94154990F0FD6E8DE1FD057DB6D9A87727004F74C04DE6DDFBFBF4CF164BC2E915676BD27B7402DFC2C74917BCFDAF9766BD4111BE9E5295A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Reputation:	low
Preview:	2021/08/04-01:08:08.455 1280 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:08:08.457 1280 Recovering log #3.2021/08/04-01:08:08.457 1280 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	317
Entropy (8bit):	5.165736399615599
Encrypted:	false
SSDEEP:	6:m4QZOq2PWXp+N23iKKdK8NIFUtpfX9VFZZmwPfMkwOWXp+N23iKKdK8+eLJ:vQZOva5KkpFUtpfX9VFZ/PfM5f5KkqJ
MD5:	8B69C2BFE2A7D52AB9EDFD285887F214
SHA1:	F467BA65C217B82EECFE780AEFC737BFF5160B32
SHA-256:	4BC10D1B3D526097D433344F0F599658192282F8B9FFBF720CF92EAA5D649F1F
SHA-512:	EE7FE7C75E39874786ADE79C799317400C8B4C91025B47804E62DEDA73E3F2F46A971795938F353B942875593204E1C5F3EE6A1F5B6EB495AC96B46F8B114C92
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:10.634 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01:08:10.635 660 Recovering log #3.2021/08/04-01:08:10.636 660 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
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.165736399615599
Encrypted:	false
SSDEEP:	6:m4QZOq2PWXp+N23iKKdK8NIFUtpfX9VFZZmwPfMkwOWXp+N23iKKdK8+eLJ:vQZOva5KkpFUtpfX9VFZ/PfM5f5KkqJ
MD5:	8B69C2BFE2A7D52AB9EDFD285887F214
SHA1:	F467BA65C217B82EECFE780AEFC737BFF5160B32
SHA-256:	4BC10D1B3D526097D433344F0F599658192282F8B9FFBF720CF92EAA5D649F1F
SHA-512:	EE7FE7C75E39874786ADE79C799317400C8B4C91025B47804E62DEDA73E3F2F46A971795938F353B942875593204E1C5F3EE6A1F5B6EB495AC96B46F8B114C92
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:10.634 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01:08:10.635 660 Recovering log #3.2021/08/04-01:08:10.636 660 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+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":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	47104
Entropy (8bit):	1.471209727411444
Encrypted:	false
SSDEEP:	96:yBCkM+dP9jf+bCTy2KgyMtPZFAg4lB7Aw4lni7ANs4lBti7AVbn4lG:lS+d9f+b0yRitDCbm
MD5:	1A78C4DF8E33BD4FD3AC2C7DB3CE0435
SHA1:	FCCEE6BA8602BCA767EFFD029E0F305F4B0729B7
SHA-256:	16D2B025A4383A0F8700978958D1364C8515FDA1CE0746635A9038E5A6123DF1
SHA-512:	B97BA09CCBBBB4A9F9FF32D47DB9C87ED52B99C109A127791B054D0ADD4C2F814128EB5DB75D27ED63315DBD1B79453341EEE13BD0A0DD2A6FD85C9C3466F96D
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Category:	dropped
Size (bytes):	57112
Entropy (8bit):	0.9910864830748752
Encrypted:	false
SSDEEP:	96:cwVdBCtl748G4cuq4PS7VgTs4Ti7O/bn4Pi71:3VLiD/Fbd
MD5:	8D21AD2ADCC58DFA828280C32C761404
SHA1:	E12396502BB4E0A41B1BDF87452CF347907ACFAF
SHA-256:	17A8994C38DFC39BE16E62D7DC9611060766DB97C27F6BF413B647F69DCF317A
SHA-512:	A52998186CAFB717C6196EBB3D3552632E772D6AC38578657156B7BEB9D6CB044AD91C945789D7787950279756B4CCFD2EAFD4BE5CBD795856CBB8C7D996C3B
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):	369
Entropy (8bit):	5.23456360961004
Encrypted:	false
SSDEEP:	6:mbaWAv4q2PWXp+N23iKKdK25+Xqx8chI+IFUtp22cZmwP20PDkwOWXp+N23iKKdP:Gjva5KkTXfchI3FUtp22c/P20b5f5KkI
MD5:	1E961BB8649EF4515B1A0931A406E84C
SHA1:	1C47377CD9311C7522BFBA3698AE8E85674CA57C
SHA-256:	A7EF5E749AC010854F3522C53D3E2ED65E9FFBB9057DB26C8383B6B7BEBE11A6
SHA-512:	8D8B8AAA52689D1CF115F0BC0329DCB59153081BFD1112AFFC06C919EEE536A1B46D361E5A2DD9747A0A40E388FA0669AACF4A408D6BD241AFCB633EA0F3521A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.265 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:08:24.266 3e0 Recovering log #3.2021/08/04-01:08:24.267 3e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.` (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.23456360961004
Encrypted:	false
SSDEEP:	6:mbaWAv4q2PWXp+N23iKKdK25+Xqx8chI+IFUtp22cZmwP20PDkwOWXp+N23iKKdP:Gjva5KkTXfchI3FUtp22c/P20b5f5KkI
MD5:	1E961BB8649EF4515B1A0931A406E84C
SHA1:	1C47377CD9311C7522BFBA3698AE8E85674CA57C
SHA-256:	A7EF5E749AC010854F3522C53D3E2ED65E9FFBB9057DB26C8383B6B7BEBE11A6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.` (copy)	
SHA-512:	8D8B8AAA52689D1CF115F0BC0329DCB59153081BFD1112AFFC06C919EEE536A1B46D361E5A2DD9747A0A40E388FA0669AACF4A408D6BD241AFCB633EA0F3521A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.265 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:08:24.266 3e0 Recovering log #3.2021/08/04-01:08:24.267 3e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.176926929872372
Encrypted:	false
SSDEEP:	6:mbqq2PWXp+N23iKKdK25+XuoIFUtp2CcZmwP2lH7kwOWXp+N23iKKdK25+XuxWLJ:Gqva5KkTXYFUtp2F/P2lb5f5KkTXHJ
MD5:	ADED2AF075CC975E3D39B0253388A7B0
SHA1:	A9440D6B97D12981B3F38417D1A9B369B5E11314
SHA-256:	64DE9F317AEE4387B2AD39E71E6C77BBED3BFD15255FDFEA592045714E02285B
SHA-512:	00D0F0C3E9BCC385453DE957750A544510621BBCD2EF93FFC7EDDA752612D8FCE33B06549CDCE134FB7585416C3B1AC83ED65BE1267B55322C280DC76CF6D5A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.246 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:08:24.248 3e0 Recovering log #3.2021/08/04-01:08:24.259 3e0 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.oldl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.176926929872372
Encrypted:	false
SSDEEP:	6:mbqq2PWXp+N23iKKdK25+XuoIFUtp2CcZmwP2lH7kwOWXp+N23iKKdK25+XuxWLJ:Gqva5KkTXYFUtp2F/P2lb5f5KkTXHJ
MD5:	ADED2AF075CC975E3D39B0253388A7B0
SHA1:	A9440D6B97D12981B3F38417D1A9B369B5E11314
SHA-256:	64DE9F317AEE4387B2AD39E71E6C77BBED3BFD15255FDFEA592045714E02285B
SHA-512:	00D0F0C3E9BCC385453DE957750A544510621BBCD2EF93FFC7EDDA752612D8FCE33B06549CDCE134FB7585416C3B1AC83ED65BE1267B55322C280DC76CF6D5A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.246 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:08:24.248 3e0 Recovering log #3.2021/08/04-01:08:24.259 3e0 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\File System\Origins\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	102
Entropy (8bit):	4.707425199545215
Encrypted:	false
SSDEEP:	3:w1tsm1ilLeNlA1jPqciKPnSc+VVn:w1tsmRLVP1/Sc+VV
MD5:	7E6074135B54581D9C9A50EC25141C6A
SHA1:	362BE82BA04A240771813665F436B0EF9D24C35F
SHA-256:	8A14329F2C4F6E9CD07FDABA314C1F29FDE90C936695F0E95118778B2E0CD7A2
SHA-512:	D715BD9AE5A94DC6F30D6B8A475DFD69DE15C3915987D6A2D9E6F761237055AB1409B24431F9F6497FE0CDF664449F13F3D52FB0C49E4221CE3145862D9048F8
Malicious:	false
Reputation:	low
Preview:	mP.....LAST_PATH.-1.X7.>.....LAST_PATH.000..ORIGIN:https_www.google.com_0.000

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.214638844563243
Encrypted:	false
SSDEEP:	3:tUK6NVd8dLVRdv1/KqFkPWXp5cViE2J5iKKKc64E/+MOMcWIDMGk4cWIV//Uv:mwhRdv4q2PWXp+N23iKKdK29MRgPRIF2
MD5:	A57617276FD94288D7B83F6DCFFB97A0
SHA1:	BDA1B41DE3B2229ACD450FE6503275AC27F64CBB
SHA-256:	8AA6EDE426114D46E1E21E6ACEC69FE70797F01A1E3284407942D59BEE578E4B
SHA-512:	EE6FA5CC83528558BD8323E30D5488AEBDFCE01834008007AE7B7EFE86E73554C9134935967DA4CE698A3985CD4DD43049F4703B26BA5842772364F44C5F280E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:18.076 1280 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins/MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAlxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 5B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.1921531411405
Encrypted:	false
SSDEEP:	6:mbVq2PWXp+N23iKKdKWT5g1IdqIFUtp2GZZmwP2tvDkwOWXp+N23iKKdKWT5g1Iu:GVva5Kkg5gSRFUtp2i/P2t75f5Kkg5gZ
MD5:	F1AAC3B446DD4BB0EEFCE2A45943037E
SHA1:	7876ED2802BAB403FA3D08D126704941E00E6FD5
SHA-256:	57D26191DB8A6CF32EC1DC2E603CAF53AC913627B0DF9F03BD3A526439A81CD0
SHA-512:	200F7CF06C256A87F4F47150C36092ADCEC4D95E2829F34B588A0ECF239AEE61B6E286D8541E271ABF40A3CB89B0CAD807996B0AA60089DAF6D714066DD2104B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.234 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:08:24.236 3e0 Recovering log #3.2021/08/04-01:08:24.237 3e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old{ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.1921531411405
Encrypted:	false
SSDEEP:	6:mbVq2PWXp+N23iKKdKWT5g1IdqIFUtp2GZZmwP2tvDkwOWXp+N23iKKdKWT5g1Iu:GVva5Kkg5gSRFUtp2i/P2t75f5Kkg5gZ
MD5:	F1AAC3B446DD4BB0EEFCE2A45943037E
SHA1:	7876ED2802BAB403FA3D08D126704941E00E6FD5
SHA-256:	57D26191DB8A6CF32EC1DC2E603CAF53AC913627B0DF9F03BD3A526439A81CD0
SHA-512:	200F7CF06C256A87F4F47150C36092ADCEC4D95E2829F34B588A0ECF239AEE61B6E286D8541E271ABF40A3CB89B0CAD807996B0AA60089DAF6D714066DD2104B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:24.234 3e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:08:24.236 3e0 Recovering log #3.2021/08/04-01:08:24.237 3e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	184320
Entropy (8bit):	0.5554469388600466
Encrypted:	false
SSDEEP:	384:xgeqgtWBRqg7yb/WBRqgysFsOyb/WBRqgbRHAesOyb/WBRqgYnUN:37drcg3nI
MD5:	6269AA50649366A5392B18B232EAAF73
SHA1:	D0D27B05410CF3D81C103352BC50143EBC1C9CEF
SHA-256:	50F64125456F84C8B18A155AB591348B363D84884175A32A0F6D964AF5FD6F50
SHA-512:	BF552210375279B9899B33DDE72A9B94F7B03FCA774331F46EBBA8699C182CA68EA7CB595C433F9D9E4DF9862E5CB9E50DDFF75DADB76DDDCB57CCCA8642229
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):	685
Entropy (8bit):	5.305432758728198
Encrypted:	false
SSDEEP:	12:KHNOnbIBg7SLqJcJhc/P9m+8BXR6WYjJLtBBk778B/xgskZBa9sdiAm3RhqU+u:KH08Bg7SLqPlN8at3Y78BJgskfa9iCBv

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
MD5:	A17094A37F43E9CFB457A14EB739AA70
SHA1:	53C5A314F5CCD977B267E799643B1D775CC21044
SHA-256:	C209015E74C146D18A9A713F8F9EBA99A2FB77BC8AA8B0B701929ABD6A5233D2
SHA-512:	446EBB48782435EE22C8DCC68172B50ACC8D2970713A2A00810D46DFD09CB9BEB62C921754BDF9B5575A9A8938E6BCABBA37C0DB180089E3A4873F173157ED1
Malicious:	false
Reputation:	low
Preview:	.....T....au..australia.s..centre..fastest..growing..home..https..medical..myhealth..net*|.....au.....australia.s.....centre.....fastest.....growing.....home.....https.....medical.....myhealth.....net..2.....a.....c.....d.....e.....f.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w.....y.....@...:\.....B|...x..... .....*.https://myhealth.net.au/2<Home-Myhealth, Australia.s fastest growing medical centre!:..J.....#+3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	187824
Entropy (8bit):	0.42314531045943854
Encrypted:	false
SSDEEP:	192:uAWqcdqqMndfWBRqqdrFQRyb/WBRqqoWKQHsOyb/WBRqqloD1KQs:uAWBqNWBRq02yb/WBRqGbsOyb/WBRqXg
MD5:	23075307C2EEC5444DE362FEEB5AE38B
SHA1:	4CEFCD75641B8FBAF87A942CD8B107B99E8EA76F
SHA-256:	88D0413FDC68DE5681D9BA9F28EC5A6755B23D05E7C574B0FB45F52160C69207
SHA-512:	7B22CF279F488AB17B5106AFF0EC2C16F6DD5D959D44242411079F56A64B7BB7CBF178F7CDC14042236553354BCCBFF630D9BEF6F18CC28210A798484006C21
Malicious:	false
Reputation:	low
Preview:	.....Oh..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessionc (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85725
Entropy (8bit):	3.3243356478999835
Encrypted:	false
SSDEEP:	768:Ud+o0vb0cf47OF4UrV30fOIhBZEV3LxOdLRNixRNpexeaB8jyf:Nlvo7Il0FKooK
MD5:	7B3A3023AD10D1875B4C41FC0A1447D9
SHA1:	CCC0FC444F7B38391024D179C9703AD609FB2223
SHA-256:	B8EBEA1B3B974EAF33EBEE781E4D2FD0F68FB8B4F0C5EE7DDF6C890FFCB2F5BC
SHA-512:	FC74E723C10131EB57B4D4D376BA7CA09302F94C26A4648F09243185DBB4064FAA901681E28959FCCBC50021A0C6AEDCB6A6F410055B145E8C162BF11C0A46F
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...abaff71f_70e4_4dab_ae96_b190a8786f2a.....:..y.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://myhealth.net.au/:...H.o.m.e.-.M.y.h.e.a.l.t.h.,. .A.u.s.t.r.a.l.i.a.. s. .f.a.s.t.e.s.t. .g.r.o.w.i.n.g. .m.e.d.i.c.a.l. .c.e.n.t.r.e.!.....h.....`.....Zv.M....[v.M..... .....8.....h.t.t.p.s.:.//.m.y.h.e.a.l.t.h...n.e.t...a.u./.....P.....8.....`.....x..... .....8.....H.....`....p.....(.....8.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs . (copy)	
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):	8399
Entropy (8bit):	5.538189381967522
Encrypted:	false
SSDEEP:	96:HVBUa7gMHdbryCfLbQ5fgGvrS03HxqcE4eHpgq5NuL8:HkygcdvyCDE5fgu3HxqcE4eHpnsQ
MD5:	E32F5A252DEAFE1C5A6A4F446BDCDAE8
SHA1:	557BD4858C707E2AEFB5231277867B9B3DEA4D1F
SHA-256:	2A876E4DE30AD5B8339237CF36A343707EFD72B1109B8F9DAF19D82090EA87BB
SHA-512:	75DFDB2F7EBA4A1C5674DCEF08CF290A0BDAFDF8EB5EC06CE2F92DC7FED4BD9012166BDD85048006A29EA33AC289D41FC180FDAB35A43D097C549D9648A9B02
Malicious:	false
Reputation:	low
Preview:	.....*.....META:https://www.google.com....._https://www.google.com..rc::a..em90anZuMTg5eGhhbA==.,_https://www.google.com..rc::d-1628064497866B.k...-.....META:https://myhealth.net.au.....f.%_https://myhealth.net.au.._grecaptchaZ.09ADKZGYps8Su__0T_0kyuYvupc3stiimkYkwWuGRP79l48MYEMwl6yrWvsMl-22qLAtUjg3hD2sdEDiYObTLUnvE...t.../.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..351840000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 01:08:25.33][INFO][mr.Init] MR instance ID: 8fdaa17d-2d58-4432-ac47-364e53565533\n","[2021-08-04 01:08:25.33][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 01:08:25.33][INFO][mr.Init] Native Mi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.108861876211293
Encrypted:	false
SSDEEP:	6:mZR+q2PWXp+N23iKKdK8a2jMGIFUtp03XZmwP0CuQLVkwOWXp+N23iKKdK8a2jM4:zva5Kk8EFUtpw/PZ5f5Kk8bJ
MD5:	2456FC9EF123A397241751E1AF36BBAB
SHA1:	CBB28758A2EEC1152E6AB0415FC9791BB656FCE3
SHA-256:	100D9BC74443AAD6A83A04025853C13470AE396ABE91F6A4DCC78B2DB49A9A6B
SHA-512:	D406E9C5F127178DBB9FBCFE9A07605DC7E4F0B91CBB49B7FA1942BE2F86D38925ABE4555E88BBEA25B6844018AAFDC07F2CF847856E874FAB4E42A9492102E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:08.200 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:08:08.202 15d8 Recovering log #3.2021/08/04-01:08:08.203 15d8 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):	332
Entropy (8bit):	5.108861876211293
Encrypted:	false
SSDEEP:	6:mZR+q2PWXp+N23iKKdK8a2jMGIFUtp03XZmwP0CuQLVkwOWXp+N23iKKdK8a2jM4:zva5Kk8EFUtpw/PZ5f5Kk8bJ
MD5:	2456FC9EF123A397241751E1AF36BBAB
SHA1:	CBB28758A2EEC1152E6AB0415FC9791BB656FCE3
SHA-256:	100D9BC74443AAD6A83A04025853C13470AE396ABE91F6A4DCC78B2DB49A9A6B
SHA-512:	D406E9C5F127178DBB9FBCFE9A07605DC7E4F0B91CBB49B7FA1942BE2F86D38925ABE4555E88BBEA25B6844018AAFDC07F2CF847856E874FAB4E42A9492102E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:08:08.200 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:08:08.202 15d8 Recovering log #3.2021/08/04-01:08:08.203 15d8 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	1.163387767681891
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOMOqAuhjspnWOedOqAuhjspnWOE3OqAuhjspnWOQ5Mg:HrrxXfF
MD5:	B7435E2307A1CA30D7FC47748D791397
SHA1:	FEB8A576CCF80B325ECFE8458B9459888A7C4289
SHA-256:	44BF1EF20B4F9C93DBFFD25771C3D0D191D600810BFAC469B892B7A2815FA3E2
SHA-512:	2F7D1134CD15FE4218CFC801788C26EE268E1FC15EC50987EE8EBF788B771903C4834FCF2D6492D8383C9A5BA76A4D2FB5D9B3A40B3D25C2112D3FE3D8DBA06
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>...,..... ....

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 01:08:11.905194044 CEST	192.168.2.3	8.8.8.8	0x92bf	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:11.912811041 CEST	192.168.2.3	8.8.8.8	0xd22d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:11.920506001 CEST	192.168.2.3	8.8.8.8	0xa4a7	Standard query (0)	myhealth.net.au	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:14.173269033 CEST	192.168.2.3	8.8.8.8	0xa88b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:14.174326897 CEST	192.168.2.3	8.8.8.8	0xfda6	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:18.235002041 CEST	192.168.2.3	8.8.8.8	0xbb09	Standard query (0)	myhealth.net.au	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:22.506105900 CEST	192.168.2.3	8.8.8.8	0x8338	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.298348904 CEST	192.168.2.3	8.8.8.8	0xde6	Standard query (0)	myhealth.net.au	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.880245924 CEST	192.168.2.3	8.8.8.8	0x7ffb	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.880923033 CEST	192.168.2.3	8.8.8.8	0x5943	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)

DNS Answers

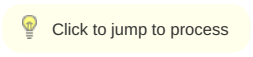
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 01:08:11.953648090 CEST	8.8.8.8	192.168.2.3	0xd22d	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 01:08:11.958724022 CEST	8.8.8.8	192.168.2.3	0x92bf	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:08:11.958724022 CEST	8.8.8.8	192.168.2.3	0x92bf	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:12.750621080 CEST	8.8.8.8	192.168.2.3	0xa4a7	No error (0)	myhealth.net.au		206.189.37.221	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:13.995008945 CEST	8.8.8.8	192.168.2.3	0x9aeb	No error (0)	gstaticadssl.l.google.com		142.250.184.99	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:14.000097990 CEST	8.8.8.8	192.168.2.3	0x31d	No error (0)	www-googletagmanager.l.google.com		142.250.184.72	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:14.197957039 CEST	8.8.8.8	192.168.2.3	0xa88b	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:14.198740005 CEST	8.8.8.8	192.168.2.3	0xfda6	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:15.132102013 CEST	8.8.8.8	192.168.2.3	0x776	No error (0)	www-google-analytics.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:18.269867897 CEST	8.8.8.8	192.168.2.3	0xbb09	No error (0)	myhealth.net.au		206.189.37.221	A (IP address)	IN (0x0001)
Aug 4, 2021 01:08:22.550410986 CEST	8.8.8.8	192.168.2.3	0x8338	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:08:22.550410986 CEST	8.8.8.8	192.168.2.3	0x8338	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.331707954 CEST	8.8.8.8	192.168.2.3	0x7cc7	No error (0)	gstaticadssl.l.google.com		142.250.184.99	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.906605959 CEST	8.8.8.8	192.168.2.3	0x7ffb	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.909930944 CEST	8.8.8.8	192.168.2.3	0x5943	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Aug 4, 2021 01:09:15.985146046 CEST	8.8.8.8	192.168.2.3	0xde6	No error (0)	myhealth.net.au		206.189.37.221	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4088 Parent PID: 4580

General

Start time:	01:08:07

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 'https://myhealth.net.au'
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: 5624 Parent PID: 4088

General

Start time:	01:08:08
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=1544,17615188742813691833,8383625610936018057,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

