ID: 438544
Cookbook: browseurl.jbs
Time: 18:25:11
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

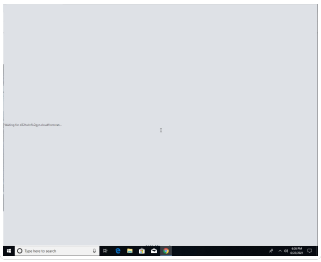
Windows Analysis Report https://lnkd.in/e9ejC3j

Overview

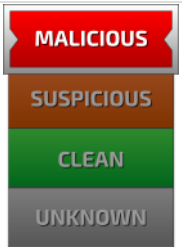
General Information

Sample URL:	http://https://lnkd.in/e9ejC3j
Analysis ID:	438544
Infos:	

Most interesting Screenshot:



Detection

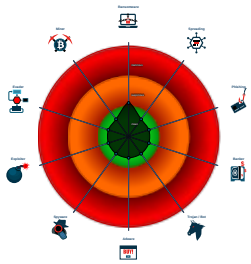


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4804 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://lnkd.in/e9ejC3j' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5772 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1628,1119372779995259193 2,7061772605032859279,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

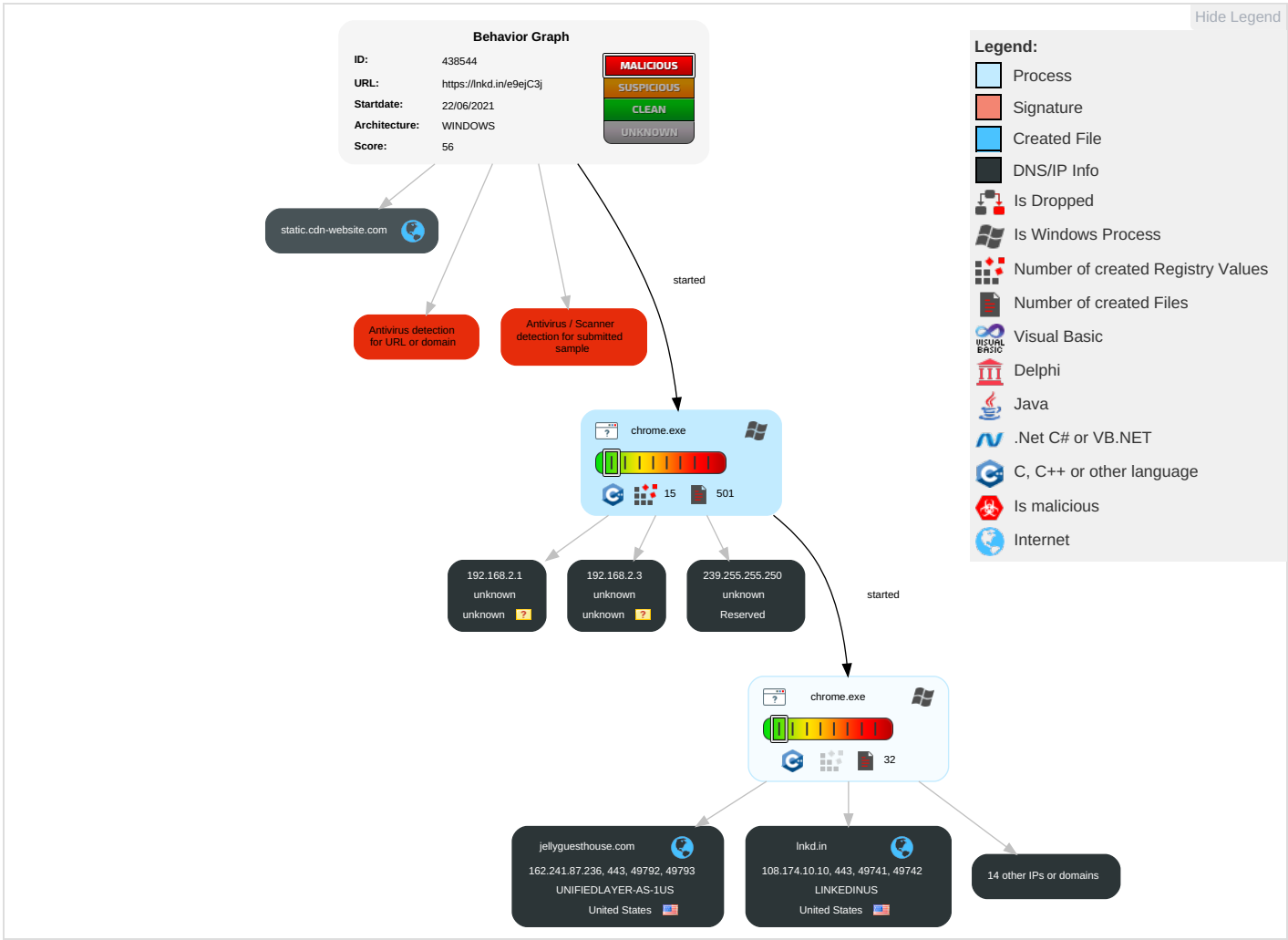
Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

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	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

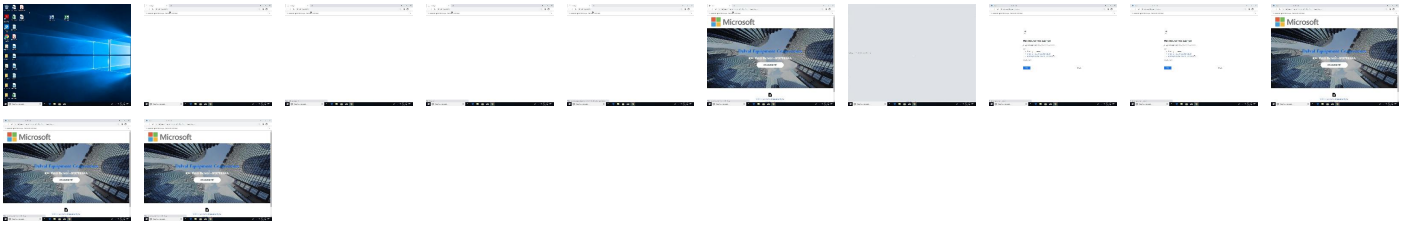
Behavior Graph

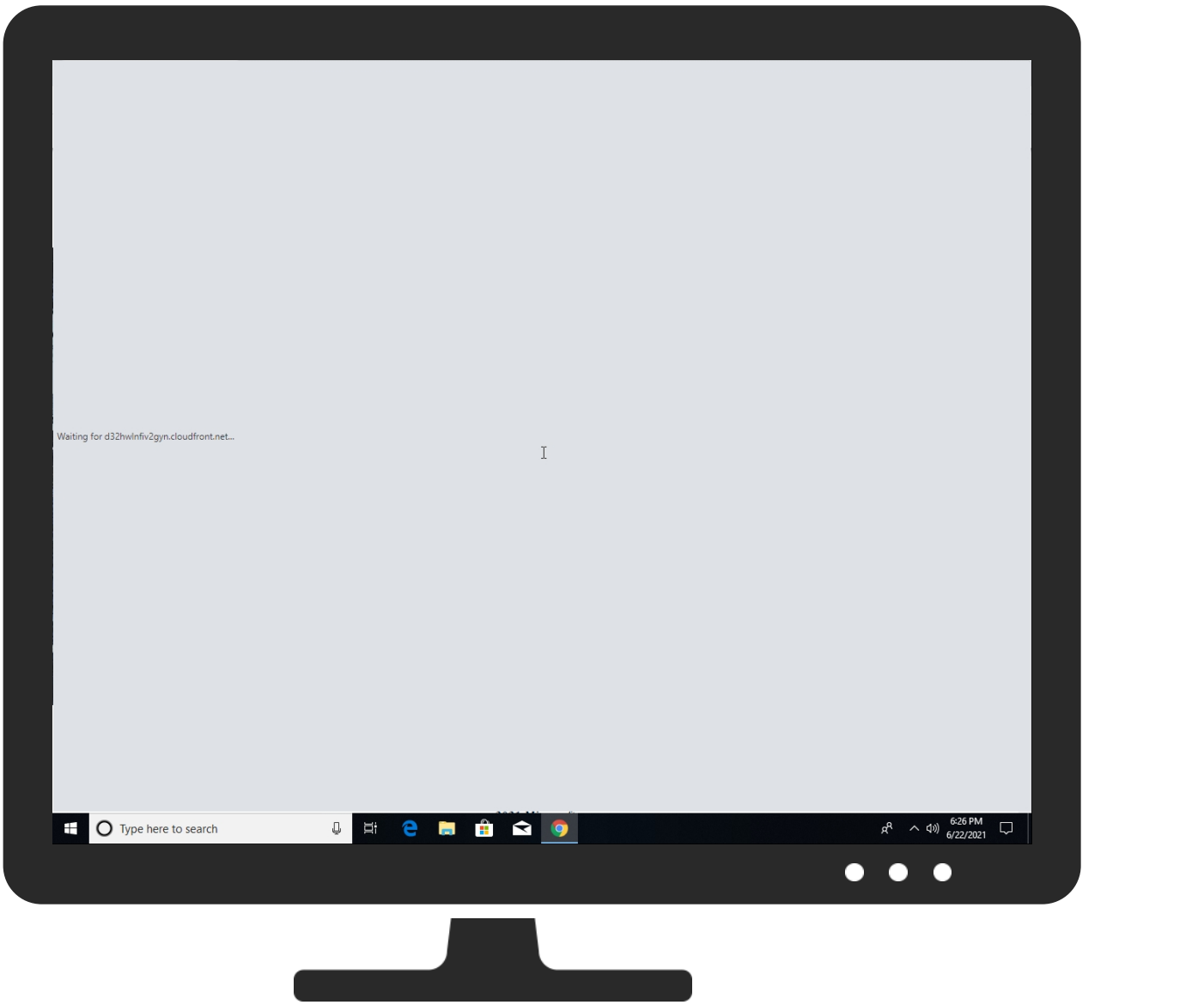


Screenshots

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://lnkd.in/e9ejC3j	0%	Virustotal		Browse
http://https://lnkd.in/e9ejC3j	0%	Avira URL Cloud	safe	
http://https://lnkd.in/e9ejC3j	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://delval-equipment-corporation17541a33.multiscreensite.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://lnkd.in	0%	Virustotal		Browse
http://https://lnkd.in	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.jsH	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.jsaD	0%	Avira URL Cloud	safe	
http://https://lnkd.in/e9ejC3j2	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.jsaD	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/11.ac6961bc2539a1d64	0%	Avira URL Cloud	safe	
http://bfs._dudamobile.com	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.js/	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/mnlt/production/1760	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://https://irp.cdn-website.com/WIDGET_CSS/production_1760/2ab06238fadc111cb27d396950534ebd.css	0%	Avira URL Cloud	safe	
http://https://lirp.cdn-website.com/	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://irp.cdn-website.com/4de34e46/files/4de34e46_1.min.css?v=4	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.jsa	0%	Avira URL Cloud	safe	
http://https://jellyguesthouse.com/mike	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://lnkd.in/e9ejC3jF	0%	Avira URL Cloud	safe	
http://https://lnkd.in/e9ejC3jG	0%	Avira URL Cloud	safe	
http://https://irp.cdn-website.com/4de34e46/files/4de34e46_home_1.min.css?v=4	0%	Avira URL Cloud	safe	
http://https://irp.cdn-website.com	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/25.1db8b4392b0d016be	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://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.jsaD	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://static.cdn-website.com/mnlt/production/1760/_dm/s/rt/dist/scripts/d-js-one-runtime-unified-d	0%	Avira URL Cloud	safe	
http://https://lirp.cdn-website.com	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.js/	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.js	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://static.cdn-website.com/runtime/favicon_d1_res.ico	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.jsH	0%	Avira URL Cloud	safe	
http://https://lirp.cdn-website.com/4de34e46/dms3rep/multi/opt/Screen	0%	Avira URL Cloud	safe	
http://https://lirp.cdn-website.com/md/dmip/dms3rep/multi/opt/skyscrapers-blue-sky-1920w.jpg	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.js	0%	Avira URL Cloud	safe	
http://https://lnkd.in/e9ejC3jHome/#	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/runtime-module-ancho	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/mnlt/production/1760/_dm/s/rt/dist/css/d-css-runtime-desktop-one-pack	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.js/	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.jsH	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/19.e04c90798724362b0	0%	Avira URL Cloud	safe	
http://https://lnkd.in/e9ejC3jHome	0%	Avira URL Cloud	safe	
http://https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lnkd.in	108.174.10.10	true	false		unknown
static-cdn.multiscreensite.com	13.225.74.4	true	false		high
stats.l.doubleclick.net	74.125.140.156	true	false		high
rtc.multiscreensite.com	54.159.252.151	true	false		high
delval-equipment-corporation17541a33.multiscreensite.com	100.24.208.97	true	false		high
lirp.cdn-website.com	13.224.193.107	true	false		unknown
irp.cdn-website.com	13.224.196.75	true	false		unknown
d32hwlnfiv2gyn.cloudfront.net	13.224.194.4	true	false		high
www.google.ch	172.217.16.131	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.161	true	false		high
static.cdn-website.com	13.225.74.51	true	false		unknown
jellyguesthouse.com	162.241.87.236	true	false		unknown
www.linkedin.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://delval-equipment-corporation17541a33.multiscreensite.com/	false		high
http://https://delval-equipment-corporation17541a33.multiscreensite.com/	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
100.24.208.97	delval-equipment-corporation17541a33.multiscreensite.com	United States		14618	AMAZON-AESUS	false
54.159.252.151	rtc.multiscreensite.com	United States		14618	AMAZON-AESUS	false
108.174.10.10	lnkd.in	United States		14413	LINKEDINUS	false
13.224.193.107	lirp.cdn-website.com	United States		16509	AMAZON-02US	false
162.241.87.236	jellyguesthouse.com	United States		46606	UNIFIEDLAYER-AS-1US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.194.4	d32hwlnfiv2gyn.cloudfront.net	United States		16509	AMAZON-02US	false
13.225.74.51	static.cdn-website.com	United States		16509	AMAZON-02US	false
13.225.74.4	static-cdn.multiscreensite.com	United States		16509	AMAZON-02US	false
74.125.140.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.212.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.224.196.75	irp.cdn-website.com	United States		16509	AMAZON-02US	false
172.217.16.131	www.google.ch	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438544
Start date:	22.06.2021
Start time:	18:25:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://lnkd.in/e9ejC3j
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:	13
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:	mal56.win@38/279@14/16
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://jellyguesthouse.com/mike • Browse: https://delval-equipment-corporation17541a33.multiscreensite.com/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:26:11	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:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ: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._..I..*..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.I..`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):	3.126375064919111
Encrypted:	false
SSDEEP:	6:kKT6se8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:r6s8kPlE99SNxAhUe3OMx
MD5:	D8705B92BE683C9A10B8F3838FD09CB2
SHA1:	F3E42BD60C7727157CC55CEBF2C9524ACA94D722
SHA-256:	96FE9916C769E2369AFB7866927FE7EAB3AE74A49FC6970661BB756D50F10EE7
SHA-512:	6914FA52B88D0EF4E979FEBACBAFBFB0281BA5E26BA950E8B1CB757125F3BDFFDB6754B4AF25C1A6879CE7404AC56FD93A17BAB6AC595F2852B6281C9DEA12F8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....bP.g..(..... .....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\4ca1ef2f-7272-4b2e-91f5-d5316d7cfb89.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7517677647745735
Encrypted:	false
SSDEEP:	384:hv9SK0vx8vUqVHZWtNqrfvem3NmchHsVGx4rTwa8x9AQwzrL6mnTxTAKu2tOosOo:VymZByMs1AeP8mUUnD2WK0WuRO
MD5:	705485CF73DAB6E4B5985C2ABDDED4C2
SHA1:	3B49A6E61220A1B24544BBB274FCA5B1710420BE
SHA-256:	47264BFFE83CAACE54CF10B515892B15D13539C4D6F294E6B61D6D98FC6BD707
SHA-512:	55D058CB3A1FEDA8188CEE55B1292FD3ED66BD2D43D0DDE2DBAB3320868E829D7F0762EF37043BD6438C628A43080BEA31636AFB1725351FE826D4F8E6FAF4E
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....=8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\51667488-5f30-4079-9455-0f7dbabbc499.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751254456940136
Encrypted:	false
SSDEEP:	384:vv9SK0vxgUDWtNqrfvem3NmchHsVGx4rTwa8x9AQwzrL6mnsTAKu2tOosONT1qrB:vmZByMN1AeP8mUUnD2WK0WuRa
MD5:	1C65038CFDD098B629733B4D5F284DF8
SHA1:	F509FA74C625160A61999F52BB35E2A6A28BC6C9
SHA-256:	57F708F590CFC53ED0CCE7699129C6ECF9196103F79DEA9352DB0EEE3DD01D19
SHA-512:	5CEC2AA9763172A7C4AC7CD281D8E02ED4571C22CDB5DF1A3BB023BE7E355BB6D94366895CFCB217662B7B4291392DCCFC420798DBD300C90E9219F8AB7DCE1
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\7d6fc287-4253-409a-8df1-adf4917c0be4.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):	173519
Entropy (8bit):	6.0798385387997875
Encrypted:	false
SSDEEP:	3072:C8TB48W0p6hRPkbz3GtzKyc2YEZJFcbXafIB0u1GOJmA3iuRc:5F4yohR830dZHaqfIlUOoSiuRc
MD5:	5A7FD9C65F5FAA8535EE1EF1738308B1
SHA1:	A57DFC2B378A656812D5E8D4BD5DE216E9D3DC6D
SHA-256:	2C2808F7E03A2D441AA136DBBB1CDEADEC2B54CFF5FB95A29B3A28CA493F2A8C
SHA-512:	C22F1DF10C13DADBE96D522650413A5113105999DF8ECE93D36CBACE61B6DE57E339DB0F17720093111E6310D9CEF904A0EFF42A5CA38691C80248022E8B04A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d6fc287-4253-409a-8df1-adf4917c0be4.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624379162338857e+12,"network":1.624379165e+12,"ticks":4937041209.0,"uncertainty":4897270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

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\02e4a6ee-b0ac-490e-9323-5e62f740d53d.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):	5189
Entropy (8bit):	4.970024760867468
Encrypted:	false
SSDEEP:	96:ndL2tMpIV35k0JCKL8cSkZS1DbOTlVuHn:ndLOMpI1h4KAkIT
MD5:	0E0A3B68DC7F98234A7E04E088AFAAEE
SHA1:	392040476CC9258D8B151CFA043D979F14E31F0A
SHA-256:	567080937A935768458D31AEE915341CE8556E353385F5E2DC437C127168702D
SHA-512:	BA1A1AD6E101F24E5592076781E9AE7A229728C8E6E499ACFC4D4BACEED9C3666161C5C8835E4A30CDD95091F361AF1F273C9C72E04AC35BBBE4DE94352DF 4E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13268852759405312","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\1c4794de-c7e0-49cb-b886-c629580a1ac1.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):	5800
Entropy (8bit):	5.179074924780962
Encrypted:	false
SSDEEP:	96:ndLkDLMRIODX299IV35k0JCKL8cSkZS1DbOTlVuHn:ndLKMRRX299I1h4KAkIT
MD5:	34D66BC9DFC6387E955E7946081B349C
SHA1:	AE66250E02C05D8B09B15FC77965DD253D867A39
SHA-256:	6971A29A846BF0BC221BB8976E33D2631931A49186923A321A8BE532F065B0A0
SHA-512:	A24486ECC4C58429DF653D4742AEE1FFA4FB4567A39A5797865EDF4B79D39785E44DD3DFDF6A7C43A3AF332C485864EE76EE1A3FCC241A9BB0D776616F8A54 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c4794de-c7e0-49cb-b886-c629580a1ac1.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13268852759405312","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","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\256488d5-b306-42d5-8f0c-efb3e01190c4.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):	5786
Entropy (8bit):	5.177832402963014
Encrypted:	false
SSDEEP:	96:ndLCDLMRIODX299IV35k0JCKL8cSkZS1DbOTlVuHn:ndLIMRRX299I1h4KAkIT
MD5:	4F7210302C050C471CAB20B956CD7775
SHA1:	41E1C688D318F3579107D0619133C896271D2169
SHA-256:	5F984FBC517975BF42F8DB85DCA7D742C0F011512F108FF0BB7A469DB5600A4A
SHA-512:	6437F19A791CA1D38BDDCE8A95D6B00E0D6EED6D6B40E02EF1A167860898AD27261BC87BA78A916F467C05320BD0FB2DBE289410724B6A85050AE0ED5A9AF9D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13268852759405312","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","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2e98b8e9-db5c-47e1-8531-29cf76b28c57.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):	1878
Entropy (8bit):	5.585853019781155
Encrypted:	false
SSDEEP:	48:YVFeUCieUz6UUhrRUPdUfKU7BsmUaqPeUekUeZwUXUeP:6FeUCieUmUUTUPdUfKU7FUhPeU3UnUXt
MD5:	E1CAB122259F1568CFCDC7B56CAA882F
SHA1:	36B5BC5B244B1AF5042FEB87538EDF6079AFCAF6
SHA-256:	2676E0ADD1229AD4765B37304C23D6B3660D3CC779BD575864202E7E7582CC5E
SHA-512:	BDFE05E13A25F6376482CB711D121FAF09E61BE1344DB67877536892CF527B550C557DBEEA260E90698658AA7261FC6E89B8C7137063B9B78A1E3F5B8AED4DC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1635265568.217084,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1624379168.217088},{"expiry":1655915167.124984,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1624379167.124991},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1655915169.260532,"host":"eUgCxH81n+La2Tm6XCimg7h97c6VJKp53NObpCO0cl4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1624379169.260545},{"expiry":1635265567.658645,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1624379167.658653},{"expiry":1655915167.075188,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\326f44b4-aad4-4e36-a1c6-de3bb88096f6.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):	5.577446836970379
Encrypted:	false
SSDEEP:	384:C1zt1LlapXi1kXqKf/pUZNCgVLH2HfD/rUPHwm4O:sLlyi1kXqKf/pUZNCgVLH2HfrrUPQml
MD5:	2D91F0E18FEC697B181D1AF6FDF5D12E
SHA1:	657BFDB761B515B52674C8BBAAF9CB6BDBF86C71
SHA-256:	B81F3AB9B27F00FF19FD77B75112DAFCB60E543432A756EF6B5181CFAB1D250A
SHA-512:	1400432E7CA6C6FC507F4361ED7B2661E7C33C9705543016890FC3897A2CAD118E42AC61C72CC81C8D67E6A37BE8E826E443046D7E4C9D318EAE3219D90C899
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\326f44b4-aad4-4e36-a1c6-de3bb88096f6.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13268852759103731","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\450c0951-6521-4620-b1d1-02ad43438887.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":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_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\66828a40-fa6e-4b15-a598-725fd1e6eb6c.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):	3879
Entropy (8bit):	4.864464576101466
Encrypted:	false
SSDEEP:	96:JzMKDHGXOTw0G6V7hRj+ArGCaCxmFr06vX9dKdC66bWRGcnMMFhM:JzMKDHGXOTw0G6V7hRj+MjaCxm106vXL
MD5:	BDB969A138485C7FE459FD3E0C6DD714
SHA1:	F5D845C56A838D75DC3A534ECA1799F113DECC1C
SHA-256:	4A876C94E040EA1AFB73AF52997D93AD1D478039E62A3C31F7046A8A4A290CC7
SHA-512:	92B9A80A47B115F4D338E84CAA1812E000C00A3AC4B69E9052F3307556C09729FA3CE8E60A070796183B6E7EE0BD7688013FB33CB2348EB7480B1732FA050809
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"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},{"isolation":[],"server":"https://lnkd.in","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271444764126534","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.linkedin.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271444768217023","port":443,"protocol_str":

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80baf639-efbf-4ed3-86cc-f0774e7d6a58.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):	5.536495026986398
Encrypted:	false
SSDEEP:	384:C1ztILlapXi1kXqKf/pUZNCgVLH2HfD/rUBHGVnZRHxm4T:nLlyi1kXqKf/pUZNCgVLH2HfrrU1GVnr
MD5:	64B9A133BB37BDD7C79EDC9EAF88FC14
SHA1:	1886A126864C64B7773BF64DB9B65C2DF8005E6D
SHA-256:	20ED378557DF9B6BD097CAEDD2F3A1DFA4B6DA10C3463AAB3A9B9AA15803A079
SHA-512:	BDD22708F10232212CF23DB60FFF352C8BF34D16028DB22B243F4F0DEBA8292ED617B6F76F7E65D1941120BAA3AD130C9F1BD0D394B82746841D90136F63E844
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80baf639-efbf-4ed3-86cc-f0774e7d6a58.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13268852759103731","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\92469f42-1f9e-4987-a285-831b062f2b70.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):	24064
Entropy (8bit):	5.534355518149597
Encrypted:	false
SSDEEP:	384:C1ztILlapXi1kXqKf/pUZNCgVLH2HfD/rU+HGVHGvnZRHYm4Z:nLlyi1kXqKf/pUZNCgVLH2HfrrUuGpGG
MD5:	D260CC5E9151910DE524F753BA025B3F
SHA1:	4F806679A1C44A9CA411C36F38C1F92558E7643D
SHA-256:	B76E32BC789AAA8A2A83900CDCA56FCF2D232026CEEE8B750A292E825CB6AD76
SHA-512:	648368743367441 29E389ED4EF4F6C07F866BAA8EFCF09831824A967BA92612CB789F4A2BDA2FDCF8BCDEA6F6C9C9681851F6FBB3BA2FD0FF1BD92BC9EF83F5
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":"13268852759103731","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.1316766594375665
Encrypted:	false
SSDEEP:	6:mvDwk+q2Pwkn23iKKdK9RXXTZIFUtpCDw+WZmwPCDwnEBVkwOwkn23iKKdK9RXXH:awk+vYf5Kk7XT2FUtpKw+W/PKwnKV5J3
MD5:	9048A321EF18B09772678EC243FEEDD2
SHA1:	50A207614BCF33EDB21813D1D970F61A11F8D685
SHA-256:	41AA1C2D9809BC351C7E772666A7CD912207C2B1100DF5260CE1F4453B5D4F75
SHA-512:	1A5E1F1FE58C38125332F916F290C8AB396BF34CDA867D163F63468420E358E92FC8E39AD370104E297B915205A30FAD10CAD5A805CE88C2A8BA9DA2E7B6D82
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:10.621 1acc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/22-18:26:10.622 1acc Recovering log #3.2021/06/22-18:26:10.623 1acc 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):	5.174019909134953
Encrypted:	false
SSDEEP:	6:mvDCER3+q2Pwkn23iKKdKyDZIFUtpCDAEGAWZmwPCDAEG3VkwOwkn23iKKdKyJLJ:aCER3+vYf5Kk02FUtpK1W/PK4V5Jf5K1
MD5:	91EDE44080B464B24C3A21B194EE0EF5
SHA1:	62BA99464905793569F7ABB4A11DC61976C1F569
SHA-256:	F7044E255F0B0ECC782417CC12CAB6E660C51A824CF7FBA3E9694DA320522FB9
SHA-512:	4DB024B66E3B30BA3744CB73F54884FA0098E8678581478295526844B6A5C7B80C414CD5D6467F04C542CC6AB81A8C7CC25A559D9175728F9099AA90AFFF23A8
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:10.588 1acc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/22-18:26:10.590 1acc Recovering log #3.2021/06/22-18:26:10.590 1acc 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\09cd82d33cb49abf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77712
Entropy (8bit):	6.076899490999161
Encrypted:	false
SSDEEP:	1536:DUbgLbD7kfJm/cLwmkCd6Fgabr3ER8epEMomIFU5ELF9dzOE:DQgLDkBmHmd66afl84zYFU+LF9N
MD5:	559A60A2E6F08E6E24CB13089E4CECAD
SHA1:	6262DD8502D076B94E58C586D4B7ECB93A677AFD
SHA-256:	FDEFCE5B7D982B7C1D993369B10D5CAC633EB48358A6947496FC5A64016674B6
SHA-512:	37CBC4CAC9B305A5D7FA502CAEDCAFAD4752981F1F36DF01BE7BC014480439661E022481EBF08DF5FE867E45E8EECC1D1126EC9498F4E227E3AED231A5135447
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....C63A509A049001560FC614EA1F63B9571C1DE008C9E83F966C0F13AC261582E8.....'.....O....P.....8.....`.....D.....P.....x.....(.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.O.R....n.....Qb^.u+....q.....Qb.kY`....r.....Qb.O.....t.....QbV!w;....v.....Qbz.~...x.....Qb..Yu....y.....Qb.....z.....QbN.^.....A.....Qb2.....B.....Qb.Nf.....C.....Qb.....F.....QbjjY`....E.....Qb.....D.....Qb~.....G.....Qbf.....H.....Qbfg.^....J.....Qb.\uY....I.....Qb..,.....K.....Qb.R.....aa....Qb./m....L.....Qb24KE....N.....Qb."....O.....Qb.Y.....P.....Qb.1.C....M.....QbR=t.....da....Qb.#.....ea....Qb.....Q.....Qb2.....S.....Qbf.o7....R.....Qb.e\.....ia....Qb.....U.....Qb..._....ha....QbJ=.....T.....Qb...{....V.....QbzU.U....W.....Qb..Y.....Z.....QbVy.....Y.....Qb&.....X.....Qbr.uA....ba....Qb.o.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c21d15e1a3a133e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114016
Entropy (8bit):	5.792724945073308
Encrypted:	false
SSDEEP:	1536:l4y5LzJL5nYpVy1AZtSz2FJHnB/CXfwhjU5vNLm/lWW6wCCz:Sy5LzZ5N1ATEMHB/CIzzUu
MD5:	7EE641800941B2BD80B54A483495BBC8
SHA1:	2ECA11108BC2B877B53927CFFB461180C5A5F435
SHA-256:	C919C66108174903572F7ECDED497B6412D239198E12E9BEC6EAF841183ED939
SHA-512:	9ABB7EBCE04E606D8B795421919F9E184196D6CC3173237168E4B5A25ABCF450A399851EE9B1F89B8F0F27C6D8DC76ED96B5C1295F0C0135F1F97C79A8CC87BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...-.....C14EC03628FBFF55ADC8797EAE9C1222519485921564E088ACC56447507581EC.....'.....O).....IV:.....D.....X.....`.....(S.0..`.....L`.....(S...`.....PL`$.....Qc~..5....document..QeF+.....currentScript.....QbV.....src...Q.@...n....window... Q.p...x....webpackJsonpruntime...Qb.b.k....push.....`.....L`.....`.....Ma.....`.....4..a.....QbF,.....7uCZC..Qb.q,.....J3gSC..Qb:].....UiZKC..Qb..j.....pcmOC..QbZ%.M....zT9CC.(S...`"....8L`.....!...Q.P...6....webpackJsonp.....`.....L`.....`.....Ma.....`.....`.....DLd.....E`.....E`....E`.....(S...`.....`L`,....`Rc,.....Qb..,.....K.....Qb...{....V.....Qb."......vt....Qb..K.....et....Qb6..T....ft.....R...Qb~.....G...f.....l`....Da.....Qb&d.\....d....(S.(.`....].K`....Dd.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ccdc33e51bd5d09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6184
Entropy (8bit):	5.73273147867443
Encrypted:	false
SSDEEP:	192:FLnK6DeaLnLAwWyEqqCeDj7KsnC9ohZSeLsDetb4K:FjleajEHT599sit1
MD5:	546C7C2771612824887337 78EB926A6E
SHA1:	4A84FB722E13C23B62C6F7606F913BB1A18F521F
SHA-256:	2F9377B4E79CFE67D3E86AD2B1323508510A7939E817D90E32FB4F2844ABBFB8
SHA-512:	AF2A96FB6E098140124C056E225BBAF4D1D1513453F3FE141EA638BA11A538F650CBC0621481402904AED80D2C6A4BE1FD41EFB30F1FDCE65DDEBF69959C246C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/runtime-module-anchors.3f49b279e2635a6e200b.js .https://multiscreensite.com/\...#/.....|.....L...s.G..q..*...C...Z....L..A..Eo.....f..+.....A..Eo.....'.f.....O...`....X.....4.....(S.0..`.....L`.....(S...`.....0L`.....Qc~..5....document..QeF+.....currentScript.....QbV.....src...Q.@...n....window... Q.p...x....webpackJsonpruntime...Qb.b.k....push.....`.....L`.....`.....Ma.....`.....a.....Qb..4.....q6BRC.(S.U..`^.....L`D.....RcT.....".....QbB.U.....h.....Qb&d.\....d.....M...QbV!w;....v.....QbN.^.....A.....Qb../.....l.....Qb..J.....f.....Qb2.....S.....Qb.H.O....m.....QbjjY`....E.....Qb.\uY....I.....Qb.=.....p.....S...Qb..Yu....y.....Qb."....O.....Qb.Nf.....C...p.....Q.`.....Pd.....push.q6BR...aF.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\429e175bc1484880_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\429e175bc1484880_0	
Size (bytes):	404
Entropy (8bit):	5.942215054259217
Encrypted:	false
SSDEEP:	12:D+xblYnWcLQm+/chClcdTsh/79IaE1Clcd:DUblSbN+/mCl9plECl
MD5:	B1D84A100E423FED586C7F3059FB104E
SHA1:	3B3208FE198C6EF4300C5C52ECD3994658D7C5B0
SHA-256:	3B0D3AF961FDAD9D3D7E8DFD658DA5197E06C5BB6CB84F5FAD1E4F715C46B6BF
SHA-512:	97D01657E9FAE63C7DB30E624D6ACC42788C3A91856A22F6FE4BCF8AE72346F52A9B4ACCAF3136CCA13DF7B0B3310071F0D7083CAC50B504209EDBD3E0D332C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/11.ac6961bc2539a1d64dd9.js .https://multiscreensite.com/w...#/.....GN...&)....u....*P.Vz..D..Iq...A..Eo.....v&.....A..Eo.....w...#/.....C14EC03628FBFF55ADC8797EAE9C1222519485921564E088ACC5644750758 1EC.GN...&)....u....*P.Vz..D..Iq...A..Eo.....K.e`L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d25e5101bb028bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.945284069517062
Encrypted:	false
SSDEEP:	6:mY9YWdSFrnH9yoPm0jeKkotHb4PRK6tYk5BeOUGuTtHb4:sdyEmgZHbcCk5ByGuZHb
MD5:	61746DAFE8AD665CC4F5A3F9EC14DB7D
SHA1:	4BED656E0C4EC75800DB9E1161199A4F5DB1782C
SHA-256:	397F748A4B0C7CCCBD3001890AE18CA74E70510C863DBE8C261A660264B40BD1
SHA-512:	C14EFCD8F8A0EDFB1ACA44321E5E3F454E27BE29EB9E3936365FA795E15927561CC6A5FB0D778F23DBC0F9F0898442780E2BCBD58A1A7B07A7957EC699656325
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^..." ....._keyhttps://d32hwlnfiv2gyn.cloudfront.net/sp-2.0.0-dm-0.1.min.js .https://multiscreensite.com/....#/.....S.....aqW\..j..$...AC1....`;.A..Eo..... R.....A..Eo.....#/.0...0635FDEC47E489742C0A87C1477368EC464F96584BA68CFFE3F9227F1F26F119S.....aqW\..j..$...AC1....`;.A..Eo.....Zbj.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\594dd4f7e7aa8aba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	76488
Entropy (8bit):	5.769677911032112
Encrypted:	false
SSDEEP:	1536:CAYiQQzg3q3d8vBXUcRoXnDTINKUTITMPaLzFqPZP4N9wIQq:CAYXQzQM8vtUcqzTAjITMCXwIQq
MD5:	0567220F265BB333BBC2CD8B88EB2E76
SHA1:	A7D14F8F2FA34CF0C0CAD590DDECB203E9B0AFE3
SHA-256:	45E39163D349CD5B73EFC03A2DA19A5F7E7FAD6B5CBE11862C294E47A2F01E63
SHA-512:	25B17C162C7696F331BB172D8EEE2A0DF0206CAA4A61D8A6DE0C9D1B1B329552B33A474F4CF0B8DCDAFC11C88D5F733696A2F71A18614BC5B2F5A193CFB6375
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....."....C901390DCF4980D6F8AD9ED6A1567E7CEA05730380DCE502FBE28C722DE0BBE3.....'..e....O.....)....f.....%.....L.....,..... .....p.....(S.0..`.....L`.....(S....%.`.I.....L`z.....].Rc.....Qb.....data..Qbr.uA....ba....QbR=t....da....Qb2#.....ka....Qb..b0....ma....Qbj.....p a....QbR.....qa....Qb~k.[....ra....Qb..^.....sa....Qb..B.....ta.....Qb.Yx.....ua....Qb..~....va...Qb...u....wa....Qb.....xa....Qb^.~.....ya....Qb..s.....za....Qb..(.....Ba....Qb..LD... .Ea....QbV.....Fa....Qb..D;....Ga....Qbv..#....Ia....Qb...n....Ja....Qb&.a.....Ka....Qbv..:....Na....Qb..f.....Oa....Qb..vc....Pa....Qb.Y.t....Ca....Qbfy%.....Ua....Qb.....Xa....Qb..fg.. ..Ya....Qb.8.,....Za....Qb>x.5....$a....Qbv.....ab....Qb.....bb....Qb>.....cb....Qb.....db....Qb6..]....eb....Qb*Q/"....hb....Qb.....fb....QbR.u....ib....Qb...8....jb....QbF.,y.. ..mb....QbjT.....ob....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e8efa2c43a44431_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94192
Entropy (8bit):	5.771552830717903
Encrypted:	false
SSDEEP:	1536:p5ImtuwovZ1Aok1jlVz6Gje1ktogsbuoWyxfu5GVArVDi59G1qvSPj:rOw6S+I9k6gsGqfuMVAZ31qs
MD5:	14FBC8EAAE8581133138D86C558B9658
SHA1:	36BB2477A7F9B9A0A8757F746B404E20378093A2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e8efa2c43a44431_0	
SHA-256:	4F8014297B2C8132739F33F2DD34F14117645A2E5D0B0F62FD93300FB7A34A06
SHA-512:	9B9C5AC0B022E1F03DEF1E4025231264591D0CAFEE3EA0FE75D15920CB2B9BF5C42344D9202D4B523056FBAFBD06B4A441225D5569814AE7DD9C2064542198F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...*.....BAE482BC187140A07A197C139C7F3806F7C020EA37F5FAD1C22C52343C6E4F24.....'.JN....O ....n..x.$n.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@6d.....module....Q.@.{>....exports...Qc~..5. ...document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!....>...https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.j s..a.....D`....D`....D`.....`z...&...&..!.&....&.(S...!..`.C.....q.L`.....Rc@.....M.....Qb&d.\....d.....Qbr..&....e.....Qb..J.....f.....QbB.U.....h.....S...Qb.....j.....QbJl.... ..k.....Qb../.....I.....Qb.O.R....n.....Qb.....o.....Qb.=.....p.....Qb^.u+....q.....Qb.kY`....r.....Qb..<&....s.....R....QbV!w;....v.....QbB.....w.....Qbz.~.....x.....Qb..Yu....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\606eca842ffe7296_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72152
Entropy (8bit):	6.02282847683586
Encrypted:	false
SSDEEP:	1536:Zb4uH4MrXs3xm4NM8lX72vNbEummW09Q5O2tihF6MzDqen:Zb4nMD2RebCNbxDWMQ5O2tuF6Uqen
MD5:	38BABB42200CCB5B2C90C8E8EAFB41DD
SHA1:	71F84BAFE7A4D5B5872605E14C3211D8F8A48C0C
SHA-256:	259A7949B98F5F39D8E992150DF56F5C444F3B0BE8D87E31B785815B7EBB6478
SHA-512:	AF46D08E4291768EF6784DE34E5D51D18F0648412730D7DAE05616D68B3BE3F804B4D8BFB5B8B73DD6B5FC6169B238770A06E96A83690A7B4C187A6D93636E4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....0635FDEC47E489742C0A87C1477368EC464F96584BA68CFFE3F9227F1F26F119.....'.....O.....F#.....d.....p..... D.....T.....(S.M...`T.....L`N....(S.x.`.....L`.....PRc$.....Qb&d.\....d.....O...QbV..w....c.....M.d$.....$.....Qbr..&....e...`....Daf.....(S....`..... ,L`.....4Rc.....Qb../.....I...`$.....`....Da.....A...Q.@:.....require..... Qf.h.....Cannot find module '..Qb&."....'.....a.....Q.@.{>....exports....a.....QbR.....call..Q.. (S.T..`d...]..K`....Do.....&...*..&...*..&.%.*..&.....&.%...%...%.&.]....,Rc.....I`....Da8.....c..... .....@.-....HP.....<...https://d32hwlnfiv2gyn.cloudfront.net/sp-2.0.0-dm-0.1.min.jsa.....D`....D`B...D`.....i....`0...&...&..a.&..A.&....&.(S.P..`\....L`.....dRc.....Q...Q.@6d.....module.....Qb^3.....JSON...gd....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83c8f7e0c9d38d57_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4340
Entropy (8bit):	5.4037166383089765
Encrypted:	false
SSDEEP:	96:g63QFll5NQIxbLpxqk98K7rrnkAfb4r6k:gOQl5NQIxbVxqkuzAfb4N
MD5:	E5D4BE8BEC9D1A051FA71DF6D0CF88C2
SHA1:	89825C0DA80DE645FA05668EB659362FCF652A75
SHA-256:	931C3AFC5970B63F5FAAA47112EE5D8012879D59E5ADBD04BCE5A2D83CDD9CFC
SHA-512:	97E8E97BAAB781402FF7465F906642A08178B3B95AB12DAE2001B742E4B59836A62A8223757E88F653B630549916AC386C08530233ABF5CC7E1BB8B7E2C67780
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}c&...._keyhttps://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/25.1db8b4392b0d016be60f.js .https://multiscreensite.com/b...#/ .....`.....=.X]e....op..F. .v....SE.A..Eo.....NX.....A..Eo.....b...#/.....'.....O....X.....q.....(S.0..`.....L`.....(S...`.....0L`.....Qc~..5.. ..document..QeF+.....currentScript.....QbV.....src...Q.@...n....window... Q.p...x....webpackJsonpruntime...Qb.b.k....push.....`.....L`.....`.....Ma....2...`.....a.....Qb>..R.. ..ONNRC.(S.Y..`h.....L`D.....Rct.....2.....Qb..<&....s.....Qb../.....I.....QbB.....w.....Qb..Yu....y.....Qb..J.....f.....QbjjY`....E.....Qb./m....L.....QbB.U.....h.....Qb&d.\....d.....Qb.H.O.. ..m.....QbN.^.....A.....Qb2.....S.....Qb.....F.....Qb.Nf.....C.....QbJ=.....T.....Qb2.....B.....Qb.\uY....I.....Qb.Y.....P.....Qb.....D.....Qb24KE....N.....O...Qb."....O.....Qbfg.^....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c1d817ea4a75421_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8962
Entropy (8bit):	5.720724498702796
Encrypted:	false
SSDEEP:	96:Cn4oE4X/AZ+qfbi8mMahhtPJEhHzyFXAKQ6V+4w89i+N4v+giCIkDLsPK8EmBzcM:C4ZK2+Yb70Whc5V4I4XLDY76snT
MD5:	4C76AC805CD2DF90E0DD778495FF5240
SHA1:	33D30CC54FD5310D84462E95F288E025C7820915
SHA-256:	2E60B0A34953324AC136C0C8B0BCFE195214A4B35935D1BADC66BFA90B4E7717
SHA-512:	C3FE37CC3F19874EF4A802793BDB520A418168361C255F4D0D4681565247D6A23EE7DC1D89538F53E8365A81FCFF83630DA0827BC039D18B92550C112874FA5D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c1d817ea4a75421_0	
Preview:	0\r..m.....b...t....._keyhttps://static.cdn-website.com/libs/bower-skrollr/skrollr.min.js .https://multiscreensite.com/z...#/.....c.....j...Xm..w.....Q....KYM....2.A..Eo..... .&>.N.....A..Eo.....'..1....O....x!...P.....|.....(S.<..`0.....L`.....(S....`X.....L`.....I.Rc.....Qb.kY`....r.....Qb.O.....t.....Qbr..&....e..... Qb.O.R....n.....Qb.....o.....M....S...Qb../.....l.....Qb..<&....s.....QbV..w....c.....Qb..J.....f.....R....Qb.H.O....m.....Qb.=.....p.....Qb&d.\....d.....QbV!w;....v.....QbB.U.....h. ....Qb..Yu....y.....QbJ=.....T.....O...Qb2.....S.....QbJl.....k.....QbB.....w.....Qbz.~.....x.....QbjjY`....E.....QbN.^.....A.....Qb.....F.....Qb.Nf.....C.....Qb.....D.....Qbf.....H..... Qb.\uY....I.....Qb.Y.....P.....Qb24KE....N.....Qb."....O.....Qb...{....V.....Qb.....z.....Qb^.u+....q.....Qb./m....L.....Qb.1.C....M.....Qb....._.....Qb2.....B.....Qb~.....G..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a6df046b2a2ccb56_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	375840
Entropy (8bit):	5.908108129423448
Encrypted:	false
SSDEEP:	6144:bIYAXnW//krPd/cXC4D1BjNHAIBazVoeLt8fUu2:bIY5/sPd/c/5pNH1EBG2
MD5:	F33E14884A95A9ADE808D74D3D17C4CE
SHA1:	9BA63250D9EA025ADBB5ADF52868CABF93171A3E
SHA-256:	B394557AD8F842F7D145B1BC1A001B5FF521CECCF7D011E4E8A5E83B62E7A1E9
SHA-512:	F0290F74BC41B535075635A8971E7DA13AFDD0EF22598053E1BA3306D0A32A81EAB27740866FAE5DD615E655457B2644B51343C75E52A9D85532E8EA92AAFAA9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...*w.....2EE46811F9171B0273CC5BB946B8C67A98B31E7116CEE3258C6AA4436707E392.....'..b....Os.....]..`.....L.....4.....| .....P.....X.....0.....0.....D..... .....4.....p.....(S.....`T....=.L`.....e.L`.....QcV*.-....Base64....Qc.WFN....hexcase...Qc.... ....b64pad...(S.....IaKd...d....Qc.'.....hex_sha1E.@.-.....P.....q...https://static.cdn-website.com/mnlt/production/1760/_dm/s/rt/dist/scripts/d-js-one-runtime-unified-desktop.min.js...a.....D`....D`'"...D`.....M....`"...&...&...(S....`.....L`.....PRc$.....Qb&d.\....d.....QbV..w....c.....O...Qb..J.....f...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad7458324f9e58f9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.912253335480623
Encrypted:	false
SSDEEP:	6:mq/PYk+xH2QAlKPUQyBPmqM+Ap8RZ44GnK6tc4k9VXhcMekoUg33Fanagl:3+xWQCUU7mbfAZeaHeTf1an/
MD5:	20B64597AE2AEC39629E0ECC32A21B64
SHA1:	4AED03F2BB3BA91F00CF9FABCB3E06ADFCA4DA51
SHA-256:	8DA9F9E01B4A8EFEC345B23450DB3A4ED5FF1F554F0989BE10BB601FA43B0111
SHA-512:	689B7052496579D8927E2BCF4819A9CC1FB778E2B390375630B7996CFEA7987E41D650C6C80C7AD3AF367C67A6F551D1B7EA3D4201FFAB415938F59467A66D6A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....._keyhttps://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.js .https://multiscreensite.com/.....#/.....y.....:.l*../KH#.y..eXZ..a+pB'd.A..Eo..... c.....A..Eo.....#/.Ho..BAE482BC187140A07A197C139C7F3806F7C020EA37F5FAD1C22C52343C6E4F24.....:.l*../KH#.y..eXZ..a+pB'd.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b0361d9912f6bce6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	5.849154595587722
Encrypted:	false
SSDEEP:	6:mbM9YGL+MIwJJaPmYABl5hIbV9zrD4K6tSpaWYhTudrdNW+hIbV9zr:s4IwvKmFlo5BaUYhyd+t5
MD5:	645EC702661C72D237A8BF5B8F081817
SHA1:	0D713970199BFC52258796F85140E6D041F4300D
SHA-256:	6D8B22D8F426D1D6D785BFE8E02FF808C5D8ADA9F29A9888D11BD69D480A4863
SHA-512:	1EC53DE2042141A985BA4FF9B16D7B918C9009FC7C1C823C33D943F9121D9AE038822DD7B0BDF5689560AE872238526C29D437684B9148E4B3DD92A9AD65A5F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....z....._keyhttps://www.google-analytics.com/analytics.js .https://multiscreensite.com/....#/.....r.....(|.p..7m~p.E.V..B..A@4.A..Eo.....A..Eo... .....#/.....C63A509A049001560FC614EA1F63B9571C1DE008C9E83F966C0F13AC261582E8...r.....(|.p..7m~p.E.V..B..A@4.A..Eo.....<:@L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bffb8a767a1be742_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\bffb8a767a1be742_0	
Size (bytes):	354
Entropy (8bit):	5.9924338427973955
Encrypted:	false
SSDEEP:	6:mlYGLSmXZCuhPm7Dxo1jt1k7/bK6tw1PxhI0Zbgheas2H8t1:e39mRoh0/Nq1ZhhZENPH8
MD5:	D05E53F6EF6247A99DE95FB72EFF56A6
SHA1:	234BCDD858D950E71EB1A19E30045685C178D8E7
SHA-256:	FC7C4B1708434C49E9DDD4A69B2EE3746D2ACD7DBA77FF7CFE1495971C80872F
SHA-512:	E03D16EC69327D4803B4E8C0626436BE78EB783483A0606DAA4A432613923835817AEBF47E85E238406D0579703EE3A69B21DDC6B24167634D9A6A2AE77E4D37
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-7265702-9 .https://multiscreensite.com/...#/.....&.....?....J.'iJ.w.c.....f.k.....A..Eo..... ..A..Eo.....#/. *..C901390DCF4980D6F8AD9ED6A1567E7CEA05730380DCE502FBE28C722DE0BBE3?....J.'iJ.w.c.....f.k.....A..Eo.....D`.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f18b98547ba4dd69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.9457125570003
Encrypted:	false
SSDEEP:	6:mIKIEYk+xbtTRMfnVaROURl4IgsOLOPmUkRA7wous0rStbK6tyQcgbxITMBmlnZu:dKl+xblYnwOUROgsOLWm9MXptNws0tG
MD5:	BAE67F29CE81D1EDDE0CC44B96267B58
SHA1:	0A8023BFD146BE6E046F639297BF1D00105BA80C
SHA-256:	3BA4C2223C5D432643E792E91B0393AEE2BB787167DE3ABF16308BC88373E438
SHA-512:	88D7009F60639190509E00EF004F10D02D6A0AC324CF28F598AD3EB931ADCA23EC5935D95F5A5204E19513D3EBF3F645CC711C05602D8FBDBC372DC1C4537C6
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://static.cdn-website.com/mnlt/production/1760/_dm/s/rt/dist/scripts/d-js-one-runtime-unified-desktop.min.js .https://multiscreensite.com/.....#/.. .....L.d.....>&?..J.y.P...w3%t.`,.A..Eo.....A..Eo.....#/.x...2EE46811F9171B0273CC5BB946B8C67A98B31E7116CEE3258C6AA4436707E39 2..L.d.....>&?..J.y.P...w3%t.`,.A..Eo.....].L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f1a198b74ba8120e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1751
Entropy (8bit):	5.506051189145999
Encrypted:	false
SSDEEP:	24:/UdotIB8xDj0zdMTqUIeqcUdsOY5dIiGU+nbtdBk7E1PHSZGl3pKrl://tIB8hQwqU35OYQBU+bvqQSZG5pE
MD5:	F46C83D1AAFC490912486EB52510A61C
SHA1:	3866DA79D31EB11F8A8C5E85BEAC672F64D5742C
SHA-256:	ADBE304394365F58FE985B6DFBD7AB7400788E9B19D00F221D852F1A26C6C33F
SHA-512:	22961FAB0304D4D98D47B64E5291EE8182819835191E334BA7B4012335086F217C0E65A499818269A35AA0972BBF81C29159CD69CB674404E8071E17FCFA1AFE
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.js .https://multiscreensite.com/....#/.....[.....[$h..U.;.}.^}.}...WY..i..:.O...A..Eo.....y. .....A..Eo.....#/.....'.B.....O....p...5.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@.{>....exports...Q.@6d.....module....Q.@^.j.....define... .Qbb3.....amd...Q.@...Z....lozad.....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da...,.....e.....`...p...@.....@.-....LP. !.....=...https://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.js...a.....D`....D`P...D`.....<...`....&...&....&.(S.h.`.....4L`.....HRc .....R....QbV..w....c.....Qb../.....l..... O.c.....I`....DaH...~....(S.....Iau.....Q.d.....@.....Qc~..5....document..Qd&..*....documentMode.,..a.....Qd...9....rootMargin....Qb.....0px..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9244f3eb97f7cf5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2324
Entropy (8bit):	5.582331777693444
Encrypted:	false
SSDEEP:	48:AF1Xb3DSy8OMkt78zF1Xb2Va7Z4Hw7wJrXKLyojSB:AfTWIV8zfhNc2wJb4JQ
MD5:	3B3E2430C81AF84E8063517CA73418EE
SHA1:	38B6CD51B954C6DAAE9A1FC145F4E8BEF8B51AE0
SHA-256:	BEDED7B45A489457308FB6386F10DC9A33C03E70C205713E3DE72D555354758F
SHA-512:	CE0BB4A4E79E2150C83A6BDEAD2B85B6F334CD18C2DCE90C992CBBA5D5D47E2334A5634B1C27CD8BCDAB1AE80575861D8800417D1E5F241067347E5DE5111 FF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9244f3eb97f7cf5_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://static.cdn-website.com/mnlt/production/1760/editor/apps/modules/runtime/19.e04c90798724362b0679.js .https://multiscreensite.com/g8..#/.....va...m.n3m..P@..6.Z].;.... }.o.A..Eo.....z.....A..Eo.....g8..#/.....'.....O.....)yS.....(S.0..`.....L`.....(S...`.....0L`.....Qc~..5....document..QeF+.....currentScript.....QbV.....src...Q.@...n....window... Q.p...x....webpackJsonpruntime...Qb.b.k....push.....`.....L`.....`.....Ma....&...`.....a.....Qb.S~&....3CslC.(S...`&....HL` ....xRc8.....Qb..J.....f.....QbB.U.....h.....QbV!w;....v.....Qb.Nf.....C.....Qb..Yu....y.....Qb.\uY....I.....QbB.....w.....Qb24KE....N.....Qb2.....S.....Qbf.....H...i.....Q.`.....Pd.....push.3Csl...aL.....Qb.kY`....r.....Qb&d.\....d....$Qg.....collectExtraDataByMetric.(S.(.`.....L`.....Q...K`....Dd.....,R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.281555187126832
Encrypted:	false
SSDEEP:	12:THlRH/++BJkOebLb7v8LRN+oB16kiUljVViwZXUyA0:THff+TzP7v8LRN+oB76Kj
MD5:	02DFC67F3E29A029903AC6508F7D2619
SHA1:	4E042B0665A359BBEB2DF4F6CF1779C6019D71FD
SHA-256:	0D5DEBAD44C0701E64794A96ED22B4901E8956A3B79652858C355E2BFA96EDD1
SHA-512:	B062C6C8CFF919AB00588D8857B4B7CA53BADBDA02B345EB4A830E5306D18F8ABFE1DFD6FAABA207B4DA502802FA59538040059AA2383D8255A29BE5F4B465(9
Malicious:	false
Reputation:	low
Preview:	......S.oy retne.....>.:.^.!..ZJ..#/.....<....ZJ..#/..1.....r./..n`.ZJ..#/.....MY.ZJ..#/..,.....V.,*k...ZJ..#/.....1D.C,..^.ZJ..#/..q.....6.....#/.....(....%M.....#/.....|..>O$.....#/.....HH.[..B.....#/.....].Q>....ZJ..#/.....!T..~....ZJ..#/..$.....W.....#/.....K.....#/.....B..zv.....#/.....i.{T.....#/.....X.O2Xt.....#/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....TW..#/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.0001467572192726
Encrypted:	false
SSDEEP:	96:dNwS5W+0eX1DczpX6WOCWO5nf/uAV18unpTMDcMDp/B0Nwe5W+WdWNSDccVkcXw0:dugrqd/N0tiuE7m+catm
MD5:	D09061E098421148341DE12D7E0986DE
SHA1:	2C0E69F358A1AE9392665FC5219D7A664C89A4F2
SHA-256:	0F4370BC85ADC1071667ECAE051946F269B5B1D8ED381FE61742243E6DF24BE3
SHA-512:	AC503105EBC30F49B5A7B4EC87EAEF177C6F8918D1035535AEDDA9A8D565366F0D63DE901F92BDEECAB9BE977D3D56C97F971BA1815AC88CC41BFB2989720(59
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	2.019024677098301
Encrypted:	false
SSDEEP:	96:bNVcNwZ5W+0eX1DczpX6WOCWO5nf/uAVLunpTMDcMDp/BYMNwY:bNVcujrqd/N1tiMuY
MD5:	93BCF668E5A6B0F9B30BA46C1FBA4B08
SHA1:	C64E5D398E91800E578831C7D3668953707749EB
SHA-256:	1C32F9E09F71F1CB874F9689DE1DC246DEDC3674D74E96E6853EBAED1DE44C76
SHA-512:	26C0D06A20BEE716CE889E8A906E0D8D7E36E9ED6B8B1C719E5632900E7221B0FB8C97A2CD7073FFF3B9274EA0F9B2A9E5D6244E2BDAE4C043E43C088864BD7E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	.....X..... ....

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):	2673
Entropy (8bit):	3.347892594058299
Encrypted:	false
SSDEEP:	48:34EjxTlPu1RcGqt192+Q0R397bgeq+lPu9coPjL:34Gu1Dq39lR39ngehlu7n
MD5:	4EBA2BE97BDDB813D934B321813BDB03
SHA1:	D122BEFE19B681C64ACA83E21FBB477675744750
SHA-256:	A2832EAE2D1A12025D79661E4C0103740C07D19E2E42D1996BCA243EA13EA686
SHA-512:	C3D1E69BE86D028911D99F3F1D0FCB6129FDB189C406D62845E9F8BA32C9A841D1E8EE5070E1273C8793F6F8E3ECF3108C6AFD6945DE0CF35BF953EF1DE1FB3
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...6672b02a_8de3_4669_878f_f4f836a6ebb9.....j..&..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....A...https://delval-equipment-corporation17541a33.multiscreensite.com/.....h.....`.....4?]....4?]...0.....H.....A...h.t.t.p.s.:././.d.e.l.v.a.l.-.e.q.u.i.p.m.e.n.t.-.c.o.r.p.o.r.a.t.i.o.n.1.7.5.4.1.a.3.3...m.u.l.t.i.s.c.r.e.e.n.s.i.t.e...c.o.m./.....8.....0.....8..... ....https://lnkd.in/e9ejC3j.....G....#/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.218282623721807

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Encrypted:	false
SSDEEP:	6:mvYElyq2Pwkn23iKKdK8aPrqIFUtpCYH1ZmwPCYU1RkwOwkn23iKKdK8amLJ:L9vYf5KkL3FUtp7H1/P7UD5Jf5KkQJ
MD5:	2DC486F3F6A9344444A73E9D74065C7B
SHA1:	E05583466A157C78E29D830BC404BF4394DA0494
SHA-256:	5D1217AA5CD17741A2AFC5B6E521B7840A6D2634467F1BA1F1EE7AD0F33A2B01
SHA-512:	02BA2EBA512FFB86ED5B3520E7D8A12BD085DA7A206AFBC3299A9B85823D2F0F9EA439C06D147883C22C5A4979A2C0F3F2589FDF3EEECDE8D212498A38A184 8
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:25:59.412 c50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/22-18 :25:59.413 c50 Recovering log #3.2021/06/22-18:25:59.414 c50 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.1875939175838965
Encrypted:	false
SSDEEP:	6:mvD2LXFOq2Pwkn23iKKdK8NIFUtpCD2LVFGWZmwPCD2LhWFkwOwkn23iKKdK8+ed:ayFOvYf5KkpFUtpKzW/PKBF5Jf5KkqJ
MD5:	C00F740DCF2B1866C642A75C851951C2
SHA1:	0B911FA6B4FCC74C85C74F3ACD7123677AC631D2
SHA-256:	9E158894751A9C4D49A67DFFCDA8A0D660A12B9A7A8DF75B33D384AEDA4D53F5
SHA-512:	5568E3BD801D53DA2A825E23A3115BB939EAB920537A7B6B7189F9FEEE69ED4CAF7C0019DEB459C55A36FCBB6103AA48F094E882823F83021EFF31AF2AF75A0 4
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:01.521 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/22-18 :26:01.523 c34 Recovering log #3.2021/06/22-18:26:01.524 c34 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\comput ed_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

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

Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","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):	16384
Entropy (8bit):	1.3336960895175571
Encrypted:	false
SSDEEP:	24:LLitYxh0GY/l1rWR1PmCx9fZjsBX+T6UwWxjuPIals1U7rtPHV7j8uqJGLPhHU7w:tBmw6fUvhuPI1QrtP1j8uOGLPhHQw
MD5:	87A01B570AF83A2FB958EB329F2E76D3
SHA1:	F129B28B7ADEF0ADAB1CDC8E38EBA86F1B6C9EF4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SHA-256:	86C4AB188F5EB1FBAECE1B0181DA79CDD30A61BBB10FC3E79907EA5FEB641A4A
SHA-512:	028B611A567257197446DB10857C1196714B35D8134C87F6D7BDCBD01D37BAF148278DA73AE2A21C6836E5540012352E25CA86ACB558A62B25624B9397B44493
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):	16972
Entropy (8bit):	0.8138536643858179
Encrypted:	false
SSDEEP:	24:mqgETl9cQJXyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6Uwv9t3n:teuCBmw6fU29t3n
MD5:	C0A8C0F5175227668A250B4A4B840F18
SHA1:	03BF433050152C6BE5E8F6FFE09EB86CA5773508
SHA-256:	D900AAD0EE41C530FF6BDA02E71FA25E204089EF2DC20D09303CD7D4DD468033
SHA-512:	8AAC47D4CA8B17BDC609AF0FA1D30A04717A9AA53A84E5614A59AA41E162AB9394E0943C4B4FEF2F99931AF06397B9C7F2AAB3CB3F05B10317ABAD2D44D0149F
Malicious:	false
Reputation:	low
Preview:	.....Q^..... ....

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):	5.203263943483508
Encrypted:	false
SSDEEP:	6:mvD8+q2Pwkn23iKKdK25+Xqx8chI+IFUtpCDfPWZmwPCDHR3VkwOwkn23iKKdK2L:a8+vYf5KkTXfchI3FUtpKfPW/PKhV5JM
MD5:	797C7F31ADFC6C06ADD66ADDD4F2F2CA
SHA1:	5E80A2D19B3B7DA976B5F5573DA774EC87753D0C
SHA-256:	30BF9996900B1679DE4310EA3F1BB0C20197513639B01C56DDBA7ED9F1196945
SHA-512:	25AF4A7BDCCA44426E243810556E47E5CB2A1CA8BA106703F014461BC40443674922783B799404CF52AC5AAB16EE42F15E6AC3C7CA42F99F1E501BD88ED8852
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:10.561 1acc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/22-18:26:10.563 1acc Recovering log #3.2021/06/22-18:26:10.566 1acc 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):	5.160916400222294
Encrypted:	false
SSDEEP:	6:mvDF1+q2Pwkn23iKKdK25+XuoIFUtpCDPWZmwPCDH1VkwOwkn23iKKdK25+XuxWd:aF1+vYf5KkTXYFUtpKPW/PKVV5Jf5Kkl
MD5:	8F797F06849264DFD322283EA0E75476
SHA1:	A854CB03E831EBE3D1E2068D3281EA9747A667E8
SHA-256:	A82A25482BF8CDF3C8E941C1D51DA745E4BC21A82CD8FFF778727B8C03E3D9E3
SHA-512:	8966BECEE305FB007ADB2DBBC2FB9A9AA27BAD39EDB0A4E3673BFB49F2B89D8E9700C45EA5D62D6F2C9654018485C4DC399B73372D91DAC219451556337CDI 34
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:10.551 1acc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/22-18:26:10.552 1acc Recovering log #3.2021/06/22-18:26:10.553 1acc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data \Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.1917196941056725
Encrypted:	false
SSDEEP:	6:mvD1Ue3+q2Pwkn23iKKdKWT5g1IdqIFUtpCDPlWZmwPCDPvVkwOwkn23iKKdKWTk:a1Ue3+vYf5Kkg5gSRFUtpKQW/PKnV5Jb
MD5:	311C99E0F98C9FED86A2F91C6EDC42B3
SHA1:	CBF416C70D145C0B8A90C646C1A18A46E53EA508
SHA-256:	06E3F2E3F753A2B3A9336202B65C5EBC0EA15DEB1DB986BD96BD674AEE764876
SHA-512:	A72600892F7947C8262B223A3DF8EEF299BC8FF1DE2F06CC90D0389ED3551F9E08FC63393A27D109990E22F40B00C437E5A74BF306EDEB72575EAB996C94DF8
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:10.540 1acc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06 /22-18:26:10.542 1acc Recovering log #3.2021/06/22-18:26:10.542 1acc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.32588448727065034
Encrypted:	false
SSDEEP:	24:TLx1oNPabBPXbnRNOpTd2h62dBNQDQwLPQPOI:TPoNPabBPXV4n2Q2doDJLPQPv
MD5:	C127AAC1D0DA4B28C8917A6A967B54DF
SHA1:	BAFE49868E606EEE39899793A64D83F2E5AC9F89
SHA-256:	C299FDB767123796B6EB739B8C22909E3200FFF9DFB834B11E700312F76BFF39
SHA-512:	2937E59CFCF39DFC72526F8EA1E0E01D8E6A16D5609A567DA7E7BFC47C0F2A7A229E9B104604DAB16300126C1D2440C9E2A68766CD0EC9FDF4DA16785F117A 6
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):	1227
Entropy (8bit):	5.688923014195624
Encrypted:	false
SSDEEP:	24:0MC19ypYVJBHrzA94D1yaw0TBJgsVgxeaT8aPd80PdX8L:3CjFNzr1Lw0TUy0/fPpP18L
MD5:	A4ACD85FAA821C713848358E711606DC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
SHA1:	2FE978360F94A51806980BDD393240E148125CFE
SHA-256:	7AB3FA305007C6DA24AE06DF182313BFFE4981DB844E78DE36FA73624EC33340
SHA-512:	D6AC8BBC329F41B06A5B58E88E3705995A6DE35B11690B5072552BB48E83BB10D5FF8FCD81EC88E9673555316BB12481F97821F66B3E4ADC8A7642A3F6B18388
Malicious:	false
Reputation:	low
Preview:	.....".....e9ejc3j..home..https..in..lnkd..code..com..linkedin..slink..www..corporation17541a33..delval..equipment..http..multiscreensite*.....code.....com.....corporation17541a33.....delval.....e9ejc3j.....equipment.....home.....http.....https.....in.....linkedin.....lnkd.....multiscreensite.....slink.....www..2.....1.....3.....4.....5.....7.....9.....a.....c.....d.....e.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w...:.....B.....?..... .....*.https://lnkd.in/e9ejC3j2.Home:.....X..... .....*+https://www.linkedin.com/slink?code=e9ejC3j2.Home:.....m..... .....*@http://delval-equipment-corporation17541

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):	42076
Entropy (8bit):	0.11692074917587604
Encrypted:	false
SSDEEP:	12:p0Es3DpIXnvopqLBj/mgz3le/4nMWQASjG9LFBQZ8fOv:p9SDp+vopqLBm+3bf1NFTf+
MD5:	D01EC50CA502C75A5DD14DEA3288A6D2
SHA1:	961A0B0C2E385DFE96DBB943D0563BBCFFAE001D
SHA-256:	10880AD88BBD651F893065A538D0A7E8DE9F4F7F23F8D4E93F7FC2F8CC7D4081
SHA-512:	E685D1C3EEF35E8A3F313FC9F2B34995D35F14CFE63DA171BE3F97892B7E670C415064FB3285DDC0F769411B57539581CEE6199CF43805163FE6E35E96FF265F
Malicious:	false
Reputation:	low
Preview:	.....O.n..... ....

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):	8900
Entropy (8bit):	5.511661992718495
Encrypted:	false
SSDEEP:	192:g5VrZGsoMzzzzzVnYfryQnd6BRFE5fgFS5VrZGsoMzzzzzVnYfs:gwsZGgSwsZj
MD5:	314DDA299232A1DC13DC9EFB2BA90D5B
SHA1:	0692716076B9AA6350BF99E11CFAA253DC42E667
SHA-256:	166E25CA710A22A704E5629828269BC489AD8637CA9247DD8892C7BD97A4D226
SHA-512:	03BE0E05C88B162E21F4FF89FB5AD2F9360373A564F7AAE69A57CE3E7819981C90F01B93601927A37D2610BDC1C7FEE13D9DCC21CD12CDD4B1C5AA077CB4A1C
Malicious:	false
Reputation:	low
Preview:	.y{E...*.....EMETA:https://delval-equipment-corporation17541a33.multiscreensite.com.....O_https://delval-equipment-corporation17541a33.multiscreensite.com..dmPagesCache...{"2854":"{\"pageUrl\":\"https://delval-equipment-corporation17541a33.multiscreensite.com/\",\"pageAlias\":\"home\",\"pageContent\":{\"content\":\" <div id=\\\"allWrapper\\\" class=\\\"allWrapper\\\"> navigation placeholders --> <div id=\\\"dm_content\\\" class=\\\"dmContent\\\"> <div dm:templateorder=\\\"170\\\" class=\\\"dmHomeRespTmpl mainBorder dmRespRowsWrapper dmFullRowRespTmpl\\\" id=\\\"1716942098\\\"> <div class=\\\"u_1880451336 dmRespRow dmSectionParallaxNew hasBackgroundOverlay\\\" id=\\\"1880451336\\\"> <div class=\\\"dmRespColsWrapper\\\" id=\\\"1749186200\\\"> <div class=\\\"dmRespCol large-12 medium-12 small-12\\\" id=\\\"1960677941\\\"> <div class=\\\"u_1236756082 dmNewParagraph\\\" data-element-type=\\\"p

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.2411876459976465
Encrypted:	false
SSDEEP:	6:mvYFSMM+q2Pwkn23iKKdK8a2jMGIFUtpCYWoqZmwPCYOSMMVkwOwkn23iKKdK8as:LFpM+vYf5Kk8EFUtp7l/P7OSMMV5Jf5i
MD5:	4C97E7ADBF234F1A42F1F6758A19171D
SHA1:	5943949C4B72C71867A451FF267CFDCF62D22105
SHA-256:	ECCEB0B4ED70E1B170058AE8CBD8F72E79A8364CABB7EFB3A2AC08389E42E667
SHA-512:	0FFC2A772D1CE6AA6E177362F2F7D33E54B1578037AA3FA1215B1E51051064F65686D6D1E9AC253B498174BA32E0EC7637CEDF6C9DD2ED25477DE091D405C8F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Reputation:	low
Preview:	2021/06/22-18:25:59.159 7fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/22-18:25:59.164 7fc Recovering log #3.2021/06/22-18:25:59.165 7fc 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):	1.2619403904146824
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWO2xOPteOqAuhjspnWOsxjXbCj6Xj2:HD8T
MD5:	8F18A04FCA711F4BB56D1B8F67BB8120
SHA1:	FC69714EA7A6B898FD258D6349C3B3E93701A038
SHA-256:	1014CB5DC16ABAB379CC647026D291A135A7FD393CF6AA2F93B60594BAFB9555
SHA-512:	9C4F63642E2F382A3B6876872394BFAD2375130CE29E315D718630E8D47ED956F62236AAC87506AF5012AC4F4F47857560CCD1148A1CFA75487D5889766C6B5D
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):	1.018897524041971
Encrypted:	false
SSDEEP:	48:qMq7w/qALihje9kqL42WOT/KYqrw/qALihje9kqL42WOT/i8:qMUOqAuhjspnWOvkOqAuhjspnWON
MD5:	BA118D0DBDE458B6FD6FFA157C5B1107
SHA1:	E3797C60FB2F0AAE7E170153905C4027F0FC06E0
SHA-256:	7C228AA96687D1DC9FBB2D0CE785C2D6909326EA98B94EA22977B1576B08ED0A
SHA-512:	4AA9DCCCCF0C25F7AE3BD1F5A9B80989B94F0F95AC40EB8C1C2E82E7E691346AFF875B81FBD37D0EE472A87612604F8D2C68BAA66E4E56C2795F711FE6FCDI 7C
Malicious:	false
Reputation:	low
Preview:	.....Ey. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.250258675300505
Encrypted:	false
SSDEEP:	6:mvYtP1yq2Pwkn23iKKdKgXz4rRIFUtpCYCNj1ZmwPCYBRkwOwkn23iKKdKgXz4qG:LB4vYf5KkgXiuFUtp7C11/P735Jf5Kkt
MD5:	F84D7912F8FC2382FE9F695F57D3DCA8
SHA1:	5E946C89FD62374097E1273AFEEC40D14C5F7DE8
SHA-256:	F24D51C00C8E994D9318E7BF07ED2343EE2E045B83D77EAA4FC7AD28DD78F056
SHA-512:	81951FBA4E55900A448C645B2166B34D54D9711B0843AE41761EB54DB235523CFDABCA8B34FCC577C1141BB10AE8A42998671413E9F7198480F9AEEBE3194D6A
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:25:59.464 c50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/22-18:25:59.469 c50 Recovering log #3.2021/06/22-18:25:59.471 c50 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	0.4964184696382689
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4P6Rc0:a96EJTv4sXK96EJTv4Y
MD5:	8B7D1C0C6399F2FAD58F370CFDAA1225
SHA1:	5C2F607745C7449D64913BEB51BF885F81C8896C
SHA-256:	9EE3EFFD108B85B22ADDA439A17CDC369795CEAC53C32E9C8B8D7AE28109D941
SHA-512:	4671FDD1A9CC6C3578BC609E5E74A7805D5BCD1BB81EDA350EA9E30F1DDD04677220BCB26C881571DD11F3C3282F5C99B27E014477F58499F485F0C0D4B7A1
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):	25672
Entropy (8bit):	0.6533354041897621
Encrypted:	false
SSDEEP:	96:nXJDw1iASsCIG+6bDdsDaBJvtHIm50I46:nXJDw8ASV96EJTv46
MD5:	9DB680EA594941115F980672C20845C1
SHA1:	68470F9A336978735254AE20F1047174F915E3D2
SHA-256:	9D9776564264188A2BDB97879F65EA33B320A045279BC73D953B9F8A26A25318
SHA-512:	1FAE12795811818369DDBD237C735942F07B6F6B42D1E72BC37D1935AF2340EB622F985582BBAD5A1492A3F2D063193D7CD9A4D2688CC1CE353003F76EC35F8/
Malicious:	false
Reputation:	low
Preview:	.....6..... ..... .c.....pp. ....

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):	1.0114539829328537
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoM:wIElwQF8mpcSJ2Y+1
MD5:	9EED421205896E98252BA5C7148307CF
SHA1:	F7C860F6BC3F00E52A7A575D6414EB077CC51B42
SHA-256:	8D44BE82164D1ECF7C2BE58E242BD8D384F09DCD6C12E63FF9936AA6F1513929
SHA-512:	228D41F9A76C1F30D29D664D13F7D590136F6F1A474CA21439AADABD7756068A29FC8B74AA9C1C01C334D466C7A1D24733F529C527771F25317B4608F364E718
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):	0.8251829027097564
Encrypted:	false
SSDEEP:	48:hSbqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU56:hSbhIElwQF8mpcSg
MD5:	7032400951CF4003D494E26F8EB64CA3
SHA1:	D226CA3344B967C44433305537BA39130F7BB3E0
SHA-256:	A4BF68205FCE99473D47CD34E42CF2128D02525F88B7EB35F7734D66A25A6A31

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
SHA-512:	C8F76CEB9393E9BA241BC4218446CA01F83B33DA69B0F76BF235D894262EED145D4016A7DEDCF945C30A2C4D39FAE4D9A281F9F9EB626CEF18486F875464F06
Malicious:	false
Reputation:	low
Preview:	.....KE<J..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\0fac2e4a65285d5d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9161
Entropy (8bit):	7.92408434504009
Encrypted:	false
SSDEEP:	192:IULCWK5hmsOUo9TcOk0WS0+2ydfNbaBGWrpj:IULvKTOxkJkBwMOj
MD5:	B06620E3EE250A3C8CDCE75F8E6DC954
SHA1:	3FDB784F865CB1F80CCD08DC638CB75A302D1A9E
SHA-256:	265BD8AD43A32963E96D1609AE28E8D76141B393C67EDCC958135DF8E0661F0E
SHA-512:	3326DF169B48CFD2198D8B1E69FEB0E75B757E4148EEA3B0F01CB468B0C91A4B60DFBB4DB07ACA4BF1FEBCD9ECE11FE6D5BB0F1E7700E337F919E0DE92A2F3A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...1.@m....https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlFQ.woff2wOF2.....>P...F..... .0.`..T.....6..6.$..h. ..D.....03.1...3n.(..e._&hG...FX...Eq.3QL.SG..;...C.B.J{...j+n.4&.'j?.{?..J .0....B.e..e.uDB..Nnx~.=.^.6m.D.....TY.`b.V.\...;W7.7].UmW..^_.?../k..D0O..Y..R...=.....F.5.;...*]N.6....^.....Jm..BX...$...R..Mz..t...p.>F.U.n.P.2u.....ll...$..^..C.^...wC... ...z...%5P....._.S.rv&..*..d0.?.....9l..B..D.B.....'.\..5.....p....P/....y.e.../.O...:..}..+XM.Wy|...E.....vx.....5..x..g.*`.O@.....,x...`..k...[.1.....j_.&....0.x..s...m.....=.S.`B0.P.....]k.....{.....N<:.h...#...n=..`.{.`P^w.....>....._.`.....0..C,*.w..<f.S.....s.3;.....2.:.<..^.c.L.'..{.K"..N.....=k.... ..3g.@.....Z,J....4.0.5.....V....%..>.... ;..I..L.N.N.Gc5....Tsc..+R.M...V:..iF...W....>...a.Q..B_.[..'dQ..F.....;....c.u`.7.{G.9...57.....4.i.../;~.....~mlSo..../.|.....|..7bl..(..W./.*.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\65349767b5af3772_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	57643
Entropy (8bit):	5.528715338476164
Encrypted:	false
SSDEEP:	384:jOuTWpk33w3GF383I3MywdFcshzwqFTBEOw2FfaaGwxFAINfwmFvlbkRwcFtvmlf:TUew8B/ofgNRJQ3hY6
MD5:	AB29EC45F4EF62624804E486CF771469
SHA1:	2B4B49939257779EC96E112E1ED68B2989E25D19
SHA-256:	CEF8B33EFDCF1FF84B53A3AE70FA9AD86DB48C7A4FC6360056D85F49A7577EBE
SHA-512:	DDBB841193F9B79E9707264032B66341F44CF46248EEB89C4A54132F3CFE9B79E0D082BEEAB655C276BCD070BE7F93616CE81D68BB950CA810CADEE1D218C43
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d.....https://fonts.googleapis.com/css?family=Amiri:100,200,300,400,500,600,700,800,900,100italic,200italic,300italic,400italic,500italic,600italic,700italic,800italic,900italic|Montserrat:100,200,300,400,500,600,700,800,900,100italic,200italic,300italic,400italic,500italic,600italic,700italic,800italic,900italic|Poppins:100,200,300,400,500,600,700,800,900,100italic,200italic,300italic,400italic,500italic,600italic,700italic,800italic,900italic|Reenie+Beanie:100,200,300,400,500,600,700,800,900,100italic,200italic,300italic,400italic,500italic,600italic,700italic,800italic,900italic&subset=latin-ext&display=swap/* arabic */.@font-face {. font-family: 'Amiri';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/amiri/v17/J7afnpd8CGxBHpUrhLQY66NL.woff2) format('woff2');. unicode-range: U+0600-06FF, U+200C-200E, U+2010-2011, U+204F, U+2E41, U+FB50-FDFF, U+FE80-FEFC;.}./* latin-ext */.@font-face {. font-family: 'Amiri';

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\80264085ed669c44_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29821
Entropy (8bit):	7.983263117780187
Encrypted:	false
SSDEEP:	384:UWos4M27xTbSltXJLi5URNZHON2UAbXv9r07DhljdZO+tfAqYlhWpNANz15lhROv:/osATGbZGwjxBr07v60lfl4Y5cxNn
MD5:	E0DE294A94A53D59289411857B0F4CEE
SHA1:	180399B5A0F43FAF215D3DA5A43DF386795A1863
SHA-256:	B893BC85E626CACE16594E59DB24B0E9EEDB5C566C0FA13BED9C50CA2F232199
SHA-512:	A5A6926B346B9E429D111F8E817E10B2439D291AF5FB93B4D630FBF48012F094BF104AC995C254293463F330AE3F0883EB0E0B74095843A933DDBF4840D276C4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\80264085ed669c44_0

Reputation:	low
Preview:	0\r..m.....Q...y.[.....https://fonts.gstatic.com/s/reeniebeanie/v11/z7NSdR76eDkaJKZJFkkjuvWxXPq1qw.woff2wOF2.....o@.....L...n.....`..`..4....s.....l..... .p.6.$..X. .....c...[X%.O.....gFY...d.;..|eE.Q$".#...o03*l..l..d.....KE.l.....o..2.@F.a..M6gt....6.VN..ex0(._..+..:Y....o..,5.....o.....;@..g$..h/.4...X....a...&!.h.4b...iO.O@.,${.d.. .p....e..P..`...v....V.,.0.....I..6..`...!.?vX....`..n.../..d.F?.8..l.!...ll.~.$...ak.t.$.`?...0#U@.4!9.:!.2.d?..d.....3..$bAu.@.....=~...P.`GwB.Cb"....,...1.....zc.....l.a`t.....u..3;..{.QG..qp D.....*.....oa..k.....`j.....?.....<=.X.....?.f...B.....&{K...%4.|...D<.....#.....D....qQ....l..\\....Y...nB_....7.{#..#.w..2W.\.#L...x..:.....:.Y.5.J..x+..D.D...4H..O.....i..J..d.I.=..{.... [.wK.&.e..bK2....!.....xE:..G|.....y.....0..R.nC....*`...2..[Z]3....&....._.[....(|<cn.7..C5.I..C.E..F.3...O....R..=....<~..;L...;..4.JT....x.v.-)...Cu.V<....._..Q..A3...N.+.A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\865ee27440fc7a8a_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	7.91969229435726
Encrypted:	false
SSDEEP:	192:X7uo9HQkQLb61fpJohl/gCvwsd2pbbhK08C8G:X7v9wkYbkfpJPlqdyhtv
MD5:	76B422DB3C8760A446F30066C4CA0D13
SHA1:	A9735481DF331822A67CAB260BF85498F402A175
SHA-256:	88F127555388E7F50E34703BDA9A8D576BE7146BADBCE804558E459DBCF368F5
SHA-512:	33F42E0272D02106266CB510F3C3284CF8B67339DE8458257145D458214FFB892DFEC7EF72B4172B6DE4D1D10601F54556F79BFE6BB756724AC7F29DEDB3B3E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....Z.....https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfecg.woff2wOF2.....?..... .0.`..T..L.6..6..6.$..h. ..\.....2.".8. .w.E.".. ..n.p.M$DDxUU.o..0.#1.g.?_.p..!./T.....X..xLW.s....$.....k.s.[...Wk"...>]+.....3Y,$.....6{.36..=..J.?..H.'..+X9s...v...v....z....z..^...."."h.....P.L...C..0...p....&o.....R....q.....)...r....{.HE. ...ig.KT..0.-.%.z.....9.|.A..|X..+%)..*..2&%$.nm.\._.e.t5...n\..G...o.2.59..}C.I.9..K..I*..)j.%..X..%K.v."b..".....D;..`..y.$H..V..h.E/.E..}.v.5.[...~.....X<GW.+..(ppWD..f.Km....6@.w? `..@....F..D..9*z,c.....jL=.....&bS...l,.+..9..>*}..@.....q...xl...j...<>.....>...._.....,....W./..|.. .b...U>...l....!0.....>... ..@1.5...Y..xS..;...._.[.%a..&).raj.....w0 ...s....<...00.sg.f.4.0>_g. ...-.....FX;.....<...S.....!-`{...j#.I...B..(%.R.....;..U.U...1S..M.V-(...j....7.z.l;b..p.MZ.X.....:E....*+^....."s.B....e,.=...PkyK..P.k..g.....j.Oi[.6..qa..}.w..-Zx...X.,.`....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\99fc33cad3abbfe7_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21244
Entropy (8bit):	7.978365029776882
Encrypted:	false
SSDEEP:	384:QY+FwcDI2V2M3BznhYDbrJQUt4/Umope/M20/MxoDljUr1Fm7T33A91Xu6q:qFt2cznhYDOUt4/upw0/MxoDexFm7rgq
MD5:	71A28916DE8C013285CDA451339D50CD
SHA1:	699F26BCC084DF68CD31D5156D163A5AFCA702F9
SHA-256:	6377FC7F44B98437A1ADEB12BF49E2DDEA336FB67F530AEE0F19830A2D836AE3
SHA-512:	945FC44B1803D03D67B9A109F45EBE6DCF3213621A7F4DE16695E55468CAABFFC10A8CBDBF6965D9FF9E210D20BEEF909D572B3014694CE60B6050A74A5929C B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.....p/....https://fonts.gstatic.com/s/amiri/v17/J7acnpd8CGxBHp2VkaY_zp4.woff2wOF2.....M.....T..Mv.....$.....<.`..l.....K..>..6.$..Z. ..@.....<..l.V ..!..s..(...A...c.....`.....6b.....a..$J...j4...i.1.....dJ...-=...B.....f.Y|s....x.;.~P.K.k.7....c.*.....b...X#..0..RD.e*...T$.G.L;<.6....".:.(."......1.....3.V..9L9..s..Mo.Oo...,...d+.....V 3q.O..e0a.he....r4.2..K.#y..2x.....}..a....?Xq.`.y.!7C..V..k.['...9...;4.X..AH.M 7.....L.S.M.4..7...W:.-...dP.....K[.....~r...<A.~..Bp.....r;..Q.....5.4.Y..Y...|..z..sA.z....GM....X +...e.\.....cY..u....9c..6.t..7./t6. L.w..u....95.W.q..Qm.v.5..Q`,...H$.<B....XY..[,K..VpU.N.....u..{..OUEDDD.-..^.q..Es~..d.N.]L.!.H..'v...B>.N..T.k.v.....5.@... J,f..C.X.....-.....)+..v...]`N8.P1$qA.....l.yt..?.x...%.r.|.....n.j(.....!..t.....h..S%kCE...CR.B.....:...A~I...Idg..|..Ez2+1.#.|...^.. K..5I..O.bB....w.OvN..16...d.f7"h.i...zOn%...Z.B.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\index

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\index	
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\0457c3bb-2bbd-49a5-99c8-54bcd8ad1393\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	3.8066293327388947
Encrypted:	false
SSDEEP:	3:ZPS9EXxYyL/tZ/lFlHcrt6lJRbll/6l9FZz/tZlhAltllnIXE8ln:pXxH/l/kwSjZkXgVln
MD5:	4634CC05261A5F6F3283726E9CC634EF
SHA1:	A87FADAF35584AB3F94982D0216843CE0F295F04
SHA-256:	15F419AAADB0C83B2A3BA83552E0D870AAEA8D7DA6AA1CE3DD310302D1B31DFE
SHA-512:	A3385C02711DF36BDE5817B107939CA18877557057673533E468E52ADE0A60D83C440FC487793C64820EF699D166B318B874AB258C68F5C43E4AAD3600531117
Malicious:	false
Reputation:	low
Preview:	(....j.=oy retne.....KRM..#/.....oy retne.....]](eJ.....%.....z.@t.^.....%.....D.f.@&.....v.....3.....T.....r7..g.4et....._.a..#/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\62042b74-0120-45fb-9bca-dd4f1ea64566\8fdaeb6e04990e31_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	86702
Entropy (8bit):	5.404507455816456
Encrypted:	false
SSDEEP:	1536:AGlYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9ao:64J+OlfOhWppCW6G9a98Hrh
MD5:	3D6B822528715A06F8ECF8FCE236E9BE
SHA1:	A75C636BA21AFB62F9B34E82159C100C54FC1003
SHA-256:	915E33EC2037D60273FA984B4C63ABFE320F8FB361D448296EB9291B481C1FCE
SHA-512:	4F6653E85B6F2861F85B3ACE819EAE9CCCAFC2C9DDC50EAC9B047D8618C85BF08AC60C277A3A964554CA31B319EABBEE5F9271F7A6D0B172A0ED80C29757720
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>.....v....https://static.cdn-website.com/libs/jquery/2.2.4/jquery.min.js/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\62042b74-0120-45fb-9bca-dd4f1ea64566\b3cc87dc8a0ffc69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13685
Entropy (8bit):	5.543428862902635
Encrypted:	false
SSDEEP:	384:Ms/sqgyOyNpXXTTKvywQyCNPsXp+CmbW5Wb2BQeC/pBrrRM:MsTq6TTKvyw5MIo3xlD/pTM
MD5:	4F1AF95857514E7800F97211DCCF413C
SHA1:	6DC513214419D5151F3D0DCF6E04092F54956CA6
SHA-256:	AE1D7F047586CD0984A7DC8418B3C77E9E35C0A95E1B180A212686B92C08F24C
SHA-512:	EA72DC9421175810FAD3EEE6F8682DA9A9497FB9422CF3F1421F97C066398BA22B7707D6650610C5360A8EF06D1EE2310BEEB602DEF69F8964007FF3BB7FA4E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....i4....https://static.cdn-website.com/libs/bower-skrollr/skrollr.min.js/*! skrollr 0.6.26 (2014-06-08) | Alexander Prinzhorn - https://github.com/Prinzhorn/skrollr | Free to use under terms of MIT license */.(function(e,t,r){"use strict";function n(r){if(o=t.documentElement,a=t.body,K(),it=this,r=r||{},ut=r.constants||{},r.easing)for(var n in r.easing)U[n]=r.easing[n];yt=r.edgeStrategy||"set",ct={beforerender:r.beforerender,render:r.render,keyframe:r.keyframe},ft=r.forceHeight!==!1,ft&&(Vt=r.scale||1),mt=r.mobileDeceleration||x,dt=r.smoothScrolling!==!1,gt=r.smoothScrollingDuration||E,vt={targetTop:it.getScrollTop()},Gt=(r.mobileCheck||function(){return/Android|iPhone|iPad|iPod|BlackBerry/i.test(navigator.userAgent||navigator.vendor||e.opera)})(),Gt?(st=t.getElementById("skrollr-body"),st&&at(),X(),Dt(o,[y,S],[T])):Dt(o,[y,b],[T]),it.refresh(),St(e,"resize orientationchange",function(){var e=o.clientWidth,t=o.clientHeight;(t!==$t\|\|e!==Mt)&&($t=t,Mt=e,_t=!0)});var i=Y()

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\62042b74-0120-45fb-9bca-dd4f1ea64566\b9e50a3cf0c5d851_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4003
Entropy (8bit):	5.6841611237173115
Encrypted:	false
SSDEEP:	96:Y+G4q0ec1e2IN6vp42SP7WxK0oocUKsjUjQjajcguTLeIfiGPTbKsDCxnQPGW0kc:YFJqe2IN6vp42SPaxK07cpsY0W8eI3ni
MD5:	4542B255554E07A990A22C1370E92369
SHA1:	44F1B0D1EA9EE5DEC5ED349B5416855B6041F745
SHA-256:	599653166EE7C31FBD9CADAF72D2A104E3B26AE2BB535726A91D3CE780FA5D2B
SHA-512:	E38553CF5835FC8420A551208BDF17755DC25DF4FB63BACB6EEF4F281A04A95955376C6F2A3B1F912255A94586925C54293F6C37D96B4773E26A60B6078912D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=....r;.....https://static.cdn-website.com/libs/lozad/1.15.0/lozad.min.js/*! lozad.js - v1.15.0 - 2020-05-23.* https://github.com/ApoorvSaxena/lozad.js.* Copyright (c) 2020 Apoorv Saxena; Licensed MIT */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.lozad=e()}(this,function(){"use strict";./**. * Detect IE browser. * @const {boolean}. * @private. */var u="undefined"!=typeof document&&document.documentMode,c={rootMargin:"0px",threshold:0,load:function(t){if("picture"===t.nodeName.toLowerCase()){var e=document.createElement("img");u&&t.getAttribute("data-iesrc")&&(e.src=t.getAttribute("data-iesrc")),t.getAttribute("data-alt")&&(e.alt=t.getAttribute("data-alt")),t.append(e)}if("video"===t.nodeName.toLowerCase()&&!t.getAttribute("data-src")&&t.children){for(var r=t.children,a=void 0,i=0;i<=r.length-1;i++)(a=r[i].getAttribute("data-src"))&&(r[i].src=a);t.load()}t.getAttribute("data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\62042b74-0120-45fb-9bca-dd4f1ea64566\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\62042b74-0120-45fb-9bca-dd4f1ea64566\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	168
Entropy (8bit):	3.732789168937511
Encrypted:	false
SSDEEP:	3:N1duTE+J6KSGctT9A/lUp/16llvAl/cltkR/alP2n:d126ZR6Wp/1ORAtUO5uu
MD5:	5BE2B738C9E60D7C5C2FD7D7BA8D702C
SHA1:	BDD357FE9F5249587E8FBFF62D8E864F319FD95C
SHA-256:	BA7A2387E688475C4CEAE93B40610C549A2758B58EFE263623869E9AB58A1FDF
SHA-512:	2053674C89932F0D2BF96EC84A51AC3B4AAECD29E2E58FE8822CF9316E287E2936450418ED5879BA98280947B02E6C39B210CFB0FE82C266277E90B193A6ADFB
Malicious:	false
Reputation:	low
Preview:	(.....%.oy retne.....".M..#/.p...tC..oy retne.....i.....7.....Q...<.....1...n.....T.....bT..#/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\2351dc7e8314e61c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	107769
Entropy (8bit):	5.9673516408768466
Encrypted:	false
SSDEEP:	3072:STv6aGkco/FbwOChSwOmnpwC4/IlFB3jT/tEGbCP:KiUcodbNwOEP3e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\2351dc7e8314e61c_0	
MD5:	320FABDD3A356D4E5AF341E11E0D0DE6
SHA1:	1C41A0DCD96A315153F2686D98260965AC5CF36B
SHA-256:	91E3130C40E7D9D517E483DFF299CA5E6DD6277D2618271FA13D10A24995422C
SHA-512:	6BA659DA7DB5BDF7FA7506404B054F82EFB0F42C6728E462366501438D8A51A0655F8AEF13E503E0EA041EF6D5D0D6E1AF45D0D6E7AB98A28A81FB7A03AE5AD B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...ahy9....https://delval-equipment-corporation17541a33.multiscreensite.com/?utm_source=homescreen<!doctype html >.<html xmlns="http://www.w3.org/1999/xhtml" lang="en". class="">.<head>. .....<script type="text/javascript">. window._currentDevice = 'desktop';. window.Parameters = window.Parameters || {. AjaxContainer: 'div.dmBody',. WrappingContainer: 'div.dmOuter',. HomeUrl: 'https://delval-equipment-corporation17541a33.multiscreensite.com/',. AccountUUID: '3ff149d9ae6549b880d4c1d546662ecb',. SystemID: 'US_DIRECT_PRODUCTION',. SiteAlias: '4de34e46',. SiteId: '2184449',. SiteType: atob('RFVEQU9ORQ==',. PublicationDate: 'Tue Jun 22 15:44:46 UTC 2021',. ExternalUid: null,. IsSiteMultilingual: false,. InitialPostAlias: '',. InitialDynamicItem: '',. InitialPageAlias: 'home',. InitialPageUuid: 'f22698230fca40cd843402c3bee4c86c',.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\9d4eacf6898e9119_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80301
Entropy (8bit):	5.29491166259716
Encrypted:	false
SSDEEP:	1536:aSf5FQG3pnrNzxrAM9pjpMaGYR1pKm1SdGe6LWlQilzN4gZ2VkEFy8UZ:aSf5FQG3pnrNzxrAMfpMaGYoZ
MD5:	5317E75EC44D2F3457C8F804485A4B2A
SHA1:	61D02A8E2341F7F782AC72E6AEEC977C6CD271B0
SHA-256:	98E6C0721A41FA75579B7E84022942C353C135C88060AD78CD1C90D75BEF1C5A
SHA-512:	FE837D74C7DE40E04C50A576CFAE8A7E654B2A913496D85444CCC128D04B623DF2D680FEBF6D403D4B56642AA51083CD910B2700229CF92F0CEF4042415AD44
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....HO:....https://delval-equipment-corporation17541a33.multiscreensite.com/?dm_ajaxCall=true{"css":"*#dm *.dmBody a.span.textonly\n{\n\tcolor:rgb(255,255,255) !important;\n}\n*#dm *.dmBody div.dmform-error\n{\n\tfont-style:normal !important;\n}\n*#dm *.dmBody div.dmforminput textarea\n{\n\tfont-style:italic !important;\n}\n*#dm *.dmBody div.dmforminput *.fileUploadLink\n{\n\tfont-style:italic !important;\n}\n*#dm *.dmBody div.checkboxwrapper span\n{\n\tfont-style:italic !important;\n}\n*#dm *.dmBody div.radiowrapper span\n{\n\tfont-style:italic !important;\n}\n*#dm *.dmBody *.u_1880451336:before\n{\n\topacity:0.5 !important;\n\tbackground-color:rgb(255,255,255) !important;\n}\n*#dm *.dmBody *.u_1880451336.before\n{\n\topacity:0.5 !important;\n\tbackground-color:rgb(255,255,255) !important;\n}\n*#dm *.dmBody *.u_1880451336>.bgExtraLayerOverlay\n{\n\topacity:0.5 !important;\n\tbackground-color:rgb(255,255,255) !important;\n}\n*#dm *.dmBody div.u_1526437833\n{\n\tbackground-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\ee90475c94f782b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	108015
Entropy (8bit):	5.96890968080126
Encrypted:	false
SSDEEP:	3072:pTv6aGkco/FbwOChSwOmnpwC4/IlFB3jT/tEGbCz:tiUcodbNwOEP3u
MD5:	7706BFCA6E3893FBC7834208630F7219
SHA1:	30A5BE96429875C2B6B52AEFA9B07E0D13FB2DBC
SHA-256:	02115E5F40FC418052F2E08345277F7F57E2550D44DBCB1F03BA5745DA39B2D5
SHA-512:	7B5833D29119516F9743DC95FF37571533FEA909FF395AAFB6F5461AC65552A1CCABCFAD939993D8C31C97025B07EABD164BC342C2393B00BA282AD96F171EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A...)..<....https://delval-equipment-corporation17541a33.multiscreensite.com/<!doctype html >.<html xmlns="http://www.w3.org/1999/xhtml" lang="en". class="">.<head>. .....<script type="text/javascript">. window._currentDevice = 'desktop';. window.Parameters = window.Parameters || {. AjaxContainer: 'div.dmBody',. WrappingContainer: 'div.dmOuter',. HomeUrl: 'https://delval-equipment-corporation17541a33.multiscreensite.com/',. AccountUUID: '3ff149d9ae6549b880d4c1d546662ecb',. SystemID: 'US_DIRECT_PRODUCTION',. SiteAlias: '4de34e46',. SiteId: '2184449',. SiteType: atob('RFVEQU9ORQ==',. PublicationDate: 'Tue Jun 22 15:44:46 UTC 2021',. ExternalUid: null,. IsSiteMultilingual: false,. InitialPostAlias: '',. InitialDynamicItem: '',. InitialPageAlias: 'home',. InitialPageUuid: 'f22698230fca40cd843402c3bee4c86c',. InitialEncoded

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\index	
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\85f77e7e-9589-4ce4-a7f3-954b6a8d2c51\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	3.8693405886528716
Encrypted:	false
SSDEEP:	3:TRMu00ExP+llv7aXl/lynxs5f/QmAzlJilXT9BV/lyH/sS/xttr/l/xs5f/QY+:eugxPTXpTAiX2/sSJz/lWpM
MD5:	0DDAF429B9C665E006A8DE71154AA46A
SHA1:	9940E101E2C05E0FBC65A17A27E45F52B36E7E10
SHA-256:	5A79E8F04E8A673C3A257AC430047DBE51CAA4B230FF64B13412C977669BDEF9
SHA-512:	49B37702838620C860B79F8667503C46DE0E34E26E20FCA3A6383F3B4ADD2E7B24FFA05768A121B7928E3948409947BBE4542871139EF91A4223AE40BE36510B
Malicious:	false
Reputation:	low
Preview:	(...N...oy retne.....-k..#/.@....}.oy retne.....~.Q#g.....*..#/.p.....~.oy retne.....N.J.....;.....\G..s.....~.Q#g.....WaQ..#/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\220224a4f1cf784b3e229f177c85aa28950b6791\index.txt.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.575016300371218
Encrypted:	false
SSDEEP:	24:va0VWBNneIoPoba0VWBNnm3rWDZWBrqoPoba0VWBNnmlrWDZWBr9qrWlu3rioPog:S0AToPoO0AubAMNqoPoO0AuNAMN9UcZQ
MD5:	4CFABA22C0A470A92203CF515478A65E
SHA1:	CD5BA752A9E80DBFA526F4E8365BB8D5BDD21A1C
SHA-256:	7A296CBD21ECDA4D90FACC21B8529201F403CC31A51A8DCE7AA3F27A0D52E6FF
SHA-512:	0F95298D33F15FFAD7351B5A4722AC19579FA5104821510758DA0A8531FC017A8C3DC5A4E54950EC2ABB04D27241F7B29A543459BE34D79D0C7F2D2F2D3AC1B
Malicious:	false
Reputation:	low
Preview:	.v./druntime-v2_40-site-pages-1044203454-2052115609.$85f77e7e-9589-4ce4-a7f3-954b6a8d2c51"....8F-..}.....(.....0..Ahttps://delval-equipment-corporation17541a33.multiscreensite.com/.q./druntime-v2_40-site-pages-1044203454-2052115609.$85f77e7e-9589-4ce4-a7f3-954b6a8d2c51...."....8F-..}.....(.0..y.2druntime-v2_40-runtime-fonts-1044203454-2052115609.$0457c3bb-2bbd-49a5-99c8-54bcd8ad1393"....8F-..}.....(.....0..Ahttps://delval-equipment-corporation17541a33.multiscreensite.com/.q./druntime-v2_40-site-pages-1044203454-2052115609.$85f77e7e-9589-4ce4-a7f3-954b6a8d2c51...."....8F-..}.....(.0..w.2druntime-v2_40-runtime-fonts-1044203454-2052115609.$0457c3bb-2bbd-49a5-99c8-54bcd8ad1393...."....8F-..}.....(....0..o.(druntime-v2_40-runtime-assets-2052115609.$62042b74-0120-45fb-9bca-dd4f1ea64566"....8F-..}.....(.....0..Ahttps://delval-equipment-corporation17541a33.multiscreensite.com/.q./druntime-v2_40-site-pages-1044203454-2052115609.$85f77e7e-9589-4ce4-a7f3-954b6a8d2c51...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\000001.dbtmp	
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1950
Entropy (8bit):	5.875852076245459
Encrypted:	false
SSDEEP:	48:F2emKdyz8OhP3PFPtPErDi10yBPjPESgMfuMfxMfvPFPtPEgi10yWPFPtPEG10ys:F1mKpOJfFNQDAfDdgMWMJMPFNfAIFNla
MD5:	4E393981CAF08A2F51DA1D1492FD42C4
SHA1:	31624BB120EEFE5CD4D99B1A9170A36E06478BEB
SHA-256:	DAA86955ED3AF616CC259A8CB43BA8F1A6009FA7BF619246644BD7F6535AA94C
SHA-512:	A5CEFFCF545E382F6CA370903743B1C5C1DB2F57714CDAEB4B16CE9C646A7F290CF4529F9251F4DCB0C105AC5513A2EBDF402FD2F4DE6620ECB6B4611B3CB B2
Malicious:	false
Reputation:	low
Preview:	....I.....URES:0...INITDATA_NEXT_RESOURCE_ID.1..INITDATA_DB_VERSION.2"..x2.....URES:1...INITDATA_NEXT_RESOURCE_ID.2=..F2.....URES:2...INITDATA_NEXT_RESOURCE_ID.3...2.....URES:3...INITDATA_NEXT_RESOURCE_ID.4"..p.....INITDATA_NEXT_REGISTRATION_ID.1..INITDATA_NEXT_VERSION_ID.1.XINITDATA_UNIQUE_ORIGIN:https://delval-equipment-corporation17541a33.multiscreensite.com/..GREG:https://delval-equipment-corporation17541a33.multiscreensite.com/.0.....Ahttps://delval-equipment-corporation17541a33.multiscreensite.com/.^https://delval-equipment-corporation17541a33.multiscreensite.com/runtime-service-worker.js?v=2 .(.0.8.....@...Z.b.....trueh..h..h..h..h..p.x.....REGID_TO_ORIGIN:0Ahttps://delval-equipment-corporation17541a33.multiscreensite.com/..RES:0.0f...^https://delval-equipment-corporation17541a33.multiscreensite.com/runtime-service-worker.js?v=2.....URES:0..PRES:0..RES:0.2\...Uhttps://storage.googleapis.com/workbox-cdn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	146
Entropy (8bit):	5.206728406442461
Encrypted:	false
SSDEEP:	3:tUKUXYUdfD/HUDKKqFkPt+kiE2J5iKKKc64E/rAXKeqh5oEWIV//Uv:mvDUq2Pwkn23iKKdKE/a2ZIFUv
MD5:	D06C4AC3E998B9249529EC96B10BB894
SHA1:	5F6730E1D9AE6BAEFB241C44C376AB338EA289AA
SHA-256:	60126A641BE6B54C313CCF1271C53F45A0C243A587E3EF2750C7FA377CC6651D
SHA-512:	B5E458BABB9B41CAE3E35828C9DD728951D1974A00EAD28EA3FB0119E39283DFAA6353CDFFC51D79FD6F700C72987CA8916D13708EDE0CDA41A1D7C027364B B9
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:26:08.226 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database/MANIFEST-000001.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_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\Service Worker\ScriptCache\2cc80dabc69f58b6_0	
Size (bytes):	22169
Entropy (8bit):	5.957646852839717
Encrypted:	false
SSDEEP:	384:Q20Uap1sTaV7xRhuKu3dsYRX+LHtC9wOd2T5R+wQayHBMmIZQc9Oi9oei:Q20Uw1B7xfu7NsIX+LHtC9wk2T5R+wQj
MD5:	F5C6BBC8C82D8D700539ED3EB059AAE2
SHA1:	91F2BC5875CCA725A1E7AC118B3F1E50D83E862E
SHA-256:	092B6672EAAACD0C8A31EF758173AC426815A4F137248A9D1295D72C66066275
SHA-512:	6259DFF4789B036ED275F91130E0FC48DFC9EC85C160C23E1C36541058AB6C13956DB1ED46979B1C644E926C898182279985A096F85A828FE3DCA39BAFD2A3B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0..... ..const pwaSettings = {};.const version = 40; // version of this file..// should any assets be cached at all.pwaSettings.shouldUseCache = true;..// version of site assets, should increase every publish.pwaSettings.SITE_VERSION = toHash('1624376686000');..// version of runtime files, should increase on every deploy .pwaSettings.RUNTIME_VERSION = toHash('2021-06-22T11_50_39');..// version of this file.pwaSettings.SERVICE_WORKER_VERSION = '2' + '_' + version;..// debug mode.pwaSettings.debug = true;..// base cache key url.pwaSettings.baseKeyUrl = '/_dm/s/rt/actions/cacheKey';..// helper function.function toHash(str){var hash=5381,i =str.length;while(i){hash=hash*33^str.charCodeAt(--i)}return hash>>>0}..// import the workbox utils.importScripts(. 'https://storage.googleapis.com/workbox-cdn/release s/3.0.0-beta.0/workbox-sw.js');.workbox.setConfig({ debug: false });.workbox.core.setLogLevel(workbox.core.LOG_LEVELS.warn);../**. * Creates a request handler

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19305
Entropy (8bit):	6.041508469942592
Encrypted:	false
SSDEEP:	384:j087rjLyicS/w4Qm0fAapt4v78KPMd2DEdtF62byB/+bQjSj6:T3jLUm0fL6gIEdtiHjj
MD5:	44FDAE3B16CB6901110DE21075392D88
SHA1:	8836D24CF12D3DDFF9AA42CA3652E780E5E5EF71
SHA-256:	38B5118EC0F321027643352F33AB96A91F3E4F48420A71808A5A1F050B3E2622
SHA-512:	7832FC6FB380A89926C102324AA008E34DDAC65603D57121C4A60B9F2B890F5B73E9EA0B0E643BADECED8F0659C43D7C50F3D3A124DD4CDB3AE40D7C05A3F9 DB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0.....'.\A....O.....J..ER.....\.....(S.%...`.....L`.....L`T....(S.X.`l.....L`.....M...Qd>.....charCodeAt....K`....Dp .....&.(. ..&.%..'%.B!.&.(...&.%.M.&.Y....;..&..!.%.K....,Rc.....Qcn.:....toHash..`....Da.....RcB....`.....Qd.....pwaSettings...Qc..!.....version...Qd.....logFromCache. Qf. .h.....logFetchedAndCached...Qd...V....SITE_VERSION..Qe.....RUNTIME_VERSION..$Qg2..P....SERVICE_WORKER_VERSION....Qc.Fg.....prefix...$Qg&w.....SIT E_ASSETS_CACHE_NAME...$Qg..i....SITE_PAGES_CACHE_NAME.... Qf.V.....RUNTIME_CACHE_NAME....Qe~fE.....FONTS_CACHE_NAME.$Qg*X%.....PAG ES_CACHE_BLACKLIST...l.....lb.....c.....W.....@.-....lP.....^...https://delval-equipment-corporation17541a33.multiscreensite .com/runtime-service-worker.js?v=2..a.....D`....D`....D.....`T...&...&..Q.&.(S.T.`b.....L`.....DRc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\4cb013792b196a35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2546
Entropy (8bit):	5.775915134530895
Encrypted:	false
SSDEEP:	48:dIBlMfCCpaxCYmpC4jDspyXX0xq9Kr37/Tz1VtcU/JKj46vQ9nye4Jg:dalMq5xC1ZjkuEM8L/TJV6DE6Tg
MD5:	47BA1EE3E7D892B640180E5E4A99BE59
SHA1:	5DB9F28AF9C31D91E50B1F47C520BA5D32C1C8E8
SHA-256:	DC3876EDA9D645B123E1F1CC4E95EEFC3985B22D4D9D0C2EBD0674BEC30A6C73
SHA-512:	D9495E3D0B99A481D854F59EA2697F0C080F3E52D553020FF3823B5D4D17BBF8F9C8C5E1CBDEDBA63091366BA17A329A54C8F0E4B61F9681A103BE737CD2E48 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....1var workbox=function(){"use strict";try{self.workbox.v["workbox:sw:3.0.0-beta.0"]=1}catch(t){}const t="https://storage.googleapis.com/workbox-cdn /releases/3.0.0-beta.0",e={backgroundSync:"background-sync",core:"core",expiration:"cache-expiration",googleAnalytics:"google-analytics",strategies:"strategies" ,precaching:"precaching",routing:"routing",cacheableResponse:"cacheable-response",broadcastUpdate:"broadcast-cache-update",rangeRequests:"range-requests"};return new class{constructor(){return this.v={},this.t={debug:"localhost"===self.location.hostname,modulePathPrefix:null,modulePathCb:null},this.e=this.t.debug?"dev":"prod",th is.s=!1,new Proxy(this,{get(t,s){if(t[s])return t[s];const o=e[s];return o&&t.loadModule(`workbox-${o}`),t[s]}})}setConfig(t={}){if(this.s)throw new Error("Config must be set before accessing workbox.* modules");Object.assign(this.t,t),this.e=this.t.debug?"dev":"prod"}skipWaiting(){self.addEventListener("install",()=>self.skipWaiting())}c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\4cb013792b196a35_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4489
Entropy (8bit):	5.70022152822861

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\4cb013792b196a35_1	
Encrypted:	false
SSDEEP:	96:smnMrgNr4IcDMYhVx3DYnEW/x/PTaO4XT60uII3H/S9CghkS4o:N9lWHhtW/x/PFU5uSH/S9CkkSF
MD5:	D268D05EAA2034C64396E3AA8747605A
SHA1:	C6D8F1564A9247F96139EA5614CBE62EF247F8DC
SHA-256:	3BDE8986FF6B0B502C5D3E61FC2CC9930C20380D17DD88226D41317D7B4E1B56
SHA-512:	966A1B15BD86DC0574E996CCCB61EB381E854CF414AA81F8AB390E9D86EDE4F87A013E17AA3F73B875C8308F66C08CDACA1E49B4398177E7C6269534696BBC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....1.....'.....O.....(S.<..`4.....L`.....L`.....Qc.d.....workbox..(S...`.....DL`.....8Rc.....Qb>.}.....t.....Qb.6O]....e...a.....I`....Da(.....Qb.G.z....self.....QbZ.6....v....$Qg.../....workbox:sw:3.0.0-beta.0.. Rc....J.....q.`.....LQqR.[n@...https://storage.googleapis.com/workbox-cdn/releases/3.0.0-beta.0.\..a*.....Qe.....backgroundSync....Qe.;.p....background-sync...Qb..A)....core.....Qd.,.....expiration....Qe.....cache-expiration..Qe.~.....googleAnalytics...Qe..p....google-analytics..Qd.....strategies.....Qd.v.....precaching....Q...Qc.k.....routing..... Qf2.z=....cacheableResponse.... Qf^.....cacheable-response....Qe...?....broadcastUpdate..$Qg:..j....broadcast-cache-update....Qe~J&V....rangeRequests.....Qe.i:.....range-requests...$La.... ....X..a.....M.`>.....`~.....`.....a.....D...].X..a.....Q.a.....QdV.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\ba23d8ecda68de77_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3863
Entropy (8bit):	5.581332435577812
Encrypted:	false
SSDEEP:	96:xCaOadgBscS67VkbUmWTTpxFz3rVt5gMJdFQVtFYgm9RtlebQKF:x3OQgUlb1Mdx53Rt5gMJdSVtVGRzC
MD5:	A6FACF9BA513E8561385D7FBD6D94F27
SHA1:	BFBF56D802B258ABFCADF2C18169A8A6AA60266D
SHA-256:	04872DDBD22787B8BC388EB88B8028D4D8B947A8479F4F46885781977DD1F322
SHA-512:	9302BD703230B15D08B4EBB951DF96AC448540B5928584D2A6A5604E47E27D384521204289205EA48D31727F5407A2599C93DA33573F2BDF121AF6334A4F26A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3this.workbox=this.workbox||{},this.workbox.routing=function(t,e){"use strict";try{self.workbox.v["workbox:routing:3.0.0-beta.0"]=1}catch(t){}const r="GET";var s=t=>t&&"object"==typeof t?t:{handle:t};class n{constructor(t,e,n){this.handler=s(e),this.match=t,this.method=n||r}}class o extends n{constructor(t,e,r){const s=({url:e})=>{const r=t.exec(e.href);return r?e.origin!==location.origin&&0!==r.index?null:r.slice(1):null};super(s,e,r)}}class i{constructor(){this.t=new Map}handleRequest(t){const e=new URL(t.request.url);if(!e.protocol.startsWith("http"))return;let r=null,s=null,n=null;const o=this.e(t,e);if(s=o.handler,n=o.params,r=o.route,!s&&this.r&&(s=this.r),!s)return;let i;try{i=s.handle({url:e,event:t,params:n})}catch(t){i=Promise.reject(t)}return i&&this.s&&(i=i.catch(r=>this.s.handle({url:e,event:t,err:r}))),i}e(t,e){const r=this.t.get(t.request.method)||[];for(const s of r){let r=s.match({url:e,event:t});if(r)return Array.isArray(r)&&0===r.length?r=void

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\ba23d8ecda68de77_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9529
Entropy (8bit):	5.762364135046581
Encrypted:	false
SSDEEP:	192:xiM2e/OuIlAMsHLkq1DswWC3WAnFDXIpNjg50bLnGGKWj3c0zgvHhBPrmdnX7PX:F2eHdLB2NjbX3dYBBDm17PX
MD5:	5117C60330D5B128872F2203C7A07BF2
SHA1:	FD3A7BA30B37A0B9C4536ECB3896E6CE2895CF9A
SHA-256:	A6FD2B7C0A16E9FEB4A5D8BB260E723DB35A8AAD5C8B6ADB0361977D0182336B
SHA-512:	A3EEA5B48876C79139F6DF245FDAAABA400EB69BCD4B9EC61A613A72AD05863050D845189CE0005689C5ACB54DCF91E520C06B3D97D1126FD5613AAF0068A58
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3.....'.....O.....$....:.....$.....X.....(S.|..`..... L`.....Qc.d.....workbox..(S....`.....L`L....hRc0.....Qb.6O]....e.....Qb>.}.....t.....Qb.....r.....Qb...J....s.....QbNU.l....n.....Qb.....o.....R.....M.g....$.....I`....Dav.....Qb.G.z....self.....QbZ.6....v....(Qh.Q.....workbox:routing:3.0.0-beta.0. Rc....J.....`.....Qbf.....GET..(S.@.`:.....L`.....a.....Qc.E.....handle..C.....K`....Dj.....%...%.s...%...}..)&.%./...%....,Rc.....A.`....DaB.....b.....@.-....dP.....X...https://storage.googleapis.com/workbox-cdn/releases/3.0.0-beta.0/workbox-routing.prod.jsa.....D`....D`....D`.....I...`2...&...&..a.&....&.(S.H..`F.....L`.....Qc..6....handler...Qc.`.....match.....QcR@.....method....K`....Dl.... .....&.]...-...%.-...%.'.....-.....0Rd.....`....Da....$.....c.....,...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\f1cdccba37924bda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7485
Entropy (8bit):	5.447135774338646
Encrypted:	false
SSDEEP:	96:EYPUmjD8d+HudbRafQi2m2WaHneKmAKyP+Pau9dv0xeDWDuKdoCAYOG3ie08+UJD:10d+HObRav2m2Lley4WDHSLTG3z9D
MD5:	802E6A7489E4673AB571C448B0EE10D6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\f1cdccba37924bda_0	
SHA1:	871EE37B75B462661EA72AC15E34107083BC8498
SHA-256:	C28F2410B7CB521F1CF8E96FFD5C271E6EEFF7CBB55C6E2449A1A49B6BFDD6FA
SHA-512:	1276B58159ADE8831FFB401363C9A5A05F9782B015A0F6F6BE6377CE95CC311E7CE37DA275D3373622C8BD985DC222070AB638E6D763F6968D63E77563C06A94
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!.....2self.babelHelpers={asyncToGenerator:function(e){return function(){var t=e.apply(this,arguments);return new Promise(function(e,r){return function n(o,i){try{var l=t[o](i),c=l.value}catch(e){return void r(e)}if(!l.done)return Promise.resolve(c).then(function(e){n("next",e)},function(e){n("throw",e)});e(c)}("next")})}}},this.workbox=this.workbox||{},this.workbox.core=function(){"use strict";try{self.workbox.v["workbox:core:3.0.0-beta.0"]=1}catch(e){}var e={debug:0,log:1,warn:2,error:3,silent:4};const t=(e,...t)=>{let r=e;return t.length>0&&(r+=` :: ${JSON.stringify(t)}`),r};class r extends Error{constructor(e,r){let n=t(e,r);super(n),this.name=e,this.details=r}}const n={prefix:"workbox",suffix:self.registration.scope,googleAnalytics:"googleAnalytics",precache:"precache",runtime:"runtime"},o=e=>[n.prefix,e,n.suffix].filter(e=>e.length>0).join("-"),i={updateDetails:e=>{Object.keys(n).forEach(t=>{void 0!==e[t]&&(n[t]=e[t])})},getGoogleAnalyticsName:e=>e||o(n.googleAn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\f1cdccba37924bda_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25761
Entropy (8bit):	5.721603399538893
Encrypted:	false
SSDEEP:	384:7eSazPkE7KuA89AIe5MXyD//KR1VPbBD9XQl8:7bC9LA/k3PlxXC8
MD5:	B3CFBADECC9D4286FFA86E1A3D6EB11D
SHA1:	CC5863109BE8173B9908C83AC7616DBB8221691D
SHA-256:	B9CC5FD19D6C5EEA1F0CE8FB767866E66AED71429711D2D27AF9F9DA27026FD9
SHA-512:	CB68672533D7E0AF1E813BB0E8EB5B734AD75A8BB261C9F238E97510D1EBB8E52361A0C197755FE5380139BFC21BD23C175242B8F0E9BDDD4FFA1E9629D1AEA8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!.....2.....'.....O.....d..T^.....(S.p..`.....,L`.....Qb.G.z....self....a.....Qej.....asyncToGeneratorC.(S.0.`.....L`.....0Rc.....Qb.6O]....e...`$.....`....DaX...z....(S.T.`^.....L`.....8Rc.....Qb>.}.....t...a.....I`....Da~...x.....(S.@.`8.....L`.....<Rc.....Qb.....r.....q.a....$...I`....Da....t.....(S...`.....,L`.....,Rc.....QbNU.I....n...`....Da$...b..... Rc.....`.....!..u...%.....(S.4..`.....L`.....K`....Dg.....&...&.^.....,Rc.....I`....Da.... .....b.....@.-....dP.....U...https://storage.googleapis.com/workbox-cdn/releases/3.0.0-beta.0/workbox-core.prod.js...a.....D`....D`....D`.....M....`....&...&....&....&..!.&..A.&..&.(S.4..`.....L`.....K`....Dg.....&...&.^.....,Rc.....I`....Da2...T.....!.....b.....A.d....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	3.7621024238343996
Encrypted:	false
SSDEEP:	3:nbRHyyEofk0Xr4l/llZFlS9Ir/Xalta0mlTllF/tNunwtFlziWG+:py9Ck7nWIr/esV/unQRG+
MD5:	B7644428231B4798E8F5003DC51C1666
SHA1:	D96890E2F1FA1D44E110BE49B78A0EF269A4C16A
SHA-256:	7501E5E535AFE582E969A41FE0E66FE65BBB4AB720186F99E430CC8019CF15E8
SHA-512:	685383A3D338677377547B31D5BF249F1F9954A9CD57AD298E5A30A94C70935C4C56F4ABEAF2F8EC815D85BE542216A321C4CFB975F381EF3F8EE7CFB71855D1
Malicious:	false
Reputation:	low
Preview:	(..:...oy retne.....:..#/.....I...oy retne.....u.....w.h...#.....5.....5j.+y..L.....K.7.....X...,.....a..#/.

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):	414
Entropy (8bit):	4.947002542326264
Encrypted:	false
SSDEEP:	12:5ljGld6RETZO1mWAIgGX+nO1mW3A/XkAv:76l8yZPyXGP1Xk8
MD5:	6531BA632E337313673E676C374357FF
SHA1:	E5F8A46AD2C557759AB47EB8B347D75D349627A0
SHA-256:	B6126275531361247 77A06AC23FD72210622A9F80B08E7D6DE540ACBCEEEB9AE
SHA-512:	9D5CF0B751F6301A6EA59EB62118C8138028D8DBF4D222AEA8895BCBF53476229A7B5B871ECFAAB6F250E20D4C80B26704AF0AD36A5169C4658DB9048D111BC F
Malicious:	false
Reputation:	low
Preview:	..&f.....>.x2.....next-map-id.1.pnamespace-6672b02a_8de3_4669_878f_f4f836a6ebb9-https://delval-equipment-corporation17541a33.multiscreensite.com/.0V .e.....V.e.....V.e.....[.....next-map-id.2.pnamespace-ef9c91b1_2afa_417a_8b41_1238dbe2247a-https://delval-equipment-corporation17541 a33.multiscreensite.com/.1. ....

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):	5.167585979477338
Encrypted:	false
SSDEEP:	6:mvYap4q2Pwkn23iKKdKrQMxIFUtpCYWtJZmwPCYWtDkwOwkn23iKKdKrQMFLJ:LaKvYf5KkCFUtp70/P705Jf5KktJ
MD5:	56CB1F87D70C91B33F3D3D43A262D90E
SHA1:	BB29BB67E4FF2341C35175195C662A732A83D98B
SHA-256:	102E366CD637978CEC98F947D032B94193F99A3C997E8AF50657A689C41EE90C
SHA-512:	AF0864CBC0FB444E30B1CBA9275A259329C870E8A4CAC90826F68440C16452B7BF24B3A2CFE2894C9BA0501712853BB19295E3679B838DD9AC2C089BF4242F8
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:25:59.321 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/22-1 8:25:59.323 16d0 Recovering log #3.2021/06/22-18:25:59.323 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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):	5.179901259967601
Encrypted:	false
SSDEEP:	6:mvYgt4q2Pwkn23iKKdK7Uh2ghZIFUtpCY9utJZmwPCYBDkwOwkn23iKKdK7Uh2gd:LguvYf5KkIhHh2FUtp79s/P7h5Jf5Kks
MD5:	09EE7D02F2789A7DFD328BB39BA10205
SHA1:	FD9DB7A88C6D810597851A547F3A8AB7BD4F1DD8
SHA-256:	31E127E7B3CAEF4D5F145728ABD5935C5E54ACDBC795EC6B770BF182B9E869FC
SHA-512:	EE5D8A551ABD485579320556CF466E7D7D510091BFC6D5F726315AF52598E66D9CBA2A9FD4DA7D5884247C77C0E384D3658A54DD421CBD004C783E2DC962BE 0
Malicious:	false
Reputation:	low
Preview:	2021/06/22-18:25:59.145 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/06/22-18:25:59.206 16d0 Recovering log #3.2021/06/22-18:25:59.209 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

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 22, 2021 18:26:04.512605906 CEST	192.168.2.4	8.8.8.8	0x982d	Standard query (0)	lnkd.in	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:05.185612917 CEST	192.168.2.4	8.8.8.8	0xe770	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:05.537988901 CEST	192.168.2.4	8.8.8.8	0x8310	Standard query (0)	delval-equipment-corporation17541a33.multiscreensite.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.519829035 CEST	192.168.2.4	8.8.8.8	0xf90b	Standard query (0)	lirp.cdn-website.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.653790951 CEST	192.168.2.4	8.8.8.8	0xa962	Standard query (0)	static.cdn-website.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.654468060 CEST	192.168.2.4	8.8.8.8	0xf237	Standard query (0)	irp.cdn-website.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.190267086 CEST	192.168.2.4	8.8.8.8	0x3da8	Standard query (0)	d32hwlnfiv2gyn.cloudfront.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.294459105 CEST	192.168.2.4	8.8.8.8	0x9fc	Standard query (0)	static-cdn.multiscreensite.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.869234085 CEST	192.168.2.4	8.8.8.8	0x8295	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:09.180188894 CEST	192.168.2.4	8.8.8.8	0x42e	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:10.873374939 CEST	192.168.2.4	8.8.8.8	0xfc12	Standard query (0)	static.cdn-website.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.393893957 CEST	192.168.2.4	8.8.8.8	0xbbcf	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.799444914 CEST	192.168.2.4	8.8.8.8	0xccd0	Standard query (0)	rtc.multiscreensite.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.817661047 CEST	192.168.2.4	8.8.8.8	0x45d1	Standard query (0)	jellyguesthouse.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:26:04.571171999 CEST	8.8.8.8	192.168.2.4	0x982d	No error (0)	lnkd.in		108.174.10.10	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:05.240107059 CEST	8.8.8.8	192.168.2.4	0xe770	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:05.602636099 CEST	8.8.8.8	192.168.2.4	0x8310	No error (0)	delval-equipment-corporation17541a33.multiscreensite.com		100.24.208.97	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:05.602636099 CEST	8.8.8.8	192.168.2.4	0x8310	No error (0)	delval-equipment-corporation17541a33.multiscreensite.com		35.172.94.1	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.584465981 CEST	8.8.8.8	192.168.2.4	0xf90b	No error (0)	lirp.cdn-website.com		13.224.193.107	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.584465981 CEST	8.8.8.8	192.168.2.4	0xf90b	No error (0)	lirp.cdn-website.com		13.224.193.103	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.584465981 CEST	8.8.8.8	192.168.2.4	0xf90b	No error (0)	lirp.cdn-website.com		13.224.193.5	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.584465981 CEST	8.8.8.8	192.168.2.4	0xf90b	No error (0)	lirp.cdn-website.com		13.224.193.66	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.716749907 CEST	8.8.8.8	192.168.2.4	0xa962	No error (0)	static.cdn-website.com		13.225.74.51	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.716749907 CEST	8.8.8.8	192.168.2.4	0xa962	No error (0)	static.cdn-website.com		13.225.74.36	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.716749907 CEST	8.8.8.8	192.168.2.4	0xa962	No error (0)	static.cdn-website.com		13.225.74.96	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.716749907 CEST	8.8.8.8	192.168.2.4	0xa962	No error (0)	static.cdn-website.com		13.225.74.4	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:07.722984076 CEST	8.8.8.8	192.168.2.4	0xf237	No error (0)	irp.cdn-website.com		13.224.196.75	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.252886057 CEST	8.8.8.8	192.168.2.4	0x3da8	No error (0)	d32hwlnfiv2gyn.cloudfront.net		13.224.194.4	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.252886057 CEST	8.8.8.8	192.168.2.4	0x3da8	No error (0)	d32hwlnfiv2gyn.cloudfront.net		13.224.194.63	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.252886057 CEST	8.8.8.8	192.168.2.4	0x3da8	No error (0)	d32hwlnfiv2gyn.cloudfront.net		13.224.194.200	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.252886057 CEST	8.8.8.8	192.168.2.4	0x3da8	No error (0)	d32hwlnfiv2gyn.cloudfront.net		13.224.194.165	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.357521057 CEST	8.8.8.8	192.168.2.4	0x9fc	No error (0)	static-cdn.multiscreensite.com		13.225.74.4	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.357521057 CEST	8.8.8.8	192.168.2.4	0x9fc	No error (0)	static-cdn.multiscreensite.com		13.225.74.36	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.357521057 CEST	8.8.8.8	192.168.2.4	0x9fc	No error (0)	static-cdn.multiscreensite.com		13.225.74.96	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.357521057 CEST	8.8.8.8	192.168.2.4	0x9fc	No error (0)	static-cdn.multiscreensite.com		13.225.74.51	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.934098959 CEST	8.8.8.8	192.168.2.4	0x8295	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:08.934098959 CEST	8.8.8.8	192.168.2.4	0x8295	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.934098959 CEST	8.8.8.8	192.168.2.4	0x8295	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:08.934098959 CEST	8.8.8.8	192.168.2.4	0x8295	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:26:08.934098959 CEST	8.8.8.8	192.168.2.4	0x8295	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:09.239293098 CEST	8.8.8.8	192.168.2.4	0x42e	No error (0)	www.google.ch		172.217.16.131	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:10.941581964 CEST	8.8.8.8	192.168.2.4	0xfc12	No error (0)	static.cdn-website.com		13.225.74.36	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:10.941581964 CEST	8.8.8.8	192.168.2.4	0xfc12	No error (0)	static.cdn-website.com		13.225.74.96	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:10.941581964 CEST	8.8.8.8	192.168.2.4	0xfc12	No error (0)	static.cdn-website.com		13.225.74.4	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:10.941581964 CEST	8.8.8.8	192.168.2.4	0xfc12	No error (0)	static.cdn-website.com		13.225.74.51	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.463287115 CEST	8.8.8.8	192.168.2.4	0xbbcf	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:11.463287115 CEST	8.8.8.8	192.168.2.4	0xbbcf	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.161	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.874631882 CEST	8.8.8.8	192.168.2.4	0xccd0	No error (0)	rtc.multiscreensite.com		54.159.252.151	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.874631882 CEST	8.8.8.8	192.168.2.4	0xccd0	No error (0)	rtc.multiscreensite.com		52.22.182.220	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.879873037 CEST	8.8.8.8	192.168.2.4	0x45d1	No error (0)	jellyguesthouse.com		162.241.87.236	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- delval-equipment-corporation17541a33.multiscreensite.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49752	100.24.208.97	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:05.769798994 CEST	1158	OUT	GET / HTTP/1.1 Host: delval-equipment-corporation17541a33.multiscreensite.com 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 22, 2021 18:26:05.936316013 CEST	1307	IN	HTTP/1.1 301 Server: nginx Date: Tue, 22 Jun 2021 16:26:05 GMT Content-Type: text/html Content-Length: 0 Connection: keep-alive d-cache: from-cache Location: https://delval-equipment-corporation17541a33.multiscreensite.com/

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

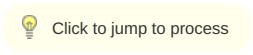
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:26:04.832659006 CEST	108.174.10.10	443	192.168.2.4	49742	CN=lnkd.in, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 07 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Wed Dec 08 00:59:59 CET 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jun 22, 2021 18:26:04.843468904 CEST	108.174.10.10	443	192.168.2.4	49741	CN=lnkd.in, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 07 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Wed Dec 08 00:59:59 CET 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jun 22, 2021 18:26:12.217437029 CEST	54.159.252.151	443	192.168.2.4	49790	CN=multiscreensite.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 20 13:38:31 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 13:38:31 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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 22, 2021 18:26:12.218691111 CEST	54.159.252.151	443	192.168.2.4	49791	CN=multiscreensite.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 20 13:38:31 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 13:38:31 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:26:12.345478058 CEST	54.159.252.151	443	192.168.2.4	49794	CN=multiscreensite.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 20 13:38:31 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 13:38:31 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					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: 4804 Parent PID: 1904

General

Start time:	18:25:58
Start date:	22/06/2021
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://lnkd.in/e9ejC3j'
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: 5772 Parent PID: 4804

General

Start time:	18:25:59
Start date:	22/06/2021
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=1628,11193727799952591932,7061772605032859279,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /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