ID: 553465
Cookbook: browseurl.jbs
Time: 23:58:51
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

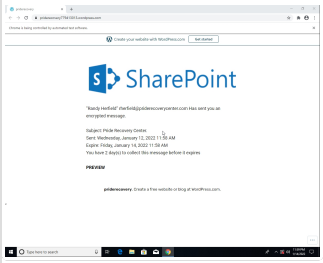
Windows Analysis Report https://priderecovery7794130…

Overview

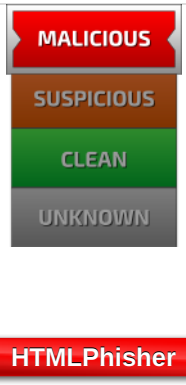
General Information

Sample URL:	http://https://priderecovery779413013.wordpress.com
Analysis ID:	553465
Infos:	

Most interesting Screenshot:



Detection



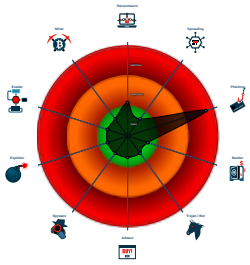
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on sh…
- Yara detected HtmlPhish7
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- HTML body contains low number of …
- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6784 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://priderecovery779413013.wordpress.com MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7000 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1528,3464267663473017341,12747655211763697408,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1912 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on shot template match)

Yara detected HtmlPhish7

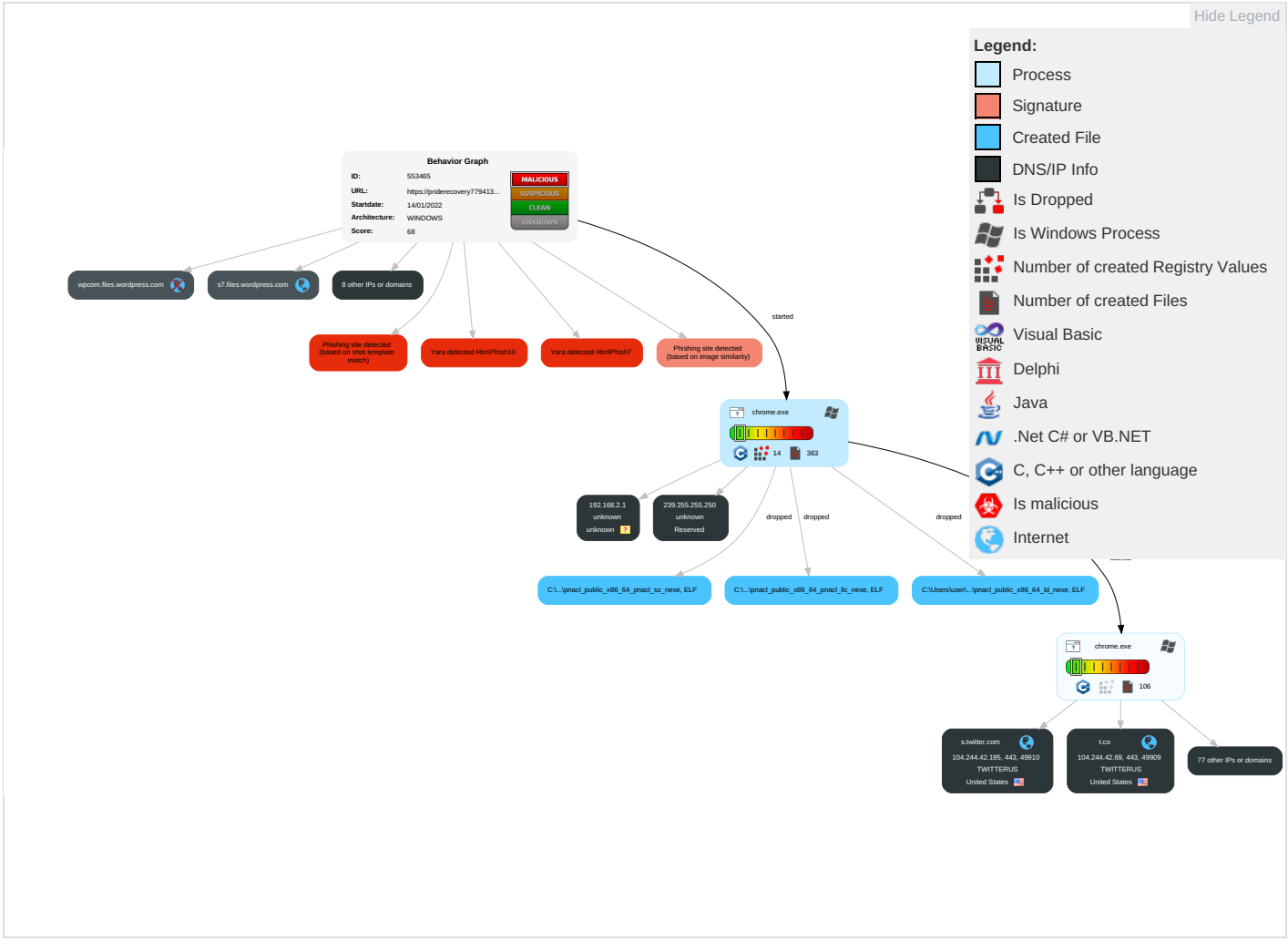
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

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

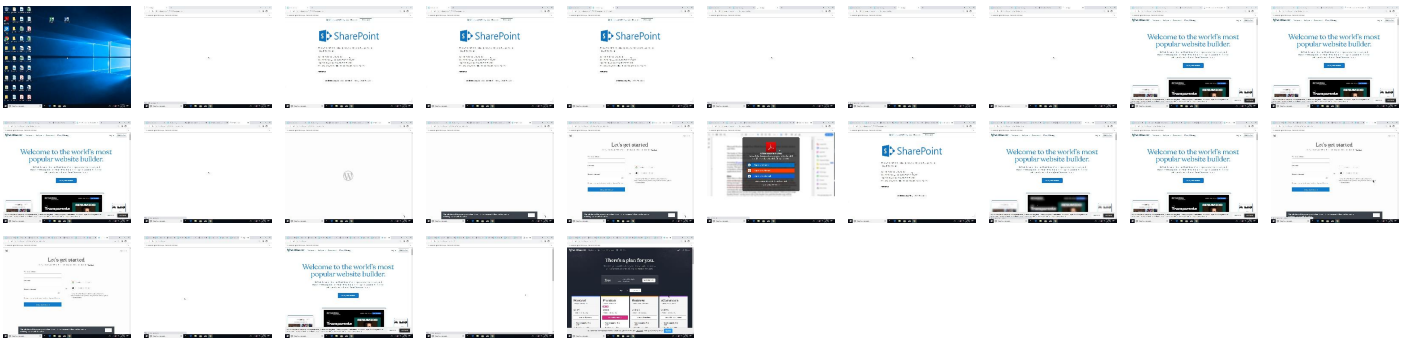
Behavior Graph

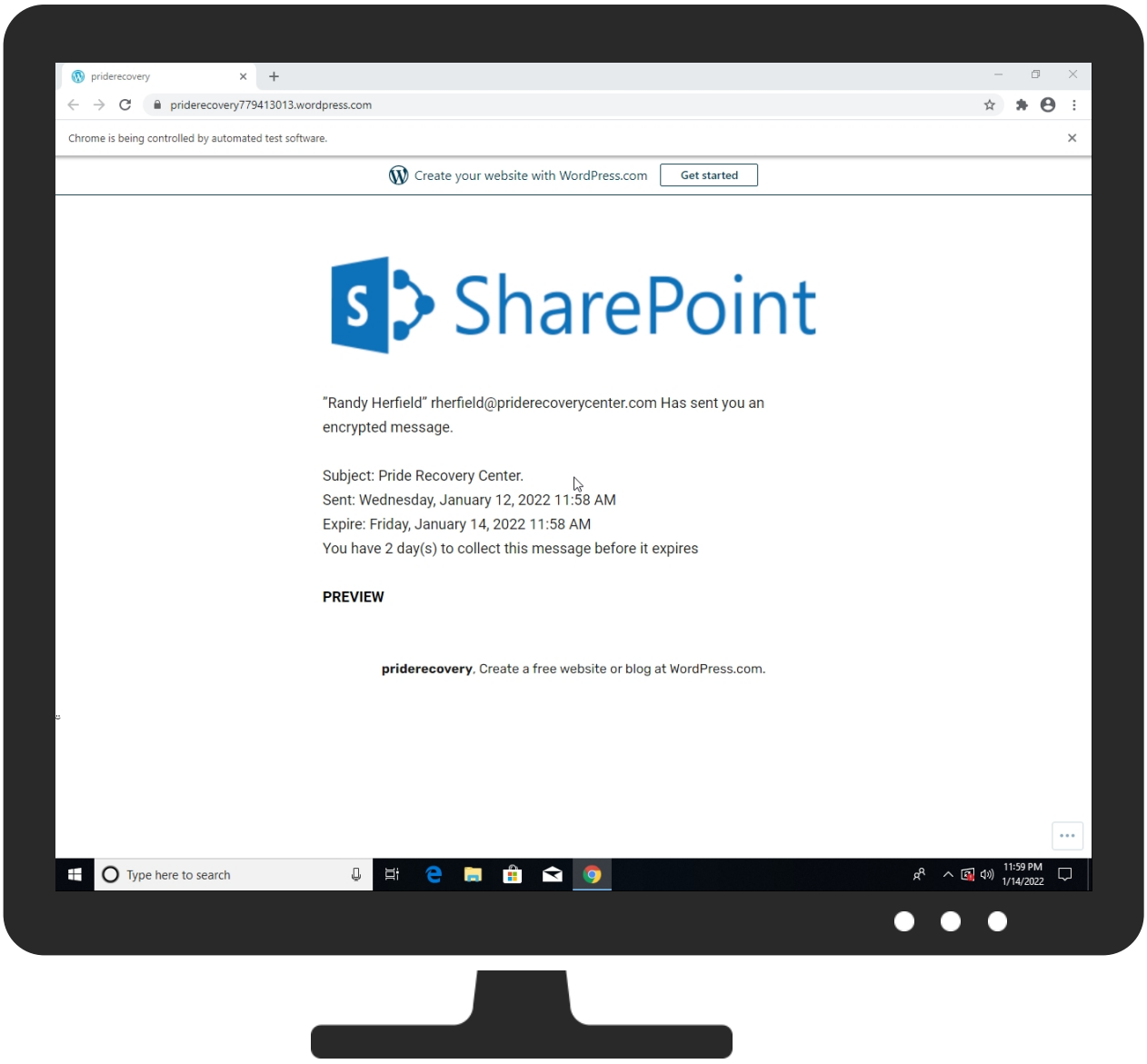


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://priderecovery779413013.wordpress.com	0%	Virustotal		Browse
http://https://priderecovery779413013.wordpress.com	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk	0%	URL Reputation	safe	
http://https://www.google.co.uk	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.163	true	false		high
stats.wp.com	192.0.76.3	true	false		high
dart.l.doubleclick.net	142.250.186.38	true	false		high
s7.files.wordpress.com	192.0.72.28	true	false		high
adservice.google.com	142.250.186.98	true	false		high
0.gravatar.com	192.0.73.2	true	false		high
s2.files.wordpress.com	192.0.72.18	true	false		high
bustling-confused-onion.glitch.me	23.23.235.119	true	false		high
platform.twitter.map.fastly.net	151.101.12.157	true	false		unknown
i.ibb.co	217.182.228.53	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
t.co	104.244.42.69	true	false		high
script.hotjar.com	13.224.96.67	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
lb.wordpress.com	192.0.78.12	true	false		high
ssl-google-analytics.l.google.com	142.250.185.136	true	false		high
www.google.com	142.250.185.164	true	false		high
cdn-content.ampproject.org	142.250.185.225	true	false		high
static-cdn.hotjar.com	13.224.96.124	true	false		high
star-mini.c10r.facebook.com	157.240.27.35	true	false		high
pagead46.l.doubleclick.net	142.250.186.66	true	false		high
nydc1.outbrain.org	64.202.112.255	true	false		unknown
accounts.google.com	142.250.184.205	true	false		high
www-google-analytics.l.google.com	142.250.186.78	true	false		high
s.twitter.com	104.244.42.195	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
plus.l.google.com	142.250.185.110	true	false		high
wordpress.com	192.0.78.17	true	false		high
www-googletagmanager.l.google.com	142.250.186.136	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
i1.wp.com	192.0.77.2	true	false		high
vars.hotjar.com	13.224.96.12	true	false		high
prod.pinterest.global.map.fastly.net	151.101.0.84	true	false		unknown
s2.wp.com	192.0.77.32	true	false		high
googleads.g.doubleclick.net	142.250.184.226	true	false		high
pixel.wp.com	192.0.76.3	true	false		high
www.google.co.uk	142.250.186.99	true	false		unknown
public-api.wordpress.com	192.0.78.22	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clients.l.google.com	142.250.181.238	true	false		high
s0.wp.com	192.0.77.32	true	false		high
s1.wp.com	192.0.77.32	true	false		high
googlehosted.l.googleusercontent.com	142.250.181.225	true	false		high
refer.wordpress.com	192.0.66.2	true	false		high
amplify.outbrain.com	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
v.pinimg.com	unknown	unknown	false		high
6355556.fls.doubleclick.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
d.turn.com	unknown	unknown	false		high
priderecovery779413013.wordpress.com	unknown	unknown	false		high
www.pinterest.com	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
i.pinimg.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
wpcom.files.wordpress.com	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
priderecovery779413013.files.wordpress.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
www.pinterest.ch	unknown	unknown	false		high
cdn.ampproject.org	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high
tr.outbrain.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://s0.wp.com/wp-includes/js/wp-emoji-release.min.js?m=1625065786h&ver=5.9-beta4-52004	false		high
http://https://vars.hotjar.com/box-21ccaa45726c0f3c8c458f7a87eb2298.html	false		high
http://https://www.pinterest.ch/ct.html	false		high
http://https://wordpress.com/start/user?ref=marketing_bar	false		high
http://https://priderecovery779413013.wordpress.com/	false		high
http://https://priderecovery779413013.wordpress.com/	false		high
http://https://6355556.fls.doubleclick.net/activityi;dc_pre=CKWC0ZqssvUCFeZDHQkdpD0Ksg;src=6355556;type=wordp0;cat=wppv;ord=7500112938201;gtm=2od1c0;auiddc=1940049009.1642233602;u4=;u6=%2F;u7=PEpDIG3owFmaLsJ7HP3n4z3Y7kNixUDZ;u5=A6WCvw3T6DnExOR4ibWg1d6%2F;~oref=https%3A%2F%2Fwordpress.com%2F%3Fref%3Dfooter_website?	false		high
http://https://accounts.google.com/o/oauth2/iframe#origin=https%3A%2F%2Fwordpress.com&rpcToken=503092991.1424817	false		high
http://https://s1.wp.com/_static/??-eJx9jkEKAjEMRS9kjXVAcCGepa2xVtOkTFIHb++spCK4+w/+gwdLc0nYkA3shhUVWo+giBdCg8lJlpakOrUX4TapbmBQaneNei6skFEcSQpWhL/AXSmU+Z86YyTJ68ywvgb8kYbESIEfLgV+BoVP3bme/MEfd95P0/7+BoNnUh8=?cssminify=yes	false		high
http://https://wordpress.com/start/?ref=marketing_bar	false		high
http://https://accounts.google.com/o/oauth2/iframe#origin=https%3A%2F%2Fwordpress.com&rpcToken=488416529.12363875&clearCache=1	false		high
http://https://s0.wp.com/wp-content/themes/h4/global.css?m=1420737423h&cssminify=yes	false		high
http://https://wordpress.com/pricing/	false		high
http://https://s1.wp.com/_static/??/wp-content/mu-plugins/comment-likes/css/comment-likes.css,/i/noticons/noticons.css?m=1436783281j&cssminify=yes	false		high
http://https://wordpress.com/?ref=footer_website	false		high
http://https://adservice.google.com/ddm/fls/i/dc_pre=CKCx0ZqssvUCFYiEhQodq20JYg;src=6355556;type=wordp0;cat=wpvisit;gtm=2od1c0;auiddc=1940049009.1642233602;u4=;u6=%2F;u7=PEpDIG3owFmaLsJ7HP3n4z3Y7kNixUDZ;u5=A6WCvw3T6DnExOR4ibWg1d6%2F;~oref=https%3A%2F%2Fwordpress.com%2F%3Fref%3Dfooter_website	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://wordpress.com/?ref=footer_blog	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://6355556.fls.doubleclick.net/activityi;dc_pre=CKCx0ZqssvUCFYiEhQodq20JYg;src=6355556;type=wordp0;cat=wpvisit;gtm=2od1c0;auiddc=1940049009.1642233602;u4=;u6=%2F;u7=PEpDIG3owFmaLsJ7HP3n4z3Y7kNixUDZ;u5=A6WCvw3T6DnExOR4ibWg1d6%2F;~oref=https%3A%2F%2Fwordpress.com%2F%3Fref%3Dfooter_website?	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://s0.wp.com/wp-content/themes/pub/seedlet/style.css?m=1640216290h&cssminify=yes	false		high
http://https://priderecovery779413013.wordpress.com/#content	false		high
http://https://s1.wp.com/_static/??/wp-content/js/mobile-useragent-info.js,/wp-content/js/rlt-proxy.js?m=1637704497j	false		high
http://https://wordpress.com/	false		high
http://https://s0.wp.com/_static/??-eJyNkdFOwzAMRX+INHQbiBfEtzipFbzZaeQkm/L3pENM3aYBL5GunWNf2/aUjJ9jwVisVJO4BorZnpKfxWQhxnajBp/zk11hjudwAQX0gIViMA7U9q/XkTv4hwu1S4caekbRHsfNsB021lXiaengD4bJKWizuTTGSyGKnuuE2e57K5wIkFHO06xEYmiohjGAb4NQ/BvvubW+gh6bPzvtxbAkWCxDm2sxQWm6sf3vEgrL7vIDfHWyZW89Lgnuzf+Cfd/WuaSYs+mvUBVTPjt4PvWHvI+vu3H3PL68bfdfcBLSYw==?cssminify=yes	false		high
http://https://adservice.google.com/ddm/fls/i/dc_pre=CKWC0ZqssvUCFeZDHQkdpD0Ksg;src=6355556;type=wordp0;cat=wppv;ord=7500112938201;gtm=2od1c0;auiddc=1940049009.1642233602;u4=;u6=%2F;u7=PEpDIG3owFmaLsJ7HP3n4z3Y7kNixUDZ;u5=A6WCvw3T6DnExOR4ibWg1d6%2F;~oref=https%3A%2F%2Fwordpress.com%2F%3Fref%3Dfooter_website	false		high
http://s1.wp.com/wp-content/themes/h4/landing/marketing/pages/_common/media/jan-2019-texture.jpg	false		high
http://https://bustling-confused-onion.glitch.me/ewindex.html	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.0.84	prod.pinterest.global.map.fastly.net	United States		54113	FASTLYUS	false
192.0.78.17	wordpress.com	United States		2635	AUTOMATTICUS	false
142.250.185.225	cdn-content.ampproject.org	United States		15169	GOOGLEUS	false
192.0.78.12	lb.wordpress.com	United States		2635	AUTOMATTICUS	false
64.202.112.255	nydc1.outbrain.org	United States		22075	AS-OUTBRAINUS	false
142.250.184.226	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
157.240.27.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
142.250.186.78	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.38	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
192.0.77.2	i1.wp.com	United States		2635	AUTOMATTICUS	false
142.250.185.110	plus.l.google.com	United States		15169	GOOGLEUS	false
192.0.72.28	s7.files.wordpress.com	United States		2635	AUTOMATTICUS	false
192.0.73.2	0.gravatar.com	United States		2635	AUTOMATTICUS	false
74.125.140.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.0.77.32	s2.wp.com	United States		2635	AUTOMATTICUS	false
217.182.228.53	i.ibb.co	France		16276	OVHFR	false
151.101.12.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
192.0.72.18	s2.files.wordpress.com	United States		2635	AUTOMATTICUS	false
192.0.66.2	refer.wordpress.com	United States		2635	AUTOMATTICUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
13.224.96.12	vars.hotjar.com	United States		16509	AMAZON-02US	false
142.250.184.205	accounts.google.com	United States		15169	GOOGLEUS	false
13.224.96.124	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
23.23.235.119	bustling-confused-onion.glitch.me	United States		14618	AMAZON-AESUS	false
142.250.186.136	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.99	www.google.co.uk	United States		15169	GOOGLEUS	false
142.250.186.98	adservice.google.com	United States		15169	GOOGLEUS	false
192.0.78.9	unknown	United States		2635	AUTOMATTICUS	false
104.244.42.69	t.co	United States		13414	TWITTERUS	false
142.250.186.163	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
192.0.76.3	stats.wp.com	United States		2635	AUTOMATTICUS	false
104.244.42.195	s.twitter.com	United States		13414	TWITTERUS	false
142.250.185.136	ssl-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.181.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
192.0.78.22	public-api.wordpress.com	United States		2635	AUTOMATTICUS	false
13.224.96.67	script.hotjar.com	United States		16509	AMAZON-02US	false
142.250.186.66	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553465
Start date:	14.01.2022
Start time:	23:58:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://priderecovery779413013.wordpress.com
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:	20
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:	mal68.phis.win@48/217@61/44
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://priderecovery779413013.wordpress.com/#content • Browse: https://bustling-confused-onion.glitch.me/ewindex.html • Browse: https://wordpress.com/?ref=footer_website • Browse: https://wordpress.com/start/?ref=marketing_bar • Browse: https://bustling-confused-onion.glitch.me/ewindex.html • Browse: https://priderecovery779413013.wordpress.com/ • Browse: https://wordpress.com/?ref=footer_blog • Browse: https://wordpress.com/start/?ref=marketing_bar • Browse: https://wordpress.com/ • Browse: https://wordpress.com/pricing/
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0503c04d-40b1-4a6f-8716-fda9045806f1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7486296893380295
Encrypted:	false
SSDEEP:	384:h3xe2ILR8D0KVjFqNNGrDvai3py8hHspGdErf8aAxRMQEzrLamHz9PMuuSNO0Aum:tOmxpScw1AeXsmYofXWyKECuhI
MD5:	CBD79C201C01888AAF179242DFCB8CC5
SHA1:	304092078E8915D10B7338BBB95A0DEECB99C452
SHA-256:	35D1701116FD98A3C2C149BA6BB1408F0CBA5315DCF91A42A1C909A0004553B7
SHA-512:	B8396B64DFBD2CD6D4DF307CFCD5CC179EC76CC9661D65EBEC2D5B087C91B8EF61F614BA87FF5D9DC0D20CDE923F211024BA22DDA25E16D94348C424DAA2D4B
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....P8.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\29d2d554-6f03-46ee-a95f-0180d07f5719.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):	201812
Entropy (8bit):	6.073494826581988
Encrypted:	false
SSDEEP:	6144:Sjh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:S9hOAAtWHlDsoF
MD5:	F01AFF044281A241CF297E62BCD138D6
SHA1:	12E86C9C47DFAB61985A69FBBA8189CF2F566976
SHA-256:	DC71F1FE66388C87ED95149C53CB2EE0E87DB1FB30CB3BD9D04D9624E211AE4C
SHA-512:	2285699231F33CA73EE5ACB949536FD7A778FCD970E72CE21AFAEE78B08F1B45D2F8086FD7273F183CA63757A29690A56B66BF9462543830A92623DC416EE2FF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4843892c-a2dd-42db-a3d4-a60c8d4133ea.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):	193338
Entropy (8bit):	6.044727701550017
Encrypted:	false
SSDEEP:	3072:W6peUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:5h2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	8FBEA69B26D4D3ECF75FE25B619F141A
SHA1:	3FD40F42BB558CDEB18E57921CF008781B187B03
SHA-256:	CE2D34CE78704CCAF0DA8567DAC397F5476E7190AC059D61882E8568C43BF647

C:\Users\user\AppData\Local\Google\Chrome\User Data\4843892c-a2dd-42db-a3d4-a60c8d4133ea.tmp	
SHA-512:	5B4DC9B19D923A8596C22BFC6506F96278F58160BE7DDE6B11059DA31FAB421E235BCBB19F2B58A3029A4F198598DA7600A481AE54D9CCB796670D60334D676
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\66d50b6b-ef72-422c-8c08-f9a405246278.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):	201811
Entropy (8bit):	6.07349331330988
Encrypted:	false
SSDEEP:	6144:WJh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:WHhOAAtWHlDsoF
MD5:	0A999F4A30582AC63E0CEF7D39F372CD
SHA1:	31BAB665D790C39CD5E381158B82CEC7C5C54063
SHA-256:	93A1456F3FB85D4C4DBBE40723501ED1BA3AF266C088D7A33DEF6F90842AA87A
SHA-512:	50820F0BD4F1172EFB5D2EC5D10C26024EFFDDFE6A8A85EF927355AABF58841B08418EF20264A2740E691C5264C46DA9AE026B4E1AF4DA961DE89742683E044
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7100976a-91e0-4847-99f0-9ed14698f0a2.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):	201812
Entropy (8bit):	6.073492318374945
Encrypted:	false
SSDEEP:	6144:+fh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:+ZhOAAtWHlDsoF
MD5:	6F61BFBB60B14288E91A730BA2362BC6
SHA1:	86ADC0A4DEB7FB7A1E26ED39B55AC1C15EA0C6E6
SHA-256:	CD08ADA1D76F7A08529E267E02E2598A63302A3FB236337A35554D4BC14F0EB2
SHA-512:	8A8C051F42F2E11AEA3F1E441D788E0FCAA226F50600AFCD55326D7E2DAA70F42A786DF443D86B9CA966C18E6911835E3DAEF5BC6AF4BDA9EBFD1CA7C5634B2
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\715c0c55-9ddd-47cb-839d-d8c05ebde22c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7483623836118354
Encrypted:	false
SSDEEP:	384:X3xe2ILRg0jqNNGrDvai3py8hHspGdErf8aAxRMQEzrLamHMPMuuSNO0AuNP1enL:bmxpSc91AeXsmYofXWyKECuhI
MD5:	B356656EF2F88C7894A94AB09F188D97
SHA1:	184FA18AB14C3F14D4C5D531FB7BA8347998B20B
SHA-256:	6D05ECA0D397DAF23C8234E3979F366B094C889203D752FDFCBA149BCF892AE0
SHA-512:	39872EE89C87A1918E9276367159E7A74065297F344B59370C46D52AA03D1F6A71E047BC5C9DEAA347F207605ED9FD7A0577275237D668A13F48A098F7B1538A

C:\Users\user\AppData\Local\Google\Chrome\User Data\715c0c55-9ddd-47cb-839d-d8c05ebde22c.tmp

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....P8.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\737fa9f7-95fd-496e-9802-e2743c59a8ef.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):	193432
Entropy (8bit):	6.044989090704115
Encrypted:	false
SSDEEP:	3072:7YpeUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:Eh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	178F01178D62DD66942C0CB596C5C355
SHA1:	431FE345B98A825D0A60639DECD4E3DB216FA2DB
SHA-256:	EF88224F09FCF49A1DCC36A883C37C86B20D40C719ED0A17459296EB58404FF2
SHA-512:	2B5DE27BA4B705A994B1654696E85B3F34968D8D71C63DFC3D086973D14C9644FD019249D8236667AD9E600E172CA7D70B0E61AC60FC6B9C46670F5B5E60D26
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7b422aea-f9ef-4323-b2dc-5b1af27f82f7.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7487759243820804
Encrypted:	false
SSDEEP:	384:x3xe2ILR8D0KVjFqNNGrDvai3py8hHspGdErf8aAxRMQEzrLamHMPMuuSNO0AuNA:9OmxpSc91AeXsmYofXWyKECuhE
MD5:	DA8D7EBBC7716C5586962E1745EE5E41
SHA1:	C4BABA78AA990C467475002E1ABE40AF2DF354E0
SHA-256:	A6788D1DAA4D3BE5DB64698BE77C41C52F55FE61697BBA088DABF36A93CE0208
SHA-512:	419A4C2AF5D06C293785D10142724E74B990F4D54C7E0B45D668BA23410977A1AB87D8103719D48F438A955D492433222D28D1886488847AB220716ABA5BCA63
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...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....P8.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\7f74181e-939f-4e9e-9bbc-c89ff5bdbbfa.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):	193432
Entropy (8bit):	6.044988780771987
Encrypted:	false
SSDEEP:	3072:i6peUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:9h2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	BCF66F2AFA91E8A7ED63DBEBE14A931F
SHA1:	D5D1C1EB4DC5C712150BD0E8614CDF0A5BE24486
SHA-256:	C6E75D0FB65713EB60BCAE943180CC05B17F89376C3064FC293287F75B6DB5E0
SHA-512:	BA424C5E8178A1B8CD6D5571C8CEAB5F6D0911A41E3426E73A5B60E22443812B41E608B661FEA9DABF1088A1854601EF19C046FC8C11E74C61B67391A35BAE7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f74181e-939f-4e9e-9bbc-c89ff5bdbbfa.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\11a47abe-4635-47bf-8f21-95d705ef28e7.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):	22596
Entropy (8bit):	5.535728777988123
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUxHG5nTEan4B:YLlCw1kXqKf/pUZNCgVLH2HforUlG5nc
MD5:	781B5164DCCEF2C889B0DC99FB5195B3
SHA1:	DF396F3FDE309B364974ACA87FBFCD78DF7A5F64
SHA-256:	2A170A3BECAC11FE830AB96C5E3AD5BD0A95BF9FDAB4DC89FC4EF9450A3C1672
SHA-512:	C43CE3A4A13F714E8AB186B5D934B225B1227391B8256EC7EABFE36D9B1CC52FCC90DEA49B65DCE72412DE3F93633AE3A44E9B61EE9A9BCEBE5902C0E15CC188
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":"13286707181852743","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\141acf48-304a-4d1c-bde1-99c5c5ec8acd.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):	5692
Entropy (8bit):	4.9949587668154605
Encrypted:	false
SSDEEP:	96:nKC/vGM9pcKlJokG2AJCKL8HYkIS14bOTQVotwn:nKC/39pcjA4KTkHK
MD5:	09204DDB7746D4006518324F48268614
SHA1:	F3BC180A6581FCB429441CDDE99596732E0854DB
SHA-256:	9CC1E43A765686412030785BB2D27CF39D4926861FF60AC037C6BCD49D6CEC9B
SHA-512:	0FC41C6E94A81CF9573ACD4A39AB13206EC532509E084BB7B07958F5F7A2F35999B60ED29B950B7A4BB1364D44741A83C306B872D18963A3754364E6EB650A52
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\141acf48-304a-4d1c-bde1-99c5c5ec8acd.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2daba679-0fa4-48b4-a437-06780fa73bff.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2ed7eaa7-d467-4d00-bb41-ba060a0fe0e6.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):	5224
Entropy (8bit):	4.986922640921434
Encrypted:	false
SSDEEP:	96:nKC/+5M9pcKIXok0JCKL8HYkIS14bOTQVuwn:nKC/B9pcQ4KTkHc
MD5:	890EEC5BEEFB2B2D370946E88365D096
SHA1:	CA7D91C0B1B2F4D2620DCF8BB34076D25F9FD2FD
SHA-256:	0303513DF5E7BF8AE68CEDF8C2259C215117015260FC4D2A75CC5579A7CB230F
SHA-512:	0639A168E98E0D8E672049FC42E27638BEC4E60BC05CFE0EB161AE8D18CC5D75F4F46AF4C8351E2A8F0B9D4D8CD223272432C1ACE1244155435CD530009344E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\30028cd4-ece0-4ed6-8755-8fa8db6406d0.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):	1040
Entropy (8bit):	5.551403329486667
Encrypted:	false
SSDEEP:	24:Ywvm9RAeU+zQRKrfwUtvCcG1KUXMkq/HeUcooobH3wUUY+Ogv3r33wUkBHQ:YwiieU+zQbUtvCbKUXlqPeUnL0U1+nrV
MD5:	CAEB89660EB7A20D8121CD96C825AF6F
SHA1:	8BF9323FE12C09C1B441588650C8404699889498
SHA-256:	6BA9CAB54A3AC3CB3B332F77FCF580A348A93C639F06CA8E75549895A2D364BE
SHA-512:	FB9EE51E00258C70BE0C291DB81A4AC490C54FAD22060199C33E2F9D3E771093678207099668CFD8F12AA028C5F9F64A1974B035A6536BEC4B291F4E38969C9E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts _observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subd omains":true,"sts_observed":1642233602.302465},{"expiry":1673769612.903523,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https", "sts_include_subdomains":false,"sts_observed":1642233612.903527},{"expiry":1673769629.788023,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V 8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233629.788027},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n 1l6Lt7yHkg5h2IYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945},{"expiry":1673769651.639498,"host":"/Vfi BGkIXip4Q8zRkQjWM6M2ec5UAwjM0Pe7EbAVj4o=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d16d078-912f-49bb-aca1-5506bea2611e.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):	17092
Entropy (8bit):	5.5828697762202095
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUm0n4U/:YLlCw1kXqKf/pUZNCgVLH2HforU9nn/
MD5:	086950BFE105FAFE15906866050EC13A
SHA1:	C538FFF0B8C219659BFAB1A941F17C42D79B58BA
SHA-256:	0B1E048626AC708EF6105AC5B4303639E751A6D46C2424545D261BB88FF93AB5
SHA-512:	8F49A2F34A1D00491900E4BE19C6DE967508236BB513367C8B98D70F1976185C069ACA79F530EB1F213673C253F2244264EF87A1C8D2ABDF18CAA42B71D5FA7E
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":"13286707181852743","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\420bc19c-9dc6-4468-80fc-403de20f892c.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:	modified
Size (bytes):	19181
Entropy (8bit):	5.570018518937232
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUxHGbjn4Qc:YLlCw1kXqKf/pUZNCgVLH2HforUlGXnm
MD5:	22D66CDFEB949376023792F28A1AF324
SHA1:	5E74478372F8922163854F34C15C2B40BEB1683B
SHA-256:	AA8207AD2E801D4E4F3E0E499F6AA0A1F39122C4BDD8369CDFF66AE1E21309ED
SHA-512:	7344F4B1AE98CC106870C2CEA6DB32FB04199372B7544BD882F312D8A8332BF1E46C39CD6494538D805119A7DEED15D4C5BFFD1EDDDC6AD0B5BD97234C000E5
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":"13286707181852743","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\566be0f1-d0bb-4a6c-8b7d-c5bc6ed37d45.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):	5225
Entropy (8bit):	4.986848200727695
Encrypted:	false
SSDEEP:	96:nKC//5M9pcKIeok0JCKL8HYkIS14bOTQVuwn:nKC/C9pcX4KTkHc
MD5:	5B9C124FF7A653B5A79205EED4093450
SHA1:	D1D9B1D652153382721DDDC9BB570A738ED0874F
SHA-256:	7F31BB4462EE2BE112B864ABA319AFCFDB07B488EA39B94EDC0C254C333E8BE5
SHA-512:	9FC37CA2CD8EBBB90CBA28E9FE77D51A18F75A8E773A4F198D60EC84294D6D2C9D664AD7AA6640D45754A7EEC6144656B2E5638010AB16229E935DC4EED750F0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71c8c452-8298-44c3-be17-586de69171ce.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71c8c452-8298-44c3-be17-586de69171ce.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):	873
Entropy (8bit):	5.5405717596062445
Encrypted:	false
SSDEEP:	24:Ywvm9RAeU+zQRKrfwUtvCcG1KUXMkq/HeUcooobH3wUIQ:YwiieU+zQbUtvCbKUXlqPeUnL0Uh
MD5:	16168B816E96927CE95A8FE57D8ACE4C
SHA1:	68291C6C6A134A4A6789361EB723387D3A34F68C
SHA-256:	0275370183914D1500AC5531BB9AA1A28F3DEF73A99F600816BF31D1910B15AF
SHA-512:	5EFA71B691AF4F7340C0671249FB8AD905900574B34458EAF6B0B2C24D173BD00FD663FC6F23DA78A44ABA330A20BCD87CECA16C84BD47BDF36F6C070C363E7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.302465},{"expiry":1673769612.903523,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233612.903527},{"expiry":1673769629.788023,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233629.788027},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n1l6Lt7yHkg5h2lYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82e0ecf9-234c-4560-9cc3-194ad3b04dcc.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):	19182
Entropy (8bit):	5.56998954548892
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUxHGI1n4N:YLlCw1kXqKf/pUZNCgVLH2HforUlGmnC
MD5:	941808E8A88C12D7AF3FCAEC226A3324
SHA1:	2660B07C4360A83AC10C536FA27F68EEB98DC8A6
SHA-256:	F8387BE89B55AE679725E0CE1DBEFCFF547D2FD03562DD7B4DAD900D92350050
SHA-512:	9D9B0B74282F51719D6E434413ECBE2F2A3B97800A8C1BF8746B00CA3AA7432F8791946312E880C94798B34D7814DBAB1DF2DE848820CDC06F2E06F94AE666B(
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":"13286707181852743","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\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

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):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low
Preview:	.f.5.....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):	5.298317768240179
Encrypted:	false
SSDEEP:	6:MIt2N+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTItTZmwYVTItk3VkwOWXp+N23U:MIJva5KkTXfchI3FUtuI5/0I+F5f5KkI
MD5:	6501C9D52A28EF8F0ACBCA880A17E8AA
SHA1:	0F419790CC70B259F189E26B4F6AB3ED83E0A140
SHA-256:	BEBE2E7ADD00FC904FE98DBEFF6F06FA2C4B438005FDE9CAB50D9A87BD09A9DD
SHA-512:	0B75875A705041CCD232930A825FC9825A35161978AECCA7A4436228784149 30ACB4759D8B450A085D5E634C7701996D85783F1AD28C28C20ADD7E0F0D37A171
Malicious:	false
Reputation:	low
Preview:	2022/01/14-23:59:47.953 1ae8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/14-23:59:47.954 1ae8 Recovering log #3.2022/01/14-23:59:47.955 1ae8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.oldeF (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.298317768240179
Encrypted:	false
SSDEEP:	6:MIt2N+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTItTZmwYVTItk3VkwOWXp+N23U:MIJva5KkTXfchI3FUtuI5/0I+F5f5KkI

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.oldeF (copy)	
MD5:	6501C9D52A28EF8F0ACBCA880A17E8AA
SHA1:	0F419790CC70B259F189E26B4F6AB3ED83E0A140
SHA-256:	BEBE2E7ADD00FC904FE98DBEFF6F06FA2C4B438005FDE9CAB50D9A87BD09A9DD
SHA-512:	0B75875A705041CCD232930A825FC9825A35161978AECCA7A443622878414930ACB4759D8B450A085D5E634C7701996D85783F1AD28C28C20ADD7E0F0D37A171
Malicious:	false
Reputation:	low
Preview:	2022/01/14-23:59:47.953 1ae8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/14-23:59:47.954 1ae8 Recovering log #3.2022/01/14-23:59:47.955 1ae8 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\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	534
Entropy (8bit):	5.213143233540573
Encrypted:	false
SSDEEP:	12:2O27Qwkyt2L8eaItHj7CEYmlQSWXZPStKBk778B/HnLmxIgVJk9s:e7QRyoL8eaQHPDqPeIY78Bfn6bky
MD5:	7F7459BEF0D39529DE1B7C653D940F17
SHA1:	A9AE97E09DF155942EFB4B312F7B07768D97618A
SHA-256:	4B60BBB1C6868780F58F9E5F38320BCEB5DB5027E21369745A4C28E36B1983AE
SHA-512:	A156723645C970106BFB543DF7808B8B81718D4783A6084DCB0D49FB1D727781B9C820B785F2323431FE2464998186E265F31FCF484736A5E89A0F66913F7097
Malicious:	false
Reputation:	low
Preview:	......"@....com..https..priderecovery..priderecovery779413013..wordpress*T.....com.....https.....priderecovery.....priderecovery779413013.....wordpress..2.....0.....1.....3.....4.....7.....9.....c.....d.....e.....h.....i.....m.....o.....p.....r.....s.....t.....v.....w.....y...../.....Bb...^.....*-https://priderecovery779413013.wordpress.com/2.priderecovery:.....J.....)...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_wordpress.com_0.indexeddb.leveldb\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_wordpress.com_0.indexeddb.leveldb\CURRENT. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_wordpress.com_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_wordpress.com_0.indexeddb.leveldb\MANIFEST-000001	
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	........idb_cmp1......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State3} (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5692
Entropy (8bit):	4.9949587668154605
Encrypted:	false
SSDEEP:	96:nKC/vGM9pcKIJokG2AJCKL8HYkIS14bOTQVotwn:nKC/39pcjA4KTkHK
MD5:	09204DDB7746D4006518324F48268614
SHA1:	F3BC180A6581FCB429441CDDE99596732E0854DB
SHA-256:	9CC1E43A765686412030785BB2D27CF39D4926861FF60AC037C6BCD49D6CEC9B
SHA-512:	0FC41C6E94A81CF9573ACD4A39AB13206EC532509E084BB7B07958F5F7A2F35999B60ED29B950B7A4BB1364D44741A83C306B872D18963A3754364E6EB650A52
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5678
Entropy (8bit):	4.993722182407564
Encrypted:	false
SSDEEP:	96:nKC/v5M9pcKITokG2AJCKL8HYkIS14bOTQVotwn:nKC/y9pcFA4KTkHK
MD5:	6F1B628DBD88D8E8BD024999141EB933
SHA1:	93CA8CE50B0623FB311158606E71B287AF443EE9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy)	
SHA-256:	6F04718C1AE1E1BE73F58310DFD38152DB488C56DE8D9B808C67489677893E4C
SHA-512:	8758928D0E4A8E5F628E953A100BCAF104795AE7C89DC179A7F7BD3A9DF27F9C52A3C8436F865D1A507CD6F58525BA7140B0C827EBFA7B4760763A53FB4F1CE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences\ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5224
Entropy (8bit):	4.986922640921434
Encrypted:	false
SSDEEP:	96:nKC/+5M9pcKIXok0JCKL8HYkIS14bOTQVuwn:nKC/B9pcQ4KTkHc
MD5:	890EEC5BEEFB2B2D370946E88365D096
SHA1:	CA7D91C0B1B2F4D2620DCF8BB34076D25F9FD2FD
SHA-256:	0303513DF5E7BF8AE68CEDF8C2259C215117015260FC4D2A75CC5579A7CB230F
SHA-512:	0639A168E98E0D8E672049FC42E27638BEC4E60BC05CFE0EB161AE8D18CC5D75F4F46AF4C8351E2A8F0B9D4D8CD223272432C1ACE1244155435CD530009344E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17091
Entropy (8bit):	5.58286365896113
Encrypted:	false
SSDEEP:	384:68Wt4Ll5SXw1kXqKf/pUZNCgVLH2HfD0rUz0n4m:HLlCw1kXqKf/pUZNCgVLH2HforUwn1
MD5:	DA5A0AD3E102245EF0DF82A2E0F9638F
SHA1:	B9D8DA70B8727D36CCB4B63E4A6813FDFE672846
SHA-256:	71CEA85E21E243B354FB191B211F0C634F841A42B44F508E8CD93E1E8B5EFA03
SHA-512:	C509788C4E033D47ADEA0F88CA438C083AF4642C257B3830A79366EE19B75BF788AE421CF529751AD3F58B350419F85073A0CF429103B63440284CABCD53F3F6
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":"13286707181852743","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\Secure PreferencesYS (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19181
Entropy (8bit):	5.570018518937232
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUxHGbjn4Qc:YLlCw1kXqKf/pUZNCgVLH2HforUlGXnm
MD5:	22D66CDFEB949376023792F28A1AF324
SHA1:	5E74478372F8922163854F34C15C2B40BEB1683B
SHA-256:	AA8207AD2E801D4E4F3E0E499F6AA0A1F39122C4BDD8369CDFF66AE1E21309ED
SHA-512:	7344F4B1AE98CC106870C2CEA6DB32FB04199372B7544BD882F312D8A8332BF1E46C39CD6494538D805119A7DEED15D4C5BFFD1EDDDC6AD0B5BD97234C000 E5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesYS (copy)	
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":"13286707181852743","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferenceseo (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17092
Entropy (8bit):	5.5828697762202095
Encrypted:	false
SSDEEP:	384:68WtFLl5SXw1kXqKf/pUZNCgVLH2HfD0rUm0n4U/:YLlCw1kXqKf/pUZNCgVLH2HforU9nn/
MD5:	086950BFE105FAFE15906866050EC13A
SHA1:	C538FFF0B8C219659BFAB1A941F17C42D79B58BA
SHA-256:	0B1E048626AC708EF6105AC5B4303639E751A6D46C2424545D261BB88FF93AB5
SHA-512:	8F49A2F34A1D00491900E4BE19C6DE967508236BB513367C8B98D70F1976185C069ACA79F530EB1F213673C253F2244264EF87A1C8D2ABDF18CAA42B71D5FA7E
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":"13286707181852743","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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
Size (bytes):	6250
Entropy (8bit):	6.872507305933139
Encrypted:	false
SSDEEP:	96:oZPS8ZZKNTKiYjfQAg+DFvjdHOMvKH/emVbyL/K3KbT1jkwbtQXV2:oxMqjzFjdnyHhyLfJZbtMV2
MD5:	0BC492C5A221E554E4F4CE9FE62FD191
SHA1:	6A80E5F7E7ACF12CCD2355641BB1910EA700918C
SHA-256:	4B13696B124365EB0536D7AF23AAD209062F6C758BA636684E3FF239A9971BD4
SHA-512:	8356AE7834BC4A484AFDBDF3459CE0BF1DA82A35FB65E47AA469A7FEFFB520D7D69ADE23628C220C8AE7503B49544D4C003EE03166AF3D9C731485FCDB2D17 DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0/**. * WARNING: DO NOT USE ES2015+ OR COMMONJS. This file is served as-is and isn't. * transpiled by Babel or bundled by Webpack.. */..// eslint-disable-next-line strict.'use strict';..const queuedMessages = [];../**. * We want to make sure that if the service worker gets updated that we. * immediately claim it, to ensure we're not running stale versions of the worker. *.See: https://developer.mozilla.org/en-US/docs/Web/API/ServiceWorkerGlobalScope/skipWaiting. */..self.addEventListener('install', function (event) {..event.waitUntil(self.skipWaiting());.});..self.addEventListener('activate', function (event) {..event.waitUntil(self.clients.claim());.});..self.addEventListener('push', function (event) {..if (typeof event.data !== 'object' && typeof event.data.json !== 'function') {...return;..}...const notification = event.data.json();...event.waitUntil(...self.registration.....showNotification(notification.msg, {.....tag: 'note_' + notificat

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):	3905
Entropy (8bit):	5.608049154557378
Encrypted:	false
SSDEEP:	96:0ufKDFsx9wnUL10bWnxSvivJEXvIeWjaSchEUIdwR:0v5sx9SQSvus1RSchEBE
MD5:	860C03BA04032293CD39CD9DBE4B9B4C
SHA1:	8840796C3AE290393231BCFEB40A66B0EA91E01A
SHA-256:	08C128AD6F2C7F74FAA554ADC8371F10148C512210E9C7D198C7192F56663F2F
SHA-512:	60C7D794747204F5ACB13DD8D6CF9BC094B1FDDACE1C8FBE35610D49F411892119F2E43B63C59D69A03858427E312EA87694FE91C40B9F574EC8715F0D3D9C0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0.....'.....O.....s..A.....(S....`R....@L`.....QbBd.....self..Qe.2.....addEventListener..Q.@..+.....install..(S.@.`<....L`.....Qd.|9... .waitUntil.....Qd.....skipWaiting...K`....Dj .....(...&....&.(...&.X...&.Y.....,Rc.....I`....Da....p....,Rc.....`.....Qe.,9Q....queuedMessages..`....Ib.....c..... .P.....@.-....4P.....'...https://wordpress.com/service-worker.js.a.....D`....D`....D`.....4...`....&...&....&.(S.H.`H.....L`.....QcBJ.....clients...Qc6M.....claim.....K`....Dl ..... (...&....&.(...&.(...&.X...&.Y.....,Rc.....I`....Da....@.....Q....c.....P...@.....d.....@..@.....&.(S....`X....LL`"....4Rc.....Qd&5.q....notification`....I`....Da..... ..Qb...Z....data..Qb...`....json.....Qd._.....registration..Qe.|.....showNotification..Qb^>.....msg.,,.a.....Qb...G....tag.C..Qb.a?:....iconC..Qd.PW.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\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\ScriptCache\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72
Entropy (8bit):	3.3712491399084956
Encrypted:	false
SSDEEP:	3:N5nXl/lvll/lxELo/tVllw+:D4L4j
MD5:	F811762675CFF922D71FC190C477E5BC
SHA1:	329415DA49F47762F9F57DB5EE37FB59DF45D5A5
SHA-256:	6E2F9C4DEC99BDF15FD768B4768A01490C1C7565AC3BC2E431BC49E1C009CD26
SHA-512:	BE4C1393889E6E5CF6FC5D3C249FF3CADAEC07274ABB0143ED49918EE6BD2B295DB5652FB00B743CC3286312C312D34069F8075CD9E4F80243781F13F5C1513
Malicious:	false
Reputation:	low
Preview:	@.....=eoy retne.....(.....X....,`.....(.....f..04/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72
Entropy (8bit):	3.3712491399084956
Encrypted:	false
SSDEEP:	3:N5nXl/lvll/lxELo/tVllw+:D4L4j
MD5:	F811762675CFF922D71FC190C477E5BC
SHA1:	329415DA49F47762F9F57DB5EE37FB59DF45D5A5
SHA-256:	6E2F9C4DEC99BDF15FD768B4768A01490C1C7565AC3BC2E431BC49E1C009CD26
SHA-512:	BE4C1393889E6E5CF6FC5D3C249FF3CADAEC07274ABB0143ED49918EE6BD2B295DB5652FB00B743CC3286312C312D34069F8075CD9E4F80243781F13F5C1513
Malicious:	false
Reputation:	low
Preview:	@.....=eoy retne.....(.....X....,`.....(.....f..04/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index% (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72
Entropy (8bit):	3.3712491399084956
Encrypted:	false
SSDEEP:	3:N5nXl/lvll/lxELo/tVllw+:D4L4j
MD5:	F811762675CFF922D71FC190C477E5BC
SHA1:	329415DA49F47762F9F57DB5EE37FB59DF45D5A5
SHA-256:	6E2F9C4DEC99BDF15FD768B4768A01490C1C7565AC3BC2E431BC49E1C009CD26
SHA-512:	BE4C1393889E6E5CF6FC5D3C249FF3CADAEC07274ABB0143ED49918EE6BD2B295DB5652FB00B743CC3286312C312D34069F8075CD9E4F80243781F13F5C1513
Malicious:	false
Reputation:	low
Preview:	@.....=eoy retne.....(.....X....,`.....(.....f..04/.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I 58
Malicious:	false
Reputation:	low
Preview:	.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\fc671d3a-8292-4f78-b6f1-fb39c348853a.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\0338d0e0-676a-4fc9-adb6-a88c5ecafaed.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\0338d0e0-676a-4fc9-adb6-a88c5ecafaed.tmp	
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.207380765000157
Encrypted:	false
SSDEEP:	12:M439Ova5KkkGHArqiuFUtu43b/043U5f5KkkGHArq2J:MW6a5KkkGgCguWgWef5KkkGg7
MD5:	7459DBACF0AD6326E69D59A89CD832DF
SHA1:	B40CCC6987F96719FA32C4F6EA1E03288C966904
SHA-256:	AAFB61A3622AAD5304CA9E7FB218A7D2140571193191C5F39E91A492AB988970
SHA-512:	FD74555AEE84990FE50F53A0B3BE22FC4598486BD4264C7F8524CD40E9753971515E78DC20B1D35A0CA5155D81E53518B066D886DF13C322673C9363E8014CF2
Malicious:	false
Reputation:	low
Preview:	2022/01/15-00:00:37.693 bd0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2022/01/15-00:00:37.695 bd0 Recovering log #3.2022/01/15-00:00:37.696 bd0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.207380765000157
Encrypted:	false
SSDEEP:	12:M439Ova5KkkGHArqiuFUtu43b/043U5f5KkkGHArq2J:MW6a5KkkGgCguWgWef5KkkGg7
MD5:	7459DBACF0AD6326E69D59A89CD832DF
SHA1:	B40CCC6987F96719FA32C4F6EA1E03288C966904
SHA-256:	AAFB61A3622AAD5304CA9E7FB218A7D2140571193191C5F39E91A492AB988970
SHA-512:	FD74555AEE84990FE50F53A0B3BE22FC4598486BD4264C7F8524CD40E9753971515E78DC20B1D35A0CA5155D81E53518B066D886DF13C322673C9363E8014CF2
Malicious:	false
Reputation:	low
Preview:	2022/01/15-00:00:37.693 bd0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2022/01/15-00:00:37.695 bd0 Recovering log #3.2022/01/15-00:00:37.696 bd0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.155068589515975
Encrypted:	false
SSDEEP:	12:M4aXzi+va5KkkGHArAFUtu4aXU/04aX0V5f5KkkGHArfJ:MLfa5KkkGgkguLFLef5KkkGgV
MD5:	5074FDD17E885D9A7FA247AE85ECAA98
SHA1:	4748FC6513A9FBB5AA2A9DBA99F93C32954D5B15
SHA-256:	9C90CF3630F72551C554B4560256EF9C1B8BAED58A5F0197386C60F611D87810
SHA-512:	206286055076B8C06D2DA72B6E73105E5909FD5AFE4F56CD211D5106F98AC7ED3EAA3D8FFDB5169F19062351D1FDC1824888A954C263DA74AF136690D4A8BDF
Malicious:	false
Reputation:	low
Preview:	2022/01/15-00:00:52.905 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/15-00:00:52.907 1b9c Recovering log #3.2022/01/15-00:00:52.907 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.298374562805823
Encrypted:	false
SSDEEP:	12:M4e+va5KkkOrsFUtu4UZ/0443V5f5KkkOrzJ:Msa5Kk+guK1Xf5Kkn
MD5:	B641434F933658CE0D6A97514B52D1C3
SHA1:	1A736BBB55B8AF0C49BD3AC21C8071E40845D086
SHA-256:	44C08C8473413753E3CE64704600D3E0B2415F500A968BBF7733A021D778D98C
SHA-512:	D380CD51985258DAB490F82004A53C1B6560D1A4BC2BB858B4D0CFBE3239E284F39A2CCFB8BFD993196EB775D495F5A1DCFF7EFBBD640610BE9CAC7AD753D81
Malicious:	false
Reputation:	low
Preview:	2022/01/15-00:01:44.917 1b9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2022/01/15-00:01:44.919 1b9c Recovering log #3.2022/01/15-00:01:44.920 1b9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	705
Entropy (8bit):	5.514071302734389
Encrypted:	false
SSDEEP:	12:Y5uzbm9RAJ9+UAnIIYRcdQRVDMpL/fN+UAnI/vmcEErNgmh4r+UAnIDBM7XQbo83:Ywvm9RAeU+zQRKrfwUtvCcG1KUXoooo5
MD5:	FF36916246A6FD3831B8BA7477FA818F
SHA1:	AC0DAAF20A820CDBFB656687DAA66F07A55A7274
SHA-256:	783F311E48AB3B8E641D79F83AD521DD866168DED9B3BCD735043D9AF7F340DA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
SHA-512:	3299A424D0482547A4FD31BF895E6A039E378A3453E06649941E586CECB081FAE73EEF69787BFCCF036477E89C95B028C459A7AE8B590F3B6BB32FBEBEC4EFC 8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.302465},{"expiry":1673769612.903523,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233612.903527},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n1l6Lt7yHkg5h2IYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurityMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	704
Entropy (8bit):	5.516640647722841
Encrypted:	false
SSDEEP:	12:Y5uzbm9RAJ9+UAnIIYRcdQRVDMpL/fN+UAnI/vmcdrNgmh4r+UAnI67XQbo8dbHV:Ywvm9RAeU+zQRKrfwUtv3G1KUkooobHV
MD5:	8D294EF3AADC531C887E5173D21C3F36
SHA1:	A4B521DA1B4547CD9A4300B729CD91290F2CF7B0
SHA-256:	A29560F724B3A5C11F3BA668F3A7ABE2C98BAD6C3603AC03B8E5F7F92D7F47D9
SHA-512:	A0B758787E515FE15AB6A65DAE18B2A8A7C19E31BEE17FE465FDD463A59316D4150C4B8D9AD7E77E9F5C90B28D809F57B513BCC58C4F2E44491E9239D4852E 8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.302465},{"expiry":1673769600.912605,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233600.91261},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n1l6Lt7yHkg5h2IYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\add058f8-5744-4e7c-a6b6-a6754962f205.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):	6022
Entropy (8bit):	5.027188951194478
Encrypted:	false
SSDEEP:	96:nKC/vZM9pcKIvokGTOJCKL8HYkIS1FokVhmbOTQVotwn:nKC/S9pcEO4KTkHYkVI
MD5:	4257D84DB10B99058FEB784B1B1B7F93
SHA1:	3025691607CE62088D5FDB879497E3F626DE174D
SHA-256:	368E7E4C4DB6895D1090043367381E6465515200BCD76842F6ECBDDC13D2EBAE
SHA-512:	281C6EA46866CBAF7D066A63D5A05D20EEB8711818999975341EC51C3D9BDC14148576D0991ED36D77E61C6284258191F061C0EF9DCF49AC69D71D7024804CA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bc5c34f7-b00a-4e33-b739-ac14e9714ad3.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):	5678
Entropy (8bit):	4.993722182407564
Encrypted:	false
SSDEEP:	96:nKC/v5M9pcKITokG2AJCKL8HYkIS14bOTQVotwn:nKC/y9pcFA4KTkHK
MD5:	6F1B628DBD88D8E8BD024999141EB933
SHA1:	93CA8CE50B0623FB311158606E71B287AF443EE9
SHA-256:	6F04718C1AE1E1BE73F58310DFD38152DB488C56DE8D9B808C67489677893E4C
SHA-512:	8758928D0E4A8E5F628E953A100BCAF104795AE7C89DC179A7F7BD3A9DF27F9C52A3C8436F865D1A507CD6F58525BA7140B0C827EBFA7B4760763A53FB4F1CE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bc5c34f7-b00a-4e33-b739-ac14e9714ad3.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c5277422-7029-47f1-8a3c-8a8bbe18096c.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):	4783
Entropy (8bit):	4.907889032016278
Encrypted:	false
SSDEEP:	96:JTGDHazUvrsXFKEI6VK1ELMNTQMFETrWGlDpGSw/5KN6GKGuH:JTGDHazUvoXF/I6VKKLMNTQLTrWsDpPg
MD5:	AF952DBF5BDA5A600493EE9EDB13D08B
SHA1:	75CCB8DEB6CE26EBE822F922DEAAF630420C2907
SHA-256:	74144CC1D02AA5911CFF9E54E2BDCF864DEF70ED2731EF35824B043C17A4DDCE
SHA-512:	5EF56E5BBF96C8F2120A655980CD492DB6EA1F1A3D17398B97ECE68FD466FD82EA5B2B9E7F1B15045878CBBC0D61339CADED6BC62B33D160E75F550DC6FF66 4F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299183720709","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299183848239","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13289299183848243","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r4---sn-4g5ednse.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299188329174","port":443,"protocol_str":"quic"}],"isolation":[],"server

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c674060c-aa8f-40d9-8a33-655e68090542.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):	6618
Entropy (8bit):	5.200788992420991
Encrypted:	false
SSDEEP:	96:nKC/vMM9SkpeL8TM4cKIvokGTOJCKL8HYkIS1FokVhmbOTQVotwn:nKC/h9SQer4cEO4KTkHYkVI
MD5:	E8209F6AEFFF1A811743467CCA6815F4
SHA1:	84402F4FC6F60A34D25150EDE84E543DE065800C
SHA-256:	4E0CE87F9AAF7ACF62926B382AEAB3B4286BEE7CCB3B9CA6448DD38B9B9F46E5
SHA-512:	ED3755A808B856B56B9C25040CDD08B411BC51A4690656011F711D8514764F1DC796B6AF72190B1BC37735847444C6DD2F5DC11594CAAB693EFA60C0FD94361
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286707182370380","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c9b257aa-e5f4-4bb6-89ed-5559cda14dd2.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):	705
Entropy (8bit):	5.514071302734389
Encrypted:	false
SSDEEP:	12:Y5uzbm9RAJ9+UAnIIYRcdQRVDMpL/fN+UAnI/vmcEErNgmh4r+UAnIDBM7XQbo83:Ywvm9RAeU+zQRKrfwUtvCcG1KUXoooo5
MD5:	FF36916246A6FD3831B8BA7477FA818F
SHA1:	AC0DAAF20A820CDBFB656687DAA66F07A55A7274
SHA-256:	783F311E48AB3B8E641D79F83AD521DD866168DED9B3BCD735043D9AF7F340DA
SHA-512:	3299A424D0482547A4FD31BF895E6A039E378A3453E06649941E586CECB081FAE73EEF69787BFCCF036477E89C95B028C459A7AE8B590F3B6BB32FBEBEC4EFC 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c9b257aa-e5f4-4bb6-89ed-5559cda14dd2.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.302465},{"expiry":1673769612.903523,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233612.903527},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n1l6Lt7yHkg5h2IYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cdc1fa39-4b9b-4cac-ad51-9a7cab4937b7.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):	5355
Entropy (8bit):	4.902146270759711
Encrypted:	false
SSDEEP:	96:JTGDHzUvrs4I6VK1EfMFETrWGlR6G5FGerGfNGsG4Gi/5G7GqGoG2GIGvZxhH:JTGDHzUvo4I6VKKfLTrWsR6cFpuN5jXF
MD5:	98A2D6589D414803ED3ADA3914655E9A
SHA1:	256FC76473741003973CCD1263C2D3A9529C4B21
SHA-256:	34BF0E5D27232F146624C9BCA39BFCEE8E621231DF0CD22E72FA3EA515E1EEDB
SHA-512:	22A49D34A8D4A8A820715305C6C80FFDE1698C830BAA079BBAF3BEE3258EC2424F8743DA5B5D92992FAFB6DEA2D75F6946EBE2677C841A0797AF80A9B4C1E9A
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299183720709","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299183848239","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13289299183848243","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r4---sn-4g5ednse.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289299188329174","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternati

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d54afa36-9eee-468e-ba91-d7aaf4913fdb.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):	704
Entropy (8bit):	5.516640647722841
Encrypted:	false
SSDEEP:	12:Y5uzbm9RAJ9+UAnIIYRcdQRVDMpL/fN+UAnI/vmcdrNgmh4r+UAnI67XQbo8dbHV:Ywvm9RAeU+zQRKrfwUtv3G1KUkooobHV
MD5:	8D294EF3AADC531C887E5173D21C3F36
SHA1:	A4B521DA1B4547CD9A4300B729CD91290F2CF7B0
SHA-256:	A29560F724B3A5C11F3BA668F3A7ABE2C98BAD6C3603AC03B8E5F7F92D7F47D9
SHA-512:	A0B758787E515FE15AB6A65DAE18B2A8A7C19E31BEE17FE465FDD463A59316D4150C4B8D9AD7E77E9F5C90B28D809F57B513BCC58C4F2E44491E9239D4852E68
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1673769602.436955,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.436961},{"expiry":1673769602.302458,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642233602.302465},{"expiry":1673769600.912605,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233600.91261},{"expiry":1642255203.09794,"host":"23jQ7D4e77YQ4YwjymtW/n1l6Lt7yHkg5h2IYCkrybo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1642233603.097945}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d92fa27a-180c-435e-9ccc-ec23c804ef62.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d92fa27a-180c-435e-9ccc-ec23c804ef62.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e4afc1ea-76f0-4dac-8b20-ea2631afeca7.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):	17091
Entropy (8bit):	5.58286365896113
Encrypted:	false
SSDEEP:	384:68Wt4Ll5SXw1kXqKf/pUZNCgVLH2HfD0rUz0n4m:HLlCw1kXqKf/pUZNCgVLH2HforUwn1
MD5:	DA5A0AD3E102245EF0DF82A2E0F9638F
SHA1:	B9D8DA70B8727D36CCB4B63E4A6813FDFE672846
SHA-256:	71CEA85E21E243B354FB191B211F0C634F841A42B44F508E8CD93E1E8B5EFA03
SHA-512:	C509788C4E033D47ADEA0F88CA438C083AF4642C257B3830A79366EE19B75BF788AE421CF529751AD3F58B350419F85073A0CF429103B63440284CABCD53F3F6
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":"13286707181852743","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\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4(
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	193338
Entropy (8bit):	6.0447271381049115
Encrypted:	false
SSDEEP:	3072:fepeUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:2h2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	E2B321AB56E71D620562FC97FC5EBB48
SHA1:	47ACAB5C16D3BAD51231008F9DF8292650FF7683
SHA-256:	08C3DC84394EF3241520DA40454E5152905CD7C6FD3A64250A0C5B4BB382A6FF
SHA-512:	4CE366288D6BEC94E303D836FDC89D06246050E3F500F29C1ADDFBE0CF1A9A34D57A8DAAF201B3968985E196B75FAD4544B54C47CEDFA65C89197F7C0464DF0
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201812
Entropy (8bit):	6.073494328606638
Encrypted:	false
SSDEEP:	6144:ZCh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:ZehOAAtWHlDsoF
MD5:	72B0C09153329289D21B8709361CD306
SHA1:	07E38E60604D4A6290F887B9CABE8BEDAB1164F5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateMP (copy)	
SHA-256:	DCA944CDD0C8B5B2D28561130CF0658CD178D08DC5470D8BF070F889FF84872E
SHA-512:	A132E1EEE5325EE968EE193206CE62AAF02BCD7639A5E18B7FA4D426864C3FA0BD4113062CF2584B7230B87308F75A564B295152695BD1D890BF902229B23317
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Stateez (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201812
Entropy (8bit):	6.073494826581988
Encrypted:	false
SSDEEP:	6144:Sjh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:S9hOAAtWHlDsoF
MD5:	F01AFF044281A241CF297E62BCD138D6
SHA1:	12E86C9C47DFAB61985A69FBBA8189CF2F566976
SHA-256:	DC71F1FE66388C87ED95149C53CB2EE0E87DB1FB30CB3BD9D04D9624E211AE4C
SHA-512:	2285699231F33CA73EE5ACB949536FD7A778FCD970E72CE21AFAEE78B08F1B45D2F8086FD7273F183CA63757A29690A56B66BF9462543830A92623DC416EE2FF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7487759243820804
Encrypted:	false
SSDEEP:	384:x3xe2ILR8D0KVjFqNNGrDvai3py8hHspGdErf8aAxRMQEzrLamHMPMuuSNO0AuNA:9OmxpSc91AeXsmYofXWyKECuhE
MD5:	DA8D7EBBC7716C5586962E1745EE5E41
SHA1:	C4BABA78AA990C467475002E1ABE40AF2DF354E0
SHA-256:	A6788D1DAA4D3BE5DB64698BE77C41C52F55FE61697BBA088DABF36A93CE0208
SHA-512:	419A4C2AF5D06C293785D10142724E74B990F4D54C7E0B45D668BA23410977A1AB87D8103719D48F438A955D492433222D28D1886488847AB220716ABA5BCA63
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...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....P8.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\a9753840-4812-4b18-a691-554e7e88ddab.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):	201812
Entropy (8bit):	6.073494328606638
Encrypted:	false
SSDEEP:	6144:ZCh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:ZehOAAtWHlDsoF
MD5:	72B0C09153329289D21B8709361CD306
SHA1:	07E38E60604D4A6290F887B9CABE8BEDAB1164F5
SHA-256:	DCA944CDD0C8B5B2D28561130CF0658CD178D08DC5470D8BF070F889FF84872E
SHA-512:	A132E1EEE5325EE968EE193206CE62AAF02BCD7639A5E18B7FA4D426864C3FA0BD4113062CF2584B7230B87308F75A564B295152695BD1D890BF902229B23317

C:\Users\user\AppData\Local\Google\Chrome\User Data\a9753840-4812-4b18-a691-554e7e88ddab.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\a99ea2e0-387a-4aa4-8990-6f298d5a5868.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):	193432
Entropy (8bit):	6.044989090704115
Encrypted:	false
SSDEEP:	3072:7YpeUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:Eh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	178F01178D62DD66942C0CB596C5C355
SHA1:	431FE345B98A825D0A60639DECD4E3DB216FA2DB
SHA-256:	EF88224F09FCF49A1DCC36A883C37C86B20D40C719ED0A17459296EB58404FF2
SHA-512:	2B5DE27BA4B705A994B1654696E85B3F34968D8D71C63DFC3D086973D14C9644FD019249D8236667AD9E600E172CA7D70B0E61AC60FC6B9C46670F5B5E60D26
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\b4ebe853-e99b-4cc2-8434-38f1ccc523db.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):	193338
Entropy (8bit):	6.0447271381049115
Encrypted:	false
SSDEEP:	3072:fepeUzebDqOAEYEMAFwxx2tf/4exijqMARtxgAGDdFcbXafIB0u1GOJmA3iuRO:2h2qOAOntfJ/MQxglD7aqfIlUOoSiuRO
MD5:	E2B321AB56E71D620562FC97FC5EBB48
SHA1:	47ACAB5C16D3BAD51231008F9DF8292650FF7683
SHA-256:	08C3DC84394EF3241520DA40454E5152905CD7C6FD3A64250A0C5B4BB382A6FF
SHA-512:	4CE366288D6BEC94E303D836FDC89D06246050E3F500F29C1ADDFBE0CF1A9A34D57A8DAAF201B3968985E196B75FAD4544B54C47CEDFA65C89197F7C0464DF0
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799870886"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d1d6e876-632b-4f54-9eb9-96c28dae5208.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):	201812
Entropy (8bit):	6.0734935462982795
Encrypted:	false
SSDEEP:	6144:iJh2qOAOntfJ/MQxglD7aqfIlUOoSiuRO:iHhOAAtWHlDsoF
MD5:	865CFDAF7E4D9E9CA801CBBD8E259259
SHA1:	C7F939246019BBF3C925B3F9578C6D83F193C2AF
SHA-256:	4BE54A23CC38AFB8CBA453ADC38DDE49387B71811F0CA3C0251904360D3D7BC3
SHA-512:	E407D6DB3D936F0A0C4786F27F01B889B0BCDCD0211D482A81DECC4DA4B3D486256C1F0578F01D2854A7ADBD97CFBB33C8630B5B573396F95AAB14EE770DF3A

C:\Users\user\AppData\Local\Google\Chrome\User Data\d1d6e876-632b-4f54-9eb9-96c28dae5208.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642233583854067e+12,"network":1.642201185e+12,"ticks":130837785.0,"uncertainty":3897309.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\6382a364-252a-4577-810f-14b7f6a6e6fc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\6784_1503633797_metadata\verified_contents.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):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F52
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uliwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9qcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1l4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_pnacl_json	
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prev ent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 0
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<.....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p .....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95F
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h.....fff..... .....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_ client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 6
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j.,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@...`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A631 E
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.n acl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4 xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A.....D.. D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `....;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''..*...1...:....D...K...T ...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....\_pnacl_wrapper_start.\_\_pnacl_real_irt_query_func.\_\_pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `.....\_pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DDF00
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....!.....!.....'.....G.....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i.....0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."..".."..".....@.....`..... ...@...`..... ...@...`..... ...@...`..... ...@...`.....`... ...@...`.....`...`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H...F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\6784_1503633797_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870E
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y..... .....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`... ...@... @.....@.....Y@.....p.....@.....?.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..? .y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`... ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\6784_1503633797\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C 2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6784_1503633797\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",.. "name": "PNaCl Translator Multi-CRX",.. "manifest_version": 2,.. "minimum_chrome_version": "30.0.0.0",.. "version": "0.57.44.2492",.. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\8298008f-3662-4216-90ec-e2630b3148be.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp\8298008f-3662-4216-90ec-e2630b3148be.tmp	
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\9a049afa-4a47-419c-b5e8-3bb039aff12b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!.,~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\ce632748-29b9-4758-822e-ba5b5d4cc01c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6784_1263058439\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6784_1263058439\CRX_INSTALL_locales\am\messages.json	
Preview:	{.. "10198456148852051 7": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "12827687646031907 5": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874943 76": {.. "message": "... ...".. },.. "18027627465894571 77": {.. "message": "...".. },.. "18503975003120203 88": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6784_1263058439\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6784_1263058439\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .. ..".. },.. "14284488690781267 31": {.. "message": "..... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".... .. ..".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

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
Jan 14, 2022 23:59:43.271359921 CET	192.168.2.3	8.8.8.8	0x941a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:43.278521061 CET	192.168.2.3	8.8.8.8	0x6b8d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:43.279082060 CET	192.168.2.3	8.8.8.8	0x174	Standard query (0)	priderecovery779413013.wordpress.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.078952074 CET	192.168.2.3	8.8.8.8	0x3596	Standard query (0)	s0.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.081656933 CET	192.168.2.3	8.8.8.8	0x5da	Standard query (0)	s2.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.088732958 CET	192.168.2.3	8.8.8.8	0xa694	Standard query (0)	s1.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.107484102 CET	192.168.2.3	8.8.8.8	0xb5ee	Standard query (0)	wordpress.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.261518002 CET	192.168.2.3	8.8.8.8	0xd799	Standard query (0)	0.gravatar.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.346728086 CET	192.168.2.3	8.8.8.8	0xdb82	Standard query (0)	stats.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.347831964 CET	192.168.2.3	8.8.8.8	0xa1ee	Standard query (0)	priderecovery779413013.files.wordpress.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.509013891 CET	192.168.2.3	8.8.8.8	0xbddd	Standard query (0)	pixel.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.484065056 CET	192.168.2.3	8.8.8.8	0xea15	Standard query (0)	s1.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.568753004 CET	192.168.2.3	8.8.8.8	0xebc8	Standard query (0)	priderecovery779413013.files.wordpress.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.577625036 CET	192.168.2.3	8.8.8.8	0x19eb	Standard query (0)	s2.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.585235119 CET	192.168.2.3	8.8.8.8	0x89c	Standard query (0)	pixel.wp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:47.963175058 CET	192.168.2.3	8.8.8.8	0x35fd	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.512003899 CET	192.168.2.3	8.8.8.8	0xe121	Standard query (0)	bustling-confused-onion.glitch.me	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.706842899 CET	192.168.2.3	8.8.8.8	0xbc6f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.707983971 CET	192.168.2.3	8.8.8.8	0x3f03	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.714729071 CET	192.168.2.3	8.8.8.8	0x9dc6	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.054177046 CET	192.168.2.3	8.8.8.8	0x872f	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.059103012 CET	192.168.2.3	8.8.8.8	0xfc83	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.070238113 CET	192.168.2.3	8.8.8.8	0x63ed	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:00.762005091 CET	192.168.2.3	8.8.8.8	0x920c	Standard query (0)	i1.wp.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.350438118 CET	192.168.2.3	8.8.8.8	0xae26	Standard query (0)	public-api.wordpress.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.611665964 CET	192.168.2.3	8.8.8.8	0x44dc	Standard query (0)	amplify.outbrain.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.611705065 CET	192.168.2.3	8.8.8.8	0x8728	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.642297029 CET	192.168.2.3	8.8.8.8	0xe9a2	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.692365885 CET	192.168.2.3	8.8.8.8	0x2c11	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.699153900 CET	192.168.2.3	8.8.8.8	0x3334	Standard query (0)	d.turn.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.700980902 CET	192.168.2.3	8.8.8.8	0x3cbb	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2022 00:00:01.894788027 CET	192.168.2.3	8.8.8.8	0xc0c1	Standard query (0)	refer.wordpress.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.990606070 CET	192.168.2.3	8.8.8.8	0x1784	Standard query (0)	tr.outbrain.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.139348030 CET	192.168.2.3	8.8.8.8	0xbe4c	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.152518988 CET	192.168.2.3	8.8.8.8	0xe4f5	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.153017998 CET	192.168.2.3	8.8.8.8	0x5bf9	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.210514069 CET	192.168.2.3	8.8.8.8	0xa6da	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.226959944 CET	192.168.2.3	8.8.8.8	0xf3cb	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.270838976 CET	192.168.2.3	8.8.8.8	0x104d	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.381444931 CET	192.168.2.3	8.8.8.8	0xf8c8	Standard query (0)	6355556.fls.doubleclick.net	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.539916992 CET	192.168.2.3	8.8.8.8	0x77e3	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.541702986 CET	192.168.2.3	8.8.8.8	0x77e2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.541912079 CET	192.168.2.3	8.8.8.8	0x77a5	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.864924908 CET	192.168.2.3	8.8.8.8	0xebd0	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.376816034 CET	192.168.2.3	8.8.8.8	0xc51a	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.413893938 CET	192.168.2.3	8.8.8.8	0xe6dc	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.791635990 CET	192.168.2.3	8.8.8.8	0xbf0d	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.137912035 CET	192.168.2.3	8.8.8.8	0x3b13	Standard query (0)	www.pinterest.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.139151096 CET	192.168.2.3	8.8.8.8	0xed8c	Standard query (0)	wpcom.files.wordpress.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.432279110 CET	192.168.2.3	8.8.8.8	0x3b82	Standard query (0)	www.pinterest.ch	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.913002968 CET	192.168.2.3	8.8.8.8	0x7350	Standard query (0)	0.gravatar.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.935275078 CET	192.168.2.3	8.8.8.8	0xc8b	Standard query (0)	i1.wp.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:05.024573088 CET	192.168.2.3	8.8.8.8	0xee28	Standard query (0)	v.pinimg.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:05.025624037 CET	192.168.2.3	8.8.8.8	0xef63	Standard query (0)	i.pinimg.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:13.284295082 CET	192.168.2.3	8.8.8.8	0x856f	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.290359020 CET	192.168.2.3	8.8.8.8	0x8a25	Standard query (0)	s1.wp.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.291217089 CET	192.168.2.3	8.8.8.8	0xcae2	Standard query (0)	wordpress.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.548762083 CET	192.168.2.3	8.8.8.8	0xfd6f	Standard query (0)	stats.wp.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.549601078 CET	192.168.2.3	8.8.8.8	0xf6e3	Standard query (0)	pixel.wp.com	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:50.463182926 CET	192.168.2.3	8.8.8.8	0x3ff7	Standard query (0)	cdn.ampproject.org	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:53.094598055 CET	192.168.2.3	8.8.8.8	0x12d5	Standard query (0)	wpcom.files.wordpress.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 23:59:43.297365904 CET	8.8.8.8	192.168.2.3	0x941a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:43.297365904 CET	8.8.8.8	192.168.2.3	0x941a	No error (0)	clients.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:43.300388098 CET	8.8.8.8	192.168.2.3	0x174	No error (0)	priderecovery779413013.wordpress.com	lb.wordpress.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 23:59:43.300388098 CET	8.8.8.8	192.168.2.3	0x174	No error (0)	lb.wordpress.com		192.0.78.12	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:43.300388098 CET	8.8.8.8	192.168.2.3	0x174	No error (0)	lb.wordpress.com		192.0.78.13	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:43.306035042 CET	8.8.8.8	192.168.2.3	0x6b8d	No error (0)	accounts.google.com		142.250.184.205	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.097914934 CET	8.8.8.8	192.168.2.3	0x3596	No error (0)	s0.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.100008965 CET	8.8.8.8	192.168.2.3	0x5da	No error (0)	s2.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.108072996 CET	8.8.8.8	192.168.2.3	0xa694	No error (0)	s1.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.126509905 CET	8.8.8.8	192.168.2.3	0xb5ee	No error (0)	wordpress.com		192.0.78.17	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.126509905 CET	8.8.8.8	192.168.2.3	0xb5ee	No error (0)	wordpress.com		192.0.78.9	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.265007019 CET	8.8.8.8	192.168.2.3	0xd82	No error (0)	gstaticadssl.l.google.com		142.250.186.163	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.280177116 CET	8.8.8.8	192.168.2.3	0xd799	No error (0)	0.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.365479946 CET	8.8.8.8	192.168.2.3	0xdb82	No error (0)	stats.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.369323969 CET	8.8.8.8	192.168.2.3	0xa1ee	No error (0)	priderecovery77941301 3.files.wordpress.com	s2.files.wordpress.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:44.369323969 CET	8.8.8.8	192.168.2.3	0xa1ee	No error (0)	s2.files.wordpress.com		192.0.72.18	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.369323969 CET	8.8.8.8	192.168.2.3	0xa1ee	No error (0)	s2.files.wordpress.com		192.0.72.19	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:44.525988102 CET	8.8.8.8	192.168.2.3	0xbddd	No error (0)	pixel.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.503129005 CET	8.8.8.8	192.168.2.3	0xea15	No error (0)	s1.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.589519978 CET	8.8.8.8	192.168.2.3	0xebc8	No error (0)	priderecovery77941301 3.files.wordpress.com	s2.files.wordpress.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:45.589519978 CET	8.8.8.8	192.168.2.3	0xebc8	No error (0)	s2.files.wordpress.com		192.0.72.18	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.589519978 CET	8.8.8.8	192.168.2.3	0xebc8	No error (0)	s2.files.wordpress.com		192.0.72.19	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.596854925 CET	8.8.8.8	192.168.2.3	0x19eb	No error (0)	s2.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:45.604296923 CET	8.8.8.8	192.168.2.3	0x89c	No error (0)	pixel.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:47.990917921 CET	8.8.8.8	192.168.2.3	0x35fd	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:47.990917921 CET	8.8.8.8	192.168.2.3	0x35fd	No error (0)	googlehosted.l.googleusercontent.com		142.250.181.225	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		23.23.235.119	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		3.90.93.100	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		52.45.138.32	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		3.234.98.145	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		3.86.152.72	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:55.539558887 CET	8.8.8.8	192.168.2.3	0xe121	No error (0)	bustling-confused-onion.glitch.me		52.44.125.193	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.726969957 CET	8.8.8.8	192.168.2.3	0xbc6f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:58.727900028 CET	8.8.8.8	192.168.2.3	0x3f03	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.727900028 CET	8.8.8.8	192.168.2.3	0x3f03	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:58.734662056 CET	8.8.8.8	192.168.2.3	0x9dc6	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:59.075995922 CET	8.8.8.8	192.168.2.3	0x872f	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.075995922 CET	8.8.8.8	192.168.2.3	0x872f	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.082039118 CET	8.8.8.8	192.168.2.3	0xfc83	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 23:59:59.170551062 CET	8.8.8.8	192.168.2.3	0x63ed	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.170551062 CET	8.8.8.8	192.168.2.3	0x63ed	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.170551062 CET	8.8.8.8	192.168.2.3	0x63ed	No error (0)	i.ibb.co		51.210.32.103	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.170551062 CET	8.8.8.8	192.168.2.3	0x63ed	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)
Jan 14, 2022 23:59:59.170551062 CET	8.8.8.8	192.168.2.3	0x63ed	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:00.763588905 CET	8.8.8.8	192.168.2.3	0x7749	No error (0)	ssl-google-analytics.l.google.com		142.250.185.136	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:00.780752897 CET	8.8.8.8	192.168.2.3	0x920c	No error (0)	i1.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.367491961 CET	8.8.8.8	192.168.2.3	0xae26	No error (0)	public-api.wordpress.com		192.0.78.22	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.367491961 CET	8.8.8.8	192.168.2.3	0xae26	No error (0)	public-api.wordpress.com		192.0.78.23	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.632085085 CET	8.8.8.8	192.168.2.3	0x44dc	No error (0)	amplify.outbrain.com	wildcard.outbrain.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.633052111 CET	8.8.8.8	192.168.2.3	0x8728	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.633052111 CET	8.8.8.8	192.168.2.3	0x8728	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.638953924 CET	8.8.8.8	192.168.2.3	0x9a6d	No error (0)	www-google tagmanager.l.google.com		142.250.186.136	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.649476051 CET	8.8.8.8	192.168.2.3	0xb1b5	No error (0)	www-google-analytics.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.670864105 CET	8.8.8.8	192.168.2.3	0xe9a2	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:00:01.670864105 CET	8.8.8.8	192.168.2.3	0xe9a2	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.711242914 CET	8.8.8.8	192.168.2.3	0x2c11	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.711242914 CET	8.8.8.8	192.168.2.3	0x2c11	No error (0)	platform.twitter.map.fastly.net		151.101.12.157	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.719866037 CET	8.8.8.8	192.168.2.3	0x3334	No error (0)	d.turn.com	d.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.734790087 CET	8.8.8.8	192.168.2.3	0x3cbb	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:01.734790087 CET	8.8.8.8	192.168.2.3	0x3cbb	No error (0)	static-cdn.hotjar.com		13.224.96.124	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.734790087 CET	8.8.8.8	192.168.2.3	0x3cbb	No error (0)	static-cdn.hotjar.com		13.224.96.116	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.734790087 CET	8.8.8.8	192.168.2.3	0x3cbb	No error (0)	static-cdn.hotjar.com		13.224.96.91	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.734790087 CET	8.8.8.8	192.168.2.3	0x3cbb	No error (0)	static-cdn.hotjar.com		13.224.96.61	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:01.914005041 CET	8.8.8.8	192.168.2.3	0xc0c1	No error (0)	refer.wordpress.com		192.0.66.2	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.009368896 CET	8.8.8.8	192.168.2.3	0x1784	No error (0)	tr.outbrain.com	alldcs.outbrain.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.009368896 CET	8.8.8.8	192.168.2.3	0x1784	No error (0)	alldcs.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.009368896 CET	8.8.8.8	192.168.2.3	0x1784	No error (0)	alldcs.outbrain.org	nydc1.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.009368896 CET	8.8.8.8	192.168.2.3	0x1784	No error (0)	nydc1.outbrain.org		64.202.112.255	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.162386894 CET	8.8.8.8	192.168.2.3	0xbe4c	No error (0)	script.hotjar.com		13.224.96.67	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.162386894 CET	8.8.8.8	192.168.2.3	0xbe4c	No error (0)	script.hotjar.com		13.224.96.63	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.162386894 CET	8.8.8.8	192.168.2.3	0xbe4c	No error (0)	script.hotjar.com		13.224.96.11	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.162386894 CET	8.8.8.8	192.168.2.3	0xbe4c	No error (0)	script.hotjar.com		13.224.96.104	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171322107 CET	8.8.8.8	192.168.2.3	0xe4f5	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171322107 CET	8.8.8.8	192.168.2.3	0xe4f5	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171322107 CET	8.8.8.8	192.168.2.3	0xe4f5	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171322107 CET	8.8.8.8	192.168.2.3	0xe4f5	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.171905041 CET	8.8.8.8	192.168.2.3	0x5bf9	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	prod.pinterest.global.map.fastly.net		151.101.0.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	prod.pinterest.global.map.fastly.net		151.101.64.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	prod.pinterest.global.map.fastly.net		151.101.128.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.232215881 CET	8.8.8.8	192.168.2.3	0xa6da	No error (0)	prod.pinterest.global.map.fastly.net		151.101.192.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.250531912 CET	8.8.8.8	192.168.2.3	0xf3cb	No error (0)	vars.hotjar.com		13.224.96.12	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.250531912 CET	8.8.8.8	192.168.2.3	0xf3cb	No error (0)	vars.hotjar.com		13.224.96.92	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.250531912 CET	8.8.8.8	192.168.2.3	0xf3cb	No error (0)	vars.hotjar.com		13.224.96.22	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.250531912 CET	8.8.8.8	192.168.2.3	0xf3cb	No error (0)	vars.hotjar.com		13.224.96.118	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.288222075 CET	8.8.8.8	192.168.2.3	0x104d	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.288222075 CET	8.8.8.8	192.168.2.3	0x104d	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.288222075 CET	8.8.8.8	192.168.2.3	0x104d	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.288222075 CET	8.8.8.8	192.168.2.3	0x104d	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.288222075 CET	8.8.8.8	192.168.2.3	0x104d	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.409342051 CET	8.8.8.8	192.168.2.3	0xf8c8	No error (0)	6355556.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.409342051 CET	8.8.8.8	192.168.2.3	0xf8c8	No error (0)	dart.l.doubleclick.net		142.250.186.38	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.567528963 CET	8.8.8.8	192.168.2.3	0x77e3	No error (0)	googleads.g.doubleclick.net		142.250.184.226	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.569186926 CET	8.8.8.8	192.168.2.3	0x77a5	No error (0)	www.google.co.uk		142.250.186.99	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.569307089 CET	8.8.8.8	192.168.2.3	0x77e2	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:02.883691072 CET	8.8.8.8	192.168.2.3	0xebd0	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:02.883691072 CET	8.8.8.8	192.168.2.3	0xebd0	No error (0)	star-mini.c10r.facebook.com		157.240.27.35	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.406085014 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:00:03.406085014 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.406085014 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.406085014 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.406085014 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	i.ibb.co		51.210.32.103	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.442353010 CET	8.8.8.8	192.168.2.3	0xe6dc	No error (0)	adservice.google.com		142.250.186.98	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:03.817276001 CET	8.8.8.8	192.168.2.3	0xbf0d	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:03.817276001 CET	8.8.8.8	192.168.2.3	0xbf0d	No error (0)	pagead46.l.doubleclick.net		142.250.186.66	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.158868074 CET	8.8.8.8	192.168.2.3	0xed8c	No error (0)	wpcom.files.wordpress.com	s7.files.wordpress.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.158868074 CET	8.8.8.8	192.168.2.3	0xed8c	No error (0)	s7.files.wordpress.com		192.0.72.28	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.158868074 CET	8.8.8.8	192.168.2.3	0xed8c	No error (0)	s7.files.wordpress.com		192.0.72.29	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.161439896 CET	8.8.8.8	192.168.2.3	0x3b13	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.161439896 CET	8.8.8.8	192.168.2.3	0x3b13	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	www.pinterest.ch	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	prod.pinterest.global.map.fastly.net		151.101.0.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	prod.pinterest.global.map.fastly.net		151.101.64.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	prod.pinterest.global.map.fastly.net		151.101.128.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.458250999 CET	8.8.8.8	192.168.2.3	0x3b82	No error (0)	prod.pinterest.global.map.fastly.net		151.101.192.84	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.934031963 CET	8.8.8.8	192.168.2.3	0x7350	No error (0)	0.gravatar.com		192.0.73.2	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:04.957941055 CET	8.8.8.8	192.168.2.3	0xc8b	No error (0)	i1.wp.com		192.0.77.2	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:05.050013065 CET	8.8.8.8	192.168.2.3	0xee28	No error (0)	v.pinimg.com	v.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:05.050013065 CET	8.8.8.8	192.168.2.3	0xee28	No error (0)	v.pinimg.com.gslb.pinterest.com	2-01-37d2-0007.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:05.050363064 CET	8.8.8.8	192.168.2.3	0xef63	No error (0)	i.pinimg.com	i.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:05.050363064 CET	8.8.8.8	192.168.2.3	0xef63	No error (0)	i.pinimg.com.gslb.pinterest.com	2-01-37d2-0004.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:13.311547995 CET	8.8.8.8	192.168.2.3	0x856f	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 00:00:13.311547995 CET	8.8.8.8	192.168.2.3	0x856f	No error (0)	plus.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.308614969 CET	8.8.8.8	192.168.2.3	0x8a25	No error (0)	s1.wp.com		192.0.77.32	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.311822891 CET	8.8.8.8	192.168.2.3	0xcae2	No error (0)	wordpress.com		192.0.78.9	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.311822891 CET	8.8.8.8	192.168.2.3	0xcae2	No error (0)	wordpress.com		192.0.78.17	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.565778017 CET	8.8.8.8	192.168.2.3	0xfd6f	No error (0)	stats.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.566596985 CET	8.8.8.8	192.168.2.3	0xf6e3	No error (0)	pixel.wp.com		192.0.76.3	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:46.577728987 CET	8.8.8.8	192.168.2.3	0x8d96	No error (0)	gstaticadssl.l.google.com		142.250.186.163	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:50.489156961 CET	8.8.8.8	192.168.2.3	0x3ff7	No error (0)	cdn.ampproject.org	cdn-content.ampproject.org		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:50.489156961 CET	8.8.8.8	192.168.2.3	0x3ff7	No error (0)	cdn-content.ampproject.org		142.250.185.225	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:53.115041971 CET	8.8.8.8	192.168.2.3	0x12d5	No error (0)	wpcom.files.wordpress.com	s7.files.wordpress.com		CNAME (Canonical name)	IN (0x0001)
Jan 15, 2022 00:00:53.115041971 CET	8.8.8.8	192.168.2.3	0x12d5	No error (0)	s7.files.wordpress.com		192.0.72.28	A (IP address)	IN (0x0001)
Jan 15, 2022 00:00:53.115041971 CET	8.8.8.8	192.168.2.3	0x12d5	No error (0)	s7.files.wordpress.com		192.0.72.29	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- priderecovery779413013.wordpress.com
- accounts.google.com
- clients2.google.com
- https:
  - s0.wp.com
  - s1.wp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49757	192.0.78.12	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	0	OUT	GET / HTTP/1.1 Host: priderecovery779413013.wordpress.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 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	5	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Vary: Cookie X-hacker: If you're reading this, you should visit automattic.com/jobs and apply to join the fun, mention this header. Host-Header: WordPress.com Link: <https://wp.me/PdEfT4-2>; rel=shortlink X-ac: 1.hhn _dca Strict-Transport-Security: max-age=15552000
2022-01-14 22:59:43 UTC	5	IN	Data Raw: 65 66 34 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 20 2f 3e 0a 09 3c 74 69 74 6c 65 3e 70 72 69 64 65 72 65 63 6f 76 65 72 79 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 Data Ascii: ef4<!doctype html><html lang="en"><head><meta charset="UTF-8" /><meta name="viewport" content="wid th=device-width, initial-scale=1" /><link rel="profile" href="https://gmpg.org/xfn/11" /><title>priderecovery</title><meta name='robots' content
2022-01-14 22:59:43 UTC	6	IN	Data Raw: 09 69 66 20 28 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 2e 6f 6e 6c 6f 61 64 20 21 3d 20 27 66 75 6e 63 74 69 6f 6e 27 29 20 7b 0a 09 09 09 09 77 69 6e 64 6f 77 2e 6f 6e 6c 6f 61 64 20 3d 20 66 75 6e 63 3b 0a 09 09 09 7d 20 65 6c 73 65 20 7b 0a 09 09 09 09 77 69 6e 64 6f 77 2e 6f 6e 6c 6f 61 64 20 3d 20 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0a 09 09 09 09 09 6f 6c 64 6f 6e 6c 6f 61 64 28 29 3b 0a 09 09 09 09 09 66 75 6e 63 28 29 3b 0a 09 09 09 09 7d 0a 09 09 09 7d 0a 09 09 09 7d 0a 09 09 2f 2a 20 5d 5d 3e 20 2a 2f 0a 09 3c 2f 73 63 72 69 70 74 3e 0a 09 09 09 3c 73 63 72 69 70 74 3e 0a 09 09 09 77 69 6e 64 6f 77 2e 5f 77 70 65 6d 6f 6a 69 53 65 74 74 69 6e 67 73 20 3d 20 7b 22 62 61 73 65 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 30 2e 77 70 2e 63 6f Data Ascii: if (typeof window.onload != 'function') {window.onload = func;} else {window.onload = function () {oldonload ();func();}}}/* ... */</script><script>window._wpemojiSettings = {"baseUrl":"https:\/\/s0.wp.co
2022-01-14 22:59:43 UTC	7	IN	Data Raw: 33 35 36 2c 35 37 33 33 32 2c 35 36 31 32 38 2c 35 36 34 32 33 2c 35 36 31 32 38 2c 35 36 34 31 38 2c 35 36 31 32 38 2c 35 36 34 32 31 2c 35 36 31 32 38 2c 35 36 31 32 38 2c 35 36 34 32 33 2c 35 36 31 32 38 2c 35 36 34 34 37 5d 2c 5b 35 35 33 35 36 2c 35 37 33 33 32 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 32 33 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 31 38 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 32 31 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 33 30 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 32 33 2c 38 32 30 33 2c 35 36 31 32 38 2c 35 36 34 34 37 5d 29 3b 63 61 73 65 22 65 6d 6f 6a 69 22 3a 72 65 74 75 72 6e 21 73 28 5b 31 30 30 38 34 2c 36 35 30 33 39 2c 38 32 30 35 2c 35 35 33 35 37 2c 35 36 36 31 33 5d 2c 5b 31 30 Data Ascii: 356,57332,56128,56423,56128,56418,56128,56421,56128,56430,56128,56423,56128,56447],[5535 6,57332,8203,56128,56423,8203,56128,56418,8203,56128,56421,8203,56128,56430,8203,56128,56423,8203,56 128,56447]);case"emoji":return!s([10084,65039,8205,55357,56613],[10
2022-01-14 22:59:43 UTC	9	IN	Data Raw: 65 66 3d 27 68 74 74 70 73 3a 2f 2f 73 30 2e 77 70 2e 63 6f 6d 2f 5f 73 74 61 74 69 63 2f 3f 3f 2d 65 4a 79 4e 6b 64 46 4f 77 7a 41 4d 52 58 2b 49 4e 48 51 62 69 42 66 45 74 7a 69 70 46 62 7a 5a 61 65 51 6b 6d 2f 4c 33 70 45 4e 4d 33 61 59 42 4c 35 47 75 6e 57 4e 66 32 2f 61 55 6a 4a 39 6a 77 56 69 73 56 4a 4f 34 42 6f 72 5a 6e 70 4b 66 78 57 51 68 78 6e 61 6a 42 70 2f 7a 6b 31 31 68 6a 75 64 77 41 51 58 30 67 49 56 69 4d 41 37 55 39 71 2f 58 6b 54 76 34 68 77 75 31 53 34 63 61 65 6b 62 52 48 73 66 4e 73 42 30 32 31 6c 58 69 61 65 6e 0d 0a 31 30 37 64 0d 0a 67 44 34 62 4a 4b 57 69 7a 75 54 54 47 53 79 47 4b 6e 75 75 45 32 65 35 37 4b 35 77 49 6b 46 48 4f 30 36 78 45 59 6d 69 6f 68 6a 47 41 62 34 4e 51 2f 42 76 76 75 62 57 2b 67 68 36 62 50 7a 76 74 78 62 Data Ascii: ef='https://s0.wp.com/_static/??-eJyNkdFOwzAMRX+INHQbiBfEtzipFbzZaeQkm/L3pENM3aYBL5GunWN f2/aUjJ9jwVisVJO4BorZnpKfxWQhxnajBp/zk11hjudwAQX0gIViMA7U9q/XkTv4hwu1S4caekbRHsfNsB021lXiaen107dgD4b JKWizuTTGSyGKnuuE2e57K5wIkFHO06xEYmiohjGAb4NQ/BvvubW+gh6bPzvtxb
2022-01-14 22:59:43 UTC	10	IN	Data Raw: 35 35 2c 38 31 2c 32 32 34 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 6c 69 67 68 74 2d 67 72 65 65 6e 2d 63 79 61 6e 2d 74 6f 2d 76 69 76 69 64 2d 67 72 65 65 6e 2d 63 79 61 6e 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 31 33 35 64 65 67 2c 72 67 62 28 31 32 32 2c 32 32 30 2c 31 38 30 29 20 30 25 2c 72 67 62 28 30 2c 32 30 38 2c 31 33 30 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 61 6d 62 65 72 2d 74 6f 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 31 33 35 64 65 67 2c 72 67 62 61 28 32 35 32 2c 31 38 35 2c 30 2c 31 29 20 Data Ascii: 55,81,224) 100%);--wp--preset--gradient--light-green-cyan-to-vivid-green-cyan: linear-gradient(135deg,rgb(12 2,220,180) 0%,rgb(0,208,130) 100%);--wp--preset--gradient--luminous-vivid-amber-to-luminous-vivid-orange: linear-gradien t(135deg,rgba(252,185,0,1)
2022-01-14 22:59:43 UTC	11	IN	Data Raw: 28 32 2c 33 2c 31 32 39 29 20 30 25 2c 72 67 62 28 34 30 2c 31 31 36 2c 32 35 32 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 68 61 72 64 2d 64 69 61 67 6f 6e 61 6c 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 20 62 6f 74 74 6f 6d 20 72 69 67 68 74 2c 20 23 31 61 31 61 31 61 20 34 39 2e 39 25 2c 20 23 66 61 66 61 66 61 20 35 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 68 61 72 64 2d 64 69 61 67 6f 6e 61 6c 2d 69 6e 76 65 72 74 65 64 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 74 6f 20 74 6f 70 20 6c 65 66 74 2c 20 23 31 61 31 61 31 61 20 34 39 2e 39 25 2c 20 23 66 61 66 61 66 61 20 35 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 Data Ascii: (2,3,129) 0%,rgb(40,116,252) 100%);--wp--preset--gradient--hard-diagonal: linear-gradient(to bottom right, # 1a1a1a 49.9%, #fafafa 50%);--wp--preset--gradient--hard-diagonal-inverted: linear-gradient(to top left, #1a1a1a 49.9%, # fafafa 50%);--wp--preset--g
2022-01-14 22:59:43 UTC	13	IN	Data Raw: 77 70 2d 2d 70 72 65 73 65 74 2d 2d 64 75 6f 74 6f 6e 65 2d 2d 62 6c 75 65 2d 6f 72 61 6e 67 65 3a 20 75 72 6c 28 27 23 77 70 2d 64 75 6f 74 6f 6e 65 2d 62 6c 75 65 2d 6f 72 61 6e 67 65 27 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 73 6d 61 6c 6c 3a 20 31 36 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 6d 65 64 69 75 6d 3a 20 32 30 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 6c 61 72 67 65 3a 20 32 34 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 78 2d 6c 61 72 67 65 3a 20 34 32 70 78 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 2d 74 69 6e 79 3a 20 31 34 70 78 3b 2d 2d 77 Data Ascii: wp--preset--duotone--blue-orange: url('#wp-duotone-blue-orange');--wp--preset--font-size--small: 16px;--wp-- preset--font-size--medium: 20px;--wp--preset--font-size--large: 24px;--wp--preset--font-size--x-large: 42px;--wp--preset--font- size--tiny: 14px;--w

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	14	IN	Data Raw: 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 70 72 69 6d 61 72 79 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 73 65 63 6f 6e 64 61 72 79 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 73 65 63 6f 6e 64 61 72 79 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 66 6f 72 65 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 66 6f 72 65 67 72 6f 75 6e 64 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 74 65 72 74 69 61 72 79 2d 63 6f 6c 6f 72 7b 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d Data Ascii: or: var(--wp--preset--color--primary) !important;}.has-secondary-color{color: var(--wp--preset--color--secondary) !important;}.has-foreground-color{color: var(--wp--preset--color--foreground) !important;}.has-tertiary-color{color: var(--wp--preset--color-
2022-01-14 22:59:43 UTC	15	IN	Data Raw: 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 70 61 6c 65 2d 63 79 61 6e 2d 62 6c 75 65 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 76 69 76 69 64 2d 63 79 61 6e 2d 62 6c 75 65 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 76 69 76 69 64 2d 70 75 72 70 6c 65 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 76 69 76 69 64 2d 70 75 72 70 6c 65 29 20 21 69 6d 70 Data Ascii: --wp--preset--color--pale-cyan-blue) !important;}.has-vivid-cyan-blue-background-color{background-color: var(--wp--preset--color--vivid-cyan-blue) !important;}.has-vivid-purple-background-color{background-color: var(--wp--preset--color--vivid-purple) !imp
2022-01-14 22:59:43 UTC	17	IN	Data Raw: 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 61 6d 62 65 72 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 6c 69 67 68 74 2d 67 72 65 65 6e 2d 63 79 61 6e 2d 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 6c 69 67 68 74 2d 67 72 65 65 6e 2d 63 79 61 6e 2d 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 63 6f 6c 6f 72 2d 2d 76 69 76 69 64 2d 67 72 65 65 6e 2d 63 79 61 6e 2d 62 6c 75 65 29 20 21 69 6d Data Ascii: (--wp--preset--color--luminous-vivid-amber) !important;}.has-light-green-cyan-border-color{border-color: var(--wp--preset--color--light-green-cyan) !important;}.has-vivid-green-cyan-border-color{border-color: var(--wp--preset--color--vivid-green-cyan) !im
2022-01-14 22:59:43 UTC	18	IN	Data Raw: 72 6f 75 6e 64 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 61 6d 62 65 72 2d 74 6f 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 2d 74 6f 2d 76 69 76 69 64 2d 72 65 64 2d 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 6c 75 6d 69 6e 6f 75 73 2d 76 69 76 69 64 2d 6f 72 61 6e 67 65 2d 74 6f 2d 76 69 76 69 64 2d 72 65 64 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 Data Ascii: round{background: var(--wp--preset--gradient--luminous-vivid-amber-to-luminous-vivid-orange) !important;}.has-luminous-vivid-orange-to-vivid-red-gradient-background{background: var(--wp--preset--gradient--luminous-vivid-orange-to-vivid-red) !important;}.h
2022-01-14 22:59:43 UTC	19	IN	Data Raw: 76 65 72 74 65 64 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 68 61 72 64 2d 68 6f 72 69 7a 6f 6e 74 61 6c 2d 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 68 61 72 64 2d 68 6f 72 69 7a 6f 6e 74 61 6c 2d 69 6e 76 65 72 74 65 64 29 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 2e 68 61 73 2d 68 61 72 64 2d 68 6f 72 69 7a 6f 6e 74 61 6c 2d 69 6e 76 65 72 74 65 64 2d 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 76 61 72 28 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 68 61 72 64 2d 68 6f 72 69 7a 6f 6e 74 61 6c 2d 69 6e 76 65 72 74 65 64 29 20 21 69 6d 70 6f 72 74 61 6e Data Ascii: verted) !important;}.has-hard-horizontal-gradient-background{background: var(--wp--preset--gradient--hard-horizontal) !important;}.has-hard-horizontal-inverted-gradient-background{background: var(--wp--preset--gradient--hard-horizontal-inverted) !importan
2022-01-14 22:59:43 UTC	21	IN	Data Raw: 68 65 65 74 27 20 69 64 3d 27 61 6c 6c 2d 63 73 73 2d 32 2d 31 27 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 73 31 2e 77 70 2e 63 6f 6d 2f 5f 73 74 61 74 69 63 2f 3f 3f 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 6d 75 2d 70 6c 75 67 69 6e 73 2f 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2f 63 73 73 2f 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2e 63 73 73 2c 2f 69 2f 6e 6f 74 69 63 6f 6e 73 2f 6e 6f 74 69 63 6f 6e 73 2e 63 73 73 3f 6d 3d 31 34 33 36 37 38 33 32 38 31 6a 26 63 73 73 6d 69 6e 69 66 79 3d 79 65 73 27 20 74 79 70 65 3d 27 74 65 78 74 2f 63 73 73 27 20 6d 65 64 69 61 3d 27 61 6c 6c 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 69 64 3d 27 73 65 65 Data Ascii: heet' id='all-css-2-1' href='https://s1.wp.com/_static/??/wp-content/mu-plugins/comment-likes/css/comment-likes.css,/i/noticons/noticons.css?m=1436783281j&cssminify=yes' type='text/css' media='all' /><link crossorigin="anonymous" rel='stylesheet' id='see
2022-01-14 22:59:43 UTC	22	IN	Data Raw: 6d 69 62 6f 6c 64 2c 62 6f 6c 64 2c 69 74 61 6c 69 63 2c 62 6f 6c 64 69 74 61 6c 69 63 2c 65 78 74 72 61 62 6f 6c 64 2c 62 6c 61 63 6b 7c 27 29 3b 3a 72 6f 6f 74 20 7b 20 2d 2d 66 6f 6e 74 2d 68 65 61 64 69 6e 67 73 3a 20 52 75 62 69 6b 3b 20 2d 2d 66 6f 6e 74 2d 62 61 73 65 3a 20 52 6f 62 6f 74 6f 3b 20 2d 2d 66 6f 6e 74 2d 68 65 61 64 69 6e 67 73 2d 64 65 66 61 75 6c 74 3a 20 2d 61 70 70 6c 65 2d 73 79 73 74 65 6d 2c 42 6c 69 6e 6b 4d 61 63 53 79 73 74 65 6d 46 6f 6e 74 2c 22 53 65 67 6f 65 20 55 49 22 2c 52 6f 62 6f 74 6f 2c 4f 78 79 67 65 6e 2d 53 61 6e 73 2c 55 62 75 6e 74 75 2c 43 61 6e 74 61 72 65 6c 6c 2c 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 73 61 6e 73 2d 73 65 72 69 66 3b 20 2d 2d 66 6f 6e 74 2d 62 61 73 65 2d 64 65 66 61 75 6c 74 Data Ascii: mibold,bold,italic,bolditalic,extrabold,black|');:root { --font-headings: Rubik; --font-base: Roboto; --font-headings-default: -apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,Oxygen-Sans,Ubuntu,Cantarell,"Helvetica Neue",sans-serif; --font-base-default
2022-01-14 22:59:43 UTC	23	IN	Data Raw: 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3e 0a 09 77 69 6e 64 6f 77 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 20 27 44 4f 4d 43 6f 6e 74 65 6e 74 4c 6f 61 64 65 64 27 2c 20 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 09 09 72 6c 74 49 6e 69 74 69 61 6c 69 7a 65 28 20 7b 22 74 6f 6b 65 6e 22 3a 6e 75 6c 6c 2c 22 69 66 72 61 6d 65 4f 72 69 67 69 6e 73 22 3a 5b 22 68 74 74 70 73 3a 5c 2f 5c 2f 77 69 64 67 65 74 73 2e 77 70 2e 63 6f 6d 22 5d 7d 20 29 3b 0a 09 7d 20 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 45 64 69 74 55 52 49 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 64 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 52 53 44 22 20 68 72 65 66 3d 22 68 74 74 70 Data Ascii: script type='text/javascript'>window.addEventListener('DOMContentLoaded', function() {rltInitialize({"token":null,"iframeOrigins":["https:\/\/widgets.wp.com"]});});</script><link rel="EditURI" type="application/rsd+xml" title="RSD" href="http

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	25	IN	Data Raw: 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d 2f 32 30 32 32 2f 30 31 2f 75 6e 6e 61 6d 65 64 2e 70 6e 67 3f 77 3d 36 36 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 3a 61 6c 74 22 20 63 6f 6e 74 65 6e 74 3d 22 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 55 53 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 74 65 78 74 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 70 72 69 64 65 72 65 63 6f 76 65 72 79 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 73 3a 2f 2f 70 72 69 64 65 72 65 63 6f 76 65 72 79 37 37 39 34 31 Data Ascii: wordpress.com/2022/01/unnamed.png?w=668" /><meta property="og:image:alt" content="" /><meta property="og:locale" content="en_US" /><meta name="twitter:text:title" content="priderecovery" /><meta name="twitter:image" content="https://priderecovery77941
2022-01-14 22:59:43 UTC	26	IN	Data Raw: 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 61 6d 65 3d 53 75 62 73 63 72 69 62 65 3b 61 63 74 69 6f 6e 2d 75 72 69 3d 68 74 74 70 73 3a 2f 2f 70 72 69 64 65 72 65 63 6f 76 65 72 79 37 37 39 34 31 33 30 31 33 2e 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d 2f 66 65 65 64 2f 3b 69 63 6f 6e 2d 75 72 69 3d 68 74 74 70 73 3a 2f 2f 73 31 2e 77 70 2e 63 6f 6d 2f 69 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6d 73 61 70 70 6c 69 63 61 74 69 6f 6e 2d 74 61 73 6b 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 61 6d 65 3d 53 69 67 6e 20 75 70 20 66 6f 72 20 61 20 66 72 65 65 20 62 6c 6f 67 3b 61 63 74 69 6f 6e 2d 75 72 69 3d 68 74 74 70 3a 2f 2f 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d 2f 73 69 67 6e 75 70 2f 3b 69 63 6f 6e 2d 75 72 69 3d 68 74 74 70 Data Ascii: " content="name=Subscribe;action-uri=https://priderecovery779413013.wordpress.com/feed/;icon-uri=https://s1.wp.com/i/favicon.ico" /><meta name="msapplication-task" content="name=Sign up for a free blog;action-uri=http://wordpress.com/signup/;icon-uri=http
2022-01-14 22:59:43 UTC	27	IN	Data Raw: 2d 63 6f 6c 6f 72 2d 73 65 63 6f 6e 64 61 72 79 3a 20 23 31 61 31 61 31 61 3b 0a 09 09 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 73 65 63 6f 6e 64 61 72 79 2d 68 6f 76 65 72 3a 20 68 73 6c 28 20 30 2c 30 25 2c 32 30 2e 31 39 36 30 37 38 34 33 31 33 37 33 25 29 3b 0a 09 09 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 74 65 72 74 69 61 72 79 3a 20 23 66 61 66 61 66 61 3b 0a 09 7d 0a 0a 09 2e 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 7d 0a 2e 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 20 7b 20 63 6f 6c 6f 72 3a 20 23 31 61 31 61 31 61 3b 7d 0a 2e 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 70 72 69 6d 61 72 Data Ascii: -color-secondary: #1a1a1a;--global--color-secondary-hover: hsl(0,0%,20.196078431373%);--global--color-tertiary: #fafafa;}.global--color-background { background-color: #ffffff;}.global--color-foreground { color: #1a1a1a;}.global--color-primar
2022-01-14 22:59:43 UTC	29	IN	Data Raw: 2f 3e 3c 2f 66 69 6c 74 65 72 3e 3c 2f 64 65 66 73 3e 3c 2f 73 76 67 3e 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 30 20 30 20 30 22 20 77 69 64 74 68 3d 22 30 22 20 68 65 69 67 68 74 3d 22 30 22 20 66 6f 63 75 73 61 62 6c 65 3d 22 66 61 6c 73 65 22 20 72 6f 6c 65 3d 22 6e 6f 6e 65 22 20 73 74 79 6c 65 3d 22 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 20 6c 65 66 74 3a 20 2d 39 39 39 39 70 78 3b 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 22 20 3e 3c 64 65 66 73 3e 3c 66 69 6c 74 65 72 20 69 64 3d 22 77 70 2d 64 75 6f 74 6f 6e 65 2d 67 72 61 79 73 63 61 6c 65 22 3e Data Ascii: /></filter></defs></svg><svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 0 0" width="0" height="0" focusable="false" role="none" style="visibility: hidden; position: absolute; left: -9999px; overflow: hidden;" ><defs><filter id="wp-duotone-grayscale">
2022-01-14 22:59:43 UTC	30	IN	Data Raw: 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 31 20 31 22 20 2f 3e 3c 2f 66 65 43 6f 6d 70 6f 6e 65 6e 74 54 72 61 6e 73 66 65 72 3e 3c 66 65 43 6f 6d 70 6f 73 69 74 65 20 69 6e 32 3d 22 53 6f 75 72 63 65 47 72 61 70 68 69 63 22 20 6f 70 65 72 61 74 6f 72 3d 22 69 6e 22 20 2f 3e 3c 2f 66 69 6c 74 65 72 3e 3c 2f 64 65 66 73 3e 3c 2f 73 76 67 3e 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 30 20 30 22 20 77 69 64 74 68 3d 22 30 22 20 68 65 69 67 68 74 3d 22 30 22 20 66 6f 63 75 73 61 62 6c 65 3d 22 66 61 6c 73 65 22 20 72 6f 6c 65 3d 22 6e 6f 6e 65 22 20 73 74 79 6c 65 3d 22 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 Data Ascii: e="table" tableValues="1 1" /></feComponentTransfer><feComposite in2="SourceGraphic" operator="in" /></filter></defs></svg><svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 0 0" width="0" height="0" focusable="false" role="none" style="visibility: hidd
2022-01-14 22:59:43 UTC	31	IN	Data Raw: 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 30 20 30 2e 36 34 37 30 35 38 38 32 33 35 32 39 34 31 22 20 2f 3e 3c 66 65 46 75 6e 63 42 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 30 20 31 22 20 2f 3e 3c 66 65 46 75 6e 63 41 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 31 20 31 22 20 2f 3e 3c 2f 66 65 43 6f 6d 70 6f 6e 65 6e 74 54 72 61 6e 73 66 65 72 3e 3c 66 65 43 6f 6d 70 6f 73 69 74 65 20 69 6e 32 3d 22 53 6f 75 72 63 65 47 72 61 70 68 69 63 22 20 6f 70 65 72 61 74 6f 72 3d 22 69 6e 22 20 2f 3e 3c 2f 66 69 6c 74 65 72 3e 3c 2f 64 65 66 73 3e 3c 2f 73 76 67 3e 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 Data Ascii: e" tableValues="0 0.64705882352941" /><feFuncB type="table" tableValues="0 1" /><feFuncA type="table" tableValues="1 1" /></feComponentTransfer><feComposite in2="SourceGraphic" operator="in" /></filter></defs></svg><svg xmlns="http://www.w3.org/2000/svg"
2022-01-14 22:59:43 UTC	33	IN	Data Raw: 3c 66 65 43 6f 6d 70 6f 6e 65 6e 74 54 72 61 6e 73 66 65 72 20 63 6f 6c 6f 72 2d 69 6e 74 65 72 70 6f 6c 61 74 69 6f 6e 2d 66 69 6c 74 65 72 73 3d 22 73 52 47 42 22 20 3e 3c 66 65 46 75 6e 63 52 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 30 2e 36 35 30 39 38 30 33 39 32 31 35 36 38 36 20 30 2e 34 30 33 39 32 31 35 36 38 36 32 37 34 35 22 20 2f 3e 3c 66 65 46 75 6e 63 47 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 30 20 31 22 20 2f 3e 3c 66 65 46 75 6e 63 42 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 6c 65 56 61 6c 75 65 73 3d 22 30 2e 34 34 37 30 35 38 38 32 33 35 32 39 34 31 20 30 2e 34 22 20 2f 3e 3c 66 65 46 75 6e 63 41 20 74 79 70 65 3d 22 74 61 62 6c 65 22 20 74 61 62 Data Ascii: <feComponentTransfer color-interpolation-filters="sRGB" ><feFuncR type="table" tableValues="0.6509 8039215686 0.40392156862745" /><feFuncG type="table" tableValues="0 1" /><feFuncB type="table" tableValues="0.44705882352941 0.4" /><feFuncA type="table" tab
2022-01-14 22:59:43 UTC	34	IN	Data Raw: 6d 61 69 6e 22 3e 0a 0a 09 09 09 0a 3c 61 72 74 69 63 6c 65 20 69 64 3d 22 70 6f 73 74 2d 32 22 20 63 6c 61 73 73 3d 22 70 6f 73 74 2d 32 20 70 61 67 65 20 74 79 70 65 2d 70 61 67 65 20 73 74 61 74 75 73 2d 70 75 62 6c 69 73 68 20 68 65 6e 74 72 79 20 65 6e 74 72 79 22 3e 0a 09 0a 09 0a 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 22 3e 0a 09 09 0a 3c 70 3e 20 3c 2f 70 3e 0a 0a 0a 0a 3c 66 69 67 75 72 65 20 63 6c 61 73 73 3d 22 77 70 2d 62 6c 6f 63 6b 2d 69 6d 61 67 65 20 73 69 7a 65 2d 6c 61 72 67 65 22 3e 3c 69 6d 67 20 64 61 74 61 2d 61 74 74 61 63 68 6d 65 6e 74 2d 69 64 3d 22 36 22 20 64 61 74 61 2d 70 65 72 6d 61 6c 69 6e 6b 3d 22 68 74 74 70 73 3a 2f 2f 70 72 69 64 65 72 65 63 6f 76 65 72 79 37 37 39 34 31 33 30 31 Data Ascii: main"><article id="post-2" class="post-2 page type-page status-publish hentry entry"> <figure class="wp-block-image size-large"><img data-attachment-id="6" data-permalink="https://priderecovery77941301

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	35	IN	Data Raw: 2c 20 68 74 74 70 73 3a 2f 2f 70 72 69 64 65 72 65 63 6f 76 65 72 79 37 37 39 34 31 33 30 31 33 2e 66 69 6c 65 73 2e 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d 2f 32 30 32 32 2f 30 31 2f 75 6e 6e 61 6d 65 64 2e 70 6e 67 3f 77 3d 33 30 30 20 33 30 30 77 22 20 73 69 7a 65 73 3d 22 28 6d 61 78 2d 77 69 64 74 68 3a 20 36 36 38 70 78 29 20 31 30 30 76 77 2c 20 36 36 38 70 78 22 20 2f 3e 3c 2f 66 69 67 75 72 65 3e 0a 0a 0a 0a 3c 70 3e e2 80 9d 52 61 6e 64 79 20 48 65 72 66 69 65 6c 64 e2 80 9d 20 72 68 65 72 66 69 65 6c 64 40 70 72 69 64 65 72 65 63 6f 76 65 72 79 63 65 6e 74 65 72 2e 63 6f 6d 20 48 61 73 20 73 65 6e 74 20 79 6f 75 20 61 6e 20 65 6e 63 72 79 70 74 65 64 20 6d 65 73 73 61 67 65 2e 3c 2f 70 3e 0a 0a 0a 0a 3c 70 3e 53 75 62 6a 65 63 74 3a 20 50 72 69 Data Ascii: , https://priderecovery779413013.files.wordpress.com/2022/01/unnamed.png?w=300 300w" sizes="(max-width: 668px) 100vw, 668px" /></figure> Randy Herfield rherfield@priderecoverycenter.com Has sent you an encrypted message. Subject: Pri
2022-01-14 22:59:43 UTC	37	IN	Data Raw: 47 65 74 20 73 74 61 72 74 65 64 3c 2f 61 3e 3c 61 20 63 6c 61 73 73 3d 22 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 2d 6c 69 6e 6b 22 20 74 61 62 69 6e 64 65 78 3d 22 2d 31 22 20 61 72 69 61 2d 6c 61 62 65 6c 3d 22 43 72 65 61 74 65 20 79 6f 75 72 20 77 65 62 73 69 74 65 20 61 74 20 57 6f 72 64 50 72 65 73 73 2e 63 6f 6d 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d 2f 73 74 61 72 74 2f 3f 72 65 66 3d 6d 61 72 6b 65 74 69 6e 67 5f 62 61 72 22 3e 3c 2f 61 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 27 2f 2f 30 2e 67 72 61 76 61 74 61 72 2e 63 6f 6d 2f 6a 73 2f 67 70 72 6f 66 69 6c 65 73 2e 6a 73 3f 76 65 72 3d 32 30 32 32 30 32 79 27 20 69 64 3d 27 67 72 6f 66 69 6c 65 73 2d 63 61 72 64 73 2d 6a 73 27 3e Data Ascii: Get started <script src='//0.gravatar.com/js/gprofiles.js?ver=202202y' id='grofiles-cards-js'>
2022-01-14 22:59:43 UTC	38	IN	Data Raw: 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 34 20 32 34 22 3e 3c 67 3e 3c 70 61 74 68 20 64 3d 22 4d 37 20 31 32 63 30 20 31 2e 31 30 34 2d 2e 38 39 36 20 32 2d 32 20 32 73 2d 32 2d 2e 38 39 36 2d 32 2d 32 20 2e 38 39 36 2d 32 20 32 2d 32 20 32 20 2e 38 39 36 20 32 20 32 7a 6d 31 32 2d 32 63 2d 31 2e 31 30 34 20 30 2d 32 20 2e 38 39 36 2d 32 20 32 2d 32 20 32 73 2e 38 39 36 20 32 20 32 20 32 20 32 2d 2e 38 39 36 20 32 2d 32 2d 2e 38 39 36 2d 32 2d 32 2d 32 7a 6d 2d 37 20 30 63 2d 31 2e 31 30 34 20 30 2d 32 20 2e 38 39 36 2d 32 20 32 73 2e 38 39 36 20 32 20 32 20 32 20 32 2d 2e 38 39 36 20 32 2d 32 2d 2e 38 39 36 2d 32 2d 32 2d 32 7a 22 2f 3e 3c 2f 67 3e 3c 2f 73 76 67 3e 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 63 74 Data Ascii: rg/2000/svg" viewBox="0 0 24 24"><g><path d="M7 12c0 1.104-.896 2-2 2s-2-.896-2-2 .896-2 2-2 2 .896 2 2zm12-2c-1.104 0-2 .896-2 2s.896 2 2 2 2-.896 2-2-.896-2-2-2zm-7 0c-1.104 0-2 .896-2 2s.896 2 2 2 2-.896 2-2-.896-2-2-2z"/></g></svg><div class="actn
2022-01-14 22:59:43 UTC	39	IN	Data Raw: 38 34 38 2d 36 2e 38 34 38 63 31 2e 38 38 35 20 31 2e 39 32 38 20 33 2e 38 37 34 20 33 2e 37 35 33 20 35 2e 39 37 37 20 35 2e 34 35 6c 31 2e 34 32 35 20 31 2e 31 34 38 20 31 2e 35 2d 31 2e 35 2d 31 2e 31 35 2d 31 2e 34 32 35 63 2d 31 2e 36 39 35 2d 32 2e 31 30 33 2d 33 2e 35 32 2d 34 2e 30 39 32 2d 35 2e 34 34 38 2d 35 2e 39 37 37 7a 22 2f 3e 3c 2f 67 3e 3c 2f 73 76 67 3e 09 09 09 09 09 09 09 09 09 3c 73 70 61 6e 3e 43 75 73 74 6f 6d 69 7a 65 3c 2f 73 70 61 6e 3e 0a 09 09 09 09 09 09 09 09 3c 2f 61 3e 0a 09 09 09 09 09 09 09 3c 2f 6c 69 3e 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 3c 6c 69 20 63 6c 61 73 73 3d 22 61 63 74 6e 62 72 2d 73 69 67 6e 75 70 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 6f 72 64 70 72 65 73 73 2e 63 6f 6d Data Ascii: 848-6.848c1.885 1.928 3.874 3.753 5.977 5.45l1.425 1.148 1.5-1.5-1.15-1.425c-1.695-2.103-3.52-4.092-5.448-5.977z"/></g></svg>Customize <li class="actnbr-signup"><a href="https://wordpress.com
2022-01-14 22:59:43 UTC	41	IN	Data Raw: 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 09 09 09 3c 64 69 76 20 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 6c 6f 61 64 69 6e 67 2d 6f 76 65 72 6c 61 79 22 3e 0a 09 09 09 3c 64 69 76 20 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 6c 6f 61 64 69 6e 67 2d 77 72 61 70 70 65 72 22 3e 0a 09 09 09 3c 73 70 61 6e 20 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 6c 69 62 72 61 72 79 2d 6c 6f 61 64 69 6e 67 22 3e 26 6e 62 73 70 3b 3c 2f 73 70 61 6e 3e 0a 09 09 09 3c 2f 64 69 76 3e 0a 09 09 3c 2f 64 69 76 3e 0a 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 6f 76 65 72 6c 61 79 22 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 22 3e 0a 0a 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f Data Ascii:);</script> <div class="jp-caro
2022-01-14 22:59:43 UTC	42	IN	Data Raw: 39 38 31 34 20 37 2e 34 31 4c 31 30 2e 30 30 31 32 20 36 4c 31 35 2e 39 37 31 38 20 31 32 4c 31 30 2e 30 30 31 32 20 31 38 4c 38 2e 35 39 38 31 34 20 31 36 2e 35 39 5a 22 20 66 69 6c 6c 3d 22 77 68 69 74 65 22 2f 3e 0a 09 09 09 09 09 09 3c 2f 6d 61 73 6b 3e 0a 09 09 09 09 09 09 3c 67 20 6d 61 73 6b 3d 22 75 72 6c 28 23 6d 61 73 6b 4e 65 78 74 29 22 3e 0a 09 09 09 09 09 09 09 3c 72 65 63 74 20 78 3d 22 30 2e 33 34 33 37 35 22 20 77 69 64 74 68 3d 22 32 33 2e 38 38 32 32 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 66 69 6c 6c 3d 22 23 46 46 46 46 46 46 22 2f 3e 0a 09 09 09 09 09 09 3c 2f 67 3e 0a 09 09 09 09 09 3c 2f 73 76 67 3e 0a 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 3c 21 2d 2d 20 54 68 65 20 6d 61 69 6e 20 63 6c 6f 73 65 Data Ascii: 9814 7.41L10.0012 6L15.9718 12L10.0012 18L8.59814 16.59Z" fill="white"/></mask><g mask="url(#maskNext)"><rect x="0.34375" width="23.8822" height="24" fill="#FFFFFF"/></g></svg> ... The main close
2022-01-14 22:59:43 UTC	44	IN	Data Raw: 65 6c 2d 69 63 6f 6e 2d 69 6e 66 6f 22 20 61 72 69 61 2d 6c 61 62 65 6c 3d 22 54 6f 67 67 6c 65 20 70 68 6f 74 6f 20 6d 65 74 61 64 61 74 61 20 76 69 73 69 62 69 6c 69 74 79 22 3e 0a 09 09 09 09 09 09 09 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 69 63 6f 6e 22 3e 0a 09 09 09 09 09 09 09 09 3c 73 76 67 20 77 69 64 74 68 3d 22 32 35 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 35 20 32 34 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 3e 0a 09 09 09 09 09 09 09 09 3c 6d 61 73 6b 20 69 64 3d 22 6d 61 73 6b 49 6e 66 6f 22 20 6d 61 73 6b 2d 74 79 70 65 3d 22 61 6c 70 68 61 22 20 6d 61 73 6b Data Ascii: el-icon-info" aria-label="Toggle photo metadata visibility"><svg width="25" height="24" viewBox="0 0 25 24" fill="none" xmlns="http://www.w3.org/2000/svg"><mask id="maskInfo" mask-type="alpha" mask
2022-01-14 22:59:43 UTC	45	IN	Data Raw: 64 22 20 64 3d 22 4d 34 2e 33 32 37 31 20 32 48 32 30 2e 32 34 38 36 43 32 31 2e 33 34 33 32 20 32 32 2e 32 33 38 38 20 32 2e 39 20 32 32 2e 32 33 38 38 20 34 56 31 36 43 32 32 2e 32 33 38 38 20 31 37 2e 31 20 32 31 2e 33 34 33 32 20 31 38 20 32 30 2e 32 34 38 36 20 31 38 48 36 2e 33 31 37 32 39 4c 32 2e 33 33 36 39 31 20 32 32 56 34 43 32 2e 33 33 36 39 31 20 32 2e 39 20 33 2e 32 33 32 35 20 32 20 34 2e 33 32 37 31 20 32 5a 4d 36 2e 33 31 37 32 39 20 31 36 48 32 30 2e 32 34 38 36 56 34 48 34 2e 33 32 37 31 56 31 38 4c 36 2e 33 31 37 32 39 20 31 36 5a 22 20 66 69 6c 6c 3d 22 77 68 69 74 65 22 2f 3e 0a 09 09 09 09 09 09 09 09 3c 2f 6d 61 73 6b 3e 0a 0d 0a 32 33 62 32 0d 0a 09 09 09 09 09 09 09 09 3c 67 20 6d 61 73 6b 3d 22 75 72 6c 28 23 6d 61 Data Ascii: d" d="M4.3271 2H20.2486C21.3432 2 22.2388 2.9 22.2388 4V16C22.2388 17.1 21.3432 18 20.2486 18H6.31729L2.33691 22V4C2.33691 2.9 3.2325 2 4.3271 2ZM6.31729 16H20.2486V4H4.3271V18L6.31729 16Z" fill="white"/></mask>23b2<g mask="url(#ma

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	46	IN	Data Raw: 09 09 09 09 09 09 09 09 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d 66 69 65 6c 64 20 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d 74 65 78 74 61 72 65 61 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d 63 6f 6d 6d 65 6e 74 2d 66 69 65 6c 64 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 70 6c 61 63 65 68 6f 6c 64 65 72 3d 22 57 72 69 74 65 20 61 20 43 6f 6d 6d 65 6e 74 2e 2e 2e 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 3e 3c 2f 74 65 78 74 61 72 65 61 3e 0a 09 09 09 09 09 09 09 09 09 09 09 3c 64 69 76 20 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d Data Ascii: class="jp-carousel-comment-form-field jp-carousel-comment-form-textarea"id="jp-carousel-comment-form-comment-field"placeholder="Write a Comment..."></textarea><div id="jp-carousel-comment-form-
2022-01-14 22:59:43 UTC	48	IN	Data Raw: 09 09 09 09 09 09 09 09 6e 61 6d 65 3d 22 73 75 62 6d 69 74 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d 62 75 74 74 6f 6e 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 69 64 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 63 6f 6d 6d 65 6e 74 2d 66 6f 72 6d 2d 62 75 74 74 6f 6e 2d 73 75 62 6d 69 74 22 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 76 61 6c 75 65 3d 22 50 6f 73 74 20 43 6f 6d 6d 65 6e 74 22 20 2f 3e 0a 09 09 09 09 09 09 09 09 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 09 09 09 09 09 3c 2f 66 6f 72 6d 3e 0a 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 09 09 09 09 09 09 Data Ascii: name="submit"class="jp-carousel-comment-form-button"id="jp-carousel-comment-form-button-submit"value="Post Comment" /> </form>
2022-01-14 22:59:43 UTC	49	IN	Data Raw: 3d 22 23 46 46 46 46 46 46 22 2f 3e 0a 09 09 09 09 09 09 09 09 3c 2f 67 3e 0a 09 09 09 09 09 09 09 09 3c 2f 73 76 67 3e 0a 09 09 09 09 09 09 09 09 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 64 6f 77 6e 6c 6f 61 64 2d 74 65 78 74 22 3e 3c 2f 73 70 61 6e 3e 0a 09 09 09 09 09 09 09 09 3c 2f 61 3e 0a 09 09 09 09 09 09 09 09 3c 64 69 76 20 63 6c 61 73 73 3d 22 6a 70 2d 63 61 72 6f 75 73 65 6c 2d 69 6d 61 67 65 2d 6d 61 70 22 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 22 3e 3c 2f 64 69 76 3e 0a 09 09 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 09 3c 2f 64 69 76 3e 0a 09 09 09 3c 2f 64 69 76 3e 0a 09 09 3c 2f 64 69 76 3e 0a 0a 09 09 3c 2f 64 69 76 3e 0a 09 09 3c 6c 69 6e 6b 20 Data Ascii: ="#FFFFFF"/></g></svg> <link
2022-01-14 22:59:43 UTC	50	IN	Data Raw: 30 7d 3c 73 70 61 6e 20 63 6c 61 73 73 3d 5c 22 70 68 6f 74 6f 2d 73 69 7a 65 2d 74 69 6d 65 73 5c 22 3e 5c 75 30 30 64 37 3c 5c 2f 73 70 61 6e 3e 7b 31 7d 3c 5c 2f 73 70 61 6e 3e 22 2c 22 6e 6f 5f 63 6f 6d 6d 65 6e 74 5f 74 65 78 74 22 3a 22 50 6c 65 61 73 65 20 62 65 20 73 75 72 65 20 74 6f 20 73 75 62 6d 69 74 20 73 6f 6d 65 20 74 65 78 74 20 77 69 74 68 20 79 6f 75 72 20 63 6f 6d 6d 65 6e 74 2e 22 2c 22 6e 6f 5f 63 6f 6d 6d 65 6e 74 5f 65 6d 61 69 6c 22 3a 22 50 6c 65 61 73 65 20 70 72 6f 76 69 64 65 20 61 6e 20 65 6d 61 69 6c 20 61 64 64 72 65 73 73 20 74 6f 20 63 6f 6d 6d 65 6e 74 2e 22 2c 22 6e 6f 5f 63 6f 6d 6d 65 6e 74 5f 61 75 74 68 6f 72 22 3a 22 50 6c 65 61 73 65 20 70 72 6f 76 69 64 65 20 79 6f 75 72 20 6e 61 6d 65 20 74 6f 20 63 6f 6d 6d Data Ascii: 0}<span class=\"photo-size-times\">\u00d7<\/span>{1}<\/span>","no_comment_text":"Please be sure to submit some text with your comment.","no_comment_email":"Please provide an email address to comment.","no_comment_author":"Please provide your name to comme
2022-01-14 22:59:43 UTC	52	IN	Data Raw: 69 6e 64 6f 77 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 26 26 77 69 6e 64 6f 77 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 68 61 73 68 63 68 61 6e 67 65 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 65 3d 6c 6f 63 61 74 69 6f 6e 2e 68 61 73 68 2e 73 75 62 73 74 72 69 6e 67 28 31 29 3b 2f 5e 5b 41 2d 7a 30 2d 39 5f 2d 5d 2b 24 2f 2e 74 65 73 74 28 65 29 26 26 28 74 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 65 29 29 26 26 28 2f 5e 28 3f 3a 61 7c 73 65 6c 65 63 74 7c 69 6e 70 75 74 7c 62 75 74 74 6f 6e 7c 74 65 78 74 61 72 65 61 29 24 2f 69 2e 74 65 73 74 28 74 2e 74 61 67 4e 61 6d 65 29 7c 7c 28 74 2e 74 61 62 49 6e 64 65 78 3d 2d 31 29 2c 74 2e 66 6f 63 75 73 28 29 29 7d 2c 21 31 29 3b 0a Data Ascii: indow.addEventListener&&window.addEventListener("hashchange",function(){var t,e=location.hash.substring(1);/^[A-z0-9_-]+$/.test(e)&&(t=document.getElementById(e))&&(/^(?:a|select|input|button|textarea)$/i.test(t.tagName)||(t.tabIndex=-1),t.focus())},!1);
2022-01-14 22:59:43 UTC	53	IN	Data Raw: 30 4e 70 53 31 45 76 4f 53 78 6b 62 55 31 45 59 53 78 79 65 58 46 47 65 45 63 32 56 46 56 73 4a 6b 64 5a 61 6e 4e 6f 59 58 78 2b 4e 55 64 43 50 30 4e 34 63 56 6c 4c 56 47 4a 79 61 43 35 4f 66 6d 78 33 62 31 42 74 4d 58 6c 78 62 57 70 72 4d 48 68 62 55 6b 4a 4e 54 44 4e 58 61 48 78 6f 52 44 52 51 64 46 6c 76 27 7d 5d 29 3b 0a 5f 73 74 71 2e 70 75 73 68 28 5b 20 27 63 6c 69 63 6b 54 72 61 63 6b 65 72 49 6e 69 74 27 2c 20 27 32 30 31 36 38 36 35 36 32 27 2c 20 27 32 27 20 5d 29 3b 0a 09 3c 2f 73 63 72 69 70 74 3e 0a 3c 6e 6f 73 63 72 69 70 74 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 70 69 78 65 6c 2e 77 70 2e 63 6f 6d 2f 62 2e 67 69 66 3f 76 3d 6e 6f 73 63 72 69 70 74 22 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 70 78 3b 77 69 64 74 68 Data Ascii: 0NpS1EvOSxkbU1EYSxyeXFGeEc2VFVsJkdZanNoYXx+NUdCP0N4cVlLVGJyaC5Ofmx3b1BtMXlxbWprMHhbUkJNTDNXaHxoRDRQdFlv'}]);_stq.push(['clickTrackerInit', '201686562', '2']);</script><noscript><img src="https://pixel.wp.com/b.gif?v=noscript" style="height:1px;width

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49759	142.250.184.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty 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-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:43 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	4	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 14 Jan 2022 22:59:43 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: script-src 'report-sample' 'nonce-U9tJAewFLtlK4DIl7qPoHg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-U9tJAewFLtlK4DIl7qPoHg' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-14 22:59:43 UTC	5	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-01-14 22:59:43 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49756	142.250.181.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty 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-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:43 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-FNmMCHci/19XDC/udhgBSA' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 14 Jan 2022 22:59:43 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5492 X-Daystart: 53983 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-14 22:59:43 UTC	2	IN	Data Raw: 35 31 66 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 34 39 32 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 33 39 38 33 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 6d 65 64 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 51f<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5492" elapsed_seconds="53983"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:43 UTC	3	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-01-14 22:59:43 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49766	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	54	OUT	GET /_static/??-eJyNkdFOwzAMRX+INHQbiBfEtzipFbzZaeQkm/L3pENM3aYBL5GunWNf2/aUjJ9jwVisVJO4BorZnpKfxWQhxnajBp/zk11hjudwAQX0gIViMA7U9q/XkTv4hwu1S4caekbRHsfNsB021lXiaengD4bJKWizuTTGSyGKnuuE2e57K5wIkFHO06xEYmiohjGAb4NQ/BvvubW+gh6bPzvtxbAkWCxDm2sxQWm6sf3vEgrL7vIDfHWyZW89Lgnuzf+Cfd/WuaSYs+mvUBVTPjt4PvWHvI+vu3H3PL68bfdfcBLSYw==?cssminify=yes HTTP/1.1 Host: s0.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:44 UTC	62	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:44 GMT Content-Type: text/css;charset=utf-8 Content-Length: 153702 Connection: close Vary: Accept-Encoding Last-Modified: Mon, 10 Jan 2022 23:55:11 GMT Etag: "61dcc75f-25866" Expires: Wed, 11 Jan 2023 16:00:18 GMT Cache-Control: max-age=31536000 X-ac: 2.hhn _dca Access-Control-Allow-Methods: GET, HEAD Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-nc: HIT hhn 1
2022-01-14 22:59:44 UTC	62	IN	Data Raw: 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 69 6d 67 2e 77 70 2d 73 6d 69 6c 65 79 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 68 65 69 67 68 74 3a 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 77 69 64 74 68 3a 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 6d 61 72 67 69 6e 3a 30 20 2e 30 35 65 6d 20 30 20 2e 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 2d 2e 31 65 6d 20 21 69 6d 70 6f 72 74 61 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 30 20 30 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 30 20 21 69 6d 70 6f 72 74 61 6e 74 7d 68 74 6d 6c 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 39 Data Ascii: @charset "UTF-8";img.wp-smiley{border:none !important;box-shadow:none !important;height:1em !important;width:1em !important;margin:0 .05em 0 .1em !important;vertical-align:-.1em !important;background:0 0 !important;padding:0 !important}html{margin-top:49
2022-01-14 22:59:44 UTC	76	IN	Data Raw: 2c 27 53 65 67 6f 65 20 55 49 27 2c 52 6f 62 6f 74 6f 2c 4f 78 79 67 65 6e 2d 53 61 6e 73 2c 55 62 75 6e 74 75 2c 43 61 6e 74 61 72 65 6c 6c 2c 27 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 27 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 36 70 78 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 30 30 33 63 35 36 7d 2e 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 2e 76 61 72 69 61 74 69 6f 6e 2d 67 72 61 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 33 66 36 66 38 3b 63 6f 6c 6f 72 3a 23 34 66 37 34 38 65 7d 2e 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 20 2e 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 2d 74 65 78 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 Data Ascii: ,'Segoe UI',Roboto,Oxygen-Sans,Ubuntu,Cantarell,'Helvetica Neue',sans-serif;font-size:16px;text-align:center;border-bottom:1px solid #003c56}.marketing-bar.variation-gray{background:#f3f6f8;color:#4f748e}.marketing-bar .marketing-bar-text{position:relativ
2022-01-14 22:59:44 UTC	77	IN	Data Raw: 72 67 69 6e 2d 74 6f 70 3a 34 36 70 78 20 21 69 6d 70 6f 72 74 61 6e 74 3b 73 63 72 6f 6c 6c 2d 70 61 64 64 69 6e 67 2d 74 6f 70 3a 34 36 70 78 7d 2e 61 64 6d 69 6e 2d 62 61 72 2e 68 61 73 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 35 70 78 7d 2e 61 64 6d 69 6e 2d 62 61 72 2e 68 61 73 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 20 23 6d 61 72 6b 65 74 69 6e 67 62 61 72 2e 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 7b 74 6f 70 3a 34 36 70 78 7d 2e 61 64 6d 69 6e 2d 62 61 72 2e 68 61 73 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 20 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 3e 2a 5b 69 64 5d 7b 73 63 72 6f 6c 6c 2d 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 36 70 78 7d 2e 61 64 6d 69 6e 2d 62 61 72 2e 68 61 73 2d 6d 61 72 6b 65 74 69 Data Ascii: rgin-top:46px !important;scroll-padding-top:46px}.admin-bar.has-marketing-bar{margin-top:45px}.admin-bar.has-marketing-bar #marketingbar.marketing-bar{top:46px}.admin-bar.has-marketing-bar .entry-content>*[id]{scroll-margin-top:46px}.admin-bar.has-marketi

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	79	IN	Data Raw: 6e 74 79 2d 74 77 65 6e 74 79 2d 6f 6e 65 20 2e 70 72 69 6d 61 72 79 2d 6e 61 76 69 67 61 74 69 6f 6e 7b 74 6f 70 3a 63 61 6c 63 28 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 61 64 6d 69 6e 2d 62 61 72 2d 68 65 69 67 68 74 29 20 2b 20 34 35 70 78 29 7d 7d 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 2e 77 70 2d 62 6c 6f 63 6b 2d 61 72 63 68 69 76 65 73 2d 64 72 6f 70 64 6f 77 6e 20 6c 61 62 65 6c 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 61 75 64 69 6f 7b 6d 61 72 67 69 6e 3a 30 20 30 20 31 65 6d 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 61 75 64 69 6f 20 66 69 67 63 61 70 74 69 6f 6e 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 65 6d 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2e 35 65 6d 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 61 75 Data Ascii: nty-twenty-one .primary-navigation{top:calc(var(--global--admin-bar--height) + 45px)}}@charset "UTF-8";.wp-block-archives-dropdown label{display:block}.wp-block-audio{margin:0 0 1em}.wp-block-audio figcaption{margin-bottom:1em;margin-top:.5em}.wp-block-au
2022-01-14 22:59:44 UTC	80	IN	Data Raw: 2d 2d 77 70 2d 2d 73 74 79 6c 65 2d 2d 62 6c 6f 63 6b 2d 67 61 70 2c 2e 35 65 6d 29 2a 2e 32 35 29 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 3e 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 5f 5f 77 69 64 74 68 2d 31 30 30 7b 66 6c 65 78 2d 62 61 73 69 73 3a 31 30 30 25 3b 77 69 64 74 68 3a 31 30 30 25 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 2e 69 73 2d 76 65 72 74 69 63 61 6c 3e 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 5f 5f 77 69 64 74 68 2d 32 35 7b 77 69 64 74 68 3a 32 35 25 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 2e 69 73 2d 76 65 72 74 69 63 61 6c 3e 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 2e 77 70 Data Ascii: --wp--style--block-gap,.5em)*.25)}.wp-block-buttons>.wp-block-button.wp-block-button__width-100{flex-basis:100%;width:100%}.wp-block-buttons.is-vertical>.wp-block-button.wp-block-button__width-25{width:25%}.wp-block-buttons.is-vertical>.wp-block-button.wp
2022-01-14 22:59:44 UTC	81	IN	Data Raw: 75 74 74 6f 6e 73 2e 69 73 2d 63 6f 6e 74 65 6e 74 2d 6a 75 73 74 69 66 69 63 61 74 69 6f 6e 2d 63 65 6e 74 65 72 7b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 2e 69 73 2d 63 6f 6e 74 65 6e 74 2d 6a 75 73 74 69 66 69 63 61 74 69 6f 6e 2d 63 65 6e 74 65 72 2e 69 73 2d 76 65 72 74 69 63 61 6c 7b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 2e 69 73 2d 63 6f 6e 74 65 6e 74 2d 6a 75 73 74 69 66 69 63 61 74 69 6f 6e 2d 72 69 67 68 74 7b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 66 6c 65 78 2d 65 6e 64 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 73 2e 69 73 2d 63 6f 6e 74 65 6e 74 2d 6a 75 73 74 69 66 69 63 61 Data Ascii: uttons.is-content-justification-center{justify-content:center}.wp-block-buttons.is-content-justification-center.is-vertical{align-items:center}.wp-block-buttons.is-content-justification-right{justify-content:flex-end}.wp-block-buttons.is-content-justifica
2022-01-14 22:59:44 UTC	83	IN	Data Raw: 6d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 38 32 70 78 29 7b 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 73 7b 66 6c 65 78 2d 77 72 61 70 3a 6e 6f 77 72 61 70 7d 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 73 2e 61 72 65 2d 76 65 72 74 69 63 61 6c 6c 79 2d 61 6c 69 67 6e 65 64 2d 74 6f 70 7b 61 6c 69 67 6e 2d 69 74 65 6d 73 2d 73 74 61 72 74 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 73 2e 61 72 65 2d 76 65 72 74 69 63 61 6c 6c 79 2d 61 6c 69 67 6e 65 64 2d 63 65 6e 74 65 72 7b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 73 2e 61 72 65 2d 76 65 72 74 69 63 61 6c 6c 79 2d 61 6c 69 67 6e 65 64 2d 62 6f 74 74 6f 6d 7b 61 6c 69 67 6e 2d 69 74 65 Data Ascii: m}@media (min-width:782px){.wp-block-columns{flex-wrap:nowrap}}.wp-block-columns.are-vertically-aligned-top{align-items:flex-start}.wp-block-columns.are-vertically-aligned-center{align-items:center}.wp-block-columns.are-vertically-aligned-bottom{align-ite
2022-01-14 22:59:44 UTC	84	IN	Data Raw: 68 69 6c 64 29 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 76 61 72 28 2d 2d 77 70 2d 2d 73 74 79 6c 65 2d 2d 62 6c 6f 63 6b 2d 67 61 70 2c 32 65 6d 29 7d 3a 77 68 65 72 65 28 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 73 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 29 7b 70 61 64 64 69 6e 67 3a 31 2e 32 35 65 6d 20 32 2e 33 37 35 65 6d 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 7b 66 6c 65 78 2d 67 72 6f 77 3a 31 3b 6d 69 6e 2d 77 69 64 74 68 3a 30 3b 6f 76 65 72 66 6c 6f 77 2d 77 72 61 70 3a 62 72 65 61 6b 2d 77 6f 72 64 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 62 72 65 61 6b 2d 77 6f 72 64 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 2e 69 73 2d 76 65 72 74 69 63 61 6c 6c 79 2d 61 6c 69 67 6e 65 64 2d 74 6f 70 7b 61 6c 69 67 6e 2d 73 65 6c 66 Data Ascii: hild){margin-left:var(--wp--style--block-gap,2em)}:where(.wp-block-columns.has-background){padding:1.25em 2.375em}.wp-block-column{flex-grow:1;min-width:0;overflow-wrap:break-word;word-break:break-word}.wp-block-column.is-vertically-aligned-top{align-self
2022-01-14 22:59:44 UTC	85	IN	Data Raw: 68 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6d 6d 65 6e 74 73 2d 70 61 67 69 6e 61 74 69 6f 6e 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6d 6d 65 6e 74 73 2d 70 61 67 69 6e 61 74 69 6f 6e 2d 6e 65 78 74 2d 61 72 72 6f 77 3a 6e 6f 74 28 2e 69 73 2d 61 72 72 6f 77 2d 63 68 65 76 72 6f 6e 29 7b 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 58 28 31 29 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6d 6d 65 6e 74 73 2d 70 61 67 69 6e 61 74 69 6f 6e 2e 61 6c 69 67 6e 63 65 6e 74 65 72 7b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6d 6d 65 6e 74 2d 74 65 6d 70 6c 61 74 65 7b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b Data Ascii: h}.wp-block-comments-pagination .wp-block-comments-pagination-next-arrow:not(.is-arrow-chevron){transform:scaleX(1)}.wp-block-comments-pagination.aligncenter{justify-content:center}.wp-block-comment-template{list-style:none;margin-bottom:0;max-width:100%;
2022-01-14 22:59:44 UTC	97	IN	Data Raw: 6f 72 5d 29 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 30 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 3a 62 65 66 6f 72 65 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 3a 62 65 66 6f 72 65 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 3a 62 65 66 6f 72 65 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 20 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 3a 62 65 66 6f 72 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 63 6f 6e 74 65 6e 74 3a 22 22 7d 2e 77 70 2d 62 6c 6f 63 6b 2d Data Ascii: or]){background-color:#000}.wp-block-cover-image.has-background-dim:before,.wp-block-cover-image .has-background-dim:before,.wp-block-cover.has-background-dim:before,.wp-block-cover .has-background-dim:before{background-color:inherit;content:""}.wp-block-
2022-01-14 22:59:44 UTC	99	IN	Data Raw: 63 6b 2d 63 6f 76 65 72 5f 5f 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2d 33 30 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 5f 5f 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2d 33 30 7b 6f 70 61 63 69 74 79 3a 2e 33 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 5f 5f 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2e 68 Data Ascii: ck-cover__gradient-background.has-background-dim.has-background-dim-30,.wp-block-cover .wp-block-cover__gradient-background.has-background-dim.has-background-dim-30{opacity:.3}.wp-block-cover-image .wp-block-cover__gradient-background.has-background-dim.h

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	105	IN	Data Raw: 64 69 6d 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2d 39 30 7b 6f 70 61 63 69 74 79 3a 2e 39 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 5f 5f 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2d 31 30 30 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 5f 5f 67 72 61 64 69 65 6e 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 69 6d 2d 31 30 30 7b 6f 70 61 63 69 74 79 3a 31 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f Data Ascii: dim.has-background-dim-90{opacity:.9}.wp-block-cover-image .wp-block-cover__gradient-background.has-background-dim.has-background-dim-100,.wp-block-cover .wp-block-cover__gradient-background.has-background-dim.has-background-dim-100{opacity:1}.wp-block-co
2022-01-14 22:59:44 UTC	107	IN	Data Raw: 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 68 35 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 68 36 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 70 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 20 68 31 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 20 68 32 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 20 68 33 3a 6e 6f 74 28 2e 68 61 73 2d 74 65 78 74 2d 63 6f 6c 6f 72 29 2c 2e 77 70 2d 62 Data Ascii: ck-cover-image h5:not(.has-text-color),.wp-block-cover-image h6:not(.has-text-color),.wp-block-cover-image p:not(.has-text-color),.wp-block-cover h1:not(.has-text-color),.wp-block-cover h2:not(.has-text-color),.wp-block-cover h3:not(.has-text-color),.wp-b
2022-01-14 22:59:44 UTC	112	IN	Data Raw: 6f 73 69 74 69 6f 6e 2d 62 6f 74 74 6f 6d 2d 63 65 6e 74 65 72 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2e 69 73 2d 70 6f 73 69 74 69 6f 6e 2d 62 6f 74 74 6f 6d 2d 63 65 6e 74 65 72 7b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 66 6c 65 78 2d 65 6e 64 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2d 69 6d 61 67 65 2e 69 73 2d 70 6f 73 69 74 69 6f 6e 2d 62 6f 74 74 6f 6d 2d 72 69 67 68 74 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 65 72 2e 69 73 2d 70 6f 73 69 74 69 6f 6e 2d 62 6f 74 74 6f 6d 2d 72 69 67 68 74 7b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 66 6c 65 78 2d 65 6e 64 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 66 6c 65 78 2d 65 6e 64 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 76 Data Ascii: osition-bottom-center,.wp-block-cover.is-position-bottom-center{align-items:flex-end;justify-content:center}.wp-block-cover-image.is-position-bottom-right,.wp-block-cover.is-position-bottom-right{align-items:flex-end;justify-content:flex-end}.wp-block-cov

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49764	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	55	OUT	GET /wp-content/themes/pub/seedlet/style.css?m=1640216290h&cssminify=yes HTTP/1.1 Host: s0.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:44 UTC	58	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:44 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Etag: W/"61c3b730-1f203" Expires: Wed, 28 Dec 2022 09:58:08 GMT Cache-Control: max-age=31536000 X-ac: 2.hhn _dfw Access-Control-Allow-Methods: GET, HEAD Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-nc: HIT hhn 2
2022-01-14 22:59:44 UTC	58	IN	Data Raw: 38 30 30 30 0d 0a 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 3a 72 6f 6f 74 7b 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 70 72 69 6d 61 72 79 3a 76 61 72 28 2d 2d 66 6f 6e 74 2d 68 65 61 64 69 6e 67 73 2c 20 27 50 6c 61 79 66 61 69 72 20 44 69 73 70 6c 61 79 27 2c 20 47 65 6f 72 67 69 61 2c 20 54 69 6d 65 73 2c 20 73 65 72 69 66 29 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 73 65 63 6f 6e 64 61 72 79 3a 76 61 72 28 2d 2d 66 6f 6e 74 2d 62 61 73 65 2c 20 27 46 69 72 61 20 53 61 6e 73 27 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 29 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 63 6f 64 65 3a 6d 6f 6e 6f 73 70 61 63 65 2c 20 6d 6f 6e 6f 73 70 61 63 65 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e Data Ascii: 8000@charset "UTF-8";:root{--global--font-primary:var(--font-headings, 'Playfair Display', Georgia, Times, serif);--global--font-secondary:var(--font-base, 'Fira Sans', Helvetica, Arial, sans-serif);--global--font-code:monospace, monospace;--global--fon

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	59	IN	Data Raw: 74 65 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 3a 23 33 33 33 33 33 33 33 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 2d 6c 6f 77 2d 63 6f 6e 74 72 61 73 74 3a 23 34 34 34 34 34 34 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 2d 68 69 67 68 2d 63 6f 6e 74 72 61 73 74 3a 23 30 30 30 30 30 30 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 46 46 46 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 74 65 72 74 69 61 72 79 3a 23 46 41 46 42 46 36 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 64 61 72 6b 3a 23 44 44 44 44 44 44 3b 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f Data Ascii: te;--global--color-foreground:#333333;--global--color-foreground-low-contrast:#444444;--global--color-foregr ound-high-contrast:#000000;--global--color-background:#FFFFFF;--global--color-tertiary:#FAFBF6;--global--color-background-dark:#DDDDDD;--global--co
2022-01-14 22:59:44 UTC	60	IN	Data Raw: 6f 6e 2d 2d 63 6f 6c 6f 72 2d 74 65 78 74 29 3b 2d 2d 62 75 74 74 6f 6e 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 73 65 63 6f 6e 64 61 72 79 29 3b 2d 2d 62 75 74 74 6f 6e 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 68 6f 76 65 72 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 73 65 63 6f 6e 64 61 72 79 2d 68 6f 76 65 72 29 3b 2d 2d 62 75 74 74 6f 6e 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 61 63 74 69 76 65 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 70 72 69 6d 61 72 79 29 3b 2d 2d 62 75 74 74 6f 6e 2d 2d 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 75 69 29 3b 2d 2d 62 Data Ascii: on--color-text);--button--color-background:var(--global--color-secondary);--button--color-background-hover:var(--global--color-secondary-hover);--button--color-background-active:var(--global--color-primary);--button--font-family:var(--global--font-ui);--b
2022-01-14 22:59:44 UTC	64	IN	Data Raw: 62 61 6c 2d 2d 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 29 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 2d 68 32 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 29 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 2d 68 31 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 29 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 2d 68 36 3a 31 2e 33 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 2d 68 35 3a 31 2e 33 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 2d 68 34 3a 31 2e 33 3b 2d 2d 68 65 61 64 69 6e 67 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 2d 68 33 3a Data Ascii: bal--letter-spacing);--heading--letter-spacing-h2:var(--global--letter-spacing);--heading--letter-spacing-h1:var(--global--letter-spacing);--heading--line-height-h6:1.3;--heading--line-height-h5:1.3;--heading--line-height-h4:1.3;--heading--line-height-h3:
2022-01-14 22:59:44 UTC	65	IN	Data Raw: 3b 2d 2d 70 75 6c 6c 71 75 6f 74 65 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 2d 68 65 61 64 69 6e 67 29 3b 2d 2d 70 75 6c 6c 71 75 6f 74 65 2d 2d 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 30 3b 2d 2d 70 75 6c 6c 71 75 6f 74 65 2d 2d 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 2d 2d 70 75 6c 6c 71 75 6f 74 65 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 29 3b 2d 2d 70 75 6c 6c 71 75 6f 74 65 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 62 61 63 6b 67 72 6f 75 6e 64 29 3b 2d 2d 71 75 Data Ascii: ;--pullquote--line-height:var(--global--line-height-heading);--pullquote--border-width:0;--pullquote--border-color:transparent;--pullquote--color-foreground:var(--global--color-foreground);--pullquote--color-background:var(--global--color-background);--qu
2022-01-14 22:59:44 UTC	87	IN	Data Raw: 74 2d 70 72 69 6d 61 72 79 29 3b 2d 2d 62 72 61 6e 64 69 6e 67 2d 2d 74 69 74 6c 65 2d 2d 66 6f 6e 74 2d 73 69 7a 65 3a 63 61 6c 63 28 20 31 2e 32 35 20 2a 20 76 61 72 28 2d 2d 68 65 61 64 69 6e 67 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 68 31 29 20 29 3b 2d 2d 62 72 61 6e 64 69 6e 67 2d 2d 74 69 74 6c 65 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 6d 6f 62 69 6c 65 3a 76 61 72 28 2d 2d 68 65 61 64 69 6e 67 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 68 31 29 3b 2d 2d 62 72 61 6e 64 69 6e 67 2d 2d 74 69 74 6c 65 2d 2d 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 3b 2d 2d 62 72 61 6e 64 69 6e 67 2d 2d 64 65 73 63 72 69 70 74 69 6f 6e 2d 2d 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 73 65 63 6f 6e 64 61 72 79 29 3b 2d 2d 62 72 72 Data Ascii: t-primary);--branding--title--font-size:calc(1.25 * var(--heading--font-size-h1));--branding--title--font-size-mobile:var(--heading--font-size-h1);--branding--title--font-weight:700;--branding--description--font-family:var(--global--font-secondary);--br
2022-01-14 22:59:44 UTC	88	IN	Data Raw: 2d 6c 69 6e 6b 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 66 6f 72 65 67 72 6f 75 6e 64 29 3b 2d 2d 73 6f 63 69 61 6c 2d 6e 61 76 2d 2d 63 6f 6c 6f 72 2d 6c 69 6e 6b 2d 68 6f 76 65 72 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 70 72 69 6d 61 72 79 2d 68 6f 76 65 72 29 3b 2d 2d 73 6f 63 69 61 6c 2d 6e 61 76 2d 2d 70 61 64 64 69 6e 67 3a 63 61 6c 63 28 20 30 2e 35 20 2a 20 76 61 72 28 2d 2d 70 72 69 6d 61 72 79 2d 6e 61 76 2d 2d 70 61 64 64 69 6e 67 29 20 29 3b 2d 2d 77 70 63 6f 6d 2d 6d 61 72 6b 65 74 69 6e 67 2d 62 61 72 2d 2d 68 65 69 67 68 74 3a 34 35 70 78 3b 2d 2d 77 70 61 64 6d 69 6e 2d 62 61 72 2d 2d 68 65 69 67 68 74 3a 34 36 70 78 3b 2d 2d 65 6e 74 72 79 2d 68 65 61 64 65 72 2d 2d 63 6f 6c 6f 72 3a 76 61 72 Data Ascii: -link:var(--global--color-foreground);--social-nav--color-link-hover:var(--global--color-primary-hover);--social-nav--padding:calc(0.5 * var(--primary-nav--padding));--wpcom-marketing-bar--height:45px;--wpadmin-bar--height:46px;--entry-header--color:var
2022-01-14 22:59:44 UTC	89	IN	Data Raw: 74 69 6f 6e 2d 2d 63 6f 6c 6f 72 2d 6c 69 6e 6b 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 70 72 69 6d 61 72 79 29 3b 2d 2d 70 61 67 69 6e 61 74 69 6f 6e 2d 2d 63 6f 6c 6f 72 2d 6c 69 6e 6b 2d 68 6f 76 65 72 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 63 6f 6c 6f 72 2d 70 72 69 6d 61 72 79 2d 68 6f 76 65 72 29 3b 2d 2d 70 61 67 69 6e 61 74 69 6f 6e 2d 2d 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 73 65 63 6f 6e 64 61 72 79 29 3b 2d 2d 70 61 67 69 6e 61 74 69 6f 6e 2d 2d 66 6f 6e 74 2d 73 69 7a 65 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 66 6f 6e 74 2d 73 69 7a 65 2d 73 6d 29 3b 2d 2d 70 61 67 69 6e 61 74 69 6f 6e 2d 2d 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 2d 2d Data Ascii: tion--color-link:var(--global--color-primary);--pagination--color-link-hover:var(--global--color-primary-hover);--pagination--font-family:var(--global--font-secondary);--pagination--font-size:var(--global--font-size-sm);--pagination--font-weight:normal;--
2022-01-14 22:59:44 UTC	91	IN	Data Raw: 2d 2d 61 6c 69 67 6e 77 69 64 65 2d 77 69 64 74 68 3a 63 61 6c 63 28 31 30 30 76 77 20 2d 20 76 61 72 28 2d 2d 72 65 73 70 6f 6e 73 69 76 65 2d 2d 73 70 61 63 69 6e 67 2d 68 6f 72 69 7a 6f 6e 74 61 6c 29 29 3b 2d 2d 72 65 73 70 6f 6e 73 69 76 65 2d 2d 61 6c 69 67 6e 66 75 6c 6c 2d 77 69 64 74 68 3a 31 30 30 25 3b 2d 2d 72 65 73 70 6f 6e 73 69 76 65 2d 2d 61 6c 69 67 6e 77 69 64 65 2d 77 69 64 74 68 2d 6d 75 6c 74 69 70 6c 69 65 72 3a 63 61 6c 63 28 31 36 20 2a 20 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 73 70 61 63 69 6e 67 2d 68 6f 72 69 7a 6f 6e 74 61 6c 29 29 3b 2d 2d 72 65 73 70 6f 6e 73 69 76 65 2d 2d 61 6c 69 67 6e 72 69 67 68 74 6c 65 66 74 2d 77 69 64 74 68 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 73 70 61 63 69 6e 67 2d 68 6f 72 69 7a 6f 6e Data Ascii: --alignwide-width:calc(100vw - var(--responsive--spacing-horizontal));--responsive--alignfull-width:100%;--responsive--alignwide-width-multiplier:calc(16 * var(--global--spacing-horizontal));--responsive--alignrightleft-width:var(--global--spacing-horizon

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	95	IN	Data Raw: 74 3a 61 75 74 6f 3b 7d 2e 77 69 64 65 2d 6d 61 78 2d 77 69 64 74 68 2c 20 68 72 2e 77 70 2d 62 6c 6f 63 6b 2d 73 65 70 61 72 61 74 6f 72 2e 69 73 2d 73 74 79 6c 65 2d 77 69 64 65 2e 61 6c 69 67 6e 77 69 64 65 2c 20 2e 61 6c 69 67 6e 77 69 64 65 7b 6d 61 78 2d 77 69 64 74 68 3a 76 61 72 28 2d 2d 72 65 73 70 6f 6e 73 69 76 65 2d 2d 61 6c 69 67 6e 77 69 64 65 2d 77 69 64 74 68 29 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 61 75 74 6f 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 61 75 74 6f 3b 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 34 38 32 70 78 29 7b 2e 66 75 6c 6c 2d 6d 61 78 2d 77 69 64 74 68 2c 20 68 72 2e 77 70 2d 62 6c 6f 63 6b 2d 73 65 70 61 72 61 74 6f 72 2e 69 73 2d 73 74 79 6c 65 2d 77 69 Data Ascii: t:auto;}.wide-max-width, hr.wp-block-separator.is-style-wide.alignwide, .alignwide{max-width:var(--responsive--alignwide-width);margin-left:auto;margin-right:auto;}@media only screen and (min-width:482px){.full-max-width, hr.wp-block-separator.is-style-wi
2022-01-14 22:59:44 UTC	96	IN	Data Raw: 63 69 6e 67 2d 76 65 72 74 69 63 61 6c 29 29 3b 7d 2e 73 69 74 65 2d 6d 61 69 6e 20 3e 20 2a 3a 66 69 72 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 7d 2e 73 69 74 65 2d 6d 61 69 6e 20 3e 20 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 7d 2e 65 6e 74 72 79 2d 68 65 61 64 65 72 2c 0a 2e 70 6f 73 74 2d 74 68 75 6d 62 6e 61 69 6c 2c 0a 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 2c 0a 2e 65 6e 74 72 79 2d 66 6f 6f 74 65 72 2c 0a 2e 65 6e 74 72 79 2d 61 75 74 68 6f 72 2c 0a 2e 77 69 64 67 65 74 2d 61 72 65 61 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 73 70 61 63 69 6e 67 2d 76 65 72 74 69 63 61 6c 29 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 61 75 74 6f 3b 6d 61 Data Ascii: cing-vertical));}.site-main > *:first-child{margin-top:0;}.site-main > *:last-child{margin-bottom:0;}.entry-header,.post-thumbnail,.entry-content,.entry-footer,.entry-author,.widget-area{margin-top:var(--global--spacing-vertical);margin-right:auto;ma
2022-01-14 22:59:44 UTC	103	IN	Data Raw: 73 74 2d 63 68 69 6c 64 2c 0a 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 6d 70 6c 61 74 65 2d 70 61 72 74 20 3e 20 2a 3a 66 69 72 73 74 2d 63 68 69 6c 64 2c 0a 2e 77 69 64 67 65 74 2d 61 72 65 61 20 3e 20 2a 3a 66 69 72 73 74 2d 63 68 69 6c 64 2c 0a 2e 77 69 64 67 65 74 2d 63 6f 6c 75 6d 6e 20 3e 20 2a 3a 66 69 72 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 7d 2e 73 69 74 65 2d 66 6f 6f 74 65 72 20 3e 20 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 0a 2e 73 69 74 65 2d 6d 61 69 6e 20 3e 20 61 72 74 69 63 6c 65 20 3e 20 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 0a 2e 73 69 74 65 2d 6d 61 69 6e 20 3e 20 2e 6e 6f 74 2d 66 6f 75 6e 64 20 3e 20 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 0a 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 20 3e 20 2a 3a 6c 61 73 74 Data Ascii: st-child,.wp-block-template-part > *:first-child,.widget-area > *:first-child,.widget-column > *:first-child{margin-top:0;}.site-footer > *:last-child,.site-main > article > *:last-child,.site-main > .not-found > *:last-child,.entry-content > *:last
2022-01-14 22:59:44 UTC	104	IN	Data Raw: 20 3e 20 2a 2e 61 6c 69 67 6e 66 75 6c 6c 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 7d 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 20 3e 20 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 20 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 20 3e 20 2a 2e 61 6c 69 67 6e 66 75 6c 6c 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 7d 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 20 3e 20 2a 2e 61 6c 69 67 6e 66 75 6c 6c 20 2b 20 2e 61 6c 69 67 6e 6c 65 66 74 2c 0a 2e 65 6e 74 72 79 2d 63 6f 6e 74 65 6e 74 20 3e 20 2a 2e 61 6c 69 67 6e 66 75 6c 6c 20 2b 20 2e 61 6c 69 67 6e 72 69 67 68 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 76 61 72 28 2d 2d 67 6c 6f 62 61 6c 2d 2d 73 70 61 63 69 6e 67 2d 76 65 72 74 69 63 61 6c 29 3b 7d 62 6f 64 79 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 64 Data Ascii: > *.alignfull{margin-top:0;}.entry-content > *:last-child, .entry-content > *.alignfull{margin-bottom:0;}.entry-content > *.alignfull + .alignleft,.entry-content > *.alignfull + .alignright{margin-top:var(--global--spacing-vertical);}body{display:none;d
2022-01-14 22:59:44 UTC	111	IN	Data Raw: 2d 6d 6f 72 65 2d 62 74 6e 5d 3a 61 66 74 65 72 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 63 61 6c 63 28 2e 35 65 6d 20 2a 20 76 61 72 28 2d 2d 62 75 74 74 6f 6e 2d 2d 6c 69 6e 65 2d 68 65 69 67 68 74 29 20 2b 20 2d 2e 33 39 29 3b 7d 62 75 74 74 6f 6e 3a 6e 6f 74 28 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 29 3a 61 63 74 69 76 65 2c 0a 2e 62 75 74 74 6f 6e 3a 6e 6f 74 28 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 29 3a 61 63 74 69 76 65 5b 74 79 70 65 3d 22 73 75 62 6d 69 74 22 5d 2c 20 2e 61 38 63 2d 70 6f 73 74 73 2d 6c 69 73 74 5f 5f 76 69 65 77 2d 61 6c 6c 3a 6e 6f 74 28 2e 68 61 73 2d 62 61 63 6b 67 72 6f 75 6e 64 29 3a 61 63 74 69 76 65 7b 63 Data Ascii: -more-btn]:after{margin-top:-calc(.5em * var(--button--line-height) + -.39);}button:not(.has-background):active,.button:not(.has-background):active,input:not(.has-background):active[type="submit"], .a8c-posts-list__view-all:not(.has-background):active{c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49763	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	55	OUT	GET /wp-content/themes/h4/global.css?m=1420737423h&cssminify=yes HTTP/1.1 Host: s0.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:44 UTC	63	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:44 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Etag: W/"5739124e-1d7" Expires: Sat, 05 Nov 2022 08:35:16 GMT Cache-Control: max-age=31536000 X-ac: 2.hhn _dfw Access-Control-Allow-Methods: GET, HEAD Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-nc: HIT hhn 2

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	64	IN	Data Raw: 31 34 33 0d 0a 69 6d 67 2e 6c 61 74 65 78 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 7d 2e 76 69 64 65 6f 2d 70 6c 61 79 65 72 7b 62 6f 72 64 65 72 3a 30 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 35 70 78 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 7d 2e 68 69 64 64 65 6e 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 7d 2e 73 63 72 65 65 6e 2d 72 65 61 64 65 72 2d 74 65 78 74 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6c 65 66 74 3a 2d 31 30 30 30 65 6d 3b 7d 2e 63 6f 6d 6d 65 6e 74 20 6f 62 6a 65 63 74 2c 0a 2e 63 6f 6d 6d 65 6e 74 20 65 6d 62 65 64 2c 0a 2e 65 6d 62 65 64 2d 76 69 6d 65 6f 20 69 66 72 61 Data Ascii: 143img.latex{border:none;vertical-align:middle;}.video-player{border:0;margin:auto;padding:5px;text-align:center;max-width:100%;}.hidden{display:none;}.screen-reader-text{position:absolute;left:-1000em;}.comment object ,.comment embed,.embed-vimeo ifra

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49765	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	56	OUT	GET /wp-includes/js/wp-emoji-release.min.js?m=1625065786h&ver=5.9-beta4-52004 HTTP/1.1 Host: s0.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:44 UTC	67	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:44 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Etag: W/"61beb200-4705" Expires: Thu, 05 Jan 2023 13:20:14 GMT Cache-Control: max-age=31536000 X-ac: 2.hhn _dfw Access-Control-Allow-Methods: GET, HEAD Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-nc: HIT hhn 2
2022-01-14 22:59:44 UTC	67	IN	Data Raw: 34 37 30 35 0d 0a 2f 2a 21 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 61 75 74 6f 2d 67 65 6e 65 72 61 74 65 64 20 2a 2f 0a 2f 2f 20 53 6f 75 72 63 65 3a 20 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6a 73 2f 74 77 65 6d 6f 6a 69 2e 6d 69 6e 2e 6a 73 0a 76 61 72 20 74 77 65 6d 6f 6a 69 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 66 3d 7b 62 61 73 65 3a 22 68 74 74 70 73 3a 2f 2f 74 77 65 6d 6f 6a 69 2e 6d 61 78 63 64 6e 2e 63 6f 6d 2f 76 2f 31 33 2e 31 2e 30 2f 22 2c 65 78 74 3a 22 2e 70 6e 67 22 2c 73 69 7a 65 3a 22 37 32 78 37 32 22 2c 63 6c 61 73 73 4e 61 6d 65 3a 22 65 6d 6f 6a 69 22 2c 63 6f 6e 76 65 72 74 3a 7b 66 72 6f 6d 43 6f 64 65 50 6f 69 6e 74 3a 66 75 6e 63 74 69 6f 6e 28 64 29 7b 64 3d 22 73 74 72 69 6e 67 Data Ascii: 4705/*! This file is auto-generated */// Source: wp-includes/js/twemoji.min.jsvar twemoji=function(){"use strict";var f={base:"https://twemoji.maxcdn.com/v/13.1.0/",ext:".png",size:"72x72",className:"emoji",convert:{fromCodePoint:function(d){d="string
2022-01-14 22:59:44 UTC	68	IN	Data Raw: 63 2c 65 2c 62 3d 75 2e 63 68 69 6c 64 4e 6f 64 65 73 2c 61 3d 62 2e 6c 65 6e 67 74 68 3b 66 6f 72 28 3b 61 2d 2d 3b 29 63 3d 62 5b 61 5d 2c 33 3d 3d 3d 28 65 3d 63 2e 6e 6f 64 65 54 79 70 65 29 3f 66 2e 70 75 73 68 28 63 29 3a 31 21 3d 3d 65 7c 7c 22 6f 77 6e 65 72 53 56 47 45 6c 65 6d 65 6e 74 22 69 6e 20 63 7c 7c 68 2e 74 65 73 74 28 63 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 7c 7c 64 28 63 2c 66 29 3b 72 65 74 75 72 6e 20 66 7d 28 64 2c 5b 5d 29 2c 70 3d 6c 2e 6c 65 6e 67 74 68 3b 66 6f 72 28 3b 70 2d 2d 3b 29 7b 66 6f 72 28 65 3d 21 31 2c 62 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 44 6f 63 75 6d 65 6e 74 46 72 61 67 6d 65 6e 74 28 29 2c 61 3d 6c 5b 70 5d 2c 74 3d 61 2e 6e 6f 64 65 56 61 6c 75 65 2c 6e 3d 30 3b Data Ascii: c,e,b=u.childNodes,a=b.length;for(;a--;)c=b[a],3===(e=c.nodeType)?f.push(c):1!==e||"ownerSVGElement"in c||h.test(c.nodeName.toLowerCase())||d(c,f);return f}(d,[]),p=l.length;for(;p--;){for(e=!1,b=document.createDocumentFragment(),a=l[p],t=a.nodeValue,n=0;
2022-01-14 22:59:44 UTC	69	IN	Data Raw: 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5c 75 64 66 66 64 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 38 62 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5c 75 64 66 66 65 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 38 62 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5c 75 64 66 66 66 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c Data Ascii: dfff]|\ud83d\udc68\ud83c\udffd\u200d\u2764\ufe0f\u200d\ud83d\udc8b\u200d\ud83d\udc68\ud83c[\udffb-\udfff]|\ud83d\udc68\ud83c\udffe\u200d\u2764\ufe0f\u200d\ud83d\udc8b\u200d\ud83d\udc68\ud83c[\udffb-\udfff]|\ud83d\udc68\ud83c\udfff\u200d\u2764\ufe0f\u200d\

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	71	IN	Data Raw: 30 30 64 5c 75 64 38 33 65 5c 75 64 64 64 31 5c 75 64 38 33 63 5b 5c 75 64 66 66 63 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 65 5c 75 64 64 64 31 5c 75 64 38 33 63 5c 75 64 66 66 63 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 38 62 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 64 31 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 5c 75 64 66 66 64 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 65 5c 75 64 64 64 31 5c 75 64 38 33 63 5c 75 64 66 66 64 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 64 64 31 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 5c 75 64 66 66 66 63 5c 75 64 66 66 66 65 5c 75 64 66 66 66 5d 7c 5c Data Ascii: 00d\ud83e\uddd1\ud83c[\udffc-\udfff]|\ud83e\uddd1\ud83c\udffc\u200d\u2764\ufe0f\u200d\ud83d\udc8b\u200d\ud83e\uddd1\ud83c[\udffb\udffd-\udfff]|\ud83e\uddd1\ud83c\udffd\u200d\u2764\ufe0f\u200d\ud83d\udc8b\u200d\ud83e\uddd1\ud83c[\udffb\udffc\udffe\udfff]|\
2022-01-14 22:59:44 UTC	72	IN	Data Raw: 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 62 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 62 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 31 64 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5b 5c 75 64 66 66 63 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 62 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 31 64 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5b 5c 75 64 66 66 63 2d 5c Data Ascii: [\udffb-\udfff]|\ud83d\udc69\ud83c\udffb\u200d\u2764\ufe0f\u200d\ud83d\udc69\ud83c[\udffb-\udfff]|\ud83d\udc69\ud83c\udffb\u200d\ud83e\udd1d\u200d\ud83d\udc68\ud83c[\udffc-\udfff]|\ud83d\udc69\ud83c\udffb\u200d\ud83e\udd1d\u200d\ud83d\udc69\ud83c[\udffc-\
2022-01-14 22:59:44 UTC	73	IN	Data Raw: 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 66 5c 75 32 30 30 64 5c 75 32 37 36 34 5c 75 66 65 30 66 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 66 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 31 64 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 64 38 33 63 5 b 5c 75 64 66 66 62 2d 5c 75 64 66 66 65 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5c 75 64 66 66 66 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 31 64 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 65 5d 7c 5c 75 64 38 Data Ascii: fff]|\ud83d\udc69\ud83c\udfff\u200d\u2764\ufe0f\u200d\ud83d\udc69\ud83c[\udffb-\udfff]|\ud83d\udc69\ud83c\udfff\u200d\ud83e\udd1d\u200d\ud83d\udc68\ud83c[\udffb-\udffe]|\ud83d\udc69\ud83c\udfff\u200d\ud83e\udd1d\u200d\ud83d\udc69\ud83c[\udffb-\udffe]|\ud8
2022-01-14 22:59:44 UTC	75	IN	Data Raw: 64 31 64 5c 75 32 30 30 64 5c 75 64 38 33 65 5c 75 64 64 64 31 7c 5c 75 64 38 33 64 5c 75 64 63 36 62 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 63 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 64 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 38 66 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5c 75 64 63 39 31 5c 75 64 38 33 63 5b 5c 75 64 66 66 62 2d 5c 75 64 66 66 66 5d 7c 5c 75 64 38 33 64 5b 5c 75 64 63 36 62 2d 5c 75 64 63 36 64 5c 75 64 63 38 66 5c 75 64 63 39 31 5d 29 7c 28 3f 3a 5c 75 64 38 33 64 5b 5c 75 64 63 36 38 5c 75 64 63 36 39 5d 7c 5c 75 64 38 Data Ascii: d1d\u200d\ud83e\uddd1|\ud83d\udc6b\ud83c[\udffb-\udfff]|\ud83d\udc6c\ud83c[\udffb-\udfff]|\ud83d\udc6d\ud83c[\udffb-\udfff]|\ud83d\udc8f\ud83c[\udffb-\udfff]|\ud83d\udc91\ud83c[\udffb-\udfff]|\ud83d[\udc6b-\udc6d\udc8f\udc91])|(?:\ud83d[\udc68\udc69]|\ud8
2022-01-14 22:59:44 UTC	92	IN	Data Raw: 38 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 37 5c 75 32 30 30 64 5c 75 64 38 33 64 5b 5c 75 64 63 36 36 5c 75 64 63 36 37 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 36 5c 75 32 30 30 64 5c 75 64 38 33 64 5b 5c 75 64 63 36 36 5c 75 64 63 36 37 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 38 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 32 30 30 64 5c 75 64 38 33 64 5b 5c 75 64 63 36 36 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 37 5d 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 36 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 36 7c 5c 75 64 38 33 64 5c 75 64 63 36 39 5c 75 32 30 30 64 5c 75 64 38 33 64 5c 75 64 63 36 37 5c 75 32 30 30 64 5c 75 64 38 33 64 5b 5c 75 64 Data Ascii: 8\u200d\ud83d\udc67\u200d\ud83d[\udc66\udc67]|\ud83d\udc68\u200d\ud83d\udc68\u200d\ud83d[\udc66\udc67]|\ud83d\udc68\u200d\ud83d\udc69\u200d\ud83d[\udc66\udc67]|\ud83d\udc69\u200d\ud83d\udc66\u200d\ud83d\udc66|\ud83d\udc69\u200d\ud83d\udc67\u200d\ud83d[\ud
2022-01-14 22:59:44 UTC	93	IN	Data Raw: 31 5c 75 64 64 62 32 5c 75 64 64 62 63 5c 75 64 64 63 32 2d 5c 75 64 64 63 34 5c 75 64 64 64 31 2d 5c 75 64 64 64 33 5c 75 64 64 64 63 2d 5c 75 64 64 64 65 5c 75 64 64 65 31 5c 75 64 64 65 33 5c 75 64 64 65 38 5c 75 64 64 65 66 5c 75 64 64 66 33 5c 75 64 64 66 61 5c 75 64 65 63 62 5c 75 64 65 63 64 2d 5c 75 64 65 63 66 5c 75 64 65 65 30 2d 5c 75 64 65 65 35 5c 75 64 65 65 39 5c 75 64 65 66 30 5c 75 64 65 66 33 5d 7c 5b 5c 75 32 30 33 63 5c 75 32 30 34 39 5c 75 32 31 33 39 5c 75 32 31 39 34 2d 5c 75 32 31 39 39 5c 75 32 31 61 39 5c 75 32 31 61 61 5c 75 32 33 31 62 5c 75 32 33 32 38 5c 75 32 33 63 66 5c 75 32 33 65 64 2d 5c 75 32 33 65 66 5c 75 32 33 66 31 5c 75 32 33 66 32 5c 75 32 33 66 38 2d 5c 75 32 33 66 61 5c 75 32 34 63 32 5c 75 32 Data Ascii: 1\uddb2\uddbc\uddc2-\uddc4\uddd1-\uddd3\udddc-\uddde\udde1\udde3\udde8\uddef\uddf3\uddfa\udecb\udecd-\udecf\udee0-\udee5\udee9\udef0\udef3]|[\u203c\u2049\u2139\u2194-\u2199\u21a9\u21aa\u231a\u231b\u2328\u23cf\u23ed-\u23ef\u23f1\u23f2\u23f8-\u23fa\u24c2\u2
2022-01-14 22:59:44 UTC	100	IN	Data Raw: 5c 75 64 63 36 32 5c 75 64 62 34 30 5c 75 64 63 36 35 5c 75 64 62 34 30 5c 75 64 63 36 65 5c 75 64 62 34 30 5c 75 64 63 36 37 5c 75 64 62 34 30 5c 75 64 63 37 66 7c 5c 75 64 38 33 63 5c 75 64 66 66 34 5c 75 64 62 34 30 5c 75 64 63 36 37 5c 75 64 62 34 30 5c 75 64 63 36 32 5c 75 64 62 34 30 5c 75 64 63 37 33 5c 75 64 62 34 30 5c 75 64 63 37 66 7c 5c 75 64 38 33 63 5c 75 64 66 66 34 5c 75 64 62 34 30 5c 75 64 63 36 37 5c 75 64 62 34 30 5c 75 64 63 37 34 5c 75 64 62 34 30 5c 75 64 63 37 66 7c 5c 75 64 38 33 63 5c 75 64 66 66 34 5c 75 64 62 34 30 5c 75 64 63 36 37 5c 75 64 62 34 30 5c 75 64 63 36 32 5c 75 64 62 34 30 5c 75 64 63 37 37 5c 75 64 62 34 30 5c 75 64 63 36 63 5c 75 64 62 34 30 5c 75 64 63 37 33 5c 75 64 62 34 30 5c 75 64 63 37 66 7c 5c 75 64 38 33 63 5c 75 64 64 65 36 5c 75 64 38 33 63 5b 5c 75 64 64 65 38 2d 5c 75 64 64 Data Ascii: \udc62\udb40\udc65\udb40\udc6e\udb40\udc67\udb40\udc7f|\ud83c\udff4\udb40\udc67\udb40\udc62\udb40\udc73\udb40\udc63\udb40\udc74\udb40\udc7f|\ud83c\udff4\udb40\udc67\udb40\udc62\udb40\udc77\udb40\udc6c\udb40\udc73\udb40\udc7f|\ud83c\udde6\ud83c[\udde8-\udd
2022-01-14 22:59:44 UTC	101	IN	Data Raw: 64 66 38 5c 75 64 64 66 61 5c 75 64 64 66 63 5d 7c 5c 75 64 38 33 63 5c 75 64 64 66 38 5c 75 64 38 33 63 5b 5c 75 64 64 65 36 2d 5c 75 64 64 65 61 5c 75 64 64 65 63 2d 5c 75 64 64 66 34 5c 75 64 64 66 37 2d 5c 75 64 64 66 39 5c 75 64 64 66 62 5c 75 64 64 66 64 2d 5c 75 64 64 66 66 5d 7c 5c 75 64 38 33 63 5c 75 64 64 66 39 5c 75 64 38 33 63 5b 5c 75 64 64 65 36 5c 75 64 64 65 38 5c 75 64 64 65 39 5c 75 64 64 65 62 2d 5c 75 64 64 65 64 5c 75 64 64 65 66 2d 5c 75 64 64 66 34 5c 75 64 64 66 37 5c 75 64 64 66 39 5c 75 64 64 66 62 5c 75 64 64 66 63 5c 75 64 64 66 66 5d 7c 5c 75 64 38 33 63 5c 75 64 64 61 5c 75 64 64 66 38 33 63 5b 5c 75 64 64 65 36 5c 75 64 64 65 63 5c 75 64 64 66 32 5c 75 64 64 66 33 5c 75 64 64 66 38 5c 75 64 64 66 65 5c 75 64 64 66 66 5d 7c 5c Data Ascii: df8\uddfa\uddfc]|\ud83c\uddf8\ud83c[\udde6-\uddea\uddec-\uddf4\uddf7-\uddf9\uddfb\uddfd-\uddff]|\ud83c\uddf9\ud83c[\udde6\udde8\udde9\uddeb-\udded\uddef-\uddf4\uddf7\uddf9\uddfb\uddfc\uddff]|\ud83c\uddfa\ud83c[\udde6\uddec\uddf2\uddf3\uddf8\uddfe\uddff]|\

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	108	IN	Data Raw: 37 62 66 5c 75 65 35 30 61 5d 29 7c 5c 75 66 65 30 66 2f 67 2c 63 3d 2f 5c 75 46 45 30 46 2f 67 2c 65 3d 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 38 32 30 35 29 2c 74 3d 2f 5b 26 3c 3e 27 22 5d 2f 67 2c 68 3d 2f 5e 28 3f 3a 69 66 72 61 6d 65 7c 6e 6f 66 72 61 6d 65 73 7c 6e 6f 73 63 72 69 70 74 7c 73 63 72 69 70 74 7c 73 65 6c 65 63 74 7c 73 74 79 6c 65 7c 74 65 78 74 61 72 65 61 29 24 2f 2c 62 3d 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 3b 72 65 74 75 72 6e 20 66 3b 66 75 6e 63 74 69 6f 6e 20 67 28 64 2c 75 29 7b 72 65 74 75 72 6e 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 54 65 78 74 4e 6f 64 65 28 75 3f 64 2e 72 65 70 6c 61 63 65 28 63 2c 22 22 29 3a 64 29 7d 66 75 6e 63 74 69 6f 6e 20 61 28 64 2c 75 29 7b 72 65 Data Ascii: 7bf\ue50a])|\ufe0f/g,c=/\uFE0F/g,e=String.fromCharCode(8205),t=/[&<>'"]/g,h=/^(?:iframe|noframes|noscript|script|select|style|textarea)$/,b=String.fromCharCode;return f;function g(d,u){return document.createTextNode(u?d.replace(c,""):d)}function a(d,u){re
2022-01-14 22:59:44 UTC	109	IN	Data Raw: 5d 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 65 72 72 6f 72 22 29 29 72 65 74 75 72 6e 3b 66 6f 72 28 3b 6e 2d 2d 3b 29 7b 69 66 28 33 3d 3d 3d 28 61 3d 65 5b 6e 5d 29 2e 6e 6f 64 65 54 79 70 65 29 7b 69 66 28 21 61 2e 70 61 72 65 6e 74 4e 6f 64 65 29 63 6f 6e 74 69 6e 75 65 3b 69 66 28 6f 29 66 6f 72 28 3b 61 2e 6e 65 78 74 53 69 62 6c 69 6e 67 26 26 33 3d 3d 3d 61 2e 6e 65 78 74 53 69 62 6c 69 6e 67 2e 6e 6f 64 65 54 79 70 65 3b 29 61 2e 6e 6f 64 65 56 61 6c 75 65 3d 61 2e 6e 6f 64 65 56 61 6c 75 65 2b 61 2e 6e 65 78 74 53 69 62 6c 69 6e 67 2e 6e 6f 64 65 56 61 6c 75 65 2c 61 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 72 65 6d 6f 76 65 43 68 69 6c 64 28 61 2e 6e 65 78 74 53 69 62 6c 69 6e 67 29 3b 61 3d 61 2e 70 61 72 65 6e 74 4e 6f 64 65 7d Data Ascii:].getAttribute("data-error"))return;for(;n--;){if(3===(a=e[n]).nodeType){if(!a.parentNode)continue;if(o)for(;a.nextSibling&&3===a.nextSibling.nodeType;)a.nodeValue=a.nodeValue+a.nextSibling.nodeValue,a.parentNode.removeChild(a.nextSibling);a=a.parentNode}
2022-01-14 22:59:44 UTC	113	IN	Data Raw: 75 2e 63 68 69 6c 64 4e 6f 64 65 73 2e 6c 65 6e 67 74 68 29 3f 28 65 3d 65 7c 7c 7b 7d 2c 74 3d 7b 62 61 73 65 3a 69 28 29 3f 6c 2e 73 76 67 55 72 6c 3a 6c 2e 62 61 73 65 55 72 6c 2c 65 78 74 3a 69 28 29 3f 6c 2e 73 76 67 45 78 74 3a 6c 2e 65 78 74 2c 63 6c 61 73 73 4e 61 6d 65 3a 65 2e 63 6c 61 73 73 4e 61 6d 65 7c 7c 22 65 6d 6f 6a 69 22 2c 63 61 6c 6c 62 61 63 6b 3a 66 75 6e 63 74 69 6f 6e 28 75 2c 65 29 7b 73 77 69 74 63 68 28 75 29 7b 63 61 73 65 22 61 39 22 3a 63 61 73 65 22 61 65 22 3a 63 61 73 65 22 32 31 32 32 22 3a 63 61 73 65 22 32 31 39 34 22 3a 63 61 73 65 22 32 36 36 30 22 3a 63 61 73 65 22 32 36 36 33 22 3a 63 61 73 65 22 32 36 36 35 22 3a 63 61 73 65 22 32 36 36 36 22 3a 72 65 74 75 72 6e 21 31 7d 72 65 74 75 72 6e 21 28 6c 2e 73 75 70 70 Data Ascii: u.childNodes.length)?(e=e||{},t={base:i()?l.svgUrl:l.baseUrl,ext:i()?l.svgExt:l.ext,className:e.className||"emoji",callback:function(u,e){switch(u){case"a9":case"ae":case"2122":case"2194":case"2660":case"2663":case"2665":case"2666":return!1}return!(l.supp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49769	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	56	OUT	GET /_static/??/wp-content/mu-plugins/comment-likes/css/comment-likes.css,/i/noticons/noticons.css?m=1436783281j&cssminify=yes HTTP/1.1 Host: s1.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-01-14 22:59:44 UTC	114	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 22:59:44 GMT Content-Type: text/css;charset=utf-8 Content-Length: 37496 Connection: close Vary: Accept-Encoding Last-Modified: Sat, 31 Dec 2016 05:45:37 GMT Etag: "58674601-9278" Expires: Fri, 25 Feb 2022 11:53:19 GMT Cache-Control: max-age=31536000 X-ac: 2.hhn _dfw Access-Control-Allow-Methods: GET, HEAD Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-nc: HIT hhn 2
2022-01-14 22:59:44 UTC	115	IN	Data Raw: 70 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 7b 68 65 69 67 68 74 3a 31 36 70 78 3b 66 6c 6f 61 74 3a 6e 6f 6e 65 3b 77 69 64 74 68 3a 31 30 30 25 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 32 70 78 7d 70 2e 63 6f 6d 6d 65 6e 74 2d 6e 6f 74 2d 6c 69 6b 65 64 7b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 7d 70 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 20 61 2e 76 69 65 77 2d 6c 69 6b 65 72 73 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 7d 64 69 76 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2d 6f 76 65 72 6c 61 79 7b 63 6f 6c 6f 72 3a 23 35 35 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 66 6f 6e 74 2d Data Ascii: p.comment-likes{height:16px;float:none;width:100%;clear:both;display:block;margin-left:-2px}p.comment-not-liked{cursor:pointer}p.comment-likes a.view-likers{text-decoration:underline;border:none}div.comment-likes-overlay{color:#555;position:absolute;font-

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	115	IN	Data Raw: 3a 69 6e 6c 69 6e 65 3b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 35 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 3b 74 65 78 74 2d 6f 76 65 72 66 6c 6f 77 3a 65 6c 6c 69 70 73 69 73 7d 64 69 76 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2d 6f 76 65 72 6c 61 79 20 64 69 76 2e 69 6e 6e 65 72 20 75 6c 2e 73 69 6e 67 6c 65 20 6c 69 7b 77 69 64 74 68 3a 31 30 30 25 7d 64 69 76 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2d 6f 76 65 72 6c 61 79 20 64 69 76 2e 69 6e 6e 65 72 20 75 6c 2e 64 6f 75 62 6c 65 20 6c 69 7b 77 69 64 74 68 3a 35 30 25 7d 64 69 76 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2d 6f 76 65 72 6c 61 79 20 64 69 76 2e 69 6e 6e 65 72 20 61 2c 64 69 76 2e 63 6f 6d Data Ascii: :inline;padding:0;margin:0 0 5px;overflow:hidden;white-space:nowrap;text-overflow:ellipsis}div.comment-likes-overlay div.inner ul.single li{width:100%}div.comment-likes-overlay div.inner ul.double li{width:50%}div.comment-likes-overlay div.inner a,div.com
2022-01-14 22:59:44 UTC	117	IN	Data Raw: 62 65 66 6f 72 65 2c 70 2e 63 6f 6d 6d 65 6e 74 2d 6e 6f 74 2d 6c 69 6b 65 64 3a 68 6f 76 65 72 20 61 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 2d 6c 69 6e 6b 3a 62 65 66 6f 72 65 7b 63 6f 6c 6f 72 3a 23 66 31 38 33 31 65 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 30 20 30 7d 64 69 76 2e 63 6f 6d 6d 65 6e 74 2d 6c 69 6b 65 73 2d 6f 76 65 72 6c 61 79 20 64 69 76 20 2e 73 6c 69 64 65 72 2d 6e 61 76 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 77 69 64 74 68 3a 33 31 30 70 78 3b 68 65 69 67 68 74 3a 34 30 70 78 3b 6d 61 72 67 69 6e 3a 31 35 70 78 20 30 20 2d 31 35 70 78 20 2d 31 32 70 78 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 66 64 66 64 Data Ascii: before,p.comment-not-liked:hover a.comment-like-link:before{color:#f1831e;background:0 0}div.comment-likes-overlay div .slider-nav{position:relative;clear:both;width:310px;height:40px;margin:15px 0 -15px -12px;text-align:center;border-top:1px solid #dfdfd
2022-01-14 22:59:44 UTC	118	IN	Data Raw: 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4e 6f 74 69 63 6f 6e 73 22 3b 73 72 63 3a 75 72 6c 28 2f 69 2f 6e 6f 74 69 63 6f 6e 73 2f 2e 2f 4e 6f 74 69 63 6f 6e 73 2e 65 6f 74 3f 29 20 66 6f 72 6d 61 74 28 22 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 22 29 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4e 6f 74 69 63 6f 6e 73 22 3b 73 72 63 3a 75 72 6c 28 22 64 61 74 61 3a 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 66 6f 6e 74 2d 77 6f 66 66 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3b 62 61 73 65 36 34 2c 64 30 39 47 52 67 41 42 41 41 41 41 Data Ascii: osition:relative}@font-face{font-family:"Noticons";src:url(/i/noticons/./Noticons.eot?) format("embedded-opentype");font-weight:400;font-style:normal}@font-face{font-family:"Noticons";src:url("data:application/x-font-woff;charset=utf-8;base64,d09GRgABAAAA
2022-01-14 22:59:44 UTC	119	IN	Data Raw: 77 76 6f 57 34 6a 45 6a 43 79 4d 63 41 31 4d 44 49 42 43 53 5a 30 42 52 41 76 44 32 63 41 41 50 6c 53 4f 6a 51 41 52 41 55 52 41 41 41 41 4c 41 41 73 41 43 77 41 4c 41 42 61 41 49 51 41 7a 41 44 79 41 51 41 42 48 41 46 47 41 5a 51 42 7a 67 49 49 41 72 49 44 54 41 4f 6b 41 2b 41 45 45 67 54 43 42 56 77 46 71 41 59 45 42 6e 59 48 43 41 63 71 42 32 6f 48 6a 67 66 49 43 43 59 4a 48 67 70 2b 43 7a 6f 4c 79 41 78 2b 44 4d 6f 4e 6d 41 33 71 44 69 77 4f 61 41 37 53 44 76 51 50 45 41 38 75 44 33 67 50 6d 67 2f 67 45 44 59 51 6f 42 44 65 45 52 51 52 55 68 47 63 45 66 59 53 59 42 4b 43 45 71 51 53 37 68 4d 4d 45 79 67 54 52 42 4e 79 45 34 6f 54 7a 68 51 47 46 46 67 55 6d 42 54 49 46 4e 77 55 2b 42 55 2b 46 55 77 56 59 68 57 67 46 63 34 57 4f 68 5a 6d 46 70 59 57 71 Data Ascii: wvoW4jEjCyMcA1MDIBCSZ0BRAvD2cAAPlSOjQARAURAAAALAAsACwALABaAIQAzADyAQABHAFGAZQBzgIlArIDTAOkA+AEEgTCBVwFqAYEBnYHCAcqB2oHjgfICCYJHgp+CzoLyAx+DMoNmA3qDiwOaA7SDvQPEA8uD3gPmg/gEDYQoBDeERQRUhGcEfYSYBKCEqQS7hMMEygTRBNyE4oTzhQGFFgUmBTIFNwU+BU+FUwVYhWgFc4WOhZmFpYWq
2022-01-14 22:59:44 UTC	121	IN	Data Raw: 72 39 71 39 4b 64 50 54 30 64 66 51 63 49 39 38 66 71 2b 71 6f 59 51 39 6b 64 47 77 54 55 65 62 76 39 39 39 57 4f 78 55 72 45 31 61 74 6d 6b 43 55 71 62 57 33 2b 66 66 50 78 38 71 6d 6a 2b 46 47 6c 45 33 48 6a 6d 33 43 53 6d 4c 4e 39 44 78 49 51 31 67 61 44 47 6c 6f 7a 36 45 2b 6d 64 5a 4e 6a 37 7a 51 33 68 43 72 57 79 6b 32 59 48 66 63 54 52 75 74 50 76 44 43 43 48 6b 39 74 46 36 78 73 4b 54 30 37 4e 6e 54 6f 35 41 45 4f 61 4c 67 62 51 64 4f 45 52 61 48 61 49 49 46 4a 47 67 79 66 55 51 53 75 45 38 35 64 59 42 54 7a 6b 62 33 39 47 41 49 49 52 36 6e 78 30 32 45 55 70 31 30 42 74 44 79 73 4a 4f 4f 55 79 41 57 6a 51 51 67 71 49 64 67 49 78 65 4e 2b 41 4d 30 4e 52 74 37 52 63 69 4a 31 64 58 46 5a 72 57 31 59 66 32 4d 68 51 74 6e 64 46 59 30 2b 79 61 4d 46 75 Data Ascii: r9q9KdPT0dfQcI98fq+qoYQ9kdGwTUebv999WOxUrE1atmkCUqbW3+ffPx8qmj+FGlE3Hjm3CSmLN9DxIQ1gaDGloz6E+mdZNj7zQ3hCrWyk2YHfcTRutPvDCCHk9tF6xsKT07NnTo5AEOaLgbQdOERaHaIlFJGgyfUQSuE85dYBTzkb39GAIIR6nx02EUp10BtDysJOOUyAWjQQgqIdgIxeN+AM0NRt7RciJ1dXFZrW1Yf2MhQtndFY0+yaMFu
2022-01-14 22:59:44 UTC	122	IN	Data Raw: 75 69 68 39 34 43 6c 6a 6f 47 56 45 47 67 58 6f 69 55 4c 4d 65 31 69 35 76 4c 41 66 6a 38 30 68 72 35 4f 2b 50 2f 33 4a 56 6a 35 6d 37 6c 57 74 38 52 36 37 58 5a 36 7a 71 44 68 69 31 77 6f 2f 6b 4a 4d 44 54 2f 4e 6a 63 51 58 6d 49 6c 33 54 78 38 51 63 45 73 2b 54 54 77 79 2b 63 67 2f 50 61 52 46 51 6e 33 54 62 54 45 43 5a 33 57 67 52 57 73 35 6f 67 39 56 49 42 38 58 72 67 52 57 74 4e 38 59 77 7a 46 77 73 34 52 44 4d 33 55 78 73 4e 57 46 54 4c 4e 37 49 52 79 4f 55 45 47 69 41 64 49 52 44 4e 6e 2b 52 31 79 4e 49 63 69 67 63 69 6a 58 68 6d 46 57 53 4a 52 6d 62 65 4b 41 6a 4d 5a 76 31 37 44 4d 66 44 4c 58 4d 78 34 7a 52 43 4e 2b 4b 6c 2b 4a 78 33 2b 77 59 33 6e 76 6f 31 63 38 75 50 30 6f 4f 66 37 4e 6a 78 7a 66 6b 44 36 66 66 49 56 65 33 38 50 34 62 72 68 57 Data Ascii: uih94CljoGVEGgXoiULMe1i5vLAfj80hr5O+P/3JVj5m7lWt8R67XZ6zqDhi1wo/kJMDT/NjcQXmIl3Tx8QcEs+TTwy+cg/PaRFQn3TbTECZ3WgRWs5og9VIB8XrgRWtN8YwzFws4RDM3UxsNWFTLN7IRyOUEGiAdIRDNn+R1yNIcigcijXhmFWSJRmbeKAjMZv17DMfDLXMx4zRCN+Kl+Jx3+wY3nvo1c8uP0oOf7NjxzfkD6ffIVe38P4brhW
2022-01-14 22:59:44 UTC	123	IN	Data Raw: 65 58 63 34 31 70 33 64 2b 54 47 59 35 64 4d 44 75 2f 36 6a 35 71 46 4e 7a 32 44 71 34 35 65 2f 4d 51 31 72 63 46 4a 4b 7a 66 66 50 76 48 57 42 52 5a 37 62 74 61 45 6a 46 79 44 31 72 76 37 2b 5a 58 74 2b 2b 2f 63 76 6d 35 36 53 4f 55 70 61 54 36 38 4d 49 31 74 39 4a 79 4f 67 32 59 47 59 6e 47 54 45 31 50 4f 51 68 76 46 71 34 32 79 32 71 78 41 77 6e 41 38 35 67 2b 6b 4f 41 74 4d 48 59 70 73 41 66 62 48 47 65 53 69 63 77 76 53 46 57 4c 6f 4a 4a 73 66 59 39 72 55 70 68 6a 39 34 36 32 67 6a 45 46 32 79 65 74 2f 2f 56 4e 6b 2b 70 57 37 33 75 6e 64 2b 33 4a 2f 56 64 4e 4b 4f 6c 5a 59 69 77 51 4f 51 4d 6e 69 72 71 52 6f 35 57 2b 56 52 66 64 30 31 4d 39 63 63 2f 63 36 46 52 66 56 6d 61 56 63 2f 53 49 32 4b 79 6f 58 71 4e 64 5a 62 4b 4a 52 38 69 58 2b 34 61 69 Data Ascii: eXc41p3d+TGY5dMDu/6j5qFNz2Dq45e/MQ1rcFJKzffPvHWBRZ7btaEjFyD1rv7+ZXt++/cvm56SOUpaT68MI1t9JyOg2YGYnGTE1POQhvFq42y2qxAwnA85g+kOAtMHYpsAfbHGeSicwvSFWLoJJsfnY9rUphj9462gjEF2yet//VNk+pW73und+3J/VdNKOlZYiwQOQMnirqRo5W+VRfd01M9cc/c6FRfVmaVc/SI2KyoXqNdZbKJR8iX+4ai

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49771	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	57	OUT	GET /_static/??/wp-content/js/mobile-useragent-info.js,/wp-content/js/rlt-proxy.js?m=1637704497j HTTP/1.1 Host: s1.wp.com Connection: keep-alive Origin: https://priderecovery779413013.wordpress.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49770	192.0.77.32	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 22:59:44 UTC	57	OUT	GET /_static/??-eJx9jkEKAjEMRS9kjXVAcCGepa2xVtOkTFIHb++spCK4+w/+gwdLc0nYkA3shhUVWo+giBdCg8IJlpakOrUX4TapbmBQaneNei6skFEcSQpWhL/AXSmU+Z86YyTJ68ywvgb8kYbESIEfLgV+BoVP3bme/MEfd95P0/7BoNnUh8=?cssminify=yes HTTP/1.1 Host: s1.wp.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://priderecovery779413013.wordpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6784 Parent PID: 5476

General

Start time:	23:59:40
Start date:	14/01/2022
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://priderecovery779413013.wordpress.com
Imagebase:	0x7ff68b0a0000
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: 7000 Parent PID: 6784

General

Start time:	23:59:41
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1528,3464267663473017341,12747655211763697408,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1912 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis