ID: 432851
Cookbook: browseurl.jbs
Time: 21:01:19
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

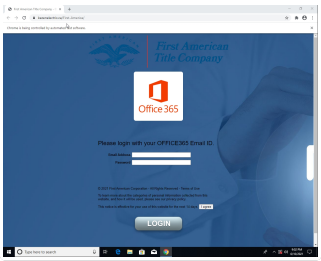
Analysis Report https://kezenelectric.ca/First-America

Overview

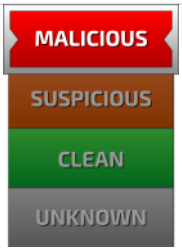
General Information

Sample URL:	http://https://kezenelectric.ca/First-America
Analysis ID:	432851
Infos:	

Most interesting Screenshot:



Detection



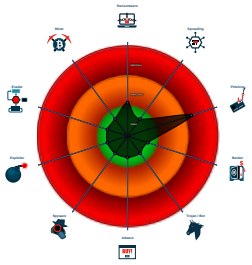
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6456 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://kezenelectric.ca/First-America' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6680 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1528,13816511049468976980,9988846167183782253,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

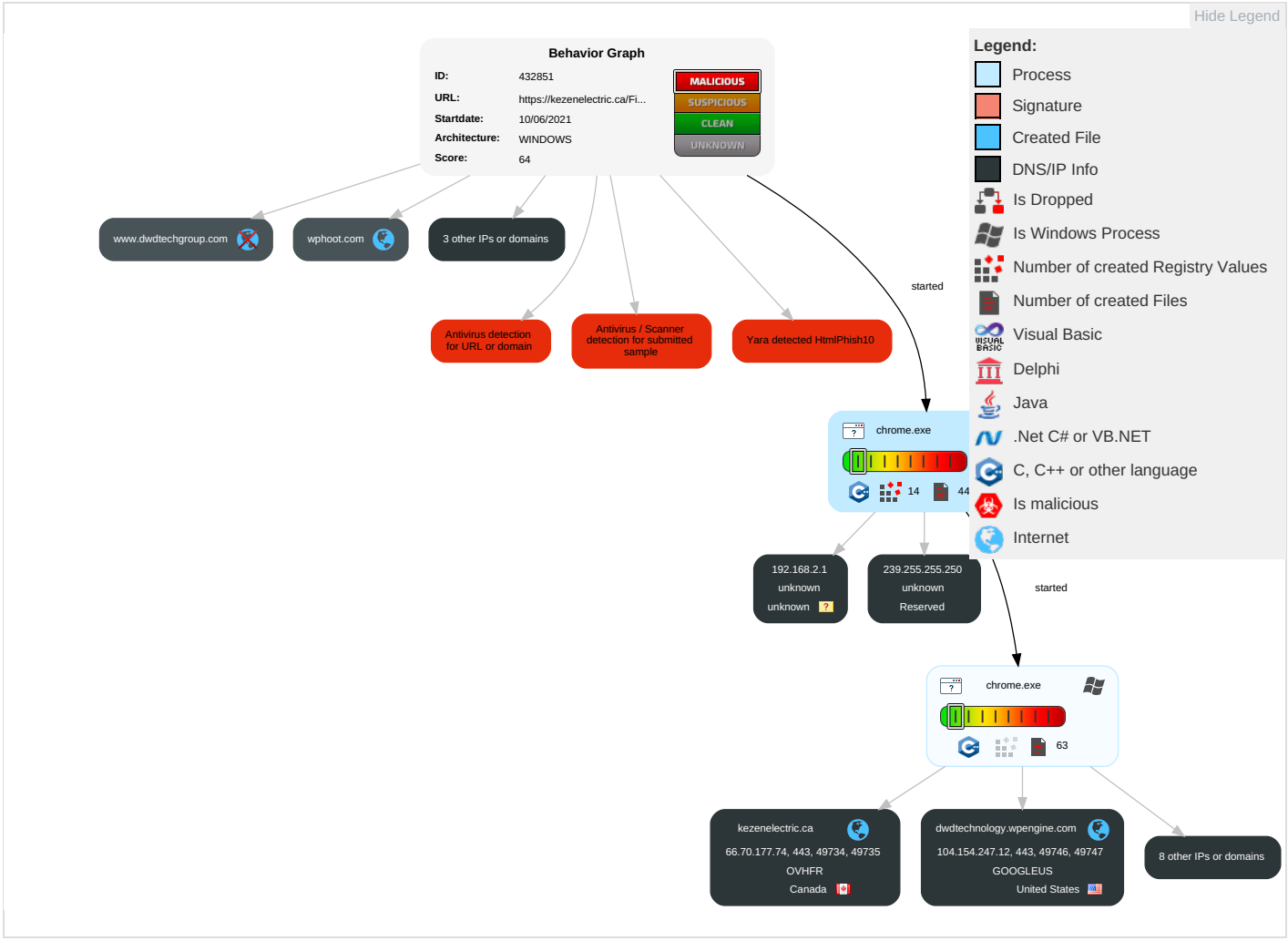
Phishing:

Yara detected HtmlPhish10

Mitre Att&ck Matrix

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

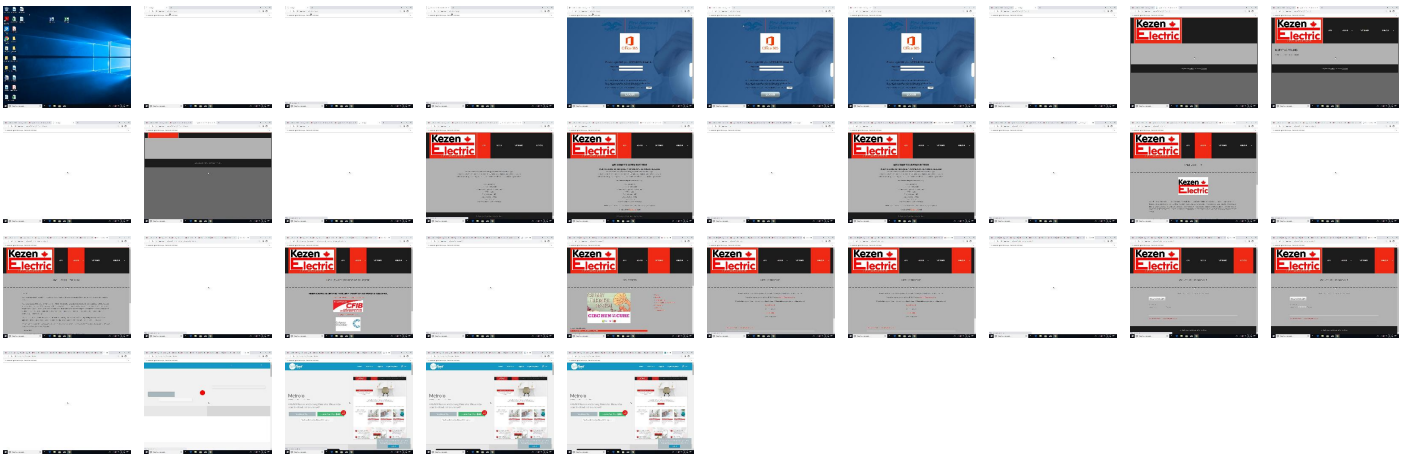
Behavior Graph

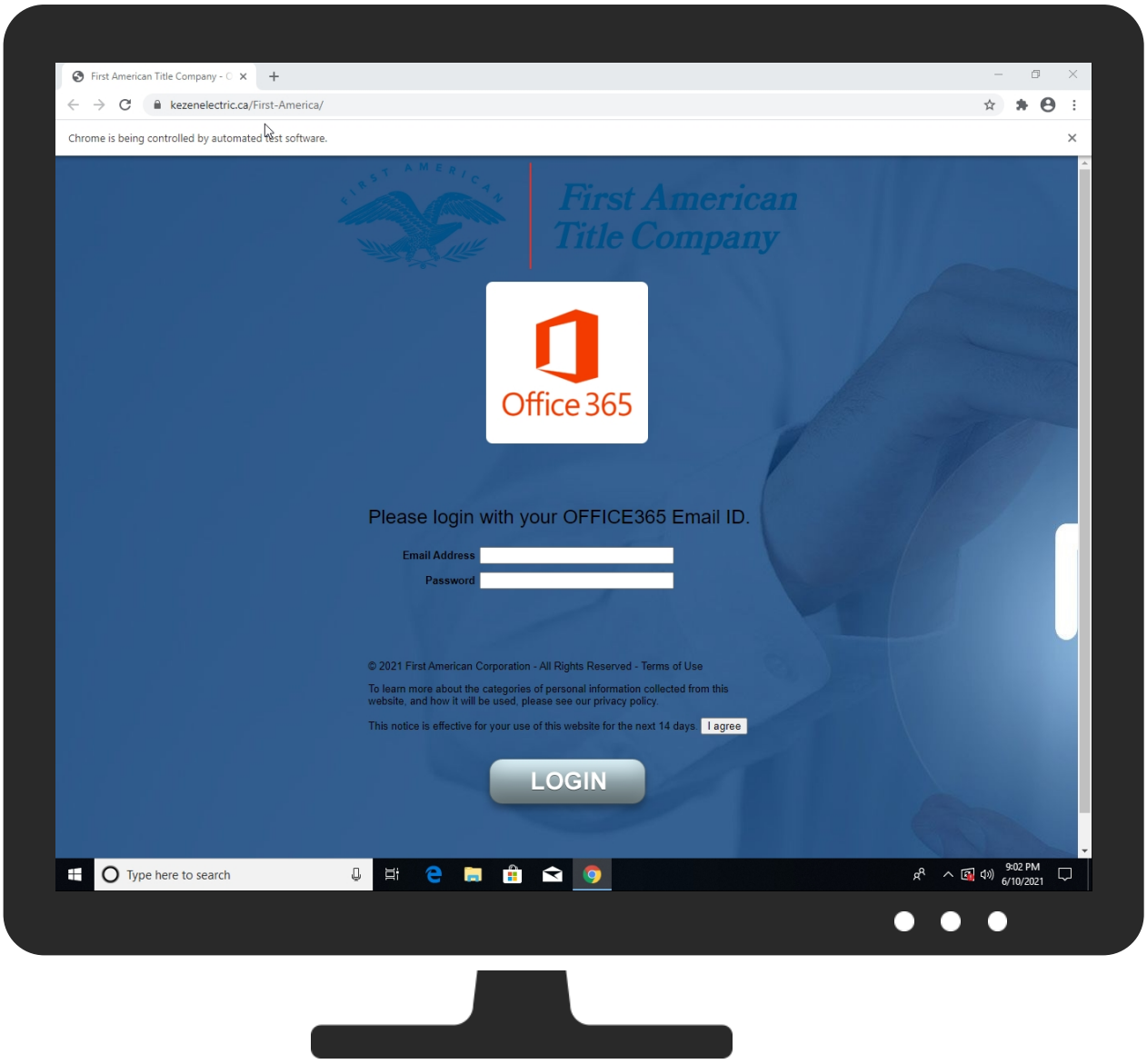


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://kezenelectric.ca/First-America	1%	Virustotal		Browse
http://https://kezenelectric.ca/First-America	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
kezenelectric.ca	1%	Virustotal		Browse
wallpaperaccess.com	0%	Virustotal		Browse
gofirstam.com	0%	Virustotal		Browse
www.dwdtechgroup.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://kezenelectric.ca/First-America/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://kezenelectric.ca/home/about-us/accreditations-certifications/c	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America/index2.php	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/plugins/wp-customer-reviews/js/wp-customer-reviews.js?ver=3.5.6	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.fitvids.js?ver=1.1aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.superfish.js?ver=1.7.5	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/modernizr.custom.js?ver=2.8.3	0%	Avira URL Cloud	safe	
http://kezenelectric.ca/Kezen	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/home/contact-us/testamonials/Testamonials	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/uploads/2018/09/cropped-LOGO-3-32x32.jpg(	0%	Avira URL Cloud	safe	
http://kezenelectric.ca/wp-content/uploads/2018/11/LOGO-300x179.jpg	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/hoverIntent.min.js?ver=1.8.1a	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/hoot.theme.js?ver=1.9.14	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/Kezen	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/wp-embed.min.js?ver=5.7.2aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/Wc	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://kezenelectric.ca/home/about-us/accreditations-certifications/Accreditations	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/home/contact-us/Contact	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.lightSlider.js?ver=1.1.1	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America2(First	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-AmericaM	0%	Avira URL Cloud	safe	
http://https://wphoot.comh	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/home/about-us/meet-our-team/Meet	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	0%	Avira URL Cloud	safe	
http://https://wallpaperaccess.com	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/modernizr.custom.js?ver=2.8.3aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.parallax.js?ver=1.4.2aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America/First	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-Americal	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-Americak	0%	Avira URL Cloud	safe	
http://kezenelectric.ca/	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/home/about-us/About	0%	Avira URL Cloud	safe	
http://kezenelectric.ca/wp-content/uploads/2018/11/CCC.jpg	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.dwdtechgroup.com	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/wp-emoji-release.min.js?ver=5.7.2	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.parallax.js?ver=1.4.2	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/k	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/plugins/wp-customer-reviews/js/wp-customer-reviews.js?ver=3.5.6a	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/wp-emoji-release.min.js?ver=5.7.2aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.fitvids.js?ver=1.1	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-AmericaFirst	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/hoot.theme.js?ver=1.9.14aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/exec/fd_helpWin?topic=8#maintHZQ	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/hoverIntent.min.js?ver=1.8.1aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.superfish.js?ver=1.7.5aD	0%	Avira URL Cloud	safe	
http://kezenelectric.ca/wp-content/uploads/2018/11/index-300x117.png	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.lightSlider.js?ver=1.1.1aD	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-content/uploads/2018/09/cropped-LOGO-3-32x32.jpg	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/home/past-projects/Past	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America/(First	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/hoverIntent.min.js?ver=1.8.1	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/wp-includes/js/jquery/jquery.min.js?ver=3.5.1aD	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://kezenelectric.ca/wp-includes/js/wp-embed.min.js?ver=5.7.2	0%	Avira URL Cloud	safe	
http://https://kezenelectric.ca/First-America/2(First	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kezenelectric.ca	66.70.177.74	true	false	• 1%, Virustotal, Browse	unknown
wallpaperaccess.com	172.67.7.204	true	false	• 0%, Virustotal, Browse	unknown
gofirstam.com	104.129.24.42	true	false	• 0%, Virustotal, Browse	unknown
dwdtechnology.wpengine.com	104.154.247.12	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
wphoot.com	35.208.111.117	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
www.dwdtechgroup.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://kezenelectric.ca/First-America/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://wphoot.com/themes/metrolo/	false		high
http://https://kezenelectric.ca/home/past-projects/	true		unknown
http://kezenelectric.ca/wp-content/uploads/2018/11/LOGO-300x179.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kezenelectric.ca/	true		unknown
http://kezenelectric.ca/	false	• Avira URL Cloud: safe	unknown
http://kezenelectric.ca/wp-content/uploads/2018/11/CCC.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kezenelectric.ca/home/about-us/	true		unknown
http://https://kezenelectric.ca/home/about-us/accreditations-certifications/	true		unknown
http://https://kezenelectric.ca/home/about-us/meet-our-team/	true		unknown
http://https://kezenelectric.ca/exec/fd_helpWin?topic=8#main	true		unknown
http://https://kezenelectric.ca/exec/fd_helpWin?topic=8	true		unknown
http://kezenelectric.ca/wp-content/uploads/2018/11/index-300x117.png	false	• Avira URL Cloud: safe	unknown
http://https://kezenelectric.ca/home/contact-us/testamonials/	true		unknown
http://https://kezenelectric.ca/home/contact-us/	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.154.247.12	dwdtechnology.wpengine.com	United States		15169	GOOGLEUS	false
104.129.24.42	gofirstam.com	United States		8100	ASN-QUADRANET-GLOBALUS	false
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
35.208.111.117	wphoot.com	United States		19527	GOOGLE-2US	false
172.67.7.204	wallpaperaccess.com	United States		13335	CLOUDFLARENETUS	false
66.70.177.74	kezenelectric.ca	Canada		16276	OVHFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432851
Start date:	10.06.2021
Start time:	21:01:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://kezenelectric.ca/First-America
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:	10
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@43/213@11/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://kezenelectric.ca/exec/fd_helpWin?topic=8 • Browse: https://kezenelectric.ca/exec/fd_helpWin?topic=8#main • Browse: https://kezenelectric.ca/ • Browse: http://kezenelectric.ca/ • Browse: https://kezenelectric.ca/home/about-us/ • Browse: https://kezenelectric.ca/home/about-us/meet-our-team/ • Browse: https://kezenelectric.ca/home/about-us/accreditations-certifications/ • Browse: https://kezenelectric.ca/home/past-projects/ • Browse: https://kezenelectric.ca/home/contact-us/ • Browse: https://kezenelectric.ca/home/contact-us/testamonials/ • Browse: https://wphoot.com/themes/metrolo/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:02:14	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wlEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|[.w.M.!<- .}%.C<tDX5\s._..l..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.l..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1179760176564173
Encrypted:	false
SSDEEP:	6:kKy6e8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:h8kPlE99SNxAhUe3OMx
MD5:	8BDFE20E18281A76BC3C987FE651E496
SHA1:	EB1D6F64D8D317ABFB5B7455AB0B31A5F86B3B95
SHA-256:	F6DB33F0782B6C6A6C9BC6CD97717E88612E7EFEBE1648994A065E31DC85CC68
SHA-512:	DA0D03983C64F17DA10D9135B172B91A16476BA2C08350A5B225822CFA17B53592A815C274D380BCFBFD4A573BB47EB6BADF2D78F165F74480158DF95D7C306
Malicious:	false
Reputation:	low
Preview:	p..... .....^ ..+^..(..... ..... L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a1a5bbe-8aa9-4dc8-8139-02fc0a5e7de4.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):	172510

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a1a5bbe-8aa9-4dc8-8139-02fc0a5e7de4.tmp	
Entropy (8bit):	6.0804072516201515
Encrypted:	false
SSDEEP:	3072:9jdOR4ryDswL0T4qxb8IHqzESFcbXafIB0u1GOJmA3iuR7:BOIAsZ8qxMaqfIlUOoSiuR7
MD5:	F4F18F9651E9CD1F8AEE84A8F31315AD
SHA1:	19AE7D01314FCFB7575CFFF4512E685149E7ED81
SHA-256:	263F3BDBC5418EB7FDD49B09D55755406F598EA7D97D863771631BE67780DC05
SHA-512:	C9D5BEA3004DC1F5DA3900BFB9D3F5F9DA2843E4AF35819830A50105221CEEAEEC9DEBEDF71F1B4842484AAC475FE76796FB56504B57CCCDFAE19DCDAD326AE2
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623351733740586e+12,"network":1.623351735e+12,"ticks":308149267.0,"uncertainty":4828244.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\76da7b8b-f094-4fb5-b0c0-393127c4b8ba.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):	172512
Entropy (8bit):	6.080402610177291
Encrypted:	false
SSDEEP:	3072:ESdPR4ryDswL0T4qxb8IHqzESFcbXafIB0u1GOJmA3iuR7:dTIAsZ8qxMaqfIlUOoSiuR7
MD5:	2359E6E16190AD4C84070731EECEC524
SHA1:	BD7263D2B30D2876EBDA7E875DA0C002518F3427
SHA-256:	6DB3152AC2734C68296B27A673009A226D3A319037C284AB8C3C3C11B6106BCE
SHA-512:	4B66A3F6DF124FC1CC649C11380A3A0FA36BC71E6CA087957E30E70DE82BDE63483F1156F907772183CA363444CF45B188A8DCC8FDD5916F6C88FA57E1E6781
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623351733740586e+12,"network":1.623351735e+12,"ticks":308149267.0,"uncertainty":4828244.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922716026734"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\9548abb1-5605-427d-b54b-4fedc2fe2c35.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7520556223906354
Encrypted:	false
SSDEEP:	384:B/JWmYj5UD8iV7diFNOrbvi63RqEZH05Glcr3EyQx58YMLrzSmfEXUmWqlOkQ2NZ:peWpJCklNQeHc+gInv2aKM6Gxd
MD5:	F7E21A47F193D74BD07DA83D03809E00
SHA1:	DD39332CE4CE9C807E8EA6E9A6A0D3BF236FA542
SHA-256:	EABE0C19BCD77DA23D0EAF4936A886A6EDDBA70002799079F2C18987D49D2C77
SHA-512:	7C011122A69B1C4A7D5F14DCD2D0B49A717EE220620B0BB5ADAD43C90565BFB14A4B2071A542365D3BB03B9A01F2C1D5AE3E813E3B85A7672819E7DD99A9F1D
Malicious:	false
Reputation:	low
Preview:	.q.....*...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....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c7b99d7-f559-43b7-a91c-0ac609b76ef8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7516311922637042

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c7b99d7-f559-43b7-a91c-0ac609b76ef8.tmp

Encrypted:	false
SSDEEP:	384:v/JWmYj5o8LiFNOrbvi63RqEZH05Glcr3EyQx58YMLrzSmfEXUmWqlOkQ2Nf1WPH:TWpJCklNQeHc+gInv2aKM6GxY
MD5:	5561C7B3F66AB9C12E73DDF051205793
SHA1:	5076E6DAFD4AAB702C37963E9BBC489C678ABD0F
SHA-256:	BCF6B5772ABF3DEFB58CF0A5E28502E4280E90F2A074D5DF291A934A123E856E
SHA-512:	F0DD4AB74E1A6DB7B349EE288FEC739B576DFC6C0D5951E5C962D77D2222336AA3B82F800B4FAFCC9BA85C88BF3782FE2F1934B7A976563379706BA4E0D1D4 4
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 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C5 9
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\02be7372-55df-4983-b6ff-7018cbaa805c.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"adverti sed_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","s upports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{ "srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1288b324-97f1-48f3-bcfc-db67dedd2185.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):	1375
Entropy (8bit):	5.5799039582399015
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSzUrfwU7G1KUwzkq/HeUeF23ZAUEzUe8hUts7wUeE4sRUeiQ:Ym6UUh/vUmKURqPeUeF2eUcUez6wUect
MD5:	C998D9210ED638B6036BD4CFA085F3FE
SHA1:	77D25FB2EE5D2361263109DF98F978D49F0EB2FD
SHA-256:	86056C2AA6C67F745DC95C6C1D4B507AF560F4D7F0841877025E2963EF8061EE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1288b324-97f1-48f3-bcfc-db67dedd2185.tmp	
SHA-512:	073D01E90C25CE1AF8D6D3DD604169759C6721DD2E841610EFC8ED2D63F6FF351EB8267A15A4D62A69F75CA06109956305BF22A5520BABC7BC6E70A1A9D52D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1634238230.695322,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623351830.695329},{"expiry":1654887829.754591,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623351829.754597},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1634238135.533594,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623351735.533599},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1e072769-31fe-439b-9f52-047825c17262.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):	5816
Entropy (8bit):	5.176850227250993
Encrypted:	false
SSDEEP:	96:nGELya2RlSOV0GgHIVw+d5k0JCKL8skG1WbOTlVuHn:nXLV2RoKgHIfdh4KvkGg
MD5:	56DF2F4EFC5AB026B42CD7A814BD8DD1
SHA1:	59BF7F02531760999EFFC0BAD45373E367047422
SHA-256:	26ABB73F58D4022F2833673A82B2CDCBD1D9100F95CDAE02C037E3859C2749BA
SHA-512:	4385F43A65F53D419217DA418F513DD9173C25203AE0BD0EAB747B0414F10F8B93B9B0103FD06AB263D97E57ACF419C2B158D598CDE41232B1ABCBD62B14BD8 D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267825330255117","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71e4fe4e-990f-4b98-aff1-06858d9696bd.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):	22602
Entropy (8bit):	5.536554649215923
Encrypted:	false
SSDEEP:	384:PY+ttLlXsXn1kXqKf/pUZNCgVLH2HfDlrU1HGXnZ5ObarB4d:rLlOn1kXqKf/pUZNCgVLH2HfprUJGXn0
MD5:	7DFEC4C5A127D923F7E3E768FD8236CC
SHA1:	CE06950A0789B8B86BCA8CD72E55051D6B22D6AA
SHA-256:	18EA735FD8EFA90C02029EAD1A706D4152E7FE6AAF6900B3E5F2F9CBFE91B923
SHA-512:	8DA0FE98615AF27C3397163862184950F231FFAEF842F7060DDA0B461F0C4A440F9CA6EDAC618266685355E078C0D3F1C688CDBFA692CA9977BB1EFFA3C2255
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":"13267825330020024","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\734753a9-f224-42a9-a38d-289cb990c9ac.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\734753a9-f224-42a9-a38d-289cb990c9ac.tmp

Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7646c7fe-eb7f-4111-baed-47a93160456f.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):	2694
Entropy (8bit):	4.8667647911042895
Encrypted:	false
SSDEEP:	48:Y2nzMKDHGXtwWs1RLsorWquuzsAZyKsb3zsH7tMHZs9MHo6zs9MHRsOEkqGYhbw:JnzMKDHGXO3TrluUZyQ7tGqGMGZEj7hM
MD5:	52E802E0DB18D45B5619FA722C3C68CB
SHA1:	620276E1FD8A378B70250DEC6A3D63756F9754A8
SHA-256:	39DC053FD252A26FB8D8563200A71D4C20426289D1720E8D1F7AEA49385E2A7B
SHA-512:	19DCF91E204532BFB9B81CE9D7F487C198AE7F89B0956E065160A3AA1BACCD187F1AD48895470CE6516C293B2D83CE81F322BA2802B66547F646BD5513065F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270417334054459","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270417335533390","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ssl.google-analytics.com"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7ce2b011-7949-43fa-aaba-66550c560841.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):	5.577697207350443
Encrypted:	false
SSDEEP:	384:PY+t4LlXsXn1kXqKf/pUZNCgVLH2HfDlrUx5ba8B4yB:mLlOn1kXqKf/pUZNCgVLH2HfprUx5bVp
MD5:	8267DDF9306C6F258ACF71CA80964C8E
SHA1:	827890DFE3AE763977210296D23BD6BAC8545EDF
SHA-256:	50F82A21876BEAC200FDC22311C283D760B72F5B86FC6E0F8615BD97D82A99D6
SHA-512:	1ACEBC04A5275372DF3E1BB4930575331510DC22F6D5D4A28901F59476A40CC6488B1F8E3E1F3A9E8C56B380092156C86D13A03E44605803DCC3212F4B945C45
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":"13267825330020024","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9516885b-c89d-4b07-9f59-157c5e4b9756.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):	5789
Entropy (8bit):	5.174684164705146
Encrypted:	false
SSDEEP:	96:nGELNa2RlSOV0GgHIVw+s5k0JCKL8skG1ObOTlVuHn:nXLw2RoKgHIfsh4KvkGs
MD5:	A097E5E24661C158095C4FFCFF0431C7
SHA1:	66E9999FC5D9C5409310CE547111F334F8CB76AD
SHA-256:	3A6159F4CFCAAD8693BD1DD851A582113204E204D52FD66E2DFE4E7357CEB850
SHA-512:	28252ADE9B7B0CF799170B97420E9EAB51EEF4923BAF7EB5C4EAF64A8EEE4BFBEB5927B7DB03225F2D4303F194823D25E93DDF346F1B31397986294BD528B951
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9516885b-c89d-4b07-9f59-157c5e4b9756.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267825330255117","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.131904463807857
Encrypted:	false
SSDEEP:	6:mwa2lyq2Pwkn23iKKdK9RXXTZIFUtpDagFz1ZmwPDadRkwOwkn23iKKdK9RXX5LJ:e6yvYf5Kk7XT2FUtpOs/POdR5Jf5Kk73
MD5:	BB56950367F6C76794008EE7C2A83797
SHA1:	02CDAE2CB6324906E38C41D92EE804D293981670
SHA-256:	DAE1950386D84ECCC9482945B1BDBBFC612C59BE9F02A732BEC1DCB1BF08554A
SHA-512:	AD71960F68C826E9D5EB90EAEB102CF1826BFA87D6E82B185D7203A3B0F1B8FBA112F821B1C68062E86666B3578C18E6B0241E5C996C82ABB4101D290B7BB17E
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:30.161 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/10-21:02:30.163 19c0 Recovering log #3.2021/06/10-21:02:30.164 19c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.140027897682369
Encrypted:	false
SSDEEP:	6:mwa89yq2Pwkn23iKKdKyDZIFUtpDap81ZmwPDa4OjRkwOwkn23iKKdKyJLJ:ewyvYf5Kk02FUtpOk/PO4OjR5Jf5KkWJ
MD5:	81C9B2DAB9EAB7A3F26DD8956FDE2C2C
SHA1:	B4305EBB207259E24B293FA7200070363FFF94C7
SHA-256:	5E2E4E7AF189CC23E10A815E7F3B908684963F51102D76143FFE03A27F628B72
SHA-512:	C570B5F0A4EAE83A4D41BD2B370D454D4092DA33AB65F873D9A0540677D6DB636C2167C253EAB45CE0217C4A944460695B36CEC4794479E58C4F38C7F1D99E1
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:30.152 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/10-21:02:30.156 19c0 Recovering log #3.2021/06/10-21:02:30.157 19c0 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\002445640ee1de89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.476375728469192
Encrypted:	false
SSDEEP:	6:m9PYsNKTOlAZ0QJ7RURiKuU91dTkXRPNK9umxM3grBlZK6t:4TYxL1KLTkXRPYIWlT
MD5:	3823F69558D90E5E80E8268F65AADB9C
SHA1:	63A2BAF33F4E66547047B93DB82760E86435F15F
SHA-256:	7C1354CF78E43AB9EA696FD9CCDF0693B29ED4941E4330F1A046DF319468F8BE
SHA-512:	81EB794233C585EE798AA1B716BC74E3382EF5F42CB6FD0329F47A4E83438C911C9E5C8605A0F79DF544649B69FC6FB34732C52528693702BFB62AB9C28436CB
Malicious:	false
Reputation:	low
Preview:	0\r..m......u....u.E...._keyhttps://wphoot.com/wp-content/uploads/siteground-optimizer-assets/hoot-theme.min.js?ver=2.12 .https://wphoot.com/.>.U.#/............P...........;.t.....rX$....n.O.0..NZ..V.A..Eo......M.\..........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05a632044e49ec3d_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\05a632044e49ec3d_0	
Size (bytes):	219
Entropy (8bit):	5.509924632655076
Encrypted:	false
SSDEEP:	6:mg9YsNKTUfYAR8M/VTHNK3XAWZHJfgopkP4XK6t:rtYgf7Rd/VTHYZdJ4opkP+
MD5:	9A5E0F049DB36EB3AB3CE9120ED56761
SHA1:	FFE1C9A806AA0DAAD9E00CAACF3B78AD203FE2EC
SHA-256:	A76CEA0E85663F4F35B728233804FCEC0218B51EB3177F1043057D349D8BC279
SHA-512:	A18F2FA7B306CC78AF5ECAFDDCA7FBF7233C03E51E44B64E312B86E6F9BB2C5614C65D5A5957E64E2872CF15A0668AB32AAE6CCF90A1494C8E1CB8D09ACA2966
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....k...._keyhttps://wphoot.com/wp-includes/js/hoverIntent.min.js?ver=1.8.1 .https://wphoot.com/x.U.#/.....H.....~....,K..HC.0...L.LeAu....A..Eo.....Z.\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\06aba3ef4a05b1d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18602
Entropy (8bit):	6.147174291310593
Encrypted:	false
SSDEEP:	384:nfOfGN5oRQNTzMWYrFVirhAPzVi77k1zZ9Xp/:nfdeRQNxOViVALVi7U7p
MD5:	E19F952C0E4100C7D01872EA3142D01F
SHA1:	3CE46F4B497D67F1B07F7CC2D07C262E440415C4
SHA-256:	400AE96B04AE97754A92E448050DBC84574D0C5AC3AFCF2DB8E9E9E680C7A5AA
SHA-512:	1BCB54C65611171BDEE62374629E82A811C27645DF191884C9468F1B593E9DDC81801EFAEB4EFCC506F0A4A6ECE62108659277389E46D2D208131CC26F451A47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...^.r...._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/modernizr.custom.js?ver=2.8.3 .https://kezenelectric.ca/.d.P.#/.....l.G...%....x...mi.(2t.p{1...H.A..Eo.....w/01.....A..Eo.....'.....O.....G.....D.....\.....(S.<..`0.....L`.....(S...`.....L`.....Rc~.....6.....QcV.~z....document..Qc.g.7....window....Qc.....classes...Qcn.l.....tests.....Q.P.N. ....Modernizr.....Qc..X)....prefixes..QbN.p.....is....Qd:+S.....docElement....Qc.w.v....isSVG.....Qd.....domPrefixes...Qez.....createElement.....Qc.p.....getBody..$Qg.....injectElementWithStyles...Qd2./.....testStyles....QefS.....cssomPrefixes.....QcF.}U....contains..Qcj..d....csToDOM..QcNLC.....fnBind....Qd>.Z.....testDOMProps..Qc.....modElem...Qc.....mStyle....Qc._k.....domToCSS..Qe.....nativeTestProps...Qd>.>q....testProps.....Qdb./...testPropsAll..Qd..[.....testAllProps{$.....$..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d1b2948d4525464_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	5.439476836131711
Encrypted:	false
SSDEEP:	12:3epGxH/stqzNLrFBR9RJP9/TWfZpGxHz1hYgH9/xq0mJ2cyQ9oRJ2q0YlX:RetsNtn99WfSlxTq0mQcl9oRJ2FlX
MD5:	0C39AC5DECED5CE11C9E9BC6DB62E86A
SHA1:	03FE60BD8A1CA866E50094B597F8D4F1E00D4C9E
SHA-256:	FDE44DCAAB340F85DC09394A2085F0269CD6FC99CB925080DE96D67F9889ED06
SHA-512:	D4CE91745AAF274B923BD1E3F234825B3D814525C951E8EF37DD053E3988AE2451E04FC1AFBF83A30796AA8E008E05F321F39C69981F4D0CCE4856DA21BFE95
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...[jN...._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.fitvids.js?ver=1.1 .https://kezenelectric.ca/...P.#/.....r.....A.....{"...).e..L`.9GK.^...WRgV..A..Eo.....2/i.....A..Eo.....P.#/.....'.....O.....F.....0.....(S.H..`F.....L`.....(S.@.`:.....L`.....0Rc.....`$...I`....Da....4.....Qb...|....fn...(S.....Pd.....$.fn.fitVidsa....r.....d.....@.....d.....@.....I..!..@.-....\P.a.....O...https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.fitvids.js?ver=1.1.a.....D`....D`....D`.....`....&...&..!.&..!..D`....DI]d.....@.....Qc.rg!....fitVids...K`....Dj.....%.....&.(...&.....-.....b.....,....A.d.....@..`.....Qc.g.7....window....Q.@...#....jQuery....Qc.@P&....Zepto.....K`....Dl.....&....&.(.....&.(...&.]...&.....$Rc....`.....Ib.....|.....c.....P.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\200e0abd4ba2ff0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.38429917407301
Encrypted:	false
SSDEEP:	6:milXYzUMOiuVN3LsNKHx6lQFTlJftm4H9K6t:MVs+4Kwlxw6X
MD5:	A89F5B00134D2DCAB41795B61E3E0FFD
SHA1:	3476B0265B014F8E41BD407EA4DE7746AEFD0FD1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\200e0abd4ba2ff0b_0	
SHA-256:	5DFC44688CE9368E18E1985C6077FBDDFA43E1FD21FF7D8C9F78A405DE6EFD0E
SHA-512:	273034E6E00166AD6A8A274CA3007B38BBE4809A3CFE0D19D52CF1BFA51B147C31EF87EF2C918B6B595E59B2488191187A00939A6BAACC951A182107D0634B5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....N...._keyhttps://ssl.google-analytics.com/ga.js .https://kezenelectric.ca/...P.#/.....=O.A..6x....l1.0.B..N.....k.A..Eo.....2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\229c73a4fe442ea3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1416
Entropy (8bit):	5.681853152017233
Encrypted:	false
SSDEEP:	24:RvBCrttavF5dR3l9FcFuhPtGBCrzhbz6ik+3LgAonYkWVjkXTJ81aD:nChteF5dJvFcFVCPs9YLlkWGXTJ81A
MD5:	DE9F7787FB065C7C5139F516FFE65E5B
SHA1:	2730FDCA4558D0EE753931C461D0B61C07CA7C73
SHA-256:	CB5FB57D2A69594BA4985CEF13808D143B2ADBA8B89DB5C9F112C383256F42D0
SHA-512:	BF165DCA7BC66F33E7D07344E04120E783CE25F186AF29672568D19493FC030459DE15B6A01B1D7AF067D0FE99F95351DBEC760580445D2F9FBDB15B39CD583
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....n...._keyhttps://kezenelectric.ca/wp-includes/js/wp-embed.min.js?ver=5.7.2 .https://kezenelectric.ca/k..P.#/.....-ef@..3..x~..|..2.".E.=....f.I.A..Eo..... .3.....A..Eo.....k..P.#/.`.....'.....O.... .....(S.<..`2.....L`.....(S..`.....0L`.....@Rc.....Qb..]}....d.....Qb.{b.....c.....Qb...B....n...b....$..... I`....DaX.....(S.....Ia.....QbR..&....t.....@.-....PP.1.....A...https://kezenelectric.ca/wp-includes/js/wp-embed.min.js?ver=5.7.2...a.....D`....D`....D`.....`....&...&....&. (S.....5.a.....!....a.....a.....QbNN.v....wp.....a..... Qf.I.....receiveEmbedMessage.a....H...I.....d.....@.....&....`....DI]d.....@.....Qe>.).....queryS elector.....Qe~]m.....addEventListener..1.....a..m...Q.`^.a.....DOMContentLoaded..Qb.r.....load..K`....D.Q.@.....%...%.....&..&.....&.(.....&.(.....&...&...&.(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5278677776ece701_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.657737639469726
Encrypted:	false
SSDEEP:	3:m+lqqH08RzYrSL1cdXWKQKDnYjWaoA3ulKNlHCv8K/5dM/o54qG35DV6RmI7t/pD:mtq1YGLKdXNQKjsRuzEupGJlMthK6t
MD5:	8BA5B69DB720FCD94B83EF0D83976D65
SHA1:	5694AB738EDA8A1E0DD1E43240FD4F846FC141B9
SHA-256:	ECE4870FC5EAB4334351AAB4A55A169B333AC915C39A2A595A3914C646FB0AD8
SHA-512:	9921F4EFCBE17AE45DCF6C3D65D02D483A1BE609B9897029A121FEBDCEEF2A82E7F9E82749B35D946F9719360072B758272266B647229859E9A56E36B5421098
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...7..P...._keyhttps://www.gstatic.com/recaptcha/releases/CdDdhZfPbLLrfYLBdThNS0-Y/recaptcha__en.js .https://google.com/;..U.#/.....z.....4.< .....p.A..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5da3893660e7a47a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	909
Entropy (8bit):	5.5058910719206775
Encrypted:	false
SSDEEP:	24:PIs1y/zx8YdCq07hP1YPdktESI6HHv6eK0x8QJ:PIKCzeYEqCxOP6/I6LK0eQJ
MD5:	81DBEFAF31C6B6DCD29330869CDC966E
SHA1:	756513380A3DB9503833CA3950CAD73728653CC5
SHA-256:	5E76482B37337EB069A28347659FB6B29D9199291E7280E9BE34C65DA94D4CDA
SHA-512:	6EFF12496A1D4DB8175FF06DA3CB588C1FF0627F5AD99C5669CCB2A11C112F372A69CDCC43FC095DFB6170EA298BC330EA499B4A2BBC981EB416EA2F2E421D 2A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....l'"...._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/hoot.theme.js?ver=1.9.14 .https://kezenelectric.ca/...P.#/.....~.....i....L]x\L..5.1.....pn.. .A..Eo.....N..J.....A..Eo.....P.#/.X.....'.@.....O.....tmy.....(S.H..`H.....L`.....Q.@...#....jQuery....QcV.~z....document..Qcfe.....ready....(S... ..Ia....>....D..m-.....@.....@.....@...$..@.&.&..@.'.'..@.(.....d.....@.....d..... .$..@."...IE.@.-....\P.a.....N...https://kezenelectric.ca/wp-content/themes/met rolo/js/hoot.theme.js?ver=1.9.14..a.....D`....D`....D`.....0...`....&...&.....D`....DI]d.....@.....K`....DI .....&....&.]...&.(...&.....&.Y....&.....$Rc....`.....Ib.....*..... .c.....@.....d.....i....L]x\L..5.1.....pn...A..Eo.....4zd.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6485724e45ee2243_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.507643736334857
Encrypted:	false
SSDEEP:	6:mdYsNKTOlAZ0QJ7RURCGudTfNKWA77MwwJDLNK6t:kYxL1KCGkTfYswwJDD
MD5:	8A97B4CA62F1945E3F9E8EAC19804947
SHA1:	91DE57CE0197D71F2C2F2F28BA0DDA79A51634B1
SHA-256:	302ADB89776349FC3F60B252BCCE8BC9A61551B31E7A25F925AD42C6684D8491
SHA-512:	1C4DE4D6C9A2AACF2BDF9A57F85B248EC44E361BA64CA87DB3C452E3DB7CBE216F412CC492B599779CA14EFEDA57D1E64A57425563EB1320E250DE03F73DC45C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...}..O...._keyhttps://wphoot.com/wp-content/uploads/siteground-optimizer-assets/contact-form-7.min.js?ver=5.3.2 .https://wphoot.com/_..U.#/.....B.....J.m...}....._..H.W...Za....n...A..Eo.....>Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c75240678e5e01e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.640485681456948
Encrypted:	false
SSDEEP:	6:mVjPYGLKdXNQKjsCNK9SzCZSowWWhK6t:iehNQKjsCY9eCZS1
MD5:	B1C11B345F3BD24353604373620CEC63
SHA1:	64D65C791C960FBBD07D7ACA9F664AEEB0CFE16F
SHA-256:	5D0878DC7FE2BF4C2F0CE5CC69D3579B75C17208849773C8C405B3349AAC09B1
SHA-512:	09E37DFB31D4A3942D09FC4D931172FD83B40810989D07E89508BBE60F3D36A654C7E1BEE2DB23328C0A101ECAE2DE8212B8C53ED460FFE2007A36A40BEF0EAD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....n....._keyhttps://www.gstatic.com/recaptcha/releases/CdDdhZfPbLLrfYLBdThNS0-Y/recaptcha__en.js .https://wphoot.com/;..U.#/.....{#.L..m7.J..T.}...,...4..K,...A..Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75ddb2c602fd7877_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2194
Entropy (8bit):	5.501418630277821
Encrypted:	false
SSDEEP:	24:afKtBmlxglE52bYNl34R5SEXKZ1hOmRrnKEWjCYCBkfPaVzboehmj7qEuekVBa0b:J2cunNpUmRYjCY5OYewjqBaU4XSZaM1
MD5:	476E6EC2CD26E9D0C5860A4C40E5CE1B
SHA1:	DE030238E2D70A50D58174C3128B565B3312FC48
SHA-256:	9FF6DB73BC0B39D813E2E801121AEF9969FB2F67F8E0C38A6A600C9864EDDE50
SHA-512:	2FD5C9DD3D888E23E13027A176A61F80234EDD53D44122C10A5B715954E5FB4930EEA77307CA7C197949B557E6488F0C945424CDB071B15354B4E39568E4FC6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....%....._keyhttps://kezenelectric.ca/wp-content/plugins/wp-customer-reviews/js/wp-customer-reviews.js?ver=3.5.6 .https://kezenelectric.ca/.c.P.#/.....2.....2....w..)hW... 7...+..o.&.....A..Eo.....[.....A..Eo.....c.P.#/.H.....'.....O.....WmJ.....(S....`....pL`4.....L`.....Qc.....wpcr3.....1...Qe6,.G....mousemove_total...Qe"Oe.....keypress_total....Qe.>.....mousemove_need....Qe2.....keypress_need....(S.....5.a.....Pd.....getPostUrl.a....0...IE.@.-....pP.....c...https://kezenelectric.ca/wp-content/plugins/wp-customer-reviews/js/wp-customer-reviews.js?ver=3.5.6.a.....D`....D`....D`.....`...`,...&...&..A.&.(S.....a.....Pc.....onhoveraK...D...IE....d.....&.(S.....a.....Pd.....set_hover..aa.....IE.d.....&.(S.....a.....1...Pd.....showform...a.....d.....IE.d.....D&.(S.....5.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\786b0adb2bd9c037_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4225
Entropy (8bit):	5.553045513314926
Encrypted:	false
SSDEEP:	48:8aCfDrlJVV0P+/Nmxj9UBFMwwtRWnqPtR9bTalwf5TojQEVq5J4tO1vA3786qd3h:cffrVV0G/SI3nAtGFwAr86AZD
MD5:	C802CFA55919B977E70BB385A9E8A98D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\786b0adb2bd9c037_0	
SHA1:	281257A327986DB12FC7921B07E712C5DB316D59
SHA-256:	427ACED1C0FFF534C9CD67DA43CB65DB02A71E0C5C0A35B0654160364D37210A
SHA-512:	0CCCD1B9C3E1C866C7B6DDB422AF158C1A407BD6D56C76881A2CEE96556ED0604E2BCCEA051E7B1322625D9D5158D54938D5251615412B37BC0D1C7C81416B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q....?....._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.parallax.js?ver=1.4.2 .https://kezenelectric.ca/...P.#/.....~.....ix*..P..U.w...%..{...({:.yL..-...A..Eo.....z.....A..Eo.....P.#/.H.....'..1....O.....@.....(S.@..`:.....L`.....(S.%..`.....xL`8....XRc(.....QcV.~z....document..Qc.g.7....window.....QcRY.l....Parallax..Qb.H.....old.e....$.....$.....l`....Da.....c...(S.....Ia..... ..f..... ....$.'.....D.....@.-....`P.q.....R...https://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.parallax.js?ver=1.4.2..a.....D`....D`....D`.....|...`:...&...&....&.(S....`t....0L`.....4Rc.....Qc.%.....lastTime`....l`....Da.....`.....M`.....Qb>3_!....ms....Qb.7. ....moz...QcRaV ....webkit....Qb.....o....M..$Qg.7.....requestAnimationFrame....$Qg.,.....RequestAnimationFrame.... Qf.t.j....CancelAnimationFrame.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80a193e1143879d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.595924647026285
Encrypted:	false
SSDEEP:	6:mpVYsNKTOlAscia5WyfladTsLJNKzD6FlIoNqAzrxgK6t:G1YxIuldTsLJYPcIIck
MD5:	F06BB81E0AD9392C86EBAA526471129F
SHA1:	11368A4F8516E11A600DD1B687871626C2E7A1A4
SHA-256:	43A1357EBC9C28939D990AE31D757E1B05F5A67BB82B93E0D72AC83B8061C93D
SHA-512:	5F4B0D9A2E4643613726D2876C12FD26B464059755D94D37E8CB6C9BCF028ACA6C88E285CE7053DCEC23F535D9D76AA0876016832A5BE9CD9EE0DAA3E006481
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.....`....._keyhttps://wphoot.com/wp-content/plugins/easy-digital-downloads/assets/js/edd-ajax.min.js?ver=2.9.26 .https://wphoot.com/...U.#/.....H.....e.:.B%.}_.....'..I..\.%.*8.A..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ed7979f48ca3039_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4954
Entropy (8bit):	5.726787359028213
Encrypted:	false
SSDEEP:	96:a9ecRDokJzUQfzFlplygflVDtVsvoCTIbAsr6tOFJa/squM/:utzUQJl/FlVDtVsvaxwsquM/
MD5:	26781ECF879BFC628A7376992739635E
SHA1:	E21D63FE3F79016B8F79CB73FEA640ACFA11EB73
SHA-256:	5D6B31CE220A6756CDB856B572EBFB44ADF3C70F57A73A9FF5F1A31C3DA252C0
SHA-512:	BDA2CE5886E369D41E7331187F89F65EE5111C38C6020AD8014CB08A7B5BA725D6E2821435DAE2041123939B4C387E65A9855CDCC8CBBB1BF29CC407C825ACC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.superfish.js?ver=1.7.5 .https://kezenelectric.ca/...P.#/.....m.....w.F.F)..sf....@=..3].!....A..Eo.....A..Eo.....'.T.....O.....y.....(S.<..`0.....L`.....(S..`P....HL` ....@Rc.....Qb...E....w.....Qc..d.....methods.b....$.....I`....Da.....:...(S...`.....lL`2.....RcN.....Qb.{b.....c.....Qb&.y.....ios...Qb..F.....wp7..$Qg.....unprefixedPointerEvents.. Qf.....toggleMenuClasses.....Qe.i.....setPathToCurrent. Qf~..Y....toggleAnchorClass.... Qf~.....toggleTouchAction.....Qc.....getMenu...Qd.S>.....getOptions....Qb.M.....over..QcbV.....close.....Qb.(.`....out...QdN.w.....touchHandler..Qev.)^....applyHandlers...n.....I`....Dal....3.....,..a.....Qc.....bcClass...Qe.%.9....sf-breadcrumb.....Qd..(.....menuC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e21f8aa16d21fc2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.495841806826102
Encrypted:	false
SSDEEP:	6:misEYsNKTOlAZ0QJ7RURoMadT7FNKnk2pt/Vhm40DK6t:ocYxL1KoMYTxYk2pVHmt1
MD5:	56A0C909F184389E11692F3D446A06C4
SHA1:	6F6D3854A2DA39F1D5D3EE27E676872EBAF79CEB
SHA-256:	A3AD7BE842B4CD9B65D9384DB60327CAD2272C1D0D05EE251ABA3D08717BA064
SHA-512:	533C2AA86313E0190DC4F73C9861967FC6EFA38CEEE377EFDE6213540C22D17D9B7FF5B722D4DDA7089D894997B89C4D1BF50F96A7551548192727072DD5FAD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e21f8aa16d21fc2_0	
Preview:	0\r..m.....q.....^X...._keyhttps://wphoot.com/wp-content/uploads/siteground-optimizer-assets/fitvids.min.js?ver=1.1 .https://wphoot.com/...U.#/.....{.:.+.:.<-.k.# ..h..VS=...w..r...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a431c1478c67bc32_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.561948072292499
Encrypted:	false
SSDEEP:	6:mh+p6EYsNKTUfIQKddTNNKkyoXkKbAPjVu0vP4jLK6t:WuYgfIQKDTNYkHrYte9
MD5:	D6733FC6380494FE5CEC072ECC815CF4
SHA1:	965C63973319B0A477DC72219613064F006F1338
SHA-256:	74ACD2C2F6127B91EA116FB90B1C525F334E4BD48BF7051D0A7B97CD1855FD0A
SHA-512:	C1DF974219CE9E83AA39DFBCADBABADD4A5C496E5CC29D84C56ACCEDFD3D64CC6B0D74D2712D1C3B78EC87EF1648C4196766F8CEC577DF36B4C94C5E749 69ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....R.|...._keyhttps://wphoot.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 .https://wphoot.com/...U.#/.....HO.Q..&.sS...f..{v8..p..v..~k.. A..Eo.....b.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8d7eb2cedf7692b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15821
Entropy (8bit):	6.047833583606386
Encrypted:	false
SSDEEP:	384:CvrSsbL0vmObR7Vn1HsPKUKivCIypFUeUsX8U8vhVhG8DCo:ejORsP0r+G8J
MD5:	64818930BC3F322172DAFA69E5E0CBB0
SHA1:	1802104150484B73CAC8F80CE7E52B4E2A4D3BB9
SHA-256:	78146DB9BA8CCF16D42664FBE70C5741455ACF709A9B449477A7708674AC41EA
SHA-512:	CEC0E4EFE6F2DF06CAC2A01EC94D616F2BAA8229228165C0CE3CCF96FDF00BD67DDD8606EC9B21AB4BF5A7610F281D4E521AE8659A9132A9E9E25B1559497 CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...U-.0...._keyhttps://kezenelectric.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 .https://kezenelectric.ca/.c.P.#/.....0.....L.4[*.znl...Q.....3a... A..Eo.....2h.....A..Eo.....'..+....O....0<...v.K.....T.....8.....(S.P..`\.....L`.....Q.@...#....jQuery....Qd..X8....migrateMute..(S...`.....4L`.... .0Rc.....QbR..&....t...`$...l`....DaR.....Q.@...8....define....QbZ..r....amd.....`.....M`.....Qc.r&.....jquery...(S.....Ia.....I.....@.-....\P.a.....N...https://kezenelectric.ca/wp- includes/js/jquery/jquery-migrate.min.js?ver=3.3.2..a.....D`....D`....D`.....!....`....&...&....&..A.&.(S.....`.....L`n....Y.Rc.....L.....Qb...B....n.....Qb...)....s.....Qb.P.^....r. ....R....Qb.....o.....M...Qb.{b.....c.....Qb..]}....d.....Qbbs.....l.....Qb*.h.....p.....QbB.|.....f.....Qb.....y.....Qb:..v....m.....Qb.;.....h.....Qb&..|....v.....Qb..&....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b92b2c27ad669878_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98040
Entropy (8bit):	5.8181407636549425
Encrypted:	false
SSDEEP:	1536:M3JL6zEVwyUCaomZgA5m3DUYkbfcd4RaywAeyDCHvF21+LNiQifwpRVlm1:CGz3/oYzSFqGCINVKR1
MD5:	963D8E9E12E430E1C1801347E043589E
SHA1:	2D825ECB4C6605E9E720B9A9C263DF23142EFCF0
SHA-256:	1CF52EF839F78F7DAF58CC3918B9ED7C8BE40BE0C5340FA749E77295574F2A86
SHA-512:	D4A5BBD468094E165258087414EF54C5869DEC1BE1DB9FFDAE4E82DB6B027A19ECDD1C2B3F175AC7C7BD9DBE6283692E4D702531F547C8F07163B6C0D877F9 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....x....4C088CF87781426E5D98DEE30649ED1B3E0FDE0DC8D2FAEF70393F9BB40FD729.....'..]....O!....}....,.....`&..... .....(S.X..`h.... L`.....(S.p.`.....L`.....0Rc.....QbR..&....t...`....l`....Da....j.....Q.@...F....module....QcJ..O....exports.. .QcV.~z....document.(S.....5.a.....Q....a.....a.....a.....a.....Pc.....exportsa..../...I..Q..@.-....TP.A.....F...https://kezenelectric.ca/wp-includes/js/jqu ery/jquery.min.js?ver=3.5.1..a.....D`....D`....D`.....`....&...&....&..A.&.(S...a&..`|L.....L`.....Rcd.....*.....QbnT.`....C.....Qb.P.^....r.....Qb...)....s.....R.....S... Qb...B....n.....Qb.....o.....Qb&..|....v.....M...Qbbs.....l.....Qb.....y.....Qb:..v....m.....Qb~..B....x.....QbfL.\....E.....Qb.{b.....c.....O...Qb...E....w.....Qb&..D....S.....Qb*.h.....p.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bda3c198988ffc1a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bda3c198988ffc1a_0	
File Type:	data
Category:	dropped
Size (bytes):	16744
Entropy (8bit):	5.648582218349142
Encrypted:	false
SSDEEP:	384:wG8rjZ/6qK7J7yQuPTbUUh31//bEP+XgA3Tp1:MA7J7zUUUh31//YWXgAjv
MD5:	5E6FCF83E1D7799A4B261F3E1D80EBE2
SHA1:	3A804056786FCCBD0F301735BAB190047878B910
SHA-256:	29360909E738F65C325BD63848917A8E78400097C94C113A6FB9E8F7E5504106
SHA-512:	188272D3D2876C697973E9FE3DE4DB444B90BD6478E01B851D19FECE09478872FE3ED07BE71D78586186641A9F7ECD15AA6EB0C832913D44F9674275F882B1A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://kezenelectric.ca/wp-includes/js/wp-emoji-release.min.js?ver=5.7.2 .https://kezenelectric.ca/...P.#/.....z.....I....I'K.k.T.].P..=W.....A ..Eo.....]....A..Eo.....'..7....O.....?..Z.....!.. .....(S.\..`n.... L`.....L`.....Qc.R2N....twemoji..(S..`j....xL`8.....RcL.....QbB.|.....f.....R. ...Qb:..v....m.....Qb.{b.....c.....Qb..CF....e.....QbR..&....t.....Qb.;.....h.....M.....O...Qb~..B....x.....Qb...B....n.....Qb.P.^....r.....Qb.....o.....S.n..... .....I`....Da.....X...(S.....law*...*.....@.-....XP.Q.....I...https://kezenelectric.ca/wp-includes/js/wp-emoji-release.min.js?ver=5.7.2...a.....D`....D` ...D`.....|..`:...&...&....&. (S.....5.a.....q....a.....a.....Qc.g.....convert....a.....Qe.....fromCodePoint...a....]..... .....d.....@.....&.(S.....Pd.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c27291f84aa51d71_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.966201433952275
Encrypted:	false
SSDEEP:	6:mmjXXYCLsNKlfIQKDTeLsNKVLy9qt16xLkvAclbK6t1tiWT5Lh6dDSk16xLkvA:jXuYfIQKDT9oLmxkvT3VTPcDixk
MD5:	43506692DEEAA5E4039A84C6EE89F407
SHA1:	1782C6E8A9F3CB812E7FD2285D3AA57A1386BAB8
SHA-256:	936C78BD2281DED653E00794F606E0902FD80EDB86F9170E65316E8B59CFC50F
SHA-512:	CC55B01DAE0A87AD03AF06CDB477D09270094FB8A798843CBA1DEB677190C83DA56B115F3E4F5DC4355FA9193C2AA9849B9F984D922DED843E41AD6D47381D B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...%)C....._keyhttps://kezenelectric.ca/wp-includes/js/jquery/jquery.min.js?ver=3.5.1 .https://kezenelectric.ca/Wc.P.#/.....#.....?..?..O.....PQ.0.. ...+.A..Eo.....o!.r.....A..Eo.....Wc.P.#/.P~..4C088CF87781426E5D98DEE30649ED1B3E0FDE0DC8D2FAEF70393F9BB40FD729.....?..?..O.....PQ.0.....+. A..Eo.....L...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d9852fc8edfab566_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3692
Entropy (8bit):	5.729715496233022
Encrypted:	false
SSDEEP:	48:6Z2eVI1+UPEwU8Q2UiZQfYJ4ah9+RXDNDFK8X0S2IlGBlEcbaRi9nq1Batl:CVnUXQ8ZQxO9+Rq8ElVBlEZRg/tl
MD5:	3D903828811A900D1B6F49DE77D3759E
SHA1:	C6C460BFCFE4D89436CF5F6160CC8C026962EF5C
SHA-256:	DE844844B9FE141C6FBEAA0B903B35A142CA0FCE37F975ABFA08981208680A86
SHA-512:	478009D642B06A8E4EFEF0127DE382979A0FAC81876317736389AF0453DBB2A0AE46F9C343A8AEAACF4A96D4525F30C09A82BE1CA8123E5C599975C67264D2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t....Zc*...._keyhttps://kezenelectric.ca/wp-content/themes/metrolo/js/jquery.lightSlider.js?ver=1.1.1 .https://kezenelectric.ca/..Q.#/.....>$.....kn.~.8p..4. V..l@..T+.. *.L....A..Eo.....o.....A..Eo.....Q.#/.0.....'.Y....O.....%6.....4.....(S.4..`$.....L`.....(S.|.`.....LL`'....8Rc.....Qc..... ..defaultsa$.....l`....DaD....x...M...a.....Qb2.....item`.....Qd6.....autoWidth...H..Qd.....slideMove...`.....Qd...y....slideMargin.`.....Qc..vd....addClassI..Qb.....mode ..Qc6~X.....slide.....Qc.u.....useCSS..G..Qdfp.....cssEasing.....Qb.....ease..Qc.z.....easing....Qc..|~....linear....QcB.....speed...` .....H..Qbn.....loopH. Qf.....slide EndAnimation...G..Qc..,.....pause...`.....QcZ.....keyPressH..Qc..f.....controlsG..Qcz.....prevHtml...Qc.....nextHtml...Qb.%.C....rtl.H..Qe..$.....adaptiveHeight..H..Qc..f.... .verticalH..Qe.....verticalHeight..`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dc6462b65c6623d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.364065592998604
Encrypted:	false
SSDEEP:	6:mvYGL+MIwJJqNKNL7rSKTlgwJm49qthK6t:ClwvqYpJrw/qt7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dc6462b65c6623d5_0	
MD5:	6194EFC7D88E73B9431AF6C3051EE085
SHA1:	1E3FC131831A58FEC94D2E81FE678A5F77D8D9E5
SHA-256:	6B0E1895BB2D394807F5DC13E832CEEECD0B7979F2DAC920C69E3BB10BA62F3D
SHA-512:	0291D7FD7E55AB725608412F7902983A41BFFDCFFACE18242BD57A5EC0A2241E70E00B20FB1A426062E90C8C0B196D6519CED2F34846A034FEBEA30CAAAEE6 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....._keyhttps://www.google-analytics.com/analytics.js .https://wphoot.com/...U.#/.....y.....d.V]..y0@.....U0..;..hu.f..A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ee05b7802d222e35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1099
Entropy (8bit):	5.340247694388013
Encrypted:	false
SSDEEP:	24:vNF5j0z+JsekeD+NnZKqOFPgGNF5qggg0Vq0ixopJF0m:lA+JsxeSNZKBZuVVqApTT
MD5:	CAD3700B78AF4EE52D78E36955A4EB56
SHA1:	FC0E0E75D2ABEFD6D0BB9E228114E895EB7F1A29
SHA-256:	6FF1995A07EC1E2EBC57FACD38436008A2C10E3C6662EE8A31C0276266E8DA6D
SHA-512:	AD96B16CD89BA8492D5F40916E564604B564879D58B1DD11A4624674DE08D4C5893CFD47CAA8F928A026941B735FB8ECE3EF43390D3895CA68561D9651C3A35
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....V....._keyhttps://kezenelectric.ca/wp-includes/js/hoverIntent.min.js?ver=1.8.1 .https://kezenelectric.ca/...P.#/.....0.....{./.R-V.-.....T..)..fUO.....A..Eo... ...]..........A..Eo.....P.#/. .....'.b.....O....._.4.....p.....(S.8..`&.....L`.....(S.@.`:.....L`.....0Rc.....Qb..9.....I...`$...I`....DaX.....Qb...|....fn...(S. .....5.a.....a.....a.....Pd.....hoverIntental...X....,.g.....[s.....d.....(.... .f.....I.....@.-....PP.1.....D...https://kezenelectric.ca/ wp-includes/js/hoverIntent.min.js?ver=1.8.1a.....D`....D`....D`....,..`....&...&....&.....D`....DI]d.....Qd.(....hoverIntent...K`....Dj.....%.....&.(...&.....-.....b... .....d..... .....Q.@...#....jQuery....K`....Dh.....&....&.]...P&.....$Rc.....`.....Ib.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f22d5e331d7c4eab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.457792999847564
Encrypted:	false
SSDEEP:	3:m+lUcuXa8RzYsNKTUe2T1A9x2aTAXcVDPNK6Ui1lHCqk0i5QZf3rmJArpK5kt:mwKYsNKTUfJCPTlFNKZdq9UMfiJ+K6t
MD5:	9D412E7AFA1AC283044BDD4E1155940C
SHA1:	BE40403B0B4C836AA3B7AC248C758EE828FFC117
SHA-256:	F575E048570623EE4880FE1B9A251860C7B2FD1E7C854278C94849A8130CFC23
SHA-512:	D9B7606A4CE02C2A0F62A3632A94C4B25DE3779E96ED20D33853745F4106F3026469B45DCE4455F2634CA098843A50926D96C111C5C184E301250A591E4DFA00
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....v....._keyhttps://wphoot.com/wp-includes/js/wp-embed.min.js?ver=5.7.2 .https://wphoot.com/.?.U.#/.....U.....0..<#m^...J,.....)e.....A..Eo.....e.....A ..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f597f914edb8e129_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.550944733071242
Encrypted:	false
SSDEEP:	6:mjCPYsNKTOlAZ0QJ7RUR6TsLVNKLphA4QAOqFNCdlZK6t:LTYxL1K6TsLVYlwAqlT
MD5:	00831FE8B31383D26997A9C29CE44547
SHA1:	0439B9855F10CF58C88DD27A9F8C6A38A90A7530
SHA-256:	BFAF6F02810D03080194E8EE5E15C30A055C13418E84C8AD45E70CED01CEE4E0
SHA-512:	545ECA9FBB645EB759A0F9EE9CBC85A16636AE040519BAA64FFE8A0FB87EF5FB25027839D5A8441BC190769FF959C824E026676A0E4AE9534162023B7597639A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t.....x....._keyhttps://wphoot.com/wp-content/uploads/siteground-optimizer-assets/megamenu.min.js?ver=2.9.2 .https://wphoot.com/.?.U.#/.....R.....D ..SW..tL.>.'T~.....^..uZ5....A..Eo.....1.....A..Eo.....

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):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	12836
Entropy (8bit):	0.9725988979366212
Encrypted:	false
SSDEEP:	24:vFe9H6pf1H1oNYqLbJLbXaFpEO5bNmISHn06Uwg8:dbfvoNYq5LLOpEO5J/Kn7Uv8
MD5:	4BA19F8A513C6A185E8A5A35B3756FF4
SHA1:	E294A3E2DE5DB3BF27C95F9B8DA2EC5A366EDE6E
SHA-256:	ACC3A114B701B099D9A1254A22778A2CF635B3F2B3EC91D65714A0F3F9A81927
SHA-512:	350C9EF44B65EA31126A9C8ECBAB85EF88925DDEED74F7D109CAD6EB1FA8726D7BCCC75C7B8DD3F77D38528D36A733476C3892562A217A6045A8FF3CFA4BD0E
Malicious:	false
Reputation:	low
Preview:	.....y& ....

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):	16017
Entropy (8bit):	3.3173383213784686
Encrypted:	false
SSDEEP:	192:3p1mM7mDnQKw2tT2ecVkkoa/PIP5A1uJyvWZbrZAEd5A1u2e:5tzg82jaRs8vWhZAEEsf
MD5:	4AE8F3525AD7BBFCC01BA8C27470DDA9
SHA1:	2D737F93DC2C7AA704D3BC11CA7A77872D9934D4
SHA-256:	5EDD32C65F695E61974BA8893285187B4793CE2EDC6899CDDCDD905B80F537A8
SHA-512:	B6F574B0ABC2FBC90F253E53CA254045189634ED411E58677E8B6A5B893833D8562FAC255C462806C4C8B8496AE556747ED608AF6B78CB4E2C6E9981BD13D204
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...ba44d2cd_cd81_48d6_af29_4f4aface9870.....#(..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....q..l.....'...https://kezenelectric.ca/First-America/.(...F.i.r.s.t. .A.m.e.r.i.c.a.n. .T.i.t.l.e. .C.o.m.p.a.n.y. .-. .O.f.f.i.c.e.3.6.5.l...h.....`.....h.....`.....n.....n.....V...'...h.t.t.p.s.:././.k.e.z.e.n.e.l.e.c.t.r.i.c...c.a./.F.i.r.s.t.-.A.m.e.r.i.c.a./.....8.....0.....8.....P.....p.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....C...h.t.t.p.s.:././.k.e.z.e.n.e.l.e.c.t.r.i.c...c.a./.F.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	5.080472113091863
Encrypted:	false
SSDEEP:	6:mw02vy+q2Pwkn23iKKdK8aPrqIFUtpD02lbXZmwPD02VUbVkwOwkn23iKKdK8amd:jrvYf5KkL3FUtpzJ/PzVUB5Jf5KkQJ
MD5:	DEF0143787AA92CE6434349DAEC6A652
SHA1:	E55EAFB926E2F1F32271602B1E991871B6B03FA2
SHA-256:	1B11497F12F3AED067B8195519224DF0772E082636192A7D0262735E9C325A97
SHA-512:	4887AF38D1C8F2B51E19FEE16B6F6EF208143FB4E4A986AD5A0E184958223781FC1EB46F624C1C2A299CCFDB5AE6660F39C8ACF331DF9A0F0F0D533E2E505DD6
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:10.300 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/10-21:02:10.301 19e8 Recovering log #3.2021/06/10-21:02:10.302 19e8 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Preview:	.f.5................f.5..............f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.134404029568919
Encrypted:	false
SSDEEP:	6:mw1zcU+q2Pwkn23iKKdK8NIFUtpD1HULZmwPD1lFNVkwOwkn23iKKdK8+eLJ:hwpvYf5KkpFUtpxHUL/PxL5Jf5KkqJ
MD5:	71984B347D1199525B4A9512C3F3EB70
SHA1:	DBEA13F97A87CB2995324009FD8657E6B5B88118
SHA-256:	E1FEEC435730231B38AC946D2A29EF0F6A7087F536C5F7400DA64240F3D8E78B
SHA-512:	394575CF1E01F711B8818F5B21FB9F67714A228D4C7945803E5916B462FACFD3A4D367AC5B859481C092DD668A954F1038F3A73BFBAAEACAC230F0223CBF465
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:13.067 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/10-21:02:13.068 19e8 Recovering log #3.2021/06/10-21:02:13.069 19e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+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):	67584
Entropy (8bit):	2.4186228498594966
Encrypted:	false
SSDEEP:	384:xUQL+9GZpMo+BXQL+zG+QL+9GepMo++IUC:xUkbpMo+BXk8k0pMo+d
MD5:	2CCE539D52FDE5A94215249CE41493A6
SHA1:	26E67A332884B285A78592C0A082E69D4896A5BF
SHA-256:	03B6944684F5F9B509E73C419FB744116DC7BB6E05F0AC52FD46A4A6F667873C
SHA-512:	C78DA335C7654911958F5550A476D42ED92AA86C6F44C191E4A03C3829B969E45EFDA1588BB50B6B3CDF3F9BF55B85FD5894004DA70EFFAACBF5A50E0A540DB4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	83840
Entropy (8bit):	1.4782619215004649
Encrypted:	false
SSDEEP:	192:1Q4qbSUQL+cDSG4VmJf4XOlp28WJa2Jj11p28W/Ja2JjfZGQL+XSDSG2l3wqp28z:1QFbSUQL+9G4ltGjQL+zG2lAe
MD5:	9DC733F3BEA37388D882D28A5D414B2A
SHA1:	4AB2B19A061142920B45864E10461BADE0FE8DDE
SHA-256:	39D2BB9FDB794FA4FF012229075F1F9C9C0425A270DF081A34F3B554DECE2880
SHA-512:	2AD41AEFF88BF1E147CDABE7EB558822B3137AB7645FDF99D38BE9975E8E988EA0CECCBC37876FF2C9FEE81FF31B79D751FB6B9D6EC8870076598306872109
Malicious:	false
Reputation:	low
Preview:	.....J@..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.1522628156233
Encrypted:	false
SSDEEP:	6:mwaBFGlyq2Pwkn23iKKdK25+Xqx8chI+IFUtpDaym1ZmwPDaywRkwOwkn23iKKdP:e/GlyvYf5KkTXfchI3FUtpOyA/POywRo
MD5:	DD93CEF8BBF7471479CF11181A55EB8F
SHA1:	5FA439FCE4CA3AB065D9EDEA7B0318405DB95893
SHA-256:	C2B94C44E335EF0FFF2F081F368722AAA5BD2D5587DF7F64E985C9AB30C323D2
SHA-512:	27776FDF553EEB38BF45216EBF12BCD5BDE6AE5F8D4E036D91BA2F076E318E978EEA85D2FD8617A6EC2181FE27F3F3D7A6F18145084C562F1057559B98EF7A5
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:30.118 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/10-21:02:30.120 19c0 Recovering log #3.2021/06/10-21:02:30.120 19c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.098682808667871
Encrypted:	false
SSDEEP:	6:mwaiGlyq2Pwkn23iKKdK25+XuoIFUtpDap8r1ZmwPDayKvlRkwOwkn23iKKdK25y:eiGlyvYf5KkTXYFUtpOy/POxR5Jf5Kkl
MD5:	5E1DF63C4A9D02F6095292A76E5612C0
SHA1:	7E797D7320BF68AA45CAE854410C4F44AB477330
SHA-256:	1B4CACCB521547429DAD69CE5BCE30EE9043E4B61C156B98F08F16F8E78D3332
SHA-512:	C460FCF7EA51DAF710B84AFB22C1AA0C9440C28C61338083B23C3049A56397046397301191B9B7E4C54AA81FAA3536C39E7E0411832B1365CB22A7C94D8A3C05
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:30.108 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/10-21:02:30.110 19c0 Recovering log #3.2021/06/10-21:02:30.111 19c0 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
File Type:	data
Category:	dropped
Size (bytes):	102
Entropy (8bit):	4.707425199545215
Encrypted:	false
SSDEEP:	3:w1tsm1iILeNlA1jPqciKPnSc+VVn:w1tsmRLVP1/Sc+VV
MD5:	7E6074135B54581D9C9A50EC25141C6A
SHA1:	362BE82BA04A240771813665F436B0EF9D24C35F
SHA-256:	8A14329F2C4F6E9CD07FDABA314C1F29FDE90C936695F0E95118778B2E0CD7A2
SHA-512:	D715BD9AE5A94DC6F30D6B8A475DFD69DE15C3915987D6A2D9E6F761237055AB1409B24431F9F6497FE0CDF664449F13F3D52FB0C49E4221CE3145862D9048F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
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\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.188830561544286
Encrypted:	false
SSDEEP:	3:tUKUUi9VUFUQQLLKqFkPt+kiE2J5iKKKc64E/+MOMcWIDMGk4cWIV//Uv:mwVFwL+q2Pwkn23iKKdK29MRgPRIFUv
MD5:	6D6A29A6A87E55E0728ED06395069B91
SHA1:	E029D265D0F1B9883440ABF1D219D0B693B7E37B
SHA-256:	7FD1556EC47BFC52751FE7A66BFC127992E4B0B13FC8CFDE2D2A367F1DB07479
SHA-512:	8E9A62447B16E54E12F68A015D2E32481BA98BBED52AD92C9CEE783848E3864EDC28C7FB6C63BF6241AA85F2834134B4A0C0D2C1BCE58AA368DDD795848C3EB4
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:03:26.821 1a38 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:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
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):	330
Entropy (8bit):	5.156927231118178
Encrypted:	false
SSDEEP:	6:mwah/339+q2Pwkn23iKKdKWT5g1IdqIFUtpDahiJZmwPDahl339VkwOwkn23iKKg:eh/3N+vYf5Kkg5gSRFUtpOh8/POhRNVH
MD5:	2AD402C77F9703C55F6046F7D4C867D7
SHA1:	13AC9E6B0F0AA9CE4B1C8237C4E577FC6C32F7D3
SHA-256:	8DF27F674434A063B98C0E1B897FCE50A6C6D7E37BBD2FE408622D5DD4E1E8D4
SHA-512:	253CFD564DDC670DAEDF378D22EC4F6BE02F079174C541F85A5F523465A7AC6C7C2F8E9A45BE24571049FC8E44DB3DAA1D29F3A3E8A42A080B0B8141C2991EB
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:30.055 1d2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/10-21:02:30.056 1d2c Recovering log #3.2021/06/10-21:02:30.057 1d2c 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):	155648
Entropy (8bit):	0.5453108650395736

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Encrypted:	false
SSDEEP:	192:R2xypi2BgoW9C2Zoyp6h2niFr2isegC2ZoypM/h2diPr2isvsigC2Zoyp5Lh2biv:rvRLzpv
MD5:	C5496384EC4091974859216FEF7E86BA
SHA1:	99A448AC429D9172330B1B1F0441842590EF27CA
SHA-256:	6997A8456FDE4C3DE51CB9AC8B7B93486FE602DC1913DF95CFFC30CB593F0447
SHA-512:	4B372346A3D1B7ECB9CD119F81A8BC5BBF9C231FB92BF006ECA50BA40F3CAAE8F2F2B6BE24C11E239FFFF1B33371387D56E79C8C3D3AE1AD91668394386FD6 94
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):	809
Entropy (8bit):	5.4813749289758285
Encrypted:	false
SSDEEP:	24:8wL4uzawSPxaGin/T2dYN5IWeos7WeKO/:7awvKdz/T/KI
MD5:	2A80FCAAF5DE7FC1348B01417FEC845F
SHA1:	ABEF18C8C68B7890F18877437BF2922A243A2DC4
SHA-256:	DD87CA5CCDBCF11E4EB78C063536E0460AE74E511B23B5B39B608139FAC95FD9
SHA-512:	2CFF7C4A92F4BF8D0CE4E018C42A7A7A3463D15647D3E908AE137B78BAC3518961EE44CEE70599F4EDF63424E62262EEDAEBB182EEF82C7E58EE6A4B0E5B1F 80
Malicious:	false
Reputation:	low
Preview:	....."Q....america..american..ca..company..first..https..kezenelectric..office365..title*u.....america.....american.....ca.....company.....first.....https.....kezenelectric.... ..office365.....title..2.....3.....5.....6.....a.....c.....e.....f.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....y.....z.. .:\.....B.....r..... .....*&https://kezenelectric.ca/First-America2(First American Title Company - Office365:..... .....x..... .....*'https://kezenelectric.ca/First-America/2(First American Title Company - Office365:.....J&.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	158572
Entropy (8bit):	0.40904495108232264
Encrypted:	false
SSDEEP:	192:usJiHPqy2uvDypVkgK2ar2is1TC2Zoypwigh2Hr2isdgC2Zoypein/h2q:u1Ytnpnd
MD5:	44079C9295AE113F65A0C5E3C72B2A43
SHA1:	B5B67DA96FD0F6A30EE9C8FB09CA21A41AED3429
SHA-256:	945942AE8268ACC7E0943C88500F91289350B49B52A8A3CDADCE30F88592883B
SHA-512:	E51FCBF2AB612072FA074766543659F4F5245525EFFA1A129A9CDAB3A3EA28FF7BBAAE1D63F39FCCB0067E05F42C31153AA6249D7018470B350A5DEF9B2DE52 A
Malicious:	false
Reputation:	low
Preview:	.....%..... ....

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):	3296
Entropy (8bit):	5.643613845045531
Encrypted:	false
SSDEEP:	48:9DiGHNaa7IMz8dbeQgvbQSefgGnNrS0U9RdiN9sNPkUJvU:/Ma7IMAdbeQgvbQ5fgGNrS0yI
MD5:	8D94E9BF917219B4388AA330504FD6CB
SHA1:	A9029F8A8B0C7897D82AA2187DC9F3ACD3391CE9
SHA-256:	01F0DB92E8383032D8542AF2CD286A73FF8C51C9308821DD2C513E4B12E0D8D7
SHA-512:	F01F1477C6424A28AD163D4BDDAE8A2FED5C7654CD04D3365A3E29FBB70227D22643FD07590157E7ECDB1747626B1B287955DD853A2B8F19A35B30178E8E008

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Malicious:	false
Reputation:	low
Preview:	.2.....*.....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..804961000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-10 21:02:31.90][INFO][mr.Init] MR instance ID: 1578df90-1901-4296-9158-1bcd9532930a\n","[2021-06-10 21:02:31.90][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-10 21:02:31.90][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-10 21:02:31.91][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-10 21:02:31.91][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-10 21:02:31.91][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-10 21:02:31.91][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.087850227724463
Encrypted:	false
SSDEEP:	6:mw0eGOq2Pwkn23iKKdK8a2jMGIFUtpD02ZmwPD0NzkwOwkn23iKKdK8a2jMmLJ:VGOvYf5Kk8EFUtpj/Pe5Jf5Kk8bJ
MD5:	6C84C36CE976FAF42EC8BC30AE016818
SHA1:	E587A19613B3D82D3F78632F3864226B9B3085DB
SHA-256:	320E2252257303 67C6D021696E06E2951971205C1069AC0A224839735BA1A7C2
SHA-512:	F534C305819EF950253B075D5A9EDC5C72A18DB5F8B86E0F4A390FC9D8718585337EE905E65F710A7DE431735D28946E113CEC214FA8DF87F39C918BE180D0A2
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:10.042 19f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:02:10.043 19f0 Recovering log #3.2021/06/10-21:02:10.044 19f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.1477500044922158
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/y0bw/qALihje9kqL42WOT/7i:vOqAuhjspnWOTOqAuhjspnWO3i
MD5:	4F8DA80267757208B4D18F53119AD2DA
SHA1:	F40ECB5F699C5FD8A930D049B7A8C135E0B667D7
SHA-256:	E8A905C2533F526E6C8B6DB813C96C10D6804BB9F30C3CBC7E705EEB4D0CFE4E
SHA-512:	906B252A819E0F80A1B0D425F9A4EBFB57692D41D0927F9519B67EC0532B33F61E9D8381CECAF4D6E73FD3A13B1B4B7DFB4E1F969B3A4B511F0775816E4F9C9
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0204375357785054
Encrypted:	false
SSDEEP:	48:Pkq7w/qALihje9kqL42WOT/D4thtWtnqrw/qALihje9kqL42WOT/l8:PkUOqAuhjspnWOgrynkOqAuhjspnWOi
MD5:	21AC81A042A95449F7C76F34167FD74F
SHA1:	28C949AF75749576EFA1E6829340456DC4171ADE
SHA-256:	A5FEB945EB0AB946958A0B55D3C42A09F0E00A366F2BE28E7A94C5917D12547D
SHA-512:	7880B95B3DD735159631F8B916B1ED82C6B7CA3D03D0DD8B8CEE7CFF2FE7311508853E1BACFD4E5208E732E91E12ECA6D30419441D8071986AA9F33CE7835EA8
Malicious:	false
Reputation:	low
Preview:	.....*,.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.126400054608968
Encrypted:	false
SSDEEP:	6:mw00acIN+q2Pwkn23iKKdKgXz4rRIFUtpD0r0ZmwPD0TVkwOwkn23iKKdKgXz4qG:tIIvYf5KkgXiuFUtpl/PG5Jf5KkgX2J
MD5:	286A4885B1C78963356C610659F97117
SHA1:	38D88BA6199DACD95F3E7DC05B36D98CAD58357E
SHA-256:	EBB19612AC0B71FE2D2429F49E39C6F324D9D0F9FDF1FA3CBBDAFBE7F370B256
SHA-512:	DE5ACBBE111135769E5F4F260EA51107209AD6892C4BDAEE0013745D9C61DDC3455F3242D32709F04704291DED15E27DD992F33FC185AB37B6E8F8A20BD84BE
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:10.326 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/10-21:02:10.330 19e8 Recovering log #3.2021/06/10-21:02:10.331 19e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
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):	53248
Entropy (8bit):	0.3622955737774043
Encrypted:	false
SSDEEP:	48:TzLbCIG+6bDdsDaKgJgKtHIm50I9a+U1cVB:vCIG+6bDdsDaBJvtHIm50I4sX
MD5:	DDC1F7FC68A5177438E7C01DE312606D
SHA1:	4DCA224B74B46D928D62140D5531B155BDC172AE
SHA-256:	3B02C2DC7E07BC74D914284428336BEA95F7A69A37098313BE7217548AD4C555
SHA-512:	59449DA60333927917FEDAAAF3B38E8A58DEF24403AA7D49934223275E9B5AE6A5F35FAAFF656DFB6134F203DC4A18950F0CBDED0020934B503E60569A606FF1
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g.....*.W.L.[....."..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21556
Entropy (8bit):	0.03657475048123613
Encrypted:	false
SSDEEP:	3:xtt/lFllxFEG2l/lSV/lolH/Fll69Xll0V/lpvlt1Xll0V/luvtfll0V/liv/NlA:/+/l/lSVt7KVtpvSVt3VtsKVtj48Vn
MD5:	FC97A42865FCF239AC439471D33E246F
SHA1:	A87E5CDE0DDF949C9BA656BFE54960FE2E296A3F
SHA-256:	072DF53017C6F2BFFB01CA5CC11941D5DED2467B3CEF21B1AD4CF7C3663CCF23
SHA-512:	BD8E2BAEF8B21A129022A2E7DC42F96CFCCDD18EBED364DDDA2EF5EE4D60C16A37F8AD0708DC1437BEBCB3D664F1775FDACE84CE12633653CEE20CF6F823530A
Malicious:	false
Reputation:	low
Preview:	.....X..... ..... .c.....+.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.0110318360026003
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoj:wIElwQF8mpcSJ2Y31
MD5:	3537C445426E66F88247B3DE03237824

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA1:	4F58D5DBB3C41FC4A6A80A05E83C143C3B06565F
SHA-256:	162D9910232CA03F384801AFDE0FE557B3DC0C383F760F3CCE4EAB49CB9579DE
SHA-512:	C622D37680F87E0BA64BCC7F557B542AED52727AD3FE4AA34F75DF2FF0AC54BA179BCE45CB3F8FF0740289574FA6420A8B50D96BED18B7E4C5A2815D15C3CC2A
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8256858414545736
Encrypted:	false
SSDEEP:	48:cpiqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUy6:cAhIElwQF8mpcSD
MD5:	AC4E69C1C4DAD83084335457063DD295
SHA1:	71D2574CC907A8F965C35829DC26A5D010278F95
SHA-256:	E33BF32592774D801597A051A2FBF2D10113CA8A784BD9E8218FB906C9BA9F66
SHA-512:	3AC5ABBD762D0BFC76E27C4DBE61EADF3655DC5274B55341E51E6FAE4702C6406B6A40B5AD189A9DDDEEE6460B481EBD590FEFAECAF82CAF867813FB64F1EE10
Malicious:	false
Reputation:	low
Preview:	.....1.X..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	936
Entropy (8bit):	4.367562704839904
Encrypted:	false
SSDEEP:	24:7ZZZZPnWfblDMmEOe/q4x2pvvdkMOKWVnOP:7ZZZZPWfbFE12jk5bc
MD5:	1AF0D6A4625C5F3DDF8DFF7B220B3702
SHA1:	0F0101459F54E95D372FAB0684767ADD79EBF5E5
SHA-256:	EFF86CD6C162CF97A7E375D3692E8B6AC0E49A4CC5367F015CA9788FEC10F040
SHA-512:	31139ED5E1AFB595E5854856DEF7277CAA636B27248D643D8D6368842447A2F9222EA63DDE4BC245F327E50DCFD1899B6C3FAFCFDFD7ABA3B5071CF25F1062
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f..... ..e.....next-map-id.1.Fnamespace-49a36818_3967_4d9f_baf5_bd2229907763-https://www.google.com/.0.o.....map-0-rc::b..0.5.A.H.j.M.t.v.1.b.d.B.7.V.o.z.5.t.O.4.B.g.r.Y.A.M.z.O.u.u.f.i.6._.Z.Q.m.A.X.U.h.l.l.5.b.P.M.W.t.e.D.p.I.2.q.5.X.x.I.2.n.2.f.w.j.Q.x.F.9._.X.2.B.F.q.m.8.I.C.L.d.5.3.B.N.u.f.q.T.7.E.M.7.A.P.d.8.5.m.x.K.X.-.Q.9.k.Q.O.P.q.e.n.o.b.d.-.6.Q._.C.t.H.N.n.b.3.m.w.j.M.F.O.f.h.a.7.B.M.n.4.g.N.H.v.S.S.z.g.K._.w.j.7._.T.G.I.R.k.W.S.e.N.j.y.a.E.9.J.1.r.K.B.i.u.g.r.r.y.s.T.B.M.L.d.P.y.x.X.i.Q.r.D.a.6.Z.h.o.Q.C.K.w.e.5.b.X.X.h.4.I.z.x.B.B.T.9.1.6.e.B.B.L.6.1._.T.-.L.R.f.6.B.z.h.Q.j.B.H.7.P.O.X.O.A.0...map-0-rc::c..B.c.b.l.c.s.F.b.K.M.M.3.q.g.F.1.V.Z.E.d.s.V.Z.N.4.i.G.l.u.W.d.q.-.b.Y.-.A.D.G.6.A.a.b.x.F.8.S.f.a.8.r.9.S.Q.E.1.5.Q.X.i.o.a.l.A.z.W.F.v.V.t.l.K.3.o.U.1.d.h.k.T.N.Y.-.Q.g.x.O.K.t.d.0.l.B.d.m.d.B.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.021034222567188
Encrypted:	false
SSDEEP:	6:mw0pyq2Pwkn23iKKdKrQMxIFUtpD0Br1ZmwPD0B9RkwOwkn23iKKdKrQMFLJ:FvYf5KkCFUtpmr1/Pm75Jf5KktJ
MD5:	96736CE75E83E18627074E7683DBCC2F
SHA1:	17ED29CC5DF47D1758BC10FA20D18600C8C98463
SHA-256:	ED7A1878222FCB315E9DCE49ABF465AAF04D139E09846246758678F369EBEF53
SHA-512:	CE62ECB949AF242851B92112FD261B5AB64599E9F19553A41C82AB9E7B53D083D6920B6A271A412F21E08D5B9C899C0223119CAFF2F074D299BD9FEA36C982F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Preview:	2021/06/10-21:02:10.229 1a50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/10-21:02:10.230 1a50 Recovering log #3.2021/06/10-21:02:10.230 1a50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.0989802275797915
Encrypted:	false
SSDEEP:	6:mwt6Qj3+q2Pwkn23iKKdK7Uh2ghZIFUtpDt6PWZmwPDt6UMVkwOwkn23iKKdK7UT:os3+vYf5KkIhHh2FUtp4PW/P4UMV5JfI
MD5:	A120E583C00762E5ECFA0A77C4AEC071
SHA1:	8363B924689F08F840E856FC5A1208D231AFBAE0
SHA-256:	E069AF671CD648F0CA88B3C305ACA2AF3978428C4899905C97F8540A9382B92F
SHA-512:	60B187426CD7EEF5110E0166461D5DA7DCCFE5ABF6E841297BC5321C89E607CEA47FC4C25504E062123DF6185E9F2C2F6D07D441F749A51FF27AF21972A798E
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:09.986 19ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/06/10-21:02:09.988 19ec Recovering log #3.2021/06/10-21:02:09.989 19ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\3085c1ef-01c8-4cfa-a8dd-fb9b1ffb49ad.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.177422877666977
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SSDEEP:	6:mw0Ejyq2Pwkn23iKKdKusNpV/2jMGIFUtpD0b1ZmwPD0+RkwOwkn23iKKdKusNp+:ZOvYf5KkFFUtpy1/PF5Jf5KkOJ
MD5:	A10D584703DD42C6D2BB5FAB3B1C1988
SHA1:	BF323D430AE90A93615011A1A6EC08B1BE6C0C50
SHA-256:	9199DD523AC56CF9A43755B951D7CF3C288FA829FA65C8D703A0A484152ED9C9
SHA-512:	484A394FC97342491106F44767E49B9F71AE94335FEDE4208B870BD126A485C2170AF2B1A5A49BC2456F9F760FC28CF372DDEADD1D3034A51C2DBA9B9E5B37E
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:10.275 1a50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:02:10.276 1a50 Recovering log #3.2021/06/10-21:02:10.277 1a50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.182844276577237
Encrypted:	false
SSDEEP:	6:mw00MERvIq2Pwkn23iKKdKusNpqz4rRIFUtpD00NXZmwPD00aER7kwOwkn23iKKi:yvYf5KkmiuFUtp/X/PFp5Jf5Kkm2J
MD5:	AE2B6356F8AF21E842BE8D7EECD5F766
SHA1:	D91EFF47681EAFEDD3556780AFD73B298E54F371
SHA-256:	39538EC7E0F71E21A812A220BA56E13B8E7E51DF5AE4FD8D3914E51B4CA43428
SHA-512:	9DDF52765393933A60AEAFFB1E9D42F7BCB2F10828773099DBFE0209DFCE4C3D92112CBC526FBCED6A5ACAF52FCA6AD1477CBAF0D272D6ABF5A4289FDC441B27
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:10.320 1a40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/06/10-21:02:10.324 1a40 Recovering log #3.2021/06/10-21:02:10.326 1a40 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.237649904590387
Encrypted:	false
SSDEEP:	6:mwv+3+q2Pwkn23iKKdKusNpZQMxIFUtpDvQAHZZmwPDvwtVkwOwkn23iKKdKusNP:bLvYf5KkMFUtpLQAHZ/PLwT5Jf5KkTJ
MD5:	8449B7AF0CDBAF7B6DB350C684EEB018
SHA1:	D582513CDA0EA77BBE4035FF1E11749698E32D3A
SHA-256:	9D6071FA7FEC19EC3F930DC028737C658B6CC3AE02B6F36A79BF5D08DD3BBFF9
SHA-512:	F2FC0F1504F9C3600CF80469237F0CD9CB8DAEC79D299613ED8DAC593D9B31B92664864FBDB475F4069CEC39292705322FFA7A62B8729FB3E781E6AE13B3130
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/06/10-21:02:27.193 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/06/10-21:02:27.194 19e8 Recovering log #3.2021/06/10-21:02:27.195 19e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\9a88bfbb-e9d5-4757-8815-bb24bda897a2.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.158001623297475
Encrypted:	false
SSDEEP:	12:boRvYf5KkkGHArBFUtpLS1/PLX5Jf5KkkGHAryJ:EdYf5KkkGgPggJf5KkkGga
MD5:	2D8F61CBA80E2E9828582B87A9F8FEE4
SHA1:	D2BA8C6C550886F49DEF4ED8B46D203CAC60ABB4
SHA-256:	BAFC4C5D63CD710F75463F7ADBA015BE21322D87569F3C20793B082FA171CD13
SHA-512:	51F2DACA313163FFD1AA0D2EC10A2AF978AA933A19FBDEA3A8FAF85BBAF78BD7BB9918E5449D688C8987F940C11ED71CF009AF654DF9C41323C8C1EAEC7DE08B
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:29.570 1a50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/06/10-21:02:29.571 1a50 Recovering log #3.2021/06/10-21:02:29.572 1a50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Entropy (8bit):	5.205366194911225
Encrypted:	false
SSDEEP:	12:bkvYf5KkkGHArqiuFUtpLE/PLk5Jf5KkkGHArq2J:CYf5KkkGgCgHJf5KkkGg7
MD5:	ED299182AC9616DD6A1A72F353A2F895
SHA1:	4060248AF6C1BCEF43BBE63D1F7EB7C2F09DFA51
SHA-256:	A6754EA19E9D5CCCAE67B53B90DF4C4588E71172CB774E514132C233A3292937
SHA-512:	9431D909FCB7299C1E86F98C0B90D97027AF6B32F3F61489035AF9C184859DF2819373B7AB7083DD4FD38E8367255D351BEF36AE09DC056F7204137719EF17CC
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:29.635 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/06/10-21:02:29.636 1a54 Recovering log #3.2021/06/10-21:02:29.636 1a54 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.190983717969176
Encrypted:	false
SSDEEP:	12:KOvYf5KkkGHArAFUtpnjZ/Pw5Jf5KkkGHArfJ:/Yf5KkkGgkgR0Jf5KkkGgV
MD5:	E5018ED9794A2A80215DCB3098C4E8CF
SHA1:	212B5F74E01B128913B5EEA2A5C96A0F071737E2
SHA-256:	917EAB78B270EAA435E763E806BCAE8071D9AF344362A5C881241A92BEF786C7
SHA-512:	13E4D69A71325B02EF30C8406C34315E0520C44D944ABDC49A4E81E80580322E9DBFCD2203C7E14DD4039754058D217F623598A8F35112F5ED91ACD4FE64C3B
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:44.896 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/06/10-21:02:44.897 1a48 Recovering log #3.2021/06/10-21:02:44.898 1a48 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.137818299705738
Encrypted:	false
SSDEEP:	6:mwt6F+q2Pwkn23iKKdKpIFUtpDt6T0ZmwPDt6TUVkwOwkn23iKKdKa/WLJ:oQvYf5KkmFUtp4T0/P4T05Jf5KkaUJ
MD5:	4D1A6CA2F8093B6D5AF09EAF4B7D3B22
SHA1:	8738FB8EA653D7ABDC088D9459875E634F369DB3
SHA-256:	60A028427187C618AE6CB146B7EEC3E836D765220DC134E9087A4B93B9F6F81F
SHA-512:	D1E8E3F0FB1B6C150DF9196C4355FA0CD3EE6468375A243A84DC5EC64F01FE2579E1C544165DF7DF722C3E38B1371EA6933DFD786E0AB20F9365FDB5E8C7143
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:09.988 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/10-21:02:09.990 19e8 Recovering log #3.2021/06/10-21:02:09.990 19e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.257918593099052
Encrypted:	false
SSDEEP:	12:zyvYf5KkkOrsFUtp+uh/P+u9R5Jf5KkkOrzJ:zYYf5Kk+gFDJf5Kkn
MD5:	D60B2B71EAAF3DA3CB670DCFB300C0B6
SHA1:	F2987B5FD562A5B1F1AD3A585D0A7D2847AADA27
SHA-256:	6B9BA7706F94A106CB55DF20366B1103F32E6B973F40FB1524E9A94B85236594
SHA-512:	F79EDFF693BA95968E459BBE7FE58F8D9F2CC404CEAE0F197CEC6A497CD65522FF3B530FBCC67CBC053C95AF04C60CAE67B6ED0043773C74D62B04919C70B0F
Malicious:	false
Reputation:	low
Preview:	2021/06/10-21:02:31.926 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/10-21:02:31.928 1a38 Recovering log #3.2021/06/10-21:02:31.928 1a38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	132
Entropy (8bit):	5.508563297802999
Encrypted:	false
SSDEEP:	3:m41ANI5SlPXEGwGh/WSmSWR5z4DPZt/lBJ+lhOlMZv/zkhlpr:j1A+oxX/wGJWf5z4Vt/lyYlYvKh
MD5:	2F8871227D78137AFD900BCD110C18DC
SHA1:	40C8FBC7FD9FE98F47124FDB9F5E7E50B917ED7C
SHA-256:	D6B538A937F81120073BEAE59564A58FD26EDA7977EC0FF362F351011FC139D6
SHA-512:	34A45AB2A8D6221546952AE647F209F88D55A065768DD581E2F88E96FEA18376B53C46B5833B9D63905039D1F648D014A61479AD30DCE451BF46660CEA4B5EA5
Malicious:	false
Reputation:	low
Preview:	.....~p.+.5_...._.(?.N|.....A..reD.....q.....4.V.....[(Ex...G.....:&...1.....+@..|.....x.G.j.....Lv`..S..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a61a9d9e-1da0-4847-b7aa-e3cdf777b186.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):	1208
Entropy (8bit):	5.568225996695263
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUeF23ZAUEzUe8hUts7wUeE4sRUeiQ:Ym6UUhyKUeiYqPeUeF2eUcUez6wUecUg
MD5:	816F31E90AF311383F7C1CD37BA94FFE
SHA1:	C3E60754109B60A1894B1B6A153A330BB77C5C62
SHA-256:	AD7B955E4B96FDA740A220EA50B2171A8B97EF846F62EE4FEBD3D974889F27DD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a61a9d9e-1da0-4847-b7aa-e3cdf777b186.tmp	
SHA-512:	C43D1161466C9B27A394A77988D1E7A00FDE0A6C295C27CE37654E5EFBBD496E16880B773E5A5FCA64A839DEFBC7EA1C24D73CF8D4270649479BDC4C40D143D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1634238135.533594,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623351735.533599},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1632987013.793603,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c1652dca-5907-4397-b613-cde51acd4b2f.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):	5816
Entropy (8bit):	5.17698205306271
Encrypted:	false
SSDEEP:	96:nGELha2RlSOV0GgHIVw+e5k0JCKL8skG1WbOTlVuHn:nXLU2RoKgHIfeh4KvkGg
MD5:	E9730C2036656456F67AA608855957B4
SHA1:	9E6F821407764394A63AB4F589164501FCAC87B8
SHA-256:	A1B470D2FC85C40B8E258CAE05FC40A90E7A3D4B44F17F2197317D4048D0EC28
SHA-512:	F54AEE7D7009D37111EBF2BC6CCAA63B10EEDDAEFCD5ED02FF9ADF1ED087445579D584033B2B9684AA17DD3287C565DA20FD87B7942FB5034EDB601295BA003
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267825330255117","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4005ad4-7ef8-4b7e-960e-ad09a8a8c684.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):	5193
Entropy (8bit):	4.965841149753694
Encrypted:	false
SSDEEP:	96:nGELMt2pIVw+g5k0JCKL8skG1ObOTlVuHn:nXLg2pIfgh4KvkGs
MD5:	C83DC660F26218BC0F0A8D7F75D6A6EF
SHA1:	8BB0AC616FB0833C8CC7160537B04B22D609EE72
SHA-256:	04BF95784489394F4C6E32BC675AA49393B028647CAC0875FED85A802E325C8F
SHA-512:	F43474DBCD77C463CFDE990BD4C852FFBB7C6EE0B0B7C793926E57BB234BEE01001DBEE48B6962596901BBEB6EF571AF67E7F7CE3574457239AC52648B0BAB4A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267825330255117","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cba595f5-4b38-4568-8eda-aa17998e16b3.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):	5789
Entropy (8bit):	5.17462045923266
Encrypted:	false
SSDEEP:	96:nGELNa2RlSOV0GgHIVw+b5k0JCKL8skG1ObOTlVuHn:nXLw2RoKgHIfbh4KvkGs
MD5:	B99727BB3BE82D864D443AC4E998C81B
SHA1:	2E2CD2B97F8AB8C2E6DEDD8B1D2A8755BCFA8079
SHA-256:	24C7A457B0D60749B5790E908336F7BC79D2F81B031FC9503115257BF0A4BA41

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cba595f5-4b38-4568-8eda-aa17998e16b3.tmp	
SHA-512:	A82F794397A3AF0ED4C42CED0EA78AA7E3677CD37841EC03C01E91EA521C2F072243C58473385622DB71E5A9785D6D6E4F754EF2893EEA2F4EFBDA3E0E0F85 F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267825330255117","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cf03e488-4006-4aed-a42e-31e7dd0c0a39.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):	1208
Entropy (8bit):	5.573368438922273
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSAkG1KU/zkq/HeUeF23ZAUEzUe8hUts7wUeE4sRUeiQ:Ym6UUhCKUgqPeUeF2eUcUez6wUecUeP
MD5:	932088854F1E30AE0B7F971ED8475B47
SHA1:	043B6A8462746D95293FE041199D3936A626ABF9
SHA-256:	D8C3BEA38ABC1E0E1200D35D71BA5640A05734718D688E56BA53F8B3B5944C31
SHA-512:	F71CAEAFDF595D554E6325B6DDFDCE2C5192FD311D388E49B26682AE41774190CEEC3022203819E2CDF35C5DF38098B3B137B448AB286A32507CBACCB85A25 E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1654887744.643402,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623351744.643407},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1634238135.533594,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623351735.533599},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1632987013.793603,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.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//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.328845202081076
Encrypted:	false
SSDEEP:	3:tUKUUiwJmvj1Zmwv3GUiwJqfhH1V8sGUiwJGEbH1WGv:mwvYr1ZmwPDvkfjVvDvkEhtv
MD5:	0F16B8691DAF61B3F08BCFB39F64D54A
SHA1:	B61CCDB928B894D5BFF4FCD0B9010666C29FF3BD
SHA-256:	5EA54C98087077492016AF319801CD245088B4DA081CE569297C92B51289ED0C
SHA-512:	E88A9AB585CA949237FF97F50CF88F1B87F424EDD911E94AA1BDDF22EAB5974A58616E417A714BC325C273FEF2854C1F69DEB544B7D0372B279CD67C495CC9 E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Preview:	2021/06/10-21:02:28.019 19c0 Recovering log #3.2021/06/10-21:02:28.068 19c0 Delete type=0 #3.2021/06/10-21:02:28.069 19c0 Delete type=3 #2.

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:02:13.425857067 CEST	192.168.2.4	8.8.8.8	0x8f7a	Standard query (0)	kezenelectric.ca	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.370786905 CEST	192.168.2.4	8.8.8.8	0x1290	Standard query (0)	gofirstam.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.372422934 CEST	192.168.2.4	8.8.8.8	0x552a	Standard query (0)	wallpapera ccess.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.373878002 CEST	192.168.2.4	8.8.8.8	0x7398	Standard query (0)	www.dwdtec hgroup.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:18.311542034 CEST	192.168.2.4	8.8.8.8	0x8eb7	Standard query (0)	www.dwdtec hgroup.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:18.311996937 CEST	192.168.2.4	8.8.8.8	0x86b6	Standard query (0)	gofirstam.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:24.684355021 CEST	192.168.2.4	8.8.8.8	0xadfe	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:27.467679024 CEST	192.168.2.4	8.8.8.8	0x55e6	Standard query (0)	kezenelectric.ca	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:28.556874037 CEST	192.168.2.4	8.8.8.8	0x9eaa	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:03:18.890535116 CEST	192.168.2.4	8.8.8.8	0xd484	Standard query (0)	wphoot.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:03:23.934819937 CEST	192.168.2.4	8.8.8.8	0x93b2	Standard query (0)	wphoot.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:02:13.576528072 CEST	8.8.8.8	192.168.2.4	0x8f7a	No error (0)	kezenelectric.ca		66.70.177.74	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.434320927 CEST	8.8.8.8	192.168.2.4	0x552a	No error (0)	wallpapera ccess.com		172.67.7.204	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.434320927 CEST	8.8.8.8	192.168.2.4	0x552a	No error (0)	wallpapera ccess.com		104.22.33.65	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.434320927 CEST	8.8.8.8	192.168.2.4	0x552a	No error (0)	wallpapera ccess.com		104.22.32.65	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:15.533024073 CEST	8.8.8.8	192.168.2.4	0x1290	No error (0)	gofirstam.com		104.129.24.42	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:02:15.553591013 CEST	8.8.8.8	192.168.2.4	0x7398	No error (0)	www.dwdtechgroup.com	dwdtechnology.wpengine.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:02:15.553591013 CEST	8.8.8.8	192.168.2.4	0x7398	No error (0)	dwdtechnology.wpengine.com		104.154.247.12	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:18.373363018 CEST	8.8.8.8	192.168.2.4	0x8eb7	No error (0)	www.dwdtechgroup.com	dwdtechnology.wpengine.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:02:18.373363018 CEST	8.8.8.8	192.168.2.4	0x8eb7	No error (0)	dwdtechnology.wpengine.com		104.154.247.12	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:18.373812914 CEST	8.8.8.8	192.168.2.4	0x86b6	No error (0)	gofirstam.com		104.129.24.42	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:24.734399080 CEST	8.8.8.8	192.168.2.4	0xadfe	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:27.526487112 CEST	8.8.8.8	192.168.2.4	0x55e6	No error (0)	kezenelectric.ca		66.70.177.74	A (IP address)	IN (0x0001)
Jun 10, 2021 21:02:28.616039038 CEST	8.8.8.8	192.168.2.4	0x9eaa	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:02:28.616039038 CEST	8.8.8.8	192.168.2.4	0x9eaa	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 10, 2021 21:03:19.067543030 CEST	8.8.8.8	192.168.2.4	0xd484	No error (0)	wphoot.com		35.208.111.117	A (IP address)	IN (0x0001)
Jun 10, 2021 21:03:24.111877918 CEST	8.8.8.8	192.168.2.4	0x93b2	No error (0)	wphoot.com		35.208.111.117	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49816	66.70.177.74	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:02:45.982975006 CEST	3472	OUT	GET / HTTP/1.1 Host: kezenelectric.ca Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Jun 10, 2021 21:02:46.121443987 CEST	3472	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 19:02:46 GMT Server: Apache Location: https://kezenelectric.ca/ Content-Length: 233 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 7a 65 6e 65 6c 65 63 74 72 69 63 2e 63 61 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49832	66.70.177.74	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:02:52.893249035 CEST	3531	OUT	GET /wp-content/uploads/2018/11/LOGO-300x179.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kezenelectric.ca
Jun 10, 2021 21:02:53.033258915 CEST	3532	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 19:02:52 GMT Server: Apache Location: https://kezenelectric.ca/wp-content/uploads/2018/11/LOGO-300x179.jpg Content-Length: 276 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 7a 65 6e 65 6c 65 63 74 72 69 63 2e 63 61 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 31 38 2f 31 31 2f 4c 4f 47 4f 2d 33 30 30 78 31 37 39 2e 6a 70 67 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49844	66.70.177.74	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:03:00.281897068 CEST	3639	OUT	GET /wp-content/uploads/2018/11/CCC.jpg HTTP/1.1 Host: kezenelectric.ca Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Jun 10, 2021 21:03:00.418772936 CEST	3660	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 19:03:00 GMT Server: Apache Location: https://kezenelectric.ca/wp-content/uploads/2018/11/CCC.jpg Content-Length: 267 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 7a 65 6e 65 6c 65 63 74 72 69 63 2e 63 61 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 31 38 2f 31 31 2f 43 43 43 2e 6a 70 67 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49852	66.70.177.74	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:03:01.418679953 CEST	3666	OUT	GET /wp-content/uploads/2018/11/index-300x117.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kezenelectric.ca

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 21:03:01.556349993 CEST	3668	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 19:03:01 GMT Server: Apache Location: https://kezenelectric.ca/wp-content/uploads/2018/11/index-300x117.png Content-Length: 277 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 7a 65 6e 65 6c 65 63 74 72 69 63 2e 63 61 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 31 38 2f 31 31 2f 69 6e 64 65 78 2d 33 30 30 78 31 31 37 2e 70 6e 67 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>
Jun 10, 2021 21:03:01.556582928 CEST	3668	OUT	GET /wp-content/uploads/2018/11/CCC.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kezenelectric.ca
Jun 10, 2021 21:03:01.694214106 CEST	3668	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 10 Jun 2021 19:03:01 GMT Server: Apache Location: https://kezenelectric.ca/wp-content/uploads/2018/11/CCC.jpg Content-Length: 267 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 65 7a 65 6e 65 6c 65 63 74 72 69 63 2e 63 61 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 31 38 2f 31 31 2f 43 43 43 2e 6a 70 67 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:02:18.678291082 CEST	104.129.24.42	443	192.168.2.4	49761	CN=gofirstam.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 31 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Aug 30 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

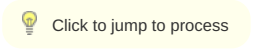
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:02:18.690851927 CEST	104.154.247.12	443	192.168.2.4	49762	CN=www.dwdtechgroup.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 16 12:22:42 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jul 15 12:22:42 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jun 10, 2021 21:02:27.805982113 CEST	66.70.177.74	443	192.168.2.4	49783	CN=kezenelectric.ca CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 01 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jul 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 10, 2021 21:03:06.631866932 CEST	66.70.177.74	443	192.168.2.4	49866	CN=kezenelectric.ca CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 01 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jul 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:03:24.453377008 CEST	35.208.111.117	443	192.168.2.4	49909	CN=wphoot.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 06 20:51:22 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 04 20:51:22 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 10, 2021 21:03:24.456837893 CEST	35.208.111.117	443	192.168.2.4	49910	CN=wphoot.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 06 20:51:22 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 04 20:51:22 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6456 Parent PID: 3096

General

Start time:	21:02:09
Start date:	10/06/2021
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://kezenelectric.ca/First-America'
Imagebase:	0x7ff609c80000
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

Key Value Modified

Analysis Process: chrome.exe PID: 6680 Parent PID: 6456

General

Start time:	21:02:10
Start date:	10/06/2021
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=1528,13816511049468976980,9988846167183782253,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff609c80000
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

