

ID: 655312
Cookbook: browseurl.jbs
Time: 22:26:36
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2

Windows Analysis Report https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*peter.boyd@southside.com*5

- Overview 5
  - General Information 5
  - Detection 5
  - Signatures 5
  - Classification 5
- Process Tree 5
- Malware Configuration 5
- Yara Signatures 5
  - HTML 5
- Sigma Signatures 5
- Snort Signatures 6
- Joe Sandbox Signatures 6
  - AV Detection 6
  - Phishing 6
  - Networking 6
- Mitre Att&ck Matrix 6
- Behavior Graph 6
- Screenshots 7
  - Thumbnails 7
- Antivirus, Machine Learning and Genetic Malware Detection 8
  - Initial Sample 8
  - Dropped Files 8
  - Unpacked PE Files 8
  - Domains 8
  - URLs 8
- Domains and IPs 9
  - Contacted Domains 9
  - Contacted URLs 9
  - URLs from Memory and Binaries 10
  - World Map of Contacted IPs 11
    - Public IPs 11
  - Private 11
- General Information 12
  - Warnings 12
- Simulations 12
  - Behavior and APIs 12
- Joe Sandbox View / Context 12
  - IPs 12
  - Domains 13
  - ASNs 13
  - JA3 Fingerprints 13
  - Dropped Files 13
- Created / dropped Files 13
  - C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 13
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\15f30535-bb9d-4e3a-9874-6ee193a2e98f.tmp 13
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\227c84e5-a814-40c6-bba2-4b27d39d35a0.tmp 14
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\4977120e-ab98-44e4-aa03-87608b796362.tmp 14
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\89a54fcc-2f3f-476a-af7e-053f29dd2229.tmp 14
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\9df95275-086d-4b48-ab14-12af502b7e05.tmp 15
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 15
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\01297bb9-9604-40c0-ae07-cda5c409bff6.tmp 15
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\563d1f68-1e7f-49cf-95b5-5aba8653d6ed.tmp 16
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5be07fa1-ccbd-401f-a548-6648548bf40b.tmp 16
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp 16
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 17
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 17
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 17
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 18
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 18
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 18
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 19
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\120193ba-0a86-4a54-9836-e68e52baf3d2.tmp 19
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 19
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 20
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d1d589aa-f29a-4400-8545-7f3988e27b0a.tmp 20
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 20
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 20
  - C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\de2ec36e-0b84-4b61-8527-33130458a3b8.tmp 21

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 22
C:\Users\user\AppData\Local\Temp\42d57711-867b-4052-ac5b-de1fc9d5eba4.tmp 22
C:\Users\user\AppData\Local\Temp\8b83a463-ed04-4238-9c6b-58bdd40b2c8e.tmp 23
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\42d57711-867b-4052-ac5b-de1fc9d5eba4.tmp 23
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\bg\messages.json 23
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ca\messages.json 24
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\cs\messages.json 24
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\da\messages.json 24
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\de\messages.json 25
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\el\messages.json 25
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\en\messages.json 25
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\en_GB\messages.json 26
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\es\messages.json 26
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\es_419\messages.json 26
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\et\messages.json 27
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\fi\messages.json 27
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\fil\messages.json 27
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\fr\messages.json 28
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\hi\messages.json 28
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\hr\messages.json 28
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\hu\messages.json 29
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\id\messages.json 29
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\it\messages.json 29
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ja\messages.json 29
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ko\messages.json 30
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\lt\messages.json 30
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\lv\messages.json 30
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\nb\messages.json 31
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\nl\messages.json 31
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\pl\messages.json 31
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\pt_BR\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\pt_PT\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ro\messages.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ru\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sk\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sl\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sr\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sv\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\th\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\tr\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\uk\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\vi\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\zh_CN\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\zh_TW\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_metadata\verified_contents.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\craw_background.js 37
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\craw_window.js 37
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\css\craw_window.css 37
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\html\craw_window.html 38
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\flapper.gif 38
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\icon_128.png 38
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\icon_16.png 39
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button.png 39
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_close.png 39
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_hover.png 40
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_maximize.png 40
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_pressed.png 40
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\manifest.json 40
Static File Info 41
Network Behavior 41
Snort IDS Alerts 41
Network Port Distribution 41
TCP Packets 41
UDP Packets 43
DNS Queries 44
DNS Answers 45
HTTP Request Dependency Graph 46
HTTPS Proxied Packets 46
Statistics 87
Behavior 87
System Behavior 87
Analysis Process: chrome.exePID: 1416, Parent PID: 5544 87
General 87
File Activities 87
Registry Activities 88
Analysis Process: chrome.exePID: 6120, Parent PID: 1416 88
General 88
File Activities 88

Copyright Joe Security LLC 2022

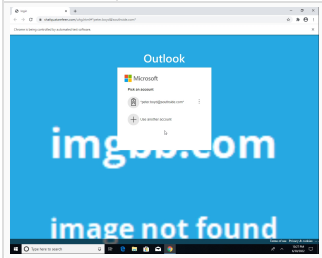
Windows Analysis Report

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

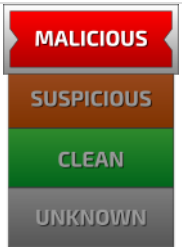
Overview

General Information

Sample URL:	http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*peter.boyd@southside.com*
Analysis ID:	655312
Infos:	



Detection



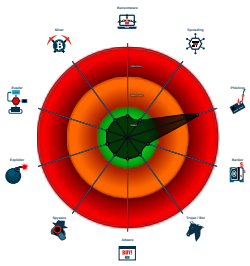
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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: 1416 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#*peter.boyd@southside.com* MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6120 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1596,15411392373280957286,14155618800222134520,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1916 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
70467.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt - Source IP: 192.154.231.67 - Destination IP: 192.168.2.5

Timestamp:	192.154.231.67192.168.2.5443497812013145 06/30/22-22:27:53.591368
SID:	2013145
Source Port:	443
Destination Port:	49781
Protocol:	TCP
Classtype:	Executable code was detected

Joe Sandbox Signatures

AV Detection



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

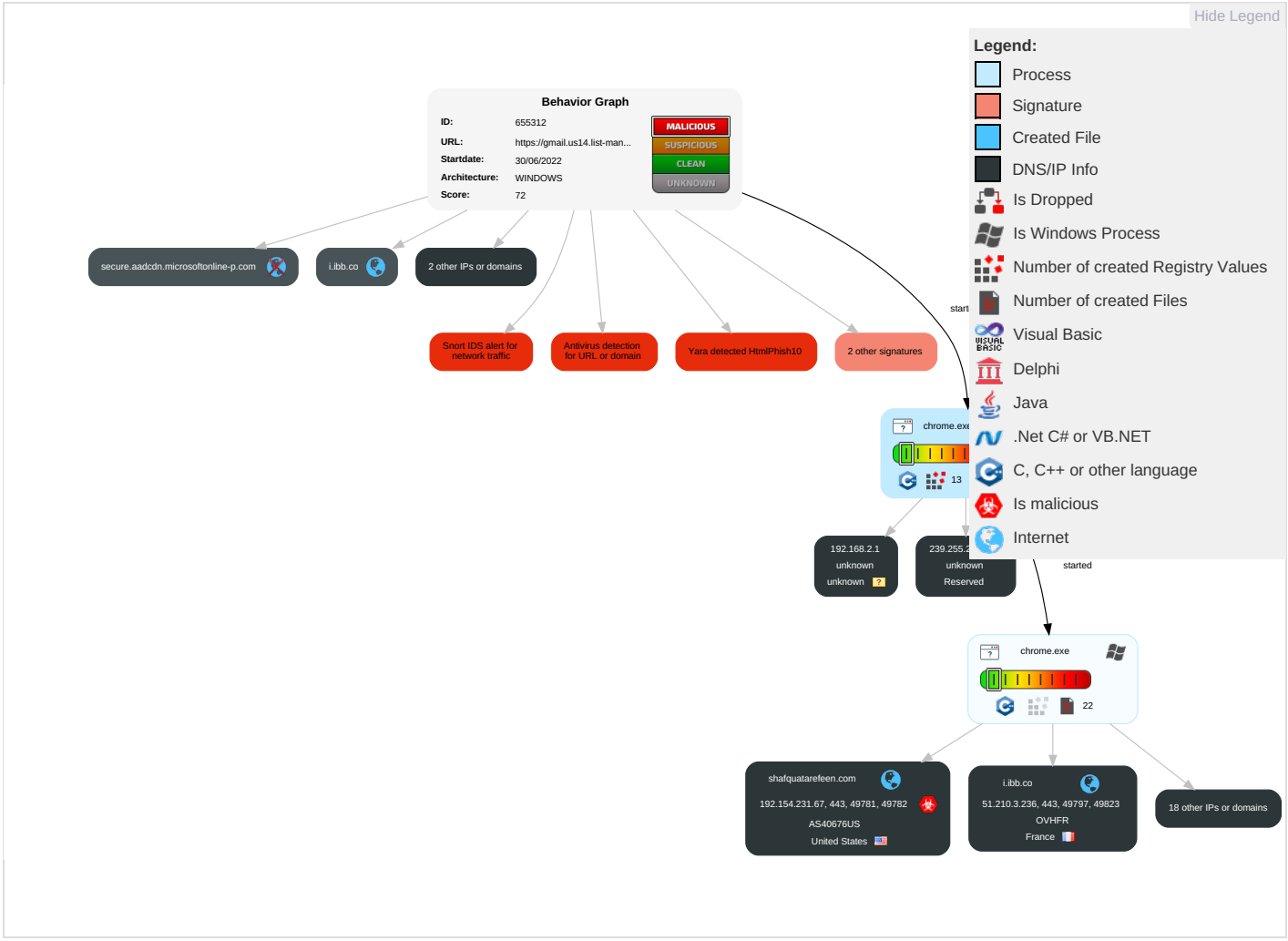


Snort IDS alert for network traffic

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

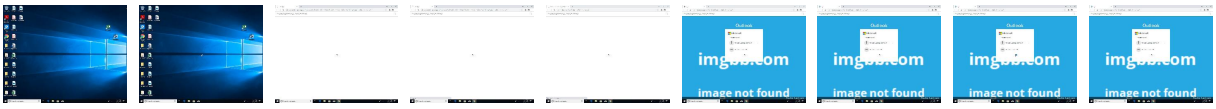
Behavior Graph

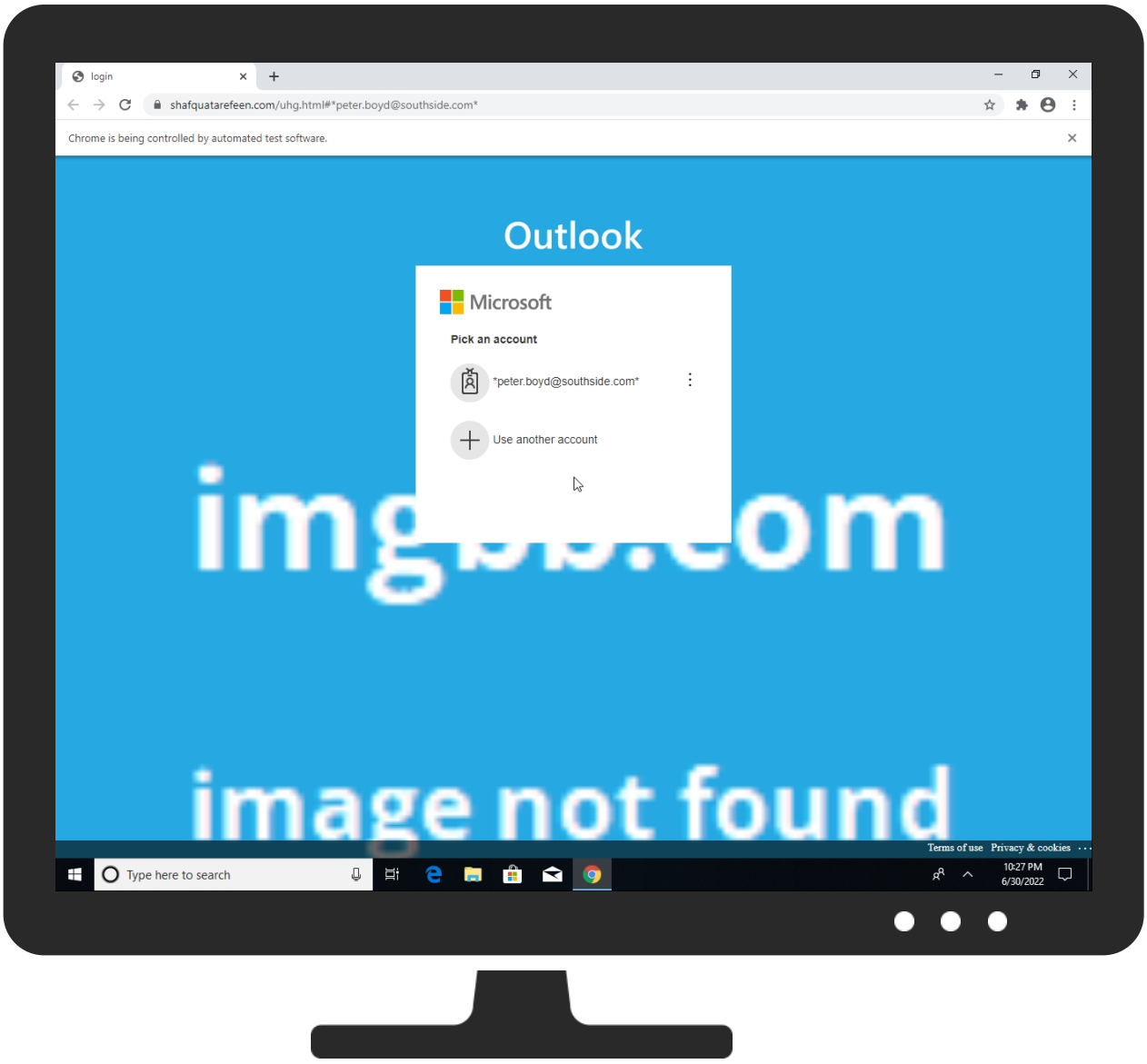


Screenshots

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#*peter.boyd@southside.com*	0%	Virustotal		Browse
http://https://gmail.us14.list-manage.com/track/click?u=957e6b6833ddd63bbe471b4e4&id=18858b02d6&e=7ce018b90e#*peter.boyd@southside.com*	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://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://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png	0%	Avira URL Cloud	safe	
http://https://shafquatarefeen.com/uhg.html#	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	0%	Avira URL Cloud	safe	
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://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f.jpg	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_kx1da7l2dz6nhe9kugk19a2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_9lddfuhsopopkddlczwbda2.css	0%	Avira URL Cloud	safe	
http://https://shafquatarefeen.com/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png	0%	Avira URL Cloud	safe	
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	104.18.10.207	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	104.17.24.14	true	false		high
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
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		unknown
i.ibb.co	51.210.3.236	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

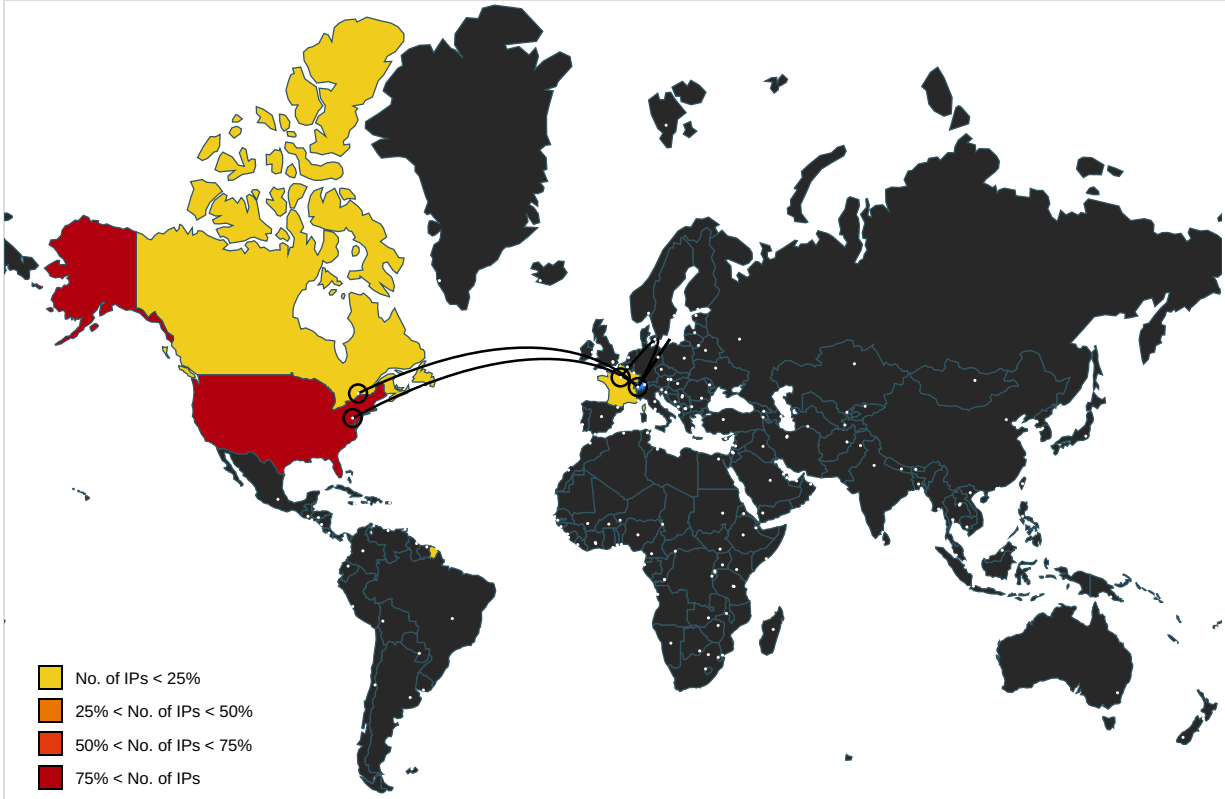
Name	Malicious	Antivirus Detection	Reputation
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	false		high
http://https://trocha.com.co/gvx	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=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://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png	false	• Avira URL Cloud: safe	unknown
http://https://shafquatarefeen.com/uhg.html#*peter.boyd@southside.com*	true		unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	false	• Avira URL Cloud: safe	unknown
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
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.svg	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f.jpg	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_kx1da7l2dz6nhe9kugk19a2.js	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://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_9lddfuhsopopkddlczwbda2.css	false	• Avira URL Cloud: safe	unknown
http://https://shafquatarefeen.com/favicon.ico	true	• Avira URL Cloud: phishing	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png	false	• Avira URL Cloud: safe	unknown
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	120193ba-0a86-4a54-9836-e68e52baf3d2.tmp.3.dr, 94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.1.dr	false		high
http://https://ogs.google.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://shafquatarefeen.com/uhg.html#	History Provider Cache.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.1.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.1.dr	false		high
http://https://www.google.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://clients2.googleusercontent.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://apis.google.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.1.dr	false		high
http://https://www.google.com/	manifest.json.1.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://clients2.google.com	94cb139c-5db3-44df-b17d-c74f0e4c05e4.tmp.3.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
69.172.198.108	trocha.com.co	Canada		54643	IDIGITALCA	false
51.210.3.236	i.ibb.co	France		16276	OVHFR	false
104.18.11.207	maxcdn.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

Private

IP
192.168.2.1
127.0.0.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655312
Start date and time: 30/06/202222:26:36	2022-06-30 22:26:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
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#*peter.boyd@southside.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:	11
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:	mal72.phis.win@25/86@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): MpCmdRun.exe, BackgroundTransferHost.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.36.206, 2.19.77.84, 74.125.111.138, 34.104.35.123, 142.251.36.195, 2.20.16.227, 20.190.159.75, 20.190.159.2, 20.190.159.71, 20.190.159.64, 40.126.31.73, 20.190.159.23, 40.126.31.69, 20.190.159.0, 69.16.175.10, 69.16.175.42, 142.251.36.170, 80.67.82.211, 80.67.82.235, 52.152.110.14, 20.238.103.94, 40.125.122.176, 142.251.36.227, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, e13829.x.akamaiedge.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, arc.msn.com, redirector.gvt1.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, e13761.dscg.akamaiedge.net, sls.update.microsoft.com, update.googleapis.com, swc.list-manage.com.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, global-entry-afdthirdparty-fallback.trafficmanager.net, glb.sls.prod.dcat.dsp.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, content-autofill.googleapis.com, r5.sn-4g5edn6k.gvt1.com, aadcdnoriginwus2.azureedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, www.tm.ak.prd.aadg.akadns.net, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupd
- 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 GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\15f30535-bb9d-4e3a-9874-6ee193a2e98f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7510967283566052
Encrypted:	false
SSDEEP:	384:7HPow6dLOWx8zNArpv8o3zQabHmvGH6rlaMaxjuC2lrRkmlypKAo8jOimwNN1g5Z:h+x52qzH8en+o6An3akKGQQVw
MD5:	C0B5CFCCDCBE205A8790A551CCEC8196
SHA1:	BAE5218BE6C7EB33D1E496E9E7E3F2DDC717C6B9
SHA-256:	95AD4854FB84FEB6E0FAB9FB7F85F31A7A0B39AC7BCF0BF948D80420D4F0399B
SHA-512:	040A9485984656561B5EBC8A287D28282A31BFDBE07BD2316CABA2B487110CBD363B50CDB6B46DDE5324A938F7A3EF7926E6F14088E07635251FE07AEA325E4B
Malicious:	false
Reputation:	low

Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\227c84e5-a814-40c6-bba2-4b27d39d35a0.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7515190250628203
Encrypted:	false
SSDEEP:	384:dHPow6dLy5WwVV38zNArpv8o3zQabHmvGH6rlaMaxjuC2lrRkmlypKAo8jOimwN0:hK+x52qzH8en+o6An3akKGQQV0
MD5:	641AA562CF3839980B22C938CAEA5287
SHA1:	781B13468511B1CB1ADD3CC4FE5CEA74917322DA
SHA-256:	78B5F894B19EA99899E0DDBF1407BAE777CED010496FA2F1D5D4061A303F0055
SHA-512:	2EC0B255F8CE53ADD7DD7B07A989D1DCE264AAC740EFAD728F62CDC50F5710CC194E0CD6E171A000FB8186CEADC3A9E408411535D1E100D64BF08AC365A8 2AF
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4977120e-ab98-44e4-aa03-87608b796362.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):	405216
Entropy (8bit):	6.013865097476903
Encrypted:	false
SSDEEP:	12288:JSPcBMFPQl3mz8yocxzurRDn9nfNxF4ijZVtilBy:JSCMNQNmzv0RzxxPjjt8y
MD5:	C3219A999559A61F67D7A73E0634E8E9
SHA1:	7FB99AF30929F93601E4EE5D5551543C3AC4DC8B
SHA-256:	C97DBF911B7C8DB1F0B13B4257AFCD5B1492FFD6314B2FD3C396D8ECDCF1DEF4
SHA-512:	0D6CFFEF713348C40110135AC380BE74D808941DDC562C80571C7C75920FDDD84DFCCD9B047AE5E3243EEB4639E5819F340080D985452CF0A559DC4EBDBA4(B
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":1.656653269274321e+12,"network":1.65662087e+12,"ticks":201200751.0,"uncertainty":4001488.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"133011268666045

C:\Users\user\AppData\Local\Google\Chrome\User Data\89a54fcc-2f3f-476a-af7e-053f29dd2229.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):	405216
Entropy (8bit):	6.013865097476903
Encrypted:	false
SSDEEP:	12288:JSPcBMFPQl3mz8yocxzurRDn9nfNxF4ijZVtilBy:JSCMNQNmzv0RzxxPjjt8y
MD5:	C3219A999559A61F67D7A73E0634E8E9
SHA1:	7FB99AF30929F93601E4EE5D5551543C3AC4DC8B
SHA-256:	C97DBF911B7C8DB1F0B13B4257AFCD5B1492FFD6314B2FD3C396D8ECDCF1DEF4
SHA-512:	0D6CFFEF713348C40110135AC380BE74D808941DDC562C80571C7C75920FDDD84DFCCD9B047AE5E3243EEB4639E5819F340080D985452CF0A559DC4EBDBA4(B

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":1.656653269274321e+12,"network":1.65662087e+12,"ticks":201200751.0,"uncertainty":4001488.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"133011268666045

C:\Users\user\AppData\Local\Google\Chrome\User Data\9df95275-086d-4b48-ab14-12af502b7e05.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):	405216
Entropy (8bit):	6.013865205733858
Encrypted:	false
SSDEEP:	12288:sSPcBMFPQl3mz8yocxzurRDn9nfNxF4ijZVtilBy:sSCMNQNmzv0RzxxPjjt8y
MD5:	5984A28520F67C0029DB3877F683D0B1
SHA1:	B59A4106CD3CC1648C62B03CC037A24A9A6E09F6
SHA-256:	B6824962F0B8E1C946F294949E87425709CAB4331B43D2BCDB830AF824671E7C
SHA-512:	34D9225560F97C3F2A011074337C0B999F0284997745CD40D7BAEB9D585E04DDE557D3EB874F35C15010167F2EBAD81A516616B670901AB357235F4B44E28CD7
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":1.656653269274321e+12,"network":1.65662087e+12,"ticks":201200751.0,"uncertainty":4001488.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469974589"},"policy":{"last_statistics_update":"133011268666045

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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9n:+Y66cR9
MD5:	7A9D405E9218ED86C7ED3BB729DAA896
SHA1:	E5BB69E833231B755B20E5A0C9B2392D8B923C66
SHA-256:	D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF
SHA-512:	F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\01297bb9-9604-40c0-ae07-cda5c409bff6.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\Google\Chrome\User Data\Default\563d1f68-1e7f-49cf-95b5-5aba8653d6ed.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):	5281
Entropy (8bit):	4.982431276391639
Encrypted:	false
SSDEEP:	96:nFdrLcq1pSKI0Ik0JCVRWL8Dkm11IbOTQVuwn:nFdrD1pSWC4VYWkmq
MD5:	7CD29A5AFBD9BCDD2ABBA9EE4258F9A7
SHA1:	F4367CADB3B190BFA8981A6ED6C48CE86D797223
SHA-256:	B4258AA78E6E09459B4A303C6B8AD4CC85FF8B130C9210EFA3B2A84EB70EDD11
SHA-512:	160E85B9A7ECF1FBD34BF8E818A45951EBEBCC6548B40618C8B892C3572F8BF7BE000D87F167EB425FC83076BA93DDAB4AA22179F249F4D3C6AD492522A8A537
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301126867693704","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324854 2628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{ "advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.goog leusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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):	374
Entropy (8bit):	5.207741834846841
Encrypted:	false
SSDEEP:	6:en+q2P923iKKdK25+Xqx8chI+IFUtqVqcXZmwYVCbVkwO923iKKdK25+Xqx8ch+Q:zv45KkTXfchI3FUtS/Z5L5KkTXfch1J
MD5:	F15FDCB29B8E1480ABE93C5CE43475CF
SHA1:	185EFB49DCEC7258BE5DB6E25070157CF9E0760C
SHA-256:	F523D469030D58E742E9C85AD8E99480B19E9C29B2A32B476B59905C0FD8B91D
SHA-512:	BD7A177F0BC2E9CE8F93C06E71D9B2F827EB648B3DA6B491B1255DC076DE77A0B8DDE93726C108229699E22376B9E40118FC232338F6CAF946AE582BAA01B44
Malicious:	false
Reputation:	low
Preview:	2022/06/30-22:28:04.364 1108 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-22:28:04.366 1108 Recovering log #3.2022/06/30-22:28:04.367 1108 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):	374
Entropy (8bit):	5.207741834846841
Encrypted:	false
SSDEEP:	6:en+q2P923iKKdK25+Xqx8chI+IFUtqVqcXZmwYVCbVkwO923iKKdK25+Xqx8ch+Q:zv45KkTXfchI3FUtS/Z5L5KkTXfch1J
MD5:	F15FDCB29B8E1480ABE93C5CE43475CF
SHA1:	185EFB49DCEC7258BE5DB6E25070157CF9E0760C
SHA-256:	F523D469030D58E742E9C85AD8E99480B19E9C29B2A32B476B59905C0FD8B91D
SHA-512:	BD7A177F0BC2E9CE8F93C06E71D9B2F827EB648B3DA6B491B1255DC076DE77A0B8DDE93726C108229699E22376B9E40118FC232338F6CAF946AE582BAA01B44
Malicious:	false
Reputation:	low
Preview:	2022/06/30-22:28:04.364 1108 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-22:28:04.366 1108 Recovering log #3.2022/06/30-22:28:04.367 1108 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):	626
Entropy (8bit):	5.225375960854259
Encrypted:	false
SSDEEP:	12:8szI8SbSAvs+AbLoSp0PzNzUun3tLT3tVUbZeZ0jnFWKBk778B/xgskZBaKETdEY:8YIfbS2s+AYS+zh3tn3t4ZJAIY78BJge
MD5:	7FE2651987471CF83391ACF860A86449
SHA1:	9AFC442128E3EC96C3FB387E4F3D66EABC34652D
SHA-256:	9F859F313650B262FD3A8489F012F6750656F568BDD96A5D203DF08DF4A786FF
SHA-512:	9F3D20A3F90F960620E8294ED70658553855FF1918B51B101BB04B3195AC6D52468B39FF922F5F7A2D5472DE49A92A2C5A48E1B0C51D5E9893EE5A8B7C6932D9
Malicious:	false
Reputation:	low
Preview:	.....".l....boyd..com..html..https..login..peter..shafquatarefeen..southside..uhg*m.....boyd.....com.....html.....https.....login.....peter.....shafquatarefeen.....southside..... .uhg..2.....a.....b.....c.....d.....e.....f.....g.....h.....i.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....y...:S..... .....Bl...h..... .....*?https://shafquatarefeen.com/uhg.html#*peter.boyd@southside.com*2.login:.....J..... &,1;...

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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DB CAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324854 2628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{ "advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.goog leusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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):	5281
Entropy (8bit):	4.982431276391639
Encrypted:	false
SSDEEP:	96:nFdrLcq1pSKI0Ik0JCVRWL8Dkm11IbOTQVuwn:nFdrD1pSWC4VYWkmq
MD5:	7CD29A5AFBD9BCDD2ABBA9EE4258F9A7
SHA1:	F4367CADB3B190BFA8981A6ED6C48CE86D797223
SHA-256:	B4258AA78E6E09459B4A303C6B8AD4CC85FF8B130C9210EFA3B2A84EB70EDD11
SHA-512:	160E85B9A7ECF1FBD34BF8E818A45951EBEBCC6548B40618C8B892C3572F8BF7BE000D87F167EB425FC83076BA93DDAB4AA22179F249F4D3C6AD492522A8A5 37
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301126867693704","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.576918095062751
Encrypted:	false
SSDEEP:	384:yX5tILlN9PXk1kXqKf/pUZNCgVLH2HfDLrUYYK/hW4T:zLlDk1kXqKf/pUZNCgVLH2HffrUYR/sM
MD5:	824B97EE64414AF59469FE37A1160EA4
SHA1:	A9FCA9704C49CDD3E91A44BC67A244942E3B337F
SHA-256:	5D7AD780BE6EA73EAA5D9BE2ED8BA5216FE4112A4D65EEA264827BA170E8EB89
SHA-512:	3FB79033A6197F5BFBD3E094432AF9FE9BBBC5B3DC315AC4CF7DC5CA53AF4146DA687D8D814E89313C5FB9447D1585DD11E9E129E4F06404656D892421B507E A
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":"13301126866953264","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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\120193ba-0a86-4a54-9836-e68e52baf3d2.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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\d1d589aa-f29a-4400-8545-7f3988e27b0a.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):	5.574523599228268
Encrypted:	false
SSDEEP:	384:yX5t1LlN9PXk1kXqKf/pUZNCgVLH2HfDLrUctA/hW4/:kLlDk1kXqKf/pUZNCgVLH2HffrUcS/s0
MD5:	7DA2A1D3E42DB2F95C24C5653BECB809
SHA1:	1FED915B328AB2185C803C9AB71AD5C3EF104726
SHA-256:	550AF05E9758409A2856EA852E7F9B80CC95088249C425B2AEF73E3DD971F068
SHA-512:	4ADCD87363F2F9F57AC5458D3866A305B2DFD50E68F3F33FD7F01D5869D2865E829C116EEFF8A89A326F7DE40AD52852680936936FD9C25CE4B494FFAEE246C
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":"13301126866953264","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\de2ec36e-0b84-4b61-8527-33130458a3b8.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):	5265
Entropy (8bit):	4.97842126592744
Encrypted:	false
SSDEEP:	96:nFdrHG1pSKl0lk0JCVRWL8Dkm11IbOTQVuwn:nFdrm1pSWC4VYWkmq
MD5:	91E35A7CCDEEBAD947F70D966DE6F197
SHA1:	0AF928C4CF225F514CC7217642536B6141BF5FAC
SHA-256:	6DB2EDC4F78A4202EBD778458DE1AE6766E9800E5B5A192888EDCFC8D2EB2F11
SHA-512:	97DFDD6828DBA13D816B6FA47605FE213685F2D74DE13C34D253F81DA5F232B2A18B6EB62C4A48398610AFF82A6A3F24F7B0E19620D04079AEAB268C1D3057D C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301126867693704","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

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):	405216
Entropy (8bit):	6.013865205733858
Encrypted:	false
SSDEEP:	12288:sSPcBMFPQl3mz8yocxzurRDn9nfNxF4ijZVtilBy:sSCMNQNmzv0RzxxPjjt8y
MD5:	5984A28520F67C0029DB3877F683D0B1
SHA1:	B59A4106CD3CC1648C62B03CC037A24A9A6E09F6
SHA-256:	B6824962F0B8E1C946F294949E87425709CAB4331B43D2BCDB830AF824671E7C
SHA-512:	34D9225560F97C3F2A011074337C0B999F0284997745CD40D7BAEB9D585E04DDE557D3EB874F35C15010167F2EBAD81A516616B670901AB357235F4B44E28CD7
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":1.656653269274321e+12,"network":1.65662087e+12,"ticks":201200751.0,"uncertainty":4001488.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469974589"},"policy":{"last_statistics_update":"133011268666045

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7515190250628203
Encrypted:	false
SSDEEP:	384:dHPow6dLy5WwVV38zNArpv8o3zQabHmvGH6rlaMaxjuC2lrRkmlypKAo8jOimwN0:hK+x52qzH8en+o6An3akKGQQV0
MD5:	641AA562CF3839980B22C938CAEA5287
SHA1:	781B13468511B1CB1ADD3CC4FE5CEA74917322DA
SHA-256:	78B5F894B19EA99899E0DDBF1407BAE777CED010496FA2F1D5D4061A303F0055
SHA-512:	2EC0B255F8CE53ADD7DD7B07A989D1DCE264AAC740EFAD728F62CDC50F5710CC194E0CD6E171A000FB8186CEADC3A9E408411535D1E100D64BF08AC365A8 2AF
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\42d57711-867b-4052-ac5b-de1fc9d5eba4.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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\8b83a463-ed04-4238-9c6b-58bdd40b2c8e.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\scoped_dir1416_1242225580\42d57711-867b-4052-ac5b-de1fc9d5eba4.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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir1416_1242225580\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CI B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	modified
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\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:YGGYpQTajDRdes6KUVJ8epQTNufIRdes6K27lO/NrnLAOK:YHYpQ67esNMpQJufI7esN27lOFvAOK
MD5:	E5BBE7DBBE75F45BDCD49DB8C797106E
SHA1:	0F069D7D19768180945F0D8B67DC71262FD586A2
SHA-256:	BFFB2248B4C66306133FA6ECBB1541F44B3BE22CC8D9A338D690E0B1D0C85532
SHA-512:	F6FE20B7A3B99BDBBF6F4737C8C63FE3098F060E6791BC40ED0E95FA5F93AA55C2643766EA2BE099E42EC378CB6E4B6FE7B5F2DA56C03A6A990B94A1F872B8 25
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":{"messag e":"Sovelluksen sis\u00e4iset maksut eiv\u00e4t ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"please_sign_in":{"message":"Kirjaudu sis\u00e 4\u00e4n Chromeen."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\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_dir1416_124225580\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:	5504F6D440779BC96571863D60B1E175EEDDC2E65B1ABBCFCFD19123F329F2E025FBA4D49BD23E33B77FFB6061BA6645132E04D4A7DEDE77F514B2151CDDF896
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\u00e9seau."},"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_dir1416_124225580\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:YHYpIcQvCjljRpVVBXPsqihQ
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1AC
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\u094d\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"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940 \u0909\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_dir1416_124225580\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_dir1416_124225580\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:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD09
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."},"plea se_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_dir1416_124225580\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":"P embayaran 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_dir1416_124225580\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":"Pagam enti 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_dir1416_124225580\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_dir1416_124225580\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_dir1416_124225580\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:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC68644 E
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_dir1416_124225580\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:YHYpp11dy9iIdlvpc2ZgWOFvAOK
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_dir1416_124225580\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_dir1416_124225580\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:	B0987002F8BC4F0B0AC41A87E90BA729464BF2F34D1CC413DD3837019F5F37FD46EB9E9FDABB97F5BDCB50768ABF808AF6E7C531CD7BCA477C71990D2F13335B
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_dir1416_124225580\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_dir1416_124225580\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	513
Entropy (8bit):	4.734605177119403
Encrypted:	false
SSDEEP:	12:YGGYpGAV9hv3/1PIc6WIc3paIBMMAV+KcIWO/NrnLAOK:YHYpGwLvt5R53pacHw1pWOFvAOK
MD5:	1F4BC8A5EFD59D61127ABEECD4B6CAE3
SHA1:	8647B4D2D643AE4F784ABDDC50D87A39AD02971A
SHA-256:	E1950CBBF056F068EA56160DDB318F3E6232BFBBE096D221C7CA6FCAACE2A8B9
SHA-512:	B58A95BBBC0A16B06826684198B481D2E15A7C760956721C3B538C62C902873A7856F328506457EE66311E45D7A16A4AAAC85B12853AA7EF09780189D28EB3DE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplicativo indispon\u00edvel no momento."},"craw_connect_to_network":{"message":"Conecte-se a uma rede."},"app_name": {"message":"Pagamentos da Chrome Web Store"},"app_description":{"message":"Pagamentos da Chrome Web Store"},"iap_unavailable":{"message":"No momento, os Pagamentos no aplicativo n\u00e3o est\u00e3o dispon\u00edveis."},"please_sign_in":{"message":"Fa\u00e7a login no Google Chrome."},"jwt_retrieve_failed":{" message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\pt_PT\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):	4.742240430473613
Encrypted:	false
SSDEEP:	12:YGGYpmvMAV9BKx1PIZUFWIZUapITEpBqMAVCWWO/NrnLAOK:YHYpmvMwOxtEUIEUapIITqMwCWWOFvAD
MD5:	D80ECE7E4B3741CD9CD29B89D006B864
SHA1:	8F0D587B78E36861ED00524ABF886FA20E14CAE4
SHA-256:	C8FF9ACAEA1D3B6F8483339CB40F66BC563CCA8DD87F2337F813C492B20F451B
SHA-512:	8A53D9618BBD1A62CD48501E5620932631C1B045612082D99429628D2BF4409AEE3FA695107E82037B5CB332111C456CF3A74235C66B61380CF1E382914F1088
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplica\u00e7\u00e3o atualmente indispon\u00edvel."},"craw_connect_to_network":{"message":"Ligue-se a uma rede."}," app_name":{"message":"Pagamentos via Chrome Web Store"},"app_description":{"message":"Pagamentos via Chrome Web Store"},"iap_unavailable":{"message":"Os Pagamentos na app est\u00e3o atualmente indispon\u00edveis."},"please_sign_in":{"message":"Inicie sess\u00e3o no Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	554
Entropy (8bit):	4.8596885592394505
Encrypted:	false
SSDEEP:	12:YGGYpqOHHEG7PMeH8EPJWb2r9EWJWb2r9RpmJW9FjkUhI3C7PMdWO/NrnLAOK:YHYpbnEG7PjlJBfJBRpmJmBh57PEWOFY
MD5:	D63E66B94A4EA2085D80E76209582FB1
SHA1:	4ECAC3EB64DD6253310A0776E6D42257FC290D77
SHA-256:	91A5AAD210C3E0241106E8821B3897EDEFEC9D85033C94DB2324FF3A5FDE5AC7
SHA-512:	09AC34CF286FD0730EED4F6DB3E2FD00A026D0F42DCC75AE49B045DDAD38DFA38B0FB7823ECAC8B0A9BC2A89F4EAF4BCE081779F2ECDF6CC39286045577DC5C9
Malicious:	false

Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u00cen prezent, aplica\u021bia nu este disponibil\u0103."},"craw_connect_to_network":{"message":"Conecteaz\u0103-te la o re \u021bea."},"app_name":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome"},"app_description":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome "},"iap_unavailable":{"message":"Pl\u0103\u021bile \u00een aplica\u021bie nu sunt disponibile momentan."},"please_sign_in":{"message":"Conecteaz\u0103-te la Chr ome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1165
Entropy (8bit):	4.224419823550506
Encrypted:	false
SSDEEP:	24:YHYpNQVFc0BHlbZ0JRiKUG0L6RqQV9zJd0L6RqQV9zJRp00EQVqaQVFc0BRTlPzU:YHYpNQLHFQYKA6wQTz+6wQTz3paQAaQ8
MD5:	22F9E62ABAD82C2190A839851245A495
SHA1:	E7F79BD875918F0D0799DB5F45FAC6297FB66AF7
SHA-256:	9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F
SHA-512:	F577F2F0C344C4E4050AF025A9FB9AC78CADF7FE177F63AB9863826A9808B7FBF5D3363E3B61D7A6DB083EF5EBAC5474D710347B701640AB9C229A3E5D1F0A4 8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043 d\u043e."},"craw_connect_to_network":{"message":"\u041f\u043e\u0434\u043a\u043b\u044e\u0447\u0438\u0442\u0435\u0441\u044c \u043a \u0441\u0435\u0442\u0 438."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044b\u0435 \u0447\u0430\u0441\u0442\u0438 \u0441\u0435\u0440\u0432\u0438\u0441\u0430 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u044b."},''

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	548
Entropy (8bit):	4.850036636276313
Encrypted:	false
SSDEEP:	12:YGGYprMpsgCmIkPJE7ZEWJE7ZRpmJEtMxfAVADJ4ZAvIWO/NrnLAOK:YHYprMFCmvJE7ZfJE7ZRpmJEtMSVGKZo
MD5:	4BBAA10FD00AADBBA3EF6E805E8E1A62
SHA1:	1991901BD6A20C4A7977F09DF30C0CFF0524C504
SHA-256:	906C4F7FDDE15DE4C841E7910BBF14D9175E894BCB244B56E8447A5ADFA5B7AB
SHA-512:	3490F8826E3DB0C8B4FE7B1866DA27F6585ADF52E74392A592A60A916E8A784FF7B92B3DE8985084546D663588369D9BB03FCB25196B7F9C6DF607BEB7DEF01(
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplik\u00e1cia moment\u00e1lne nie je dostupn\u00e1."},"craw_connect_to_network":{"message":"Pripojte sa k sieti."},"app_name": {"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message": "Platby v aplik\u00e1cii moment\u00e1lne nie s\u00fa k dispoz\u00edcii."},"please_sign_in":{"message":"Prihl\u00e1ste sa do prehliada\u010da Chrome."},"jwt_retr ieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.7695148367588285
Encrypted:	false
SSDEEP:	12:YGGYpTOEtyPFTEPJEsvmfEWJEsvmfRpmJEiArERfH5/4WO/NrnLAOK:YHYpqoyPRAJEs4fJEs4RpmJEi6AfH5/x
MD5:	F45DE58765A37FD095319D7DEB0F2FB6
SHA1:	B585A485C9BC1982EDF7AE0B9AC73A8E91D41CB5
SHA-256:	8366774AA582035BC7D949F4E28FAEC371C305D01404DF56FFF5A78B4F6ECDB7
SHA-512:	F86334E6E6F90961AD9C8E7DD1A4E923476249469180AC69D9DE59746FE26FAECB585898FC50310380F20CEB0971CA1EB7B55046DA75276840AEA6BAFF574E6(
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenutno ni na voljo."},"craw_connect_to_network":{"message":"Pove\u017eite se z omre\u017ejem."},"app_name":{"message":"Pla\u010dila v spletni trgovini Chrome"},"app_description":{"message":"Pla\u010dila v spletni trgovini Chrome"},"iap_unavailable":{"message":"Pla\u010dila v aplikacijah trenutno niso na voljo."},"please_sign_in":{"message":"Prijavite se v Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1152
Entropy (8bit):	4.2078334514915685
Encrypted:	false
SSDEEP:	24:YHYpY0f7BxQVnRl5LRO1QV1J0V8aQVEeORbo0V8aQVEeORbIp00V4i0f7BXR2QVj:YHYpV9xQVP5LyQHQQc/QcGpcH9XR2QVj
MD5:	92C1FAC62EB7F92EC3794D4A141BEF32
SHA1:	2AFA41BF51BF9A1089B0B92A9D2DC74299B79813
SHA-256:	9DF154C93B02695AF1CC39F085D9D178EC6AF131A62C2AFC65F125F8F9A5B7AC
SHA-512:	D0709E4F586EAC03548A47D72156CF48D9B4EB9AF9ED8335DF75F541AE1B4172541647EC8BA081965647A9EAE10DB342F87558977BE6075B2D3CC5C3995ED6EE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0410\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0430 \u0458\u0435 \u0442\u0440\u0435\u043d\u0443\u0442\u043d\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u043e\u0432\u0435\u0436\u0438\u0442\u0435 \u0441\u0435 \u0441\u0430 \u0438\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043e\u043c."},"app_name":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0435\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"app_description":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0435\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 \u0430\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0438 \u0441\u0443 \u0442\u0440\u0435\u043d\u0443\u0442\u043d\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0435."},"please_sign_in":{"message":"\u041f\u04

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	523
Entropy (8bit):	4.788896709100935
Encrypted:	false
SSDEEP:	12:YGGYpg6hVGZE3aFMaap8Sp5b6hwUwrdIWO/NrnLAOK:YHYpg6hPaeaap8Sr6hwXIWOFvAOK
MD5:	6E1BE9CEE29818E54E3D1C7D483DD6F7
SHA1:	B9DD926B60E225C5BE8A1DBB7EF3ACE422A204A9
SHA-256:	E348583D8C53F4A5DEC4551DA93785C17108466E427E06F84708AA383EA0E326
SHA-512:	3ADB32C0F098E064B774E7E7F615F54C44ADFB3BFC554B06A17048C6077C5885D42BD89F6733D64D65EA1785033B36B386EF0B6661FD539855484EA5A2900BB7
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen \u00e4r inte tillg\u00e4nglig f\u00f6r tillf\u00e4llet."},"craw_connect_to_network":{"message":"Anslut till ett n\u00e4tverk."},"app_name":{"message":"Betalning via Chrome Web Store"},"app_description":{"message":"Betalning via Chrome Web Store"},"iap_unavailable":{"message":"Betalning i appen \u00e4r inte tillg\u00e4ngligt f\u00f6r n\u00e4rvarande."},"please_sign_in":{"message":"Logga in i Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	4.09652661599029
Encrypted:	false
SSDEEP:	24:YHYpqQV8k6Nvgnd0BQV3d0BQV5pWdPiWdBy7MIoWOFvAOK:YHYpqQ+k6NUaBQlaBQXpW3dBUMIehQ
MD5:	283D5177FB2FC7082967988E2683EC7C
SHA1:	DEDE43967F3CEF9D9325F140872A63BFCE2AA8C5
SHA-256:	E8D5820BDE31B66A7641068FDEDD1A5F20C1A783460B98887A670F38422099CF
SHA-512:	74413C00C58B7136038D4C41D5C7C79EC02A9830779ABB719D72536B74C5E338B1548A20290559FB3F4E2A938B728CF99041050DD1970848EE9A6590EB0AB3E4
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u0e44\u0e21\u0e48\u0e2a\u0e32\u0e21\u0e32\u0e23\u0e16\u0e43\u0e0a\u0e49\u0e07\u0e32\u0e19\u0e41\u0e2d\u0e1b\u0e44\u0e14\u0e49\u0e43\u0e19\u0e02\u0e13\u0e30\u0e19\u0e35\u0e49"},"craw_connect_to_network":{"message":"\u0e42\u0e1b\u0e23\u0e14\u0e40\u0e0a\u0e37\u0e48\u0e2d\u0e21\u0e15\u0e48\u0e2d\u0e01\u0e31\u0e1a\u0e40\u0e04\u0e23\u0e37\u0e2d\u0e02\u0e48\u0e32\u0e22"},"app_name":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"app_description":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"iap_unavailable":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e43\u0e19\u0e41\u0e2d\u0e1b\u0e1e\u0e25\u0e34\u0e40\u0e04\u0e0a\u0e31\u0e19\u0e44\u0e21\u0e48\u0e1e\u0e23\u0e49\u0e2d\u0e21\u0e4

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	572
Entropy (8bit):	4.93347615778905
Encrypted:	false
SSDEEP:	12:YGGYpFh852XmYG45SfVVh5SX8pFBkw452kK/O/NrnLAOK:YHYpFhJ2Y95AJ5l8pFhlkwOFvAOK
MD5:	1BF2AA4BB904B406C9C2B7DF769BB540
SHA1:	8D29C4B7A79AB0657747CA194D1934292A46D2A8
SHA-256:	0F2E8285BA3E2BDBA6B16435FB941B07159AACFAC80196AD5941B79AB52B712A
SHA-512:	0DF48AE0A518A940489E91D8A0D6E7E47A3153747358E06CD792BFA3D826F47FA1502268F602E7D7EDFC1C111AEB3FAF0E67F845986DDA77E2FC4B3336BCF46C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Uygulama \u015fu anda kullan\u0131lam\u0131yor."},"craw_connect_to_network":{"message":"L\u00fctfen bir a\u011fa ba\u011flan\u0131n."},"app_name":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"app_description":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"iap_unavailable":{"message":"Uygulama \u0130\u00e7i \u00d6demeler \u015fu anda kullan\u0131lamaz."},"please_sign_in":{"message":"L\u00fctfen Chrome'da oturum a\u00e7\u0131n."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	4.268588181103308
Encrypted:	false
SSDEEP:	24:YHYpNQVVQVrll5eN7jAQVF0Zz0id0Zz0iRp00AQVqaQVVQVSMQVvjlkYHA1RnWOi:YHYpNQPQZ75exkQAz0/z00p2QAaQPQQN
MD5:	FD1C9890679036E1AD914218753B1E8E
SHA1:	58160F7A0FC94110A2876223E406A517C8E2660B
SHA-256:	39D19CC3387FFCE13A8F11DAD72E2FCBB7CD1A4367EC699AD7C40D6F52ECE717
SHA-512:	03E81C398EE6A5DC65A40CA07E1A4CBEC2662D2C151A76C9ECB813587D672AC71311C39C5C5DA8A1AE78A3A6CE3938609D1365F7819424FC34289C7743DF002
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u043e\u0433\u0440\u0430\u043c\u0430 \u0442\u0438\u043c\u0447\u0430\u0441\u043e\u0432\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u0456\u0434\u2019\u0454\u0434\u043d\u0430\u0439\u0442\u0435\u0441\u044f \u0434\u043e \u043c\u0435\u0440\u0435\u0436\u0456."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0456 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0438 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0456 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0438 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0456 \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u043e\u0433\u0440\u0430\u043c\u0443 \u0437\u0430\u0440\u0430\u0437 \u043d\u0435 \u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0456."},"please_sign_in":{"message":"\u0423\u0432\u0456\u0439\u0434\u0456\u0442\u044c \u0443

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\vi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.846531831162704
Encrypted:	false
SSDEEP:	12:YGGYpqp80NORWLNiNI2k8yypSNiNI2k8yy+piNiNI2miI80NO5WO/NrnLAOK:YHYpmvNcCgWgUpudiIvN6WOFvAOK
MD5:	7D52E9357AB847B4CC8DBC8CC4DA93F5
SHA1:	AF877F3992D8056C8F08462BD575595BF79FE5B0
SHA-256:	313F71F3FFDCEFC76FC746FF2029FBF8FBE38BD83DCF952FC3DDCD8AA96D5CFB
SHA-512:	E66E7FACDF35A0F72AC61DEAAEC43A2DAC976CADEA146EBE3E90E739178F173E32ADCF909F05F2657F2AD66E2ECB6015F6733CEA4B9E42337246469F89D3A12F

Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u1ee8ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"craw_connect_to_network":{"message":"Vui l\u00f2ng k\u1ebft n\u1ed1i v\u1edbi m\u1ea1ng."},"app_name":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"app_description":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"iap_unavailable":{"message":"Thanh to\u00e1n trong \u1ee9ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"please_sign_in":{"message":"Vui l\u00f2ng \u0111\u0103ng nh\u1eadp v\u00e0o Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\zh_CN\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	602
Entropy (8bit):	4.917339139635893
Encrypted:	false
SSDEEP:	12:YGGYpqrL0MdI1i1kovbdKD/vbdKopqIQfvJ19KhO/NrnLAOK:YHYpMLfjvsTvsop3QPAOFvAOK
MD5:	393680A09DEE0CB9046A62BDC0750B74
SHA1:	54E7F8215061A4AB241B87AE4E81C8F860EB2C2B
SHA-256:	D5FB52C2897FD5C294784DB63C933AC77C609D10AC91431CCB295D87452CBEE6
SHA-512:	14C214CAEFC69B085E918F492C75E2A48BC6A9C2D347D29403B26E69A474825E302A3E106710E5C04E047BD57EE684A67846A5DE956705FFBF41BB0614B8CEB2
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u5e94\u7528\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u3002"},"craw_connect_to_network":{"message":"\u8bf7\u8fde\u63a5\u5230\u7f51\u7edc\u3002"},"app_name":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"app_description":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"iap_unavailable":{"message":"\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u5e94\u7528\u5185\u4ed8\u6b3e\u3002"},"please_sign_in":{"message":"\u8bf7\u767b\u5f55 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_locales\zh_TW\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	680
Entropy (8bit):	4.916281462386558
Encrypted:	false
SSDEEP:	12:YGGYpqI8ROuDWMg0kP2uD/vbd8Em2uD/vbd8RpqI8RauDRsXwvC/KhO/NrnLAOK:YHYp38suDUSuD/v2OuD/v2Rp38cuDGbq
MD5:	CD30D132A7213FC1B7E03C6D0A49CCF7
SHA1:	1141DED39023B821FE9BB4682E0D1EB5469DAF76
SHA-256:	5717F13D10E63255947F750C79CBB6BD04A6D97A08261E8D5764AF5EB0561A28
SHA-512:	0DCD3CEB93AB58655551B00D7AD4FE4A6F1F6B24EDD31244FF9B57AE529BF1A9E0220A6258C64790F9CC9F026AB9DA3AEE1575809CC94DC4F8754194C958FD19
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u9019\u500b\u61c9\u7528\u7a0b\u5f0f\u3002"},"craw_connect_to_network":{"message":"\u8acb\u9023\u4e0a\u7db2\u8def\u3002"},"app_name":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"app_description":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"iap_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u61c9\u7528\u7a0b\u5f0f\u5167\u4ed8\u6b3e\u529f\u80fd\u3002"},"please_sign_in":{"message":"\u8acb\u767b\u5165 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	192:RktDNJ2UzsL5KcASyoH+CouKP/iNGRo/oRHMIT:AZQflcsU
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3C4
Malicious:	false

Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwYXRoIjoiX2xvY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jYWxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd
C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\craw_background.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	544643
Entropy (8bit):	5.385396177420207
Encrypted:	false
SSDEEP:	6144:abyfBNC2FRdjiRXqbe5Dq31IVlMqX+wd5/CcMMJcRULt0NjyTOEzZQ+h72W3GB0n:Ft/g
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=e||{};e.scope={};e.arrayIteratorImpl=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};};e.arrayIterator=function(a){return{next:e.arrayIteratorImpl(a)}};e.ASSUME_ES5=!1;e.ASSUME_NO_NATIVE_MAP=!1;e.ASSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");};e.global=e.getGlobal(this);.e.IS_SYMBOL_NATIVE="func

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\craw_window.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	261316
Entropy (8bit):	5.444466092380538
Encrypted:	false
SSDEEP:	3072:I5vU7I6s2M9duIWFCbmYJ4tnFWdqpMad2vywhIp81QFv9F9nNsZgiDdOFlV/mZmc:I5vqFCb2p8Gx9FNNsZ9Dd/ceR
MD5:	1709B6F00A136241185161AA3DF46A06
SHA1:	33DA7D262FFED1A5C2D85B7390E9DBC830CBE494
SHA-256:	5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8
SHA-512:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D19CB
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b,k=k||{};k.scope={};k.createTemplateTagFirstArg=function(a){return a.raw=a};k.createTemplateTagFirstArgWithRaw=function(a,c){a.raw=c;return a};k.arrayIteratorImpl=function(a){var c=0;return function(){return c<a.length?{done:!1,value:a[c++]}:{done:!0}};};k.arrayIterator=function(a){return{next:k.arrayIteratorImpl(a)}};k.makeIterator=function(a){var c="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return c?c.call(a):k.arrayIterator(a)};.k.arrayFromIterator=function(a){for(var c,d=[];!(c=a.next()).done;)d.push(c.value);return d};k.arrayFromIterable=function(a){return a instanceof Array?a:k.arrayFromIterator(k.makeIterator(a))};k.ASSUME_ES5=!1;k.ASSUME_NO_NATIVE_MAP=!1;k.ASSUME_NO_NATIVE_SET=!1;k.SIMPLE_FROUND_POLYFILL=!1;k.ISOLATE_POLYFILLS=!1;k.FORCE_POLYFILL_PROMISE=!1;k.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.k.objectCreate=k.ASSUME_ES5||"function"==typeof Object.cre

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\css\craw_window.css	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1741
Entropy (8bit):	4.912380256743454
Encrypted:	false
SSDEEP:	24:LalZ74H+rMwJHwIodHRmxt3jiu1iu1RDpfeWlMl548wJHwDwCapt/VMYXj8Eq27K:Z+rMm71le88S1tWYXmrVZFH
MD5:	67BF9AABE17541852F9DDFF8245096CD

SHA1:	A4AC74DD258E8E0689034FAA1B15A5C7C56DC3BB
SHA-256:	10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC
SHA-512:	298FA132C6F122798FDB9BC6DE8024915147ADC20355B56A92F0ED9ACCE4549BE6E7F42212E07DCA166E31624D4E66E299565845D4BA1C51CA935050641B61F
Malicious:	false
Reputation:	low
Preview:	html, body {. margin: 0;. overflow: hidden;.}..webview {. width: 100%;. height: 100%;. min-height: 100%;. position: absolute;.}...craw_overlay {. position: absolute;.. left : 0;. top: 0;. right: 0;. bottom: 0;.. background-color: white;.. -webkit-transition: opacity 250ms linear;.. display: -webkit-flex;. -webkit-flex-direction: column;. -webkit-flex: 1 0%;. -webkit-align-items: center;. -webkit-justify-content: center;.. -webkit-app-region: drag;.}...craw_overlay img {. margin: 16px;.}..#loading_overlay {. opacity: 1;.}..#offline_overlay {. opacity: 0;. display: none;.}..#offline_overlay > img {. -webkit-filter: saturate(0%);.}..#offline_overlay > span {. font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif;. font-size: 15px;. line-height: 21px;. color: #8d8d8d;. display: block;.}..#loading_splash {. width: 128px;. height: 128px;.}..#drag_overlay {. position: absolute;. left: 0;. top: 0;. right: 0;. bottom: 0;. pointer-events: none;. -webkit

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\html\craw_window.html

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	810
Entropy (8bit):	4.723481385335562
Encrypted:	false
SSDEEP:	12:hYenuEJIig5fRpvV4AEdN2sAAuzg/7RwQuLYpUH9KfRnQBGgZKy3QGgjPSWZDQL:hYeLJKTVNEuLAuzg/twQucpS9bj3
MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281E FF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/craw_window.css" rel="stylesheet">. <script src="/craw_window.js"></script>. </head>. <body>. <webview> </webview>. . . . . <div cl ass="craw_overlay" id="offline_overlay">. . . < /span>. . . . . </body>.</html>.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\flapper.gif

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	dropped
Size (bytes):	70364
Entropy (8bit):	7.119902236613185
Encrypted:	false
SSDEEP:	768:g5TXOSBAqNIPmA8NcjCWdM0VFMJEwavTeElfWupav5TXg7wV+irIPny9MTVQHydi:g5KSmiIPmAhZWiMsDfWug7DmqM6HybkF
MD5:	398ABB308EEBC355DA70BCE907B22E29
SHA1:	CFFB77B8A1724B8F81D98C6D6AD0071D10162252
SHA-256:	2B73533F47A99FFEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040
SHA-512:	FC7A56FC8A61A582161874B54ADBAD30A84840190008EDB0B6FBF84F91393CA58E988E3FE446F11A0C3C691C18249B93AEC2904B3D0C4F0857D79034F662385A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....!..NETSCAPE2.0.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:...B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.Ny Q.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:...B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m 4..7..!.....,.....'..w=.....\.)._6.k..OF...n.#\~"....2b3..I.)..eu.Q.`.e.....gr.?>.s.I0.....@.~.Tr.[8.+.,.;..EE....S.*f....., ...B8/D..;.9.q.....ukC...r.I....j.....BGY...o2J....+O4....X4.....cH%7....I....0H!.!....!,..... .....p8.a$....hh@.4....X,A.0L..(....JX.j...,.....z.X.Q....jB.d....B..

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false
SSDEEP:	96:YjlLDJjTvXUtNvX8dgb9HT6y8nviyHG5iCRYtIP:YtNTfUzvX8KM+MGRsIP
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5

SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC1417091
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:.[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....a i..w38.+....Bf././..]...{.....8...3.....3W~OJ.. /...u6V.C..U.0.+._=.c..9.X.?....L....S@.L...m.0..>.C...L|TF.p5..f4M.,.V....8..a.<...RP..@)E,..E"...h.....!...-....,I..T.....m..._[[{w{{.... {*.^.....M.x..h4.h.....\.R.E....j).7.....h4.A.E....,. ...iii.Vj?2...=/.B.FK9P..@)=Rj..D".Y...2.B..x.}0...&J...2.....f.O..e.H.....!.J)'I..R....B.....QJ;K..L...L.l".L~mhh.R.@).FFF ~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....].,w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b.. aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:..=...r.....E].o...F..P.....i...|....

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	12:6v/7vyVgSKYsfFzXxXsrPfA+b0YX+5IOUWCQKznuow7:6yVnKYsfFzhXsrIq0YXmgQGn6
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCA5134903E4C1AA3D54BC7C5ED3E65B 50C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDAT8...Mk.Q...;... .....F..QW.....F....J.?.w..7~.....'.Q..B]... .QS...M&_w..b&.|`.....p...f.?.D$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N .Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C..._...%..*.^....4.I...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a..".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7y e6X<...'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\|.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.475799237015411
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/RPJDmV7bScsP4a9zln94FptVp:6v/lhPKM4nDspnAkZJNmgPdln2TTp
MD5:	8803665A6328D23CC1014A7B0E9BE295
SHA1:	9DA6EE729D5A6E9F30658B8EC954710F107A641F
SHA-256:	D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C
SHA-512:	ECD9E71B8BA1ED8BD4CA5A0936CB66A83611C4ABCBDA76C250F4CDF4AD80320212E8F5EEB79A38910718F8346ECC1AD580A3FA835EC2B22BE497F36899FB5 930
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...Q..0.....2...(p...~Z.}'.>I%O...V!s...../...`.<..`.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_close.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	252
Entropy (8bit):	6.512071394066515
Encrypted:	false
SSDEEP:	6:6v/lhPKM4nDsp7q1hKVlomsj9rxKNgtmN0VZ+GFYep:6v/7iMXVq1ylxemNgtmKVnYM
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D77A64
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..... ..Pp.X....H...b@...|.^LC_.E.BP+.....X.P.....q..~..p/. ..s.....%D^...$.....@.!...<...).? .4{.k.G3...4..[cH..0..l.8.!r..m.R..{.....`.f...#.x.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_hover.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.423186859407619
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEHxrPLyN+ltNPhv/l2up:6v/lhPKM4nDspnAkZHVtERrPLygltNPn
MD5:	7CB6B9DC1A30F63B8BD976924B75AD96
SHA1:	0C40B0C496D2F2B5F2021C117EC8610AC03AB469
SHA-256:	721B7AAA9A42A54A349881615A12E3A26983ACA48E173FD2F66E66AA0D725735
SHA-512:	4764937364E355956B242B84010AC56102536D2AACBE4227F0E88E4DE7AB468571957EA6C33012539156E5349AE4F777115615AE3361F60ADDF9CD227424F76A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B.z.s...*.....$.<u..[.....h.....C.CA).....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_maximize.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.8155898293424775
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZttd//HmnFz1P/ZjXlUTqyCIc30ltK1p:6v/lhPKM4nDsptF/HOP/ZjXlUeyCo/p
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A86 54
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...HIDATx.....0.CQS.....~..."".....m.v+Sq....<!...M8m...'...@$..0....E.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\images\topbar_floating_button_pressed.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEXIyN+ltN1/lsg1p:6v/lhPKM4nDspnAkZHVtEZgltN1eup
MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....$.<u..[.....h.....M..x(....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1416_124225580\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.449026004350873

Encrypted:	false
SSDEEP:	24:1HEis7ViC/yox/fiqeUoLFlmF1s80FKrGfd0d3NZNZx1Fq7eY7nfj1B:WL7V2opiV1mvs8rxTZRczhB
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED548F
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. },.. "default_locale": "en",.. "description": "__MSG_APP_DESCRIPTION__",.. "display_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png",.. "16": "images/icon_16.png".. },.. "key": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0IV5/lj0wx7zJ/xcibUgDeIxobvv9XD+zO1MdjMWuqJFcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB",.. "manifest_version": 2,.. "minimum_chrome_version": "29",.. "name": "__MSG_APP_NAME__",.. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com",.. "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.readonly"].. },.

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.154.231.67192.168.2.5443497812013145 06/30/22-22:27:53.591368	TCP	2013145	ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt	443	49781	192.154.231.67	192.168.2.5

Network Port Distribution



Total Packets: 59

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:27:49.242362022 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.242384911 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.242486954 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.244329929 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.244343996 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.256239891 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.256283998 CEST	443	49751	142.251.36.238	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:27:49.256398916 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.256902933 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.256926060 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.321429014 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.322510958 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.324332952 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.324362040 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.324815035 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.324924946 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.325876951 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.325973034 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.328450918 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.328491926 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.329726934 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.329869032 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.540904999 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.541270971 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.541822910 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.541939020 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.542740107 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.542767048 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.542891979 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.542920113 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.579361916 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.579495907 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.579530954 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.579610109 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.595257998 CEST	49751	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:27:49.595308065 CEST	443	49751	142.251.36.238	192.168.2.5
Jun 30, 2022 22:27:49.607846022 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.608000040 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.608005047 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:49.608062983 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.612201929 CEST	49749	443	192.168.2.5	142.251.36.205
Jun 30, 2022 22:27:49.612246990 CEST	443	49749	142.251.36.205	192.168.2.5
Jun 30, 2022 22:27:50.076322079 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.076390028 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.076508045 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.076724052 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.076755047 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.433269024 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.433984995 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.434034109 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.435158014 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.435265064 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.443624020 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.443808079 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.444422960 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:50.444461107 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:50.632119894 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:52.479609966 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:52.505379915 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:52.505497932 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:52.531682014 CEST	49763	443	192.168.2.5	69.172.198.108
Jun 30, 2022 22:27:52.531740904 CEST	443	49763	69.172.198.108	192.168.2.5
Jun 30, 2022 22:27:52.647073984 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.647133112 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.647286892 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.647603989 CEST	49782	443	192.168.2.5	192.154.231.67

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:27:52.647634983 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.647763014 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.648001909 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.648027897 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.648168087 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.648195028 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.970596075 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.979538918 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.999670982 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.999748945 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:52.999946117 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:52.999974012 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.001761913 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.001871109 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.002902985 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.003005028 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.006175995 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.006458044 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.006624937 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.006850958 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.007055998 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.007091045 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.070317984 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.070749044 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.070769072 CEST	443	49782	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.170361042 CEST	49782	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.277889967 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.277924061 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.277935028 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.277967930 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.278045893 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.278059959 CEST	443	49781	192.154.231.67	192.168.2.5
Jun 30, 2022 22:27:53.278121948 CEST	49781	443	192.168.2.5	192.154.231.67
Jun 30, 2022 22:27:53.370336056 CEST	49781	443	192.168.2.5	192.154.231.67

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:27:49.203216076 CEST	53934	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:49.222470045 CEST	53	53934	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:49.230607986 CEST	63187	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:49.237157106 CEST	60658	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:49.254089117 CEST	53	60658	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:49.730623007 CEST	52982	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:50.075100899 CEST	53	52982	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:52.617362976 CEST	57352	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:52.636966944 CEST	53	57352	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:53.722554922 CEST	61911	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.722889900 CEST	63241	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.723217964 CEST	63538	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.723268986 CEST	61478	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.723404884 CEST	57809	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.723485947 CEST	55355	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.741506100 CEST	53	63241	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:53.743599892 CEST	53	61478	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:53.743779898 CEST	62680	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:53.744321108 CEST	53	55355	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:53.744643927 CEST	53	63538	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:53.944624901 CEST	52333	53	192.168.2.5	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:27:53.975615978 CEST	53	52333	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:56.015155077 CEST	55473	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:56.016119957 CEST	54463	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:56.025764942 CEST	63718	53	192.168.2.5	8.8.8.8
Jun 30, 2022 22:27:56.036678076 CEST	53	54463	8.8.8.8	192.168.2.5
Jun 30, 2022 22:27:56.056530952 CEST	53	63718	8.8.8.8	192.168.2.5
Jun 30, 2022 22:28:02.395631075 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:02.427856922 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:02.727988005 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.027951002 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.075061083 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.075263977 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.107311964 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.107347012 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.107362986 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.107382059 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.130865097 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.134218931 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.154990911 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.155693054 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.199402094 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.212790012 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.376709938 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.376820087 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.395509958 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.408821106 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.408849955 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.417848110 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.427180052 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.427208900 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.427217007 CEST	443	54155	142.251.36.238	192.168.2.5
Jun 30, 2022 22:28:03.428334951 CEST	54155	443	192.168.2.5	142.251.36.238
Jun 30, 2022 22:28:03.473383904 CEST	54155	443	192.168.2.5	142.251.36.238

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 22:27:49.203216076 CEST	192.168.2.5	8.8.8.8	0xf1bf	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:49.230607986 CEST	192.168.2.5	8.8.8.8	0x4ae8	Standard query (0)	gmail.us14.list-manage.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:49.237157106 CEST	192.168.2.5	8.8.8.8	0x6854	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:49.730623007 CEST	192.168.2.5	8.8.8.8	0x618a	Standard query (0)	trocha.com.co	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:52.617362976 CEST	192.168.2.5	8.8.8.8	0x1c63	Standard query (0)	shafquatarefeen.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.722554922 CEST	192.168.2.5	8.8.8.8	0xeffe	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.722889900 CEST	192.168.2.5	8.8.8.8	0x6b50	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.723217964 CEST	192.168.2.5	8.8.8.8	0x1269	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.723268986 CEST	192.168.2.5	8.8.8.8	0x6818	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.723404884 CEST	192.168.2.5	8.8.8.8	0x5789	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.723485947 CEST	192.168.2.5	8.8.8.8	0x400f	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.743779898 CEST	192.168.2.5	8.8.8.8	0x596c	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 22:27:53.944624901 CEST	192.168.2.5	8.8.8.8	0x8c6d	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.015155077 CEST	192.168.2.5	8.8.8.8	0x2f02	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.016119957 CEST	192.168.2.5	8.8.8.8	0xd807	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.025764942 CEST	192.168.2.5	8.8.8.8	0x189	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
Jun 30, 2022 22:27:49.222470045 CEST	8.8.8.8	192.168.2.5	0xf1bf	No error (0)	accounts.google.com		142.251.36.205	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:49.254089117 CEST	8.8.8.8	192.168.2.5	0x6854	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:49.254089117 CEST	8.8.8.8	192.168.2.5	0x6854	No error (0)	clients.l.google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:49.255378008 CEST	8.8.8.8	192.168.2.5	0x4ae8	No error (0)	gmail.us14.list-manage.com	swc.list-manage.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:50.075100899 CEST	8.8.8.8	192.168.2.5	0x618a	No error (0)	trocha.com.co		69.172.198.108	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:52.636966944 CEST	8.8.8.8	192.168.2.5	0x1c63	No error (0)	shafquatarefeen.com		192.154.231.67	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.741506100 CEST	8.8.8.8	192.168.2.5	0x6b50	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.741506100 CEST	8.8.8.8	192.168.2.5	0x6b50	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.743599892 CEST	8.8.8.8	192.168.2.5	0x6818	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.743599892 CEST	8.8.8.8	192.168.2.5	0x6818	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.744321108 CEST	8.8.8.8	192.168.2.5	0x400f	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:53.744321108 CEST	8.8.8.8	192.168.2.5	0x400f	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.744643927 CEST	8.8.8.8	192.168.2.5	0x1269	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.744643927 CEST	8.8.8.8	192.168.2.5	0x1269	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.744847059 CEST	8.8.8.8	192.168.2.5	0x5789	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:53.752234936 CEST	8.8.8.8	192.168.2.5	0xeffe	No error (0)	login.microsoftonline.com	ak.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:53.752234936 CEST	8.8.8.8	192.168.2.5	0xeffe	No error (0)	ak.privatelink.msidentity.com	www.tm.ak.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:53.760281086 CEST	8.8.8.8	192.168.2.5	0x596c	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:53.975615978 CEST	8.8.8.8	192.168.2.5	0x8c6d	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.975615978 CEST	8.8.8.8	192.168.2.5	0x8c6d	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.975615978 CEST	8.8.8.8	192.168.2.5	0x8c6d	No error (0)	i.ibb.co		51.210.32.103	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.975615978 CEST	8.8.8.8	192.168.2.5	0x8c6d	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:53.975615978 CEST	8.8.8.8	192.168.2.5	0x8c6d	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:54.180005074 CEST	8.8.8.8	192.168.2.5	0x51e2	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 22:27:54.180005074 CEST	8.8.8.8	192.168.2.5	0x51e2	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:54.180005074 CEST	8.8.8.8	192.168.2.5	0x51e2	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:54.180005074 CEST	8.8.8.8	192.168.2.5	0x51e2	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.034043074 CEST	8.8.8.8	192.168.2.5	0x2f02	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:56.036678076 CEST	8.8.8.8	192.168.2.5	0xd807	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:27:56.036678076 CEST	8.8.8.8	192.168.2.5	0xd807	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.056530952 CEST	8.8.8.8	192.168.2.5	0x189	No error (0)	i.ibb.co		51.210.3.236	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.056530952 CEST	8.8.8.8	192.168.2.5	0x189	No error (0)	i.ibb.co		217.182.228.53	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.056530952 CEST	8.8.8.8	192.168.2.5	0x189	No error (0)	i.ibb.co		51.210.32.132	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.056530952 CEST	8.8.8.8	192.168.2.5	0x189	No error (0)	i.ibb.co		51.210.32.106	A (IP address)	IN (0x0001)
Jun 30, 2022 22:27:56.056530952 CEST	8.8.8.8	192.168.2.5	0x189	No error (0)	i.ibb.co		51.210.32.103	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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49751	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:49 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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:49 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-wtvfCL4oruno9J5y7GOj5w' '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: Thu, 30 Jun 2022 20:27:49 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5659 X-Daystart: 48469 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"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 20:27:49 UTC	2	IN	Data Raw: 33 31 61 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 35 39 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 38 34 36 39 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 Data Ascii: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5659" elapsed_seconds="48469"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-06-30 20:27:49 UTC	2	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-06-30 20:27:49 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	192.168.2.5	49749	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:49 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
2022-06-30 20:27:49 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:49 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: Thu, 30 Jun 2022 20:27:49 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Content-Security-Policy: script-src 'report-sample' 'nonce-3XlPQrWARTGpMbm86zlYxg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-3XlPQrWARTGpMbm86zlYxg' '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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} 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
2022-06-30 20:27:49 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",[]]
2022-06-30 20:27:49 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	192.168.2.5	49793	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	95	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
2022-06-30 20:27:53 UTC	285	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: 159445 Cache-Control: public, max-age=604800 Content-MD5: HMwsHhNXdtrfirQDkzcqMA== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:27:53 GMT Etag: 0x8D641014CC1CD9F Last-Modified: Fri, 02 Nov 2018 20:25:15 GMT Server: ECAcc (muc/336D) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 56c513ed-001e-002a-394c-8b8a96000000 x-ms-version: 2009-09-19 Content-Length: 915 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	286	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 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	192.168.2.5	49797	51.210.3.236	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 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
2022-06-30 20:27:54 UTC	348	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 30 Jun 2022 20:27:54 GMT Content-Type: image/png Content-Length: 1031 Connection: close
2022-06-30 20:27:54 UTC	349	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>@(`+-Gtzzw0000 o#Bk9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49782	192.154.231.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	350	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
2022-06-30 20:27:55 UTC	785	IN	HTTP/1.1 302 Found Date: Thu, 30 Jun 2022 20:27:55 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	192.168.2.5	49802	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	350	OUT	GET /shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg 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: 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
2022-06-30 20:27:54 UTC	353	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 25875565 Cache-Control: public, max-age=31536000 Content-MD5: 5YqvyYBhSpzXeWvqe16o8A== Content-Type: image/jpeg Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8D7B007295267C8 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (muc/3346) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 92b8b433-901e-0066-4469-a1bab7000000 x-ms-version: 2009-09-19 Content-Length: 987 Connection: close
2022-06-30 20:27:54 UTC	354	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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	355	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 26664104 Cache-Control: public, max-age=31536000 Content-MD5: eRaolOvefSnCzCmyZ/Epnw== Content-Type: image/jpeg Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8D7B007294E20F8 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (muc/3371) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: b5429d44-301e-0056-1d3d-9a7bce000000 x-ms-version: 2009-09-19 Content-Length: 17453 Connection: close
2022-06-30 20:27:54 UTC	355	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 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
2022-06-30 20:27:54 UTC	371	IN	Data Raw: 04 16 20 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 28 20 a0 20 a0 20 a0 20 a0 a8 28 00 28 20 00 0a 80 0a 20 80 a0 82 80 02 82 00 28 2a 20 0a 02 0a 02 28 00 28 82 41 40 41 40 42 28 2a 45 cc 04 02 0a 08 9a a0 18 28 08 28 8a 82 80 8a 00 82 88 20 a0 22 80 00 0a 22 88 22 80 22 80 00 20 00 0a 22 80 02 28 00 00 00 02 00 02 80 00 02 00 00 8a 00 82 88 00 00 8a 88 28 02 80 00 00 00 22 80 00 00 08 a0 20 08 00 00 02 00 00 2a 02 a8 8a 08 28 08 2a 02 a0 a0 82 80 8a 00 00 00 02 00 00 00 00 00 00 00 28 00 a0 00 08 00 28 28 00 20 00 0a 8a 00 0a 20 00 28 00 08 a0 00 8a 00 00 03 ff d7 dc 00 74 73 00 00 01 44 01 00 00 00 10 50 10 54 00 00 11 40 40 00 00 10 50 10 54 00 00 00 50 00 40 00 00 02 10 01 20 a4 04 16 10 10 00 00 00 00 00 00 00 00 00 04 00 50 45 00 00 Data Ascii: ((((* ((A@A@B(*E(("""" "((" *(*((((tsDPT@@PTP@ PE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49806	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	351	OUT	GET /ests/2.1/content/images/microsoft_logo.png 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: 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
2022-06-30 20:27:54 UTC	409	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 180632 Cache-Control: public, max-age=604800 Content-MD5: 7ZyesNzhfXUr7eprWs2m2Q== Content-Type: image/png Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8D641014F7D2A46 Last-Modified: Fri, 02 Nov 2018 20:25:20 GMT Server: ECAcc (muc/335E) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 9812521e-501e-0046-5a1b-8bc4e6000000 x-ms-version: 2009-09-19 Content-Length: 1057 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	410	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	192.168.2.5	49803	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	352	OUT	GET /shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png 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: 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
2022-06-30 20:27:54 UTC	372	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 19191711 Cache-Control: public, max-age=31536000 Content-MD5: GWPGsZJrdzmG9T+ETOTDLg== Content-Type: image/png Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8D79A1BA1ED720E Last-Modified: Thu, 16 Jan 2020 00:32:56 GMT Server: ECAcc (muc/3373) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: e31b0960-001e-002c-3633-de6c57000000 x-ms-version: 2009-09-19 Content-Length: 1487 Connection: close
2022-06-30 20:27:54 UTC	373	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	192.168.2.5	49805	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	352	OUT	GET /shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png 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: 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
2022-06-30 20:27:54 UTC	374	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * 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 Age: 31504001 Cache-Control: public, max-age=31536000 Content-MD5: D3K1lQYA8k5/mmBLGG85RQ== Content-Type: image/png Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8D79A1B9F5B2B36 Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (muc/3366) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 2396fa96-a01e-003d-7238-6e2d72000000 x-ms-version: 2009-09-19 Content-Length: 1335 Connection: close
2022-06-30 20:27:54 UTC	375	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	192.168.2.5	49804	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	353	OUT	GET /ests/2.1/content/cdnbundles/converged.v2.login.min_9lddfuhsopopkddlczwbda2.css 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: 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
2022-06-30 20:27:54 UTC	376	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * 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 Age: 2116488 Cache-Control: public, max-age=31536000 Content-MD5: 4UYMAjoVPUSdaG/9PjwYKQ== Content-Type: text/css Date: Thu, 30 Jun 2022 20:27:54 GMT Etag: 0x8DA459E259D3EA4 Last-Modified: Fri, 03 Jun 2022 20:17:56 GMT Server: ECAcc (muc/3367) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5871aebe-b01e-0037-5980-790730000000 x-ms-version: 2009-09-19 Content-Length: 110657 Connection: close
2022-06-30 20:27:54 UTC	377	IN	Data Raw: 2f 2a 21 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 20 2a 2f 2f 2a 21 0a 2d 2d 2d

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:54 UTC	393	IN	Data Raw: 2d 31 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 63 6f 6c 2d 78 73 2d 38 2c 2e 63 6f 6c 2d 78 73 2d 39 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 31 33 2c 2e 63 6f 6c 2d 78 73 2d 31 34 2c 2e 63 6f 6c 2d 78 73 2d 31 35 2c 2e 63 6f 6c 2d 78 73 2d 31 36 2c 2e 63 6f 6c 2d 78 73 2d 31 37 2c 2e 63 6f 6c 2d 78 73 2d 31 38 2c 2e 63 6f 6c 2d 78 73 2d 31 39 2c 2e 63 6f 6c 2d 78 73 2d 32 30 2c 2e 63 6f 6c 2d 78 73 2d 32 31 2c 2e 63 6f 6c 2d 78 73 2d 32 32 2c 2e 63 6f 6c 2d 78 73 2d 32 33 2c 2e 63 6f 6c 2d 78 73 2d 32 34 7b 66 6c 6f 61 74 3a 6c Data Ascii: -1,.col-xs-2,.col-xs-3,.col-xs-4,.col-xs-5,.col-xs-6,.col-xs-7,.col-xs-8,.col-xs-9,.col-xs-10,.col-xs-11,.col-xs-12,.col-xs-13,.col-xs-14,.col-xs-15,.col-xs-16,.col-xs-17,.col-xs-18,.col-xs-19,.col-xs-20,.col-xs-21,.col-xs-22,.col-xs-23,.col-xs-24{float:l
2022-06-30 20:27:54 UTC	411	IN	Data Raw: 67 69 6e 2d 6c 65 66 74 3a 39 35 2e 38 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 6c 2d 6f 66 66 73 65 74 2d 32 34 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 30 25 7d 7d 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 62 6f 72 64 65 72 3a 30 3b 6d 69 6e 2d 77 69 64 74 68 3a 30 7d 6c 65 67 65 6e 64 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 3b 70 61 64 64 69 6e 67 3a 30 3b 62 6f 72 64 65 72 3a 30 7d 6c 61 62 65 6c 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 65 61 72 63 68 22 5d 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 6f Data Ascii: gin-left:95.83333%}.col-xl-offset-24{margin-left:100%}}fieldset{padding:0;margin:0;border:0;min-width:0}legend{display:block;width:100%;padding:0;border:0}label{display:inline-block;max-width:100%}input[type="search"]{-webkit-box-sizing:border-box;-moz-bo
2022-06-30 20:27:54 UTC	427	IN	Data Raw: 6c 6f Data Ascii: lo
2022-06-30 20:27:54 UTC	427	IN	Data Raw: 77 2d 78 3a 61 75 74 6f 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 2e 30 31 25 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 33 39 70 78 29 7b 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 35 70 78 3b 6f 76 65 72 66 6c 6f 77 2d 79 3a 68 69 64 64 65 6e 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 2d 6d 73 2d 61 75 74 6f 68 69 64 69 6e 67 2d 73 63 72 6f 6c 6c 62 61 72 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 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 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 3e 74 68 65 61 64 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 Data Ascii: w-x:auto;min-height:.01%}@media screen and (max-width:539px){.table-responsive{width:100%;margin-bottom:15px;overflow-y:hidden;-ms-overflow-style:-ms-autohiding-scrollbar}.table-responsive>.table{margin-bottom:0}.table-responsive>.table>thead>tr>th,.table
2022-06-30 20:27:54 UTC	443	IN	Data Raw: 2c 22 54 75 6e 67 61 22 2c 22 4c 61 6f 20 55 49 22 2c 22 52 61 61 76 69 22 2c 22 49 73 6b 6f 6f 6c 61 20 50 6f 74 61 22 2c 22 4c 61 74 68 61 22 2c 22 4c 65 65 6c 61 77 61 64 65 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 20 55 49 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4a 68 65 6e 67 48 65 69 20 55 49 22 2c 22 4d 61 6c 67 75 6e 20 47 6f 74 68 69 63 22 2c 22 45 73 74 72 61 6e 67 65 6c 6f 20 45 64 65 73 73 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 48 69 6d 61 6c 61 79 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4e 65 77 20 54 61 69 20 4c 75 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 50 68 61 67 73 50 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 54 61 69 20 4c 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 69 20 42 61 69 74 69 22 2c 22 4d 6f 6e 67 6f 6c Data Ascii: ,"Tunga","Lao UI","Raavi","Iskoola Pota","Latha","Leelawadee","Microsoft YaHei UI","Microsoft JhengHei UI","Malgun Gothic","Estrangelo Edessa","Microsoft Himalaya","Microsoft New Tai Lue","Microsoft PhagsPa","Microsoft Tai Le","Microsoft Yi Baiti","Mongol
2022-06-30 20:27:54 UTC	459	IN	Data Raw: 69 76 65 2c 2e 62 74 6e 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2d 61 63 74 69 76 65 2c 2e 62 74 6e 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 62 75 74 74 6f 6e 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 75 62 6d 69 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 72 65 73 65 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 2d 6d 73 2d 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 Data Ascii: ive,.btn.btn-primary-active,.btn.btn-primary:active,button.btn-primary:active,input[type="button"].btn-primary:active,input[type="submit"].btn-primary:active,input[type="reset"].btn-primary:active{outline:none;text-decoration:none;-ms-transform:scale(.98)
2022-06-30 20:27:54 UTC	475	IN	Data Raw: 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 36 36 36 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 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 6d 65 6d 62 65 72 6e 61 6d 65 50 72 65 66 69 6c 6c 53 65 6c 65 63 74 3a 61 63 74 69 76 65 7b 74 72 61 6e 73 66 6f 72 6d 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 30 30 37 38 64 37 3b 62 6f 72 64 65 72 2d 74 6f 70 2d 77 69 64 74 68 3a 30 3b 62 6f 72 64 65 72 2d 6c 65 66 74 2d 77 69 64 74 68 3a 30 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 2d 77 69 64 74 68 3a Data Ascii: tline:none;border-left:none;border-right:none;border-top:none;border-color:#666;background-color:transparent}.dropdown-toggle.membernamePrefillSelect:active{transform:none;border:1px solid #0078d7;border-top-width:0;border-left-width:0;border-right-width:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49809	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:55 UTC	487	OUT	GET /ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js 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: 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
2022-06-30 20:27:55 UTC	487	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: 10336330 Cache-Control: public, max-age=31536000 Content-MD5: HWW92uTq7vx3y5z+zFZbXQ== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:27:55 GMT Etag: 0x8D8DA1D9D23143A Last-Modified: Fri, 26 Feb 2021 06:13:19 GMT Server: ECAcc (muc/3323) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 9e8f8ab1-501e-0067-26bd-2e44ba000000 x-ms-version: 2009-09-19 Content-Length: 119648 Connection: close
2022-06-30 20:27:55 UTC	488	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 33 2e 35 2e 31 20 7c 20 28 63 29 20 4a 53 20 46 6f 75 6e 64 61 74 69 6f 6e 20 61 6e 64 20 6f 74 68 65 72 20 63 6f 6e 74 72 69 62 75 74 6f 72 73 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 21 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 65 2e 64 6f 63 75 6d 65 6e 74 3f 74 28 65 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 65 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 Data Ascii: /*! jQuery v3.5.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery
2022-06-30 20:27:55 UTC	504	IN	Data Raw: 3d Data Ascii: =
2022-06-30 20:27:55 UTC	504	IN	Data Raw: 28 61 3d 65 29 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 7c 7c 5b 5d 29 5b 30 5d 3d 3d 3d 6b 26 26 72 5b 31 5d 29 2c 21 31 3d 3d 64 29 77 68 69 6c 65 28 61 3d 2b 2b 73 26 26 61 26 26 61 5b 6c 5d 7c 7c 28 64 3d 73 3d 30 29 7c 7c 75 2e 70 6f 70 28 29 29 69 66 28 28 78 3f 61 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3d 3d 3d 66 3a 31 3d 3d 3d 61 2e 6e 6f 64 65 54 79 70 65 29 26 26 2b 2b 64 26 26 28 70 26 26 28 28 69 3d 28 6f 3d 61 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 3d 5b 6b 2c 64 5d 29 2c 61 3d 3d 3d 65 Data Ascii: (a=e)[S]||(a[S]={}))[a.uniqueID]||(o[a.uniqueID]={}))[h]||[])[0]===k&&r[1]),!1===d)while(a=++s&&a&&a[l]||(d=s=0)||u.pop())if((x?a.nodeName.toLowerCase()===f:1===a.nodeType)&&++d&&(p&&((i=(o=a[S]||(a[S]={}))[a.uniqueID]||(o[a.uniqueID]={}))[h]=[k,d]),a===e
2022-06-30 20:27:55 UTC	521	IN	Data Raw: 65 29 7b 72 65 74 75 72 6e 20 31 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 39 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 21 2b 65 2e 6e 6f 64 65 54 79 70 65 7d 3b 66 75 6e 63 74 69 6f 6e 20 47 28 29 7b 74 68 69 73 2e 65 78 70 61 6e 64 3d 53 2e 65 78 70 61 6e 64 2b 47 2e 75 69 64 2b 2b 7d 47 2e 75 69 64 3d 31 2c 47 2e 70 72 6f 74 6f 74 79 70 65 3d 7b 63 61 63 68 65 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3b 72 65 74 75 72 6e 20 74 7c 7c 28 74 3d 7b 7d 2c 56 28 65 29 26 26 28 65 2e 6e 6f 64 65 54 79 70 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3d 74 3a 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 68 69 73 2e 65 78 70 61 6e 64 6f 2c 7b 76 61 6c 75 Data Ascii: e){return 1===e.nodeType||9===e.nodeType||!+e.nodeType};function G(){this.expando=S.expando+G.uid++};G.uid=1,G.prototype={cache:function(e){var t=e[this.expando];return t||(t={},V(e)&&(e.nodeType?e[this.expando]=t:Object.defineProperty(e,this.expando,{valu
2022-06-30 20:27:55 UTC	537	IN	Data Raw: 65 73 74 28 73 2e 74 79 70 65 29 3f 75 2e 63 68 65 63 6b 65 64 3d 73 2e 63 68 65 63 6b 65 64 3a 22 69 6e 70 75 74 22 21 3d 3d 6c 26 26 22 74 65 78 74 61 72 65 61 22 21 3d 3d 6c 7c 7c 28 75 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 3d 73 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 29 3b 69 66 28 74 29 69 66 28 6e 29 66 6f 72 28 6f 3d 6f 7c 7c 76 65 28 65 29 2c 61 3d 61 7c 7c 76 65 28 63 29 2c 72 3d 30 2c 69 3d 6f 2e 6c 65 6e 67 74 68 3b 72 3c 69 3b 72 2b 2b 29 4f 65 28 6f 5b 72 5d 2c 61 5b 72 5d 29 3b 65 6c 73 65 20 4f 65 28 65 2c 63 29 3b 72 65 74 75 72 6e 20 30 3c 28 61 3d 76 65 28 63 2c 22 73 63 72 69 70 74 22 29 29 2e 6c 65 6e 67 74 68 26 26 79 65 28 61 2c 21 66 26 26 76 65 28 65 2c 22 73 63 72 69 70 74 22 29 29 2c 63 7d 2c 63 6c 65 61 6e 44 61 74 61 3a 66 75 Data Ascii: est(s.type)?u.checked=s.checked:"input"!==l&&"textarea"!==l||(u.defaultValue=s.defaultValue);if(t)if(n)for(o=o||ve(e),a=a||ve(c),r=0,i=o.length;r<i;r++)Oe(o[r],a[r]);else Oe(e,c);return 0<(a=ve(c,"script")).length&&ye(a,!f&&ve(e,"script")),c},cleanData:fu
2022-06-30 20:27:55 UTC	553	IN	Data Raw: 65 78 74 65 6e 64 28 7b 61 74 74 72 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 72 2c 69 2c 6f 3d 65 2e 6e 6f 64 65 54 79 70 65 3b 69 66 28 33 21 3d 3d 6f 26 26 38 21 3d 3d 6f 26 26 32 21 3d 3d 6f 29 72 65 74 75 72 6e 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 65 2e 67 65 74 41 74 74 72 69 62 75 74 65 3f 53 2e 70 72 6f 70 28 65 2c 74 2c 6e 29 3a 28 31 3d 3d 3d 6f 26 26 53 2e 69 73 58 4d 4c 44 6f 63 28 65 29 7c 7c 28 69 3d 53 2e 61 74 74 72 48 6f 6f 6b 73 5b 74 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 5d 7c 7c 28 53 2e 65 78 70 72 2e 6d 61 74 63 68 2e 62 6f 6f 6c 2e 74 65 73 74 28 74 29 3f 70 74 3a 76 6f 69 64 20 30 29 29 2c 76 6f 69 64 20 30 21 3d 3d 6e 3f 6e 75 6c 6c 3d 3d 3d 6e 3f 76 6f 69 64 20 53 2e 72 65 6d 6f 76 Data Ascii: extend({attr:function(e,t,n){var r,i,o=e.nodeType;if(3!==o&&8!==o&&2!==o)return"undefined"==typeof e.getAttribute?S.prop(e,t,n):(1===o&&S.isXMLDoc(e)||(i=S.attrHooks[t.toLowerCase()]||(S.expr.match.bool.test(t)?pt:void 0)),void 0!==n?null===n?void S.remov

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:55 UTC	569	IN	Data Raw: 28 6e 20 69 6e 20 69 2e 78 68 72 46 69 65 6c 64 73 29 72 5b 6e 5d 3d 69 2e 78 68 72 46 69 65 6c 64 73 5b 6e 5d 3b 66 6f 72 28 6e 20 69 6e 20 69 2e 6d 69 6d 65 54 79 70 65 26 26 72 2e 6f 76 65 72 72 69 64 65 4d 69 6d 65 54 79 70 65 26 26 72 2e 6f 76 65 72 72 69 64 65 4d 69 6d 65 54 79 70 65 28 69 2e 6d 69 6d 65 54 79 70 65 29 2c 69 2e 63 72 6f 73 73 44 6f 6d 61 69 6e 7c 7c 65 5b 22 58 2d 52 65 71 75 65 73 74 65 64 2d 57 69 74 68 22 5d 7c 7c 28 65 5b 22 58 2d 52 65 71 75 65 73 74 65 64 2d 57 69 74 68 22 5d 3d 22 58 4d 4c 48 74 74 70 52 65 71 75 65 73 74 22 29 2c 65 29 72 2e 73 65 74 52 65 71 75 65 73 74 48 65 61 64 65 72 28 6e 2c 65 5b 6e 5d 29 3b 6f 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 26 26 28 6f Data Ascii: (n in i.xhrFields)r[n]=i.xhrFields[n];for(n in i.mimeType&&r.overrideMimeType&&r.overrideMimeType(i.mimeType),i.crossDomain||e["X-Requested-With"]||(e["X-Requested-With"]="XMLHttpRequest"),e)r.setRequestHeade r(n,e[n]);o=function(e){return function(){o&&(o
2022-06-30 20:27:55 UTC	617	IN	Data Raw: 65 78 74 65 6e 64 28 7b 62 69 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 72 29 7b 72 65 74 75 72 6e 20 75 28 22 6a 51 75 65 72 79 2e 66 6e 2e 62 69 6e 64 28 29 20 69 73 20 64 65 70 72 65 63 61 74 65 64 22 29 2c 74 68 69 73 2e 6f 6e 28 65 2c 6e 75 6c 6c 2c 74 2c 72 29 7d 2c 75 6e 62 69 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 75 28 22 6a 51 75 65 72 79 2e 66 6e 2e 75 6e 62 69 6e 64 28 29 20 69 73 20 64 65 70 72 65 63 61 74 65 64 22 29 2c 74 68 69 73 2e 6f 66 66 28 65 2c 6e 75 6c 6c 2c 74 29 7d 2c 64 65 6c 65 67 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 72 2c 6e 29 7b 72 65 74 75 72 6e 20 75 28 22 6a 51 75 65 72 79 2e 66 6e 2e 64 65 6c 65 67 61 74 65 28 29 20 69 73 20 64 65 70 72 65 63 61 74 65 64 22 29 2c 74 68 Data Ascii: extend({bind:function(e,t,r){return u("jQuery.fn.bind() is deprecated"),this.on(e,null,t,r)},unbind:function(e,t){retu rn u("jQuery.fn.unbind() is deprecated"),this.off(e,null,t)},delegate:function(e,t,r,n){return u("jQuery.fn.delegate() is deprecat ed"),th
2022-06-30 20:27:55 UTC	633	IN	Data Raw: 32 2c 31 30 2a 28 61 2d 31 29 29 2b 62 3b 72 65 74 75 72 6e 20 63 2f 32 2a 28 2d 4d 61 74 68 2e 70 6f 77 28 32 2c 2d 31 30 2a 2d 2d 61 29 2b 32 29 2b 62 7d 2c 65 61 73 65 49 6e 43 69 72 63 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 61 2c 62 2c 63 2c 64 29 7b 72 65 74 75 72 6e 20 2d 63 2a 28 4d 61 74 68 2e 73 71 72 74 28 31 2d 28 61 2f 3d 64 29 2a 61 29 2d 31 29 2b 62 7d 2c 65 61 73 65 4f 75 74 43 69 72 63 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 61 2c 62 2c 63 2c 64 29 7b 72 65 74 75 72 6e 20 63 2a 4d 61 74 68 2e 73 71 72 74 28 31 2d 28 61 3d 61 2f 64 2d 31 29 2a 61 29 2b 62 7d 2c 65 61 73 65 49 6e 4f 75 74 43 69 72 63 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 61 2c 62 2c 63 2c 64 29 7b 69 66 28 28 61 2f 3d 64 2f 32 29 3c 31 29 72 65 74 75 72 6e 20 2d 63 2f 32 2a 28 4d 61 Data Ascii: 2,10*(a-1))+b;return c/2*(-Math.pow(2,-10*--a)+2)+b},easeInCirc:function(e,a,b,c,d){return -c*(Math.sqrt(1-(a/=d)*a)-1)+b},easeOutCirc:function(e,a,b,c,d){return c*Math.sqrt(1-(a=a/d-1)*a)+b},easeInOutCirc:function(e,a,b,c,d){if ((a/=d/2)<1)return -c/2*(Ma

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49763	69.172.198.108	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:50 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
2022-06-30 20:27:52 UTC	5	IN	HTTP/1.1 404 Not Found Date: Thu, 30 Jun 2022 20:27:49 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
2022-06-30 20:27:52 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 !== "")
2022-06-30 20:27:52 UTC	6	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49810	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:55 UTC	520	OUT	GET /ests/2.1/content/cdnbundles/aad.login.min_kx1da7l2dz6nhe9kugk19a2.js 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: 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
2022-06-30 20:27:55 UTC	585	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * 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 Age: 5480452 Cache-Control: public, max-age=31536000 Content-MD5: upI7aPOzsdXSeL+Vv8o5ww== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:27:55 GMT Etag: 0x8DA2286D5C4F576 Last-Modified: Wed, 20 Apr 2022 04:32:53 GMT Server: ECAcc (muc/3310) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: b1113ac6-701e-0017-74e7-5a7961000000 x-ms-version: 2009-09-19 Content-Length: 182667 Connection: close
2022-06-30 20:27:55 UTC	585	IN	Data Raw: 2f 2a 21 20 2d 2d 2d

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:55 UTC	686	IN	Data Raw: 74 61 74 65 Data Ascii: tate
2022-06-30 20:27:55 UTC	686	IN	Data Raw: 73 2e 4d 53 41 29 7b 43 6f 6e 74 65 78 74 2e 65 6d 61 69 6c 5f 64 69 73 63 6f 76 65 72 79 5f 77 6f 72 6b 66 6c 6f 77 5f 73 74 61 74 65 3d 6e 2e 57 6f 72 6b 66 6c 6f 77 53 74 61 74 65 73 2e 4d 53 41 3b 76 61 72 20 65 3d 7b 22 44 6f 6d 61 69 6e 4e 61 6d 65 22 3a 43 6f 6e 73 74 61 6e 74 73 2e 4d 53 41 5f 44 4f 4d 41 49 4e 2c 22 41 75 74 68 55 52 4c 22 3a 43 6f 6e 73 74 61 6e 74 73 2e 4d 53 41 5f 41 55 54 48 5f 55 52 4c 7d 0a 3b 6e 2e 48 69 64 65 53 70 6c 69 74 74 65 72 28 29 2c 6e 2e 49 6e 69 74 52 65 64 69 72 65 63 74 28 29 2c 55 73 65 72 2e 52 65 63 65 69 76 65 46 65 64 65 72 61 74 65 64 44 6f 6d 61 69 6e 28 65 29 7d 7d 2c 22 4c 6f 67 69 6e 41 44 41 63 63 6f 75 6e 74 22 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 43 6f 6e 74 65 78 74 2e 65 6d 61 69 6c 5f 64 69 Data Ascii: s.MSA){Context.email_discovery_workflow_state=n.WorkflowStates.MSA;var e={"DomainName":Constants.MSA_DOMAIN,"AuthURL":Constants.MSA_AUTH_URL};n.HideSplitter(),n.InitRedirect(),User.ReceiveFederatedDomain(e)}},"LoginAADAccount":function(){Context.email_di
2022-06-30 20:27:55 UTC	702	IN	Data Raw: 3c 64 69 76 2f 3e 22 29 2e 68 74 6d 6c 28 74 2e 6e 61 6d 65 29 2e 74 65 78 74 28 29 3b 24 28 65 29 2e 61 70 70 65 6e 64 28 24 28 22 3c 64 69 76 2f 3e 22 29 2e 61 74 74 72 28 22 69 64 22 2c 22 73 69 74 65 5f 73 61 6d 6c 22 29 2e 74 65 78 74 28 6e 2b 22 20 28 22 2b 74 2e 64 6f 6d 61 69 6e 2b 22 29 22 29 7d 7d 7d 3b 4d 53 4c 6f 67 6f 75 74 2e 54 68 69 72 64 50 61 72 74 79 43 6f 6f 6b 69 65 53 74 61 74 65 73 3d 7b 22 4e 4f 54 5f 4c 4f 41 44 45 44 22 3a 2d 31 2c 22 44 49 53 41 42 4c 45 44 22 3a 30 2c 22 45 4e 41 42 4c 45 44 22 3a 31 7d 3b 76 61 72 20 54 68 69 72 64 50 61 72 74 79 43 6f 6f 6b 69 65 53 74 61 74 65 73 3d 4d 53 4c 6f 67 6f 75 74 2e 54 68 69 72 64 50 61 72 74 79 43 6f 6f 6b 69 65 53 74 61 74 65 73 2c 50 6f 73 74 54 79 70 65 3d 7b 22 49 4e 56 41 Data Ascii: ").html(t.name).text();$(e).append($(" ").attr("id","site_saml").text(n+" ("+t.domain+")"))}}};MSLogout.ThirdPartyCookieStates={"NOT_LOADED":-1,"DISABLED":0,"ENABLED":1};var ThirdPartyCookieStates=MSLogout.ThirdPartyCookieStates,PostType={"INVA
2022-06-30 20:27:55 UTC	718	IN	Data Raw: 65 6d 70 6c 61 74 65 57 69 74 68 45 72 72 6f 72 43 6f 64 65 2e 66 6f 72 6d 61 74 28 30 7c 65 2e 45 72 72 43 6f 64 65 2c 65 2e 53 65 73 73 69 6f 6e 49 64 3f 55 74 69 6c 2e 68 74 6d 6c 45 6e 63 6f 64 65 28 65 2e 53 65 73 73 69 6f 6e 49 64 29 3a 22 22 2c 65 2e 43 6f 72 72 65 6c 61 74 69 6f 6e 49 64 3f 55 74 69 6c 2e 68 74 6d 6c 45 6e 63 6f 64 65 28 65 2e 43 6f 72 72 65 6c 61 74 69 6f 6e 49 64 29 3a 22 22 2c 28 6e 65 77 20 44 61 74 65 29 2e 74 6f 49 53 4f 53 74 72 69 6e 67 28 29 3b 24 28 22 23 74 66 61 5f 65 72 72 6f 72 5f 74 65 78 74 22 29 2e 68 74 6d 6c 28 74 29 2e 73 68 6f 77 28 29 2c 45 28 29 7d 66 75 6e 63 74 69 6f 6e 20 45 28 29 7b 76 61 72 20 65 3d 24 28 22 23 74 66 61 5f 6f 75 74 65 72 5f 6c 69 73 74 5f 63 6f 6e 74 61 69 6e 65 72 22 29 2e 68 65 69 Data Ascii: emplateWithErrorCode.format(0|e.ErrCode,e.SessionId?Util.htmlEncode(e.SessionId):"",e.CorrelationId?Util.htmlEncode(e.CorrelationId):"",(new Date).toISOString());$("#tfa_error_text").html(t).show(),E()}function E(){var e=$("#tfa_outer_list_container").hei
2022-06-30 20:27:55 UTC	734	IN	Data Raw: 6f 5f 63 6f 6e 74 65 78 74 2c 74 3d 43 6f 6e 73 74 61 6e 74 73 2e 49 53 5f 43 58 48 5f 52 45 51 55 45 53 54 3f 43 6f 6e 73 74 61 6e 74 73 2e 55 53 45 5f 44 41 52 4b 5f 54 49 4c 45 5f 4c 4f 47 4f 3f 65 2e 54 69 6c 65 44 61 72 6b 4c 6f 67 6f 7c 7c 65 2e 54 69 6c 65 4c 6f 67 6f 3a 65 2e 54 69 6c 65 4c 6f 67 6f 3a 65 2e 42 61 6e 6e 65 72 4c 6f 67 6f 0a 3b 76 6f 69 64 20 30 21 3d 74 26 26 22 22 21 3d 74 26 26 28 74 2b 3d 22 3f 74 73 3d 22 2b 43 6f 6e 74 65 78 74 2e 74 65 6e 61 6e 74 5f 62 72 61 6e 64 69 6e 67 5f 74 73 29 2c 55 73 65 72 2e 55 70 64 61 74 65 4c 6f 67 6f 28 74 2c 43 6f 6e 73 74 61 6e 74 73 2e 44 45 46 41 55 4c 54 5f 4c 4f 47 4f 5f 41 4c 54 29 2c 24 28 22 23 6c 6f 67 69 6e 5f 77 6f 72 6b 6c 6f 61 64 5f 6c 6f 67 6f 5f 74 65 78 74 22 29 2e 68 69 64 Data Ascii: o_context,t=Constants.IS_CXH_REQUEST?Constants.USE_DARK_TILE_LOGO?e.TileDarkLogo||e.TileLogo:e.TileLogo:e.BannerLogo;void 0!=t&&""!=t&&(t+="?ts="+Context.tenant_branding_ts),User.UpdateLogo(t,Constants.DEFAULT_LOGO_ALT),$("#login_workload_logo_text").hid
2022-06-30 20:27:55 UTC	750	IN	Data Raw: 64 69 72 65 63 74 22 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 24 28 22 23 63 72 65 64 5f 70 61 73 73 77 6f 72 64 5f 69 6e 70 75 74 74 65 78 74 22 29 2e 76 61 6c 28 22 22 29 2c 43 6f 6e 74 65 78 74 2e 75 73 65 72 6e 61 6d 65 5f 73 74 61 74 65 2e 6c 61 73 74 5f 63 68 65 63 6b 65 64 5f 65 6d 61 69 6c 3d 22 22 2c 0a 54 69 6c 65 73 2e 65 6e 61 62 6c 65 41 63 74 69 76 65 54 69 6c 65 28 29 2c 24 28 22 23 63 72 65 64 5f 70 61 73 73 77 6f 72 64 5f 69 6e 70 75 74 74 65 78 74 22 29 2e 76 61 6c 28 22 22 29 2c 24 28 22 23 63 74 61 5f 65 72 72 6f 72 5f 6d 65 73 73 61 67 65 5f 74 65 78 74 22 29 2e 72 65 6d 6f 76 65 28 29 2c 24 28 22 2e 6c 6f 67 69 6e 5f 63 72 65 64 5f 66 69 65 6c 64 5f 63 6f 6e 74 61 69 6e 65 72 22 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 73 68 6f 77 5f Data Ascii: direct":function(){$("#cred_password_inputtext").val(""),Context.username_state.last_checked_email="",Tiles.enableActiveTile(),$("#cred_password_inputtext").val(""),$("#cta_error_message_text").remove(),$(".login_cred_field_container").removeClass("show_
2022-06-30 20:27:55 UTC	766	IN	Data Raw: 4f 66 28 22 74 65 73 74 63 6f 6f 6b 69 65 3d 74 65 73 74 63 6f 6f 6b 69 65 22 29 7d 7d 2c 22 75 70 64 61 74 65 52 65 64 69 72 65 63 74 69 6f 6e 4d 65 73 73 61 67 65 22 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 0a 3b 74 3f 28 6e 3d 43 6f 6e 73 74 61 6e 74 73 2e 52 45 44 49 52 45 43 54 5f 4d 45 53 53 41 47 45 53 2e 43 4c 4f 55 44 46 45 44 45 52 41 54 45 44 2c 24 28 22 23 61 6c 74 65 72 6e 61 74 69 76 65 2d 69 64 65 6e 74 69 74 79 2d 70 72 6f 76 69 64 65 72 73 22 29 2e 68 69 64 65 28 29 29 3a 55 74 69 6c 2e 69 73 4d 53 41 28 65 29 3f 6e 3d 43 6f 6e 73 74 61 6e 74 73 2e 52 45 44 49 52 45 43 54 5f 4d 45 53 53 41 47 45 53 2e 4d 53 41 3a 28 6e 3d 43 6f 6e 73 74 61 6e 74 73 2e 52 45 44 49 52 45 43 54 5f 4d 45 53 53 41 47 45 53 2e 41 41 44 2c 24 Data Ascii: Of("testcookie=testcookie")}},"updateRedirectionMessage":function(e,t){var n;t?(n=Constants.REDIRECT_MESSAGES.CLOUDFEDERATED,$("#alternative-identity-providers").hide()):Util.isMSA(e)?n=Constants.REDIRECT_MESSAGES.MSA:(n=Constants.REDIRECT_MESSAGES.AAD,$
2022-06-30 20:27:55 UTC	782	IN	Data Raw: 77 73 65 72 2e 53 61 66 61 72 69 26 26 28 61 28 22 44 65 74 65 63 74 65 64 20 42 72 6f 77 73 65 72 3a 20 53 61 66 61 72 69 22 29 2c 21 30 29 7d 66 75 6e 63 74 69 6f 6e 20 45 28 29 7b 0a 61 28 22 41 74 74 65 6d 70 74 69 6e 67 20 74 6f 20 70 65 72 66 6f 72 6d 20 49 6e 74 65 67 72 61 74 65 64 20 57 69 6e 64 6f 77 73 20 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 2e 2e 2e 22 29 2c 6e 28 65 29 2e 6f 6e 28 22 6d 65 73 73 61 67 65 22 2c 6c 29 3b 76 61 72 20 74 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 69 66 72 61 6d 65 22 29 3b 74 2e 69 64 3d 22 64 73 73 6f 5f 69 66 72 61 6d 65 22 2c 74 2e 73 74 79 6c 65 2e 64 69 73 70 6c 61 79 3d 22 6e 6f 6e 65 22 2c 74 2e 73 72 63 3d 4c 7c 7c 72 28 52 2c 22 69 66 72 61 6d 65 3d 31 22 29 2c 74 2e Data Ascii: wser.Safari&&(a("Detected Browser: Safari"),!0)}function E(){a("Attempting to perform Integrated Windows Authentication..."),n(e).on("message",l);var t=document.createElement("iframe");t.id="dsso_iframe",t.style.display="none",t.src=L||r(R,"iframe=1"),t.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49821	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	785	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
2022-06-30 20:27:56 UTC	786	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: 160330 Cache-Control: public, max-age=604800 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:27:56 GMT Etag: 0x8D64101507E84BD Last-Modified: Fri, 02 Nov 2018 20:25:22 GMT Server: ECAcc (muc/3369) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5f096bc0-c01e-0068-5d4a-8b7b59000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-06-30 20:27:56 UTC	786	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
22	192.168.2.5	49822	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	785	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
2022-06-30 20:27:56 UTC	790	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: 159448 Cache-Control: public, max-age=604800 Content-MD5: HMwsHhNXdtrfirQDkzcqMA== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:27:56 GMT Etag: 0x8D641014CC1CD9F Last-Modified: Fri, 02 Nov 2018 20:25:15 GMT Server: ECAcc (muc/336D) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 56c513ed-001e-002a-394c-8b8a96000000 x-ms-version: 2009-09-19 Content-Length: 915 Connection: close
2022-06-30 20:27:56 UTC	790	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 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 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
23	192.168.2.5	49823	51.210.3.236	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	785	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
2022-06-30 20:27:56 UTC	791	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 30 Jun 2022 20:27:56 GMT Content-Type: image/png Content-Length: 1031 Connection: close
2022-06-30 20:27:56 UTC	791	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>@(`+-Gtzzw0000 o#Bk9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49818	192.154.231.67	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	792	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
2022-06-30 20:27:56 UTC	793	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:57 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
2022-06-30 20:27:56 UTC	793	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
25	192.168.2.5	49825	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	797	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.msftauth.net

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:56 UTC	797	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * 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 Age: 4318668 Cache-Control: public, max-age=31536000 Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Content-Type: image/x-icon Date: Thu, 30 Jun 2022 20:27:56 GMT Etag: 0x8D8731240E548EB Last-Modified: Sun, 18 Oct 2020 03:02:30 GMT Server: ECAcc (muc/3374) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 89c38479-601e-001b-6d78-65b5e2000000 x-ms-version: 2009-09-19 Content-Length: 17174 Connection: close
2022-06-30 20:27:56 UTC	798	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 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 00 00 00 ff ff ff 00 ef a4 00 0 0 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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 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 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 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%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%70%61%64%64%69%6E%67%2D%6
2022-06-30 20:27:53 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%
2022-06-30 20:27:53 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
2022-06-30 20:27:53 UTC	38	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
2022-06-30 20:27:53 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%
2022-06-30 20:27:53 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
2022-06-30 20:27:53 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
2022-06-30 20:27:53 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%
2022-06-30 20:27:53 UTC	77	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
2022-06-30 20:27:53 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 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	192.168.2.5	49785	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 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
2022-06-30 20:27:53 UTC	98	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:53 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 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: 7239a52d4a9fbb77-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 20:27:53 UTC	99	IN	Data Raw: 33 38 61 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 66 Data Ascii: 38a/*! * 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{f
2022-06-30 20:27:53 UTC	101	IN	Data Raw: 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 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 Data Ascii: gcaption,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-color:transpa
2022-06-30 20:27:53 UTC	102	IN	Data Raw: 37 66 66 39 0d 0a 3a 2d 2e 35 65 6d 7d 73 75 62 7b 62 6f 74 74 6f 6d 3a 2d 2e 32 35 65 6d 7d 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 73 76 67 3a 6e 6f 74 28 3a 72 6f 6f 74 29 7b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 66 69 67 75 72 65 7b 6d 61 72 67 69 6e 3a 31 65 6d 20 34 30 70 78 7d 68 72 7b 68 65 69 67 68 74 3a 30 3b 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 7d 70 72 65 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 7d 63 6f 64 65 2c 6b 62 64 2c 70 72 65 2c 73 61 6d 70 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 6d 6f 6e 6f 73 70 61 63 65 2c 6d 6f 6e 6f 73 Data Ascii: 7ff9:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{height:0;-webkit-box-sizing:content-box;-moz-box-sizing:content-box;box-sizing:content-box}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monos
2022-06-30 20:27:53 UTC	104	IN	Data Raw: 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 68 35 62 70 2f 68 74 6d 6c 35 2d 62 6f 69 6c 65 72 70 6c 61 74 65 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 73 72 63 2f 63 73 73 2f 6d 61 69 6e 2e 63 73 73 20 2a 2f 40 6d 65 64 69 61 20 70 72 69 6e 74 7b 2a 2c 3a 61 66 74 65 72 2c 3a 62 65 66 6f 72 65 7b 63 6f 6c 6f 72 3a 23 30 30 30 21 69 6d 70 6f 72 74 61 6e 74 3b 74 65 78 74 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 30 20 30 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 61 2c 61 3a 76 69 73 69 74 65 64 7b 74 65 78 74 2d 64 65 63 6f 72 61 Data Ascii: s://github.com/h5bp/html5-boilerplate/blob/master/src/css/main.css */@media print{*,:after,:before{color:#000!important;text-shadow:none!important;background:0 0!important;-webkit-box-shadow:none!important;box-shadow:none!important}a,a:visited{text-decora
2022-06-30 20:27:53 UTC	106	IN	Data Raw: 67 27 29 7d 2e 67 6c 79 70 68 69 63 6f 6e 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 74 6f 70 3a 31 70 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 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 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 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 3b 2d 77 65 62 6b 69 74 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 61 6e 74 69 61 6c 69 61 73 65 64 3b 2d 6d 6f 7a 2d 6f 73 78 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 67 72 61 79 73 63 61 6c 65 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 61 73 74 65 72 69 73 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 30 30 32 61 Data Ascii: g')}.glyphicon{position:relative;top:1px;display:inline-block;font-family:'Glyphicons Halflings';font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.glyphicon-asterisk:before{content:"\002a

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	107	IN	Data Raw: 68 69 63 6f 6e 2d 74 69 6d 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 32 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 72 6f 61 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 32 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 64 6f 77 6e 6c 6f 61 64 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 32 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 64 6f 77 6e 6c 6f 61 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 32 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 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 65 30 32 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 69 6e 62 6f 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 32 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d Data Ascii: hicon-time:before{content:"\e023"}.glyphicon-road:before{content:"\e024"}.glyphicon-download-alt:before{content:"\e025"}.glyphicon-download:before{content:"\e026"}.glyphicon-upload:before{content:"\e027"}.glyphicon-inbox:before{content:"\e028"}.glyphicon-
2022-06-30 20:27:53 UTC	109	IN	Data Raw: 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 35 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 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 35 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 69 6e 64 65 6e 74 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 35 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 69 6e 64 65 6e 74 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 35 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 66 61 63 65 74 69 6d 65 2d 76 69 64 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 35 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 69 63 74 75 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 30 36 30 22 7d 2e 67 6c 79 70 68 69 63 Data Ascii: :before{content:"\e055"}.glyphicon-list:before{content:"\e056"}.glyphicon-indent-left:before{content:"\e057"}.glyphicon-indent-right:before{content:"\e058"}.glyphicon-facetime-video:before{content:"\e059"}.glyphicon-picture:before{content:"\e060"}.glyphic
2022-06-30 20:27:53 UTC	110	IN	Data Raw: 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 72 65 6d 6f 76 65 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 65 30 38 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 6b 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 65 30 38 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 61 6e 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 65 30 39 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 61 72 72 6f 77 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 39 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 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 65 30 39 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 61 72 72 6f 77 2d 75 70 3a 62 65 66 6f Data Ascii: 7"}.glyphicon-remove-circle:before{content:"\e088"}.glyphicon-ok-circle:before{content:"\e089"}.glyphicon-ban-circle:before{content:"\e090"}.glyphicon-arrow-left:before{content:"\e091"}.glyphicon-arrow-right:before{content:"\e092"}.glyphicon-arrow-up:befo
2022-06-30 20:27:53 UTC	113	IN	Data Raw: 6e 74 3a 22 5c 65 31 32 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 75 6c 6c 68 6f 72 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 32 32 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 62 65 6c 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 32 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 65 72 74 69 66 69 63 61 74 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 32 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 68 75 6d 62 73 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 32 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 68 75 6d 62 73 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 32 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 68 61 6e 64 2d 72 69 67 68 74 3a 62 65 66 6f Data Ascii: nt:"\e121"}.glyphicon-bullhorn:before{content:"\e122"}.glyphicon-bell:before{content:"\e123"}.glyphicon-certificate:before{content:"\e124"}.glyphicon-thumbs-up:before{content:"\e125"}.glyphicon-thumbs-down:before{content:"\e126"}.glyphicon-hand-right:befo
2022-06-30 20:27:53 UTC	116	IN	Data Raw: 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 35 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 6f 72 74 2d 62 79 2d 6f 72 64 65 72 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 35 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 6f 72 74 2d 62 79 2d 61 74 74 72 69 62 75 74 65 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 35 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 6f 72 74 2d 62 79 2d 61 74 74 72 69 62 75 74 65 73 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 35 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 75 6e 63 68 65 63 6b 65 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 35 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 65 78 70 61 6e 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 Data Ascii: {content:"\e153"}.glyphicon-sort-by-order-alt:before{content:"\e154"}.glyphicon-sort-by-attributes:before{content:"\e155"}.glyphicon-sort-by-attributes-alt:before{content:"\e156"}.glyphicon-unchecked:before{content:"\e157"}.glyphicon-expand:before{content
2022-06-30 20:27:53 UTC	117	IN	Data Raw: 6e 74 65 6e 74 3a 22 5c 65 31 38 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 74 61 74 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 38 35 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 64 2d 76 69 64 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 38 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 68 64 2d 76 69 64 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 38 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 75 62 74 69 74 6c 65 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 38 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 6f 75 6e 64 2d 73 74 65 72 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 31 38 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 73 6f 75 6e 64 2d 64 6f 6c 62 79 3a 62 Data Ascii: ntent:"\e184"}.glyphicon-stats:before{content:"\e185"}.glyphicon-sd-video:before{content:"\e186"}.glyphicon-hd-video:before{content:"\e187"}.glyphicon-subtitles:before{content:"\e188"}.glyphicon-sound-stereo:before{content:"\e189"}.glyphicon-sound-dolby:b
2022-06-30 20:27:53 UTC	118	IN	Data Raw: 68 69 63 6f 6e 2d 62 65 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 31 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 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 38 66 66 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 65 72 61 73 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 32 31 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 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 32 33 31 62 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6c 61 6d 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 32 33 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 64 75 70 6c 69 63 61 74 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 32 34 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 70 69 67 67 Data Ascii: hicon-bed:before{content:"\e219"}.glyphicon-apple:before{content:"\f8ff"}.glyphicon-erase:before{content:"\e221"}.glyphicon-hourglass:before{content:"\231b"}.glyphicon-lamp:before{content:"\e223"}.glyphicon-duplicate:before{content:"\e224"}.glyphicon-pigg
2022-06-30 20:27:53 UTC	121	IN	Data Raw: 6f 72 69 7a 6f 6e 74 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 65 32 34 36 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 62 6a 65 63 74 2d 61 6c 69 67 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 32 34 37 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 62 6a 65 63 74 2d 61 6c 69 67 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 34 38 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 6f 62 6a 65 63 74 2d 61 6c 69 67 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 32 34 39 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 72 69 61 6e 67 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 65 32 35 30 22 7d 2e 67 6c 79 70 68 69 63 6f 6e 2d 74 Data Ascii: orizontal:before{content:"\e246"}.glyphicon-object-align-left:before{content:"\e247"}.glyphicon-object-align-vertical:before{content:"\e248"}.glyphicon-object-align-right:before{content:"\e249"}.glyphicon-triangle-right:before{content:"\e250"}.glyphicon-t

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	122	IN	Data Raw: 65 72 3e 2e 69 74 65 6d 3e 61 3e 69 6d 67 2c 2e 63 61 72 6f 75 73 65 6c 2d 69 6e 6e 65 72 3e 2e 69 74 65 6d 3e 69 6d 67 2c 2e 69 6d 67 2d 72 65 73 70 6f 6e 73 69 76 65 2c 2e 74 68 75 6d 62 6e 61 69 6c 20 61 3e 69 6d 67 2c 2e 74 68 75 6d 62 6e 61 69 6c 3e 69 6d 67 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 61 75 74 6f 7d 2e 69 6d 67 2d 72 6f 75 6e 64 65 64 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 36 70 78 7d 2e 69 6d 67 2d 74 68 75 6d 62 6e 61 69 6c 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 34 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 34 32 38 35 37 Data Ascii: er>.item>a>img,.carousel-inner>.item>img,.img-responsive,.thumbnail a>img,.thumbnail>img{display:b lock;max-width:100%;height:auto}.img-rounded{border-radius:6px}.img-thumbnail{display:inline-block;max-width:1 00%;height:auto;padding:4px;line-height:1.42857
2022-06-30 20:27:53 UTC	125	IN	Data Raw: 7a 65 3a 36 35 25 7d 2e 68 34 2c 2e 68 35 2c 2e 68 36 2c 68 34 2c 68 35 2c 68 36 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 30 70 78 7d 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 34 20 2e 73 6d 61 6c 6c 2c 68 34 20 73 6d 61 6c 6c 2c 68 35 20 2e 73 6d 61 6c 6c 2c 68 35 20 73 6d 61 6c 6c 2c 68 36 20 2e 73 6d 61 6c 6c 2c 68 36 20 73 6d 61 6c 6c 7b 66 6f 6e 74 2d 73 69 7a 65 3a 37 35 25 7d 2e 68 31 2c 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 33 36 70 78 7d 2e 68 32 2c 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 33 30 70 78 7d 2e 68 33 2c 68 33 7b 66 6f 6e 74 2d 73 69 Data Ascii: ze:65%}.h4,.h5,.h6,h4,h5,h6{margin-top:10px;margin-bottom:10px}.h4 .small,.h4 small,.h5 .small,.h5 small,.h6 .small,.h6 small,h4 .small,h4 small,h5 .small,h5 small,h6 .small,h6 small{font-size:75%}.h1,h1{font-size:36px}.h2,h2{font-size:30px}.h3,h3{font-si
2022-06-30 20:27:53 UTC	128	IN	Data Raw: 65 73 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 66 66 30 64 38 7d 61 2e 62 67 2d 73 75 63 63 65 73 73 3a 66 6f 63 75 73 2c 61 2e 62 67 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 72 3a 23 63 31 65 32 62 33 7d 2e 62 67 2d 69 6e 66 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 39 65 64 66 37 7d 61 2e 62 67 2d 69 6e 66 6f 3a 66 6f 63 75 73 2c 61 2e 62 67 2d 69 6e 66 6f 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 61 66 64 39 65 65 7d 2e 62 67 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 63 66 38 65 33 7d 61 2e 62 67 2d 77 61 72 6e 69 6e 67 3a 66 6f 63 75 73 2c 61 2e 62 67 2d 77 61 72 6e 69 6e 67 3a 68 6f 76 Data Ascii: ess{background-color:#dff0d8}a.bg-success:focus,a.bg-success:hover{background-color:#c1e2b3}.bg-in fo{background-color:#d9edf7}a.bg-info:focus,a.bg-info:hover{background-color:#afd9ee}.bg-warning{background-co lor:#fcf8e3}a.bg-warning:focus,a.bg-warning:hov
2022-06-30 20:27:53 UTC	130	IN	Data Raw: 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 66 6f 6e 74 2d 73 69 7a 65 3a 38 30 25 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 37 37 37 7d 62 6c 6f 63 6b 71 75 6f 74 65 20 2e 73 6d 61 6c 6c 3a 62 65 66 6f 72 65 2c 62 6c 6f 63 6b 71 75 6f 74 65 20 66 6f 6f 74 65 72 3a 62 65 66 6f 72 65 2c 62 6c 6f 63 6b 71 75 6f 74 65 20 73 6d 61 6c 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 27 5c 32 30 31 34 20 5c 30 30 41 30 27 7d 2e 62 6c 6f 63 6b 71 75 6f 74 65 2d 72 65 76 65 72 73 65 2c 62 6c 6f 63 6b 71 75 6f 74 65 2e 70 75 6c 6c 2d 72 69 67 68 74 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 31 35 70 78 3b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 3b 62 6f 72 64 Data Ascii: display:block;font-size:80%;line-height:1.42857143;color:#777}blockquote .small:before,blockquote footer:bef ore,blockquote small:before{content:'\2014 \00A0'}.blockquote-reverse,blockquote.pull-right{padding-right:15px;padding-l eft:0;text-align:right;bord
2022-06-30 20:27:53 UTC	132	IN	Data Raw: 61 6b 2d 77 6f 72 64 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 66 35 66 35 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 63 63 63 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 34 70 78 7d 70 72 65 20 63 6f 64 65 7b 70 61 64 64 69 6e 67 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 69 6e 68 65 72 69 74 3b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 2d 77 72 61 70 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 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 7d 2e 70 72 65 2d 73 63 72 6f 6c 6c 61 62 6c 65 7b 6d 61 78 2d 68 65 69 67 68 74 3a 33 34 30 70 78 3b 6f 76 65 72 66 6c 6f 77 2d 79 3a 73 63 72 6f 6c 6c 7d 2e 63 6f 6e 74 61 69 6e 65 72 7b 70 61 64 Data Ascii: ak-word;background-color:#f5f5f5;border:1px solid #ccc;border-radius:4px}pre code{padding:0;font-size:inheri t;color:inherit;white-space:pre-wrap;background-color:transparent;border-radius:0}.pre-scrollable{max-height:340px;overf low-y:scroll}.container{pad
2022-06-30 20:27:53 UTC	133	IN	Data Raw: 38 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 73 2d 39 7b 77 69 64 74 68 3a 37 35 25 7d 2e 63 6f 6c 2d 78 73 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 78 73 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 78 73 2d 36 7b 77 69 64 74 68 3a 35 30 25 7d 2e 63 6f 6c 2d 78 73 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 78 73 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 78 73 2d 33 7b 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 78 73 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 78 73 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 78 73 2d 70 Data Ascii: 83.33333333%}.col-xs-9{width:75%}.col-xs-8{width:66.66666667%}.col-xs-7{width:58.33333333%}.col-xs-6{width:50%}.col-xs-5{width:41.66666667%}.col-xs-4{width:33.33333333%}.col-xs-3{width:25%}.col-xs-2{width:16.66666667%}.col-xs-1{width:8.33333333%}.col-xs-p
2022-06-30 20:27:53 UTC	137	IN	Data Raw: 69 6e 2d 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 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 78 73 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 78 73 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 78 73 2d 6f 66 66 73 65 74 2d 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 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 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 Data Ascii: in-left:33.33333333%}.col-xs-offset-3{margin-left:25%}.col-xs-offset-2{margin-left:16.66666667%}.col-xs-offset-1{margin-left:8.33333333%}.col-xs-offset-0{margin-left:0}@media (min-width:768px){.col-sm-1,.col-sm-10,.col-sm-11,.col-sm-12,.col-sm-2,.col-sm-3
2022-06-30 20:27:53 UTC	138	IN	Data Raw: 36 36 37 25 7d 2e 63 6f 6c 2d 73 6d 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 73 6d 2d 70 75 73 68 2d 30 7b 6c 65 66 74 3a 61 75 74 6f 7d 2e 63 6f 6c 2d 73 6d 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 73 6d 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 73 6d 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 73 6d 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 73 6d 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 Data Ascii: 667%}.col-sm-push-1{left:8.33333333%}.col-sm-push-0{left:auto}.col-sm-offset-12{margin-left:100%}.col-sm-offset-11{margin-left:91.66666667%}.col-sm-offset-10{margin-left:83.33333333%}.col-sm-offset-9{margin-left:75%}.col-sm-offset-8{margin-left:66.6666666

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	141	IN	Data Raw: 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 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 6d 64 2d 70 75 6c 6c 2d 30 7b 72 69 67 68 74 3a 61 75 74 6f 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 31 32 7b 6c 65 66 74 3a 31 30 30 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 31 31 7b 6c 65 66 74 3a 39 31 2e 36 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 31 30 7b 6c 65 66 74 3a 38 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 39 7b 6c 65 66 74 3a 37 35 25 7d 2e 63 6f 6c 2 d 6d 64 2d 70 75 73 68 2d 38 7b 6c 65 66 74 3a 36 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 37 7b 6c 65 66 74 3a 35 38 2e 33 33 33 33 33 33 33 33 25 7d Data Ascii: 6.66666667%}.col-md-pull-1{right:8.33333333%}.col-md-pull-0{right:auto}.col-md-push-12{left:100%}.col-md-push-11{left:91.66666667%}.col-md-push-10{left:83.33333333%}.col-md-push-9{left:75%}.col-md-push-8{left:66.66666667%}.col-md-push-7{left:58.33333333%}
2022-06-30 20:27:53 UTC	142	IN	Data Raw: 7b 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 6c 67 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 6c 67 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 6c 67 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 6c 67 2d 70 75 6c 6c 2d 31 31 7b 72 69 67 68 74 3a 39 31 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 70 75 6c 6c 2d 31 30 7b 72 69 67 68 74 3a 38 33 2e 33 33 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6c 67 2d 70 75 6c 6c 2d 39 7b 72 69 67 68 74 3a 37 35 25 7d 2e 63 6f 6c 2d 6c 67 2d 70 75 6c 6c 2d 38 7b 72 69 67 68 74 3a 36 36 2e 36 36 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 70 75 6c 6c 2d 37 7b 72 69 67 68 74 3a 35 38 2e 33 33 33 33 33 33 33 Data Ascii: {width:25%}.col-lg-2{width:16.66666667%}.col-lg-1{width:8.33333333%}.col-lg-pull-12{right:100%}.col-lg-pull-11{right:91.66666667%}.col-lg-pull-10{right:83.33333333%}.col-lg-pull-9{right:75%}.col-lg-pull-8{right:66.66666667%}.col-lg-pull-7{right:58.3333333
2022-06-30 20:27:53 UTC	144	IN	Data Raw: 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 63 61 70 74 69 6f 6e 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 38 70 78 3b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 74 68 7b 74 65 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 7d 2e 74 61 62 6c 65 7b 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 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 30 70 78 7d 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 Data Ascii: kground-color:transparent}caption{padding-top:8px;padding-bottom:8px;color:#777;text-align:left}th{text-align:left}.table{width:100%;max-width:100%;margin-bottom:20px}.table>tbody>tr>td,.table>tbody>tr>th,.table>tfoot>tr>td,.table>tfoot>tr>th,.table>thead
2022-06-30 20:27:53 UTC	146	IN	Data Raw: 6f 6c 6f 72 3a 23 66 35 66 35 66 35 7d 74 61 62 6c 65 20 63 6f 6c 5b 63 6c 61 73 73 2a 3d 63 6f 6c 2d 5d 7b 70 6f 73 69 74 69 6f 6e 3a 73 74 61 74 69 63 3b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 63 6f 6c 75 6d 6e 3b 66 6c 6f 61 74 3a 6e 6f 6e 65 7d 74 61 62 6c 65 20 74 64 5b 63 6c 61 73 73 2a 3d 63 6f 6c 2d 5d 2c 74 61 62 6c 65 20 74 68 5b 63 6c 61 73 73 2a 3d 63 6f 6c 2d 5d 7b 70 6f 73 69 74 69 6f 6e 3a 73 74 61 74 69 63 3b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 63 65 6c 6c 3b 66 6c 6f 61 74 3a 6e 6f 6e 65 7d 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 2e 61 63 74 69 76 65 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 2e 61 63 74 69 76 65 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 62 6f 64 79 3e 74 72 3e 74 64 2e 61 63 74 69 76 65 2c 2e 74 61 Data Ascii: olor:#f5f5f5}table col[class*=col-]{position:static;display:table-column;float:none}table td[class*=col-],table th[class*=col-]{position:static;display:table-cell;float:none}.table>tbody>tr.active>td,.table>tbody>tr.active>th,.table>tbody>tr>td.active,.ta
2022-06-30 20:27:53 UTC	148	IN	Data Raw: 3e 74 62 6f 64 79 3e 74 72 3e 74 68 2e 69 6e 66 6f 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 2e 69 6e 66 6f 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 2e 69 6e 66 6f 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 3e 74 64 2e 69 6e 66 6f 2c 2e 74 61 62 6c 65 3e 74 66 6f 6f 74 3e 74 72 3e 74 68 2e 69 6e 66 6f 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 2e 69 6e 66 6f 3e 74 64 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 2e 69 6e 66 6f 3e 74 68 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 64 2e 69 6e 66 6f 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 68 2e 69 6e 66 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 39 65 64 66 37 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 Data Ascii: >tbody>tr>th.info,.table>tfoot>tr.info>td,.table>tfoot>tr.info>th,.table>tfoot>tr>td.info,.table>tfoot>tr>th.info,.table>thead>tr.info>td,.table>thead>tr.info>th,.table>thead>tr>td.info,.table>thead>tr>th.info{background-color:#d9edf7}.table-hover>tbody>t
2022-06-30 20:27:53 UTC	149	IN	Data Raw: 38 30 30 30 0d 0a 3e 74 64 2e 64 61 6e 67 65 72 2c 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 68 2e 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 66 32 64 65 64 65 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 2e 64 61 6e 67 65 72 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 64 61 6e 67 65 72 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 64 61 6e 67 65 72 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 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 3e 74 62 6f 64 79 3e 74 72 3e 74 68 2e 64 61 6e 67 65 72 3a 68 6f 76 65 72 Data Ascii: 8000>td.danger,.table>thead>tr>th.danger{background-color:#f2dede}.table-hover>tbody>tr.danger:hover>td,.table-hover>tbody>tr.danger:hover>th,.table-hover>tbody>tr:hover>.danger,.table-hover>tbody>tr>td.danger:hover,.table-hover>tbody>tr>th.danger:hover
2022-06-30 20:27:53 UTC	152	IN	Data Raw: 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 6c 61 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 68 65 61 64 3e 74 72 3e 74 68 3a 6c 61 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 68 65 61 64 3e 74 72 3e 74 68 3a 6c 61 73 74 2d 63 68 69 6c 64 7b 62 6f 72 64 65 72 2d 72 69 67 68 74 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 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 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 Data Ascii: nsive>.table-bordered>tfoot>tr>th:last-child,.table-responsive>.table-bordered>thead>tr>td:last-child,.table-responsive>.table-bordered>thead>tr>th:last-child{border-right:0}.table-responsive>.table-bordered>tbody>tr:last-child>td,.table-responsive>.table
2022-06-30 20:27:53 UTC	153	IN	Data Raw: 6d 61 67 65 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 63 63 63 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 69 6e 73 65 74 20 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 65 61 73 65 2d 69 6e 2d 6f 75 74 20 2e 31 35 73 2c 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 20 65 61 73 65 2d 69 6e 2d 6f 75 74 20 2e 31 35 73 3b 2d 6f 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c Data Ascii: mage:none;border:1px solid #ccc;border-radius:4px;-webkit-box-shadow:inset 0 1px 1px rgba(0,0,0,.075);box-shadow:inset 0 1px 1px rgba(0,0,0,.075);-webkit-transition:border-color ease-in-out .15s,-webkit-box-shadow ease-in-out .15s;-o-transition:border-col

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	154	IN	Data Raw: 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 20 69 6e 70 75 74 5b 74 79 70 65 3d 6d 6f 6e 74 68 5d 2c 69 6e 70 75 74 5b 74 79 70 65 3d 64 61 74 65 5d 2e 69 6e 70 75 74 2d 73 6d 2c 69 6e 70 75 74 5b 74 79 70 65 3d 74 69 6d 65 5d 2e 69 6e 70 75 74 2d 73 6d 2c 69 6e 70 75 74 5b 74 79 70 65 3d 64 61 74 65 74 69 6d 65 2c 69 6e 70 75 74 2d 73 6d 2c 69 6e 70 75 74 5b 74 79 70 65 3d 6d 6f 6e 74 68 5d 2e 69 6e 70 75 74 2d 73 6d 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 30 70 78 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 20 69 6e 70 75 74 5b 74 79 70 65 3d 64 61 74 65 5d 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 20 69 6e 70 75 74 5b 74 79 70 65 3d 74 69 6d 65 5d 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 20 69 6e 70 75 74 5b 74 Data Ascii: .input-group-sm input[type=month],input[type=date].input-sm,input[type=time].input-sm,input[type=datetime-local].input-sm,input[type=month].input-sm{line-height:30px}.input-group-lg input[type=date],.input-group-lg input[type=time],.input-group-lg input[t
2022-06-30 20:27:53 UTC	157	IN	Data Raw: 6c 69 6e 65 2e 64 69 73 61 62 6c 65 64 2c 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 2e 64 69 73 61 62 6c 65 64 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 7b 63 75 72 73 6f 72 3a 6e 6f 74 2d 61 6c 6c 6f 77 65 64 7d 2e 63 68 65 63 6b 62 6f 78 2e 64 69 73 61 62 6c 65 64 20 6c 61 62 65 6c 2c 2e 72 61 64 69 6f 2e 64 69 73 61 62 6c 65 64 20 6c 61 62 65 6c 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 63 68 65 63 6b 62 6f 78 20 6c 61 62 65 6c 2c 66 69 65 6c 64 73 65 74 5b 64 69 73 61 62 6c 65 64 5d 20 2e 72 61 64 69 6f 20 6c 61 62 65 6c 7b 63 75 72 73 6f 72 3a 6e 6f 74 2d 61 6c 6c 6f 77 Data Ascii: line.disabled,.radio-inline.disabled,fieldset[disabled] .checkbox-inline,fieldset[disabled] .radio-inline{cursor:not-allowed}.checkbox.disabled label,.radio.disabled label,fieldset[disabled] .checkbox label,fieldset[disabled] .radio label{cursor:not-allow
2022-06-30 20:27:53 UTC	158	IN	Data Raw: 68 74 3a 34 36 70 78 7d 2e 66 6f 72 6d 2d 67 72 6f 75 70 2d 6c 67 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 6c 67 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 6c 67 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 34 36 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 31 70 78 20 31 36 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 33 33 33 33 33 33 33 7d 2e 68 61 73 2d 66 65 65 64 62 61 63 6b 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 2e 68 Data Ascii: ht:46px}.form-group-lg select[multiple].form-control,.form-group-lg textarea.form-control{height:auto}.form-group-lg .form-control-static{height:46px;min-height:38px;padding:11px 16px;font-size:18px;line-height:1.3333333}.has-feedback{position:relative}.h
2022-06-30 20:27:53 UTC	161	IN	Data Raw: 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 2c 30 20 30 20 36 70 78 20 23 36 37 62 31 36 38 7d 2e 68 61 73 2d 73 75 63 63 65 73 73 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 33 63 37 36 33 64 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 66 66 30 64 38 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 63 37 36 33 64 7d 2e 68 61 73 2d 73 75 63 63 65 73 73 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 33 63 37 36 33 64 7d 2e 68 61 73 2d 77 61 72 6e 69 6e 67 20 2e 63 68 65 63 6b 62 6f 78 2c 2e 68 61 73 2d 77 61 72 6e 69 6e 67 20 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 2e 68 61 73 2d 77 61 72 6e 69 6e 67 20 2e 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 2c 2e Data Ascii: ba(0,0,0,.075),0 0 6px #67b168}.has-success .input-group-addon{color:#3c763d;background-color:#dff0d8;border-color:#3c763d}.has-success .form-control-feedback{color:#3c763d}.has-warning .checkbox,.has-warning .checkbox-inline,.has-warning .control-label,.
2022-06-30 20:27:53 UTC	162	IN	Data Raw: 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 38 34 33 35 33 34 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 2c 30 20 30 20 36 70 78 20 23 63 65 38 34 38 33 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 31 70 78 20 31 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 2c 30 20 30 20 36 70 78 20 23 63 65 38 34 38 33 7d 2e 68 61 73 2d 65 72 72 6f 72 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 61 39 34 34 34 32 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 32 64 65 64 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 61 39 34 34 34 32 7d 2e 68 61 73 2d 65 72 72 6f 72 20 2e 66 6f 72 6d 2d Data Ascii: order-color:#843534;-webkit-box-shadow:inset 0 1px 1px rgba(0,0,0,.075),0 0 6px #ce8483;box-shadow:inset 0 1px 1px rgba(0,0,0,.075),0 0 6px #ce8483}.has-error .input-group-addon{color:#a94442;background-color:#f2dede;border-color:#a94442}.has-error .form-
2022-06-30 20:27:53 UTC	165	IN	Data Raw: 6d 2d 63 6f 6e 74 72 6f 6c 2d 66 65 65 64 62 61 63 6b 7b 74 6f 70 3a 30 7d 7d 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 63 68 65 63 6b 62 6f 78 2c 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 63 68 65 63 6b 62 6f 78 2d 69 6e 6c 69 6e 65 2c 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 72 61 64 69 6f 2c 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 72 61 64 69 6f 2d 69 6e 6c 69 6e 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 37 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 63 68 65 63 6b 62 6f 78 2c 2e 66 6f 72 6d 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 72 61 64 69 6f 7b 6d 69 6e 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e Data Ascii: m-control-feedback{top:0}}.form-horizontal .checkbox,.form-horizontal .checkbox-inline,.form-horizontal .radio,.form-horizontal .radio-inline{padding-top:7px;margin-top:0;margin-bottom:0}.form-horizontal .checkbox,.form-horizontal .radio{min-height:27px}.
2022-06-30 20:27:53 UTC	166	IN	Data Raw: 69 6e 65 3a 30 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 33 70 78 20 35 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 69 6e 73 65 74 20 30 20 30 20 33 70 78 20 35 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 35 29 7d 2e 62 74 6e 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 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 62 74 6e 7b 63 75 72 73 6f 72 3a 6e 6f 74 2d 61 6c 6c 6f 77 65 64 3b 66 69 6c 74 65 72 3a 61 6c 70 68 61 28 6f 70 61 63 69 74 79 3d 36 35 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 6f 70 61 63 69 74 79 3a 2e 36 35 7d 61 2e 62 74 Data Ascii: ine:0;-webkit-box-shadow:inset 0 3px 5px rgba(0,0,0,.125);box-shadow:inset 0 3px 5px rgba(0,0,0,.125)}.btn.disabled,.btn[disabled],fieldset[disabled] .btn{cursor:not-allowed;filter:alpha(opacity=65);-webkit-box-shadow:none;box-shadow:none;opacity:.65}a.bt
2022-06-30 20:27:53 UTC	168	IN	Data Raw: 73 61 62 6c 65 64 5d 20 2e 62 74 6e 2d 64 65 66 61 75 6c 74 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 66 66 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 63 63 63 7d 2e 62 74 6e 2d 64 65 66 61 75 6c 74 20 2e 62 61 64 67 65 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 33 33 33 7d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 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 33 33 33 37 61 62 37 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 32 65 36 64 61 34 7d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 79 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 Data Ascii: sabled] .btn-default:hover{background-color:#fff;border-color:#ccc}.btn-default .badge{color:#fff;background-color:#333}.btn-primary{color:#fff;background-color:#337ab7;border-color:#2e6da4}.btn-primary.focus,.btn-primary:focus{color:#fff;background-color

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	169	IN	Data Raw: 63 6f 6c 6f 72 3a 23 34 63 61 65 34 63 7d 2e 62 74 6e 2d 73 75 63 63 65 73 73 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 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 34 34 39 64 34 34 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 32 35 35 36 32 35 7d 2e 62 74 6e 2d 73 75 63 63 65 73 73 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 34 34 39 64 34 34 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 39 38 34 33 39 7d 2e 62 74 6e 2d 73 75 63 63 65 73 73 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 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 73 75 63 Data Ascii: color:#4cae4c}.btn-success.focus,.btn-success:focus{color:#fff;background-color:#449d44;border-color:#255625}.btn-success:hover{color:#fff;background-color:#449d44;border-color:#398439}.btn-success.active,.btn-success:active,.open>.dropdown-toggle.btn-suc
2022-06-30 20:27:53 UTC	172	IN	Data Raw: 6e 2d 69 6e 66 6f 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 69 6e 66 6f 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 69 6e 66 6f 7b 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 31 62 30 64 35 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 32 36 39 61 62 63 7d 2e 62 74 6e 2d 69 6e 66 6f 2e 61 63 74 69 76 65 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 69 6e 66 6f 2e 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 69 6e 66 6f 2e 61 63 74 69 76 65 3a 68 6f 76 65 72 2c 2e 62 74 6e 2d 69 6e 66 6f 3a 61 63 74 69 76 65 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 69 6e 66 6f 3a 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 69 6e 66 6f 3a 61 63 74 69 76 65 3a 68 6f 76 Data Ascii: n-info.active,.btn-info:active,.open>.dropdown-toggle.btn-info{color:#fff;background-color:#31b0d5;border-color:#269abc}.btn-info.active.focus,.btn-info.active:focus,.btn-info.active:hover,.btn-info:active.focus,.btn-info:active:focus,.btn-info:active:hov
2022-06-30 20:27:53 UTC	173	IN	Data Raw: 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 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 77 61 72 6e 69 6e 67 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 77 61 72 6e 69 6e 67 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 77 61 72 6e 69 6e 67 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 64 35 38 35 31 32 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 67 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 3a 61 63 74 69 76 65 2c 2e Data Ascii: e:focus,.btn-warning:active:hover,.open>.dropdown-toggle.btn-warning.focus,.open>.dropdown-toggle.btn-warning:focus,.open>.dropdown-toggle.btn-warning:hover{color:#fff;background-color:#d58512;border-color:#985f0d}.btn-warning.active,.btn-warning:active,.
2022-06-30 20:27:53 UTC	176	IN	Data Raw: 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 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 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 64 69 73 61 62 6c 65 64 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 64 69 73 61 62 6c 65 64 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 64 69 73 61 62 6c 65 64 3a 68 6f 76 65 72 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 5b 64 69 73 61 62 6c 65 64 5d 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 5b 64 69 73 61 62 6c 65 64 5d 3a 66 6f 63 75 73 2c 2e 62 Data Ascii: ;border-color:#761c19}.btn-danger.active,.btn-danger:active,.open>.dropdown-toggle.btn-danger{background-image:none}.btn-danger.disabled.focus,.btn-danger.disabled:focus,.btn-danger.disabled:hover,.btn-danger[disabled].focus,.btn-danger[disabled]:focus,.b
2022-06-30 20:27:53 UTC	177	IN	Data Raw: 25 7d 2e 62 74 6e 2d 62 6c 6f 63 6b 2b 2e 62 74 6e 2d 62 6c 6f 63 6b 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 70 78 7d 69 6e 70 75 74 5b 74 79 70 65 3d 62 75 74 74 6f 6e 5d 2e 62 74 6e 2d 62 6c 6f 63 6b 2c 69 6e 70 75 74 5b 74 79 70 65 3d 72 65 73 65 74 5d 2e 62 74 6e 2d 62 6c 6f 63 6b 2c 69 6e 70 75 74 5b 74 79 70 65 3d 73 75 62 6d 69 74 5d 2e 62 74 6e 2d 62 6c 6f 63 6b 7b 77 69 64 74 68 3a 31 30 30 25 7d 2e 66 61 64 65 7b 6f 70 61 63 69 74 79 3a 30 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 6f 70 61 63 69 74 79 20 2e 31 35 73 20 6c 69 6e 65 61 72 3b 2d 6f 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 6f 70 61 63 69 74 79 20 2e 31 35 73 20 6c 69 6e 65 61 72 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 6f 70 61 63 69 74 79 20 2e 31 35 73 20 6c 69 6e 65 61 72 Data Ascii: %}.btn-block+.btn-block{margin-top:5px}input[type=button].btn-block,input[type=reset].btn-block,input[type=submit].btn-block{width:100%}.fade{opacity:0;-webkit-transition:opacity .15s linear;-o-transition:opacity .15s linear;transition:opacity .15s linear
2022-06-30 20:27:53 UTC	287	IN	Data Raw: 73 74 2d 63 68 69 6c 64 29 3e 2e 62 74 6e 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 7d 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 2d 67 72 6f 75 70 3a 66 69 72 73 74 2d 63 68 69 6c 64 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 3e 2e 62 74 6e 2d 67 72 6f 75 70 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 2d 67 72 6f 75 70 3a 66 69 72 73 74 2d 63 68 69 6c 64 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 3e 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 72 69 67 68 74 2d 72 61 64 69 75 73 3a 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 72 69 67 68 74 2d 72 61 64 69 75 73 3a 30 7d 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 2d 67 72 6f 75 70 3a 6c 61 73 74 2d 63 68 69 6c 64 3a 6e Data Ascii: st-child)>.btn{border-radius:0}.btn-group>.btn-group:first-child:not(:last-child)>.btn:last-child,.btn-group>.btn-group:first-child:not(:last-child)>.dropdown-toggle{border-top-right-radius:0;border-bottom-right-radius:0}.btn-group>.btn-group:last-child:n
2022-06-30 20:27:53 UTC	291	IN	Data Raw: 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 63 65 6c 6c 7d 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 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 64 64 6f 6e 3a 6e 6f 74 28 3a 66 69 72 73 74 2d 63 68 69 6c 64 29 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 3a 6e 6f 74 28 3a 66 69 72 73 74 2d 63 68 69 6c 64 29 3a 6e 6f 74 28 3a 6c 61 73 74 2d 63 68 69 6c 64 29 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 64 64 6f 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 7b 77 Data Ascii: nput-group-btn{display:table-cell}.input-group .form-control:not(:first-child):not(:last-child),.input-group-addon:not(:first-child):not(:last-child),.input-group-btn:not(:first-child):not(:last-child){border-radius:0}.input-group-addon,.input-group-btn{w
2022-06-30 20:27:53 UTC	294	IN	Data Raw: 38 30 30 30 0d 0a 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 66 66 66 7d 7d 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 7b 66 6c 6f 61 74 3a 6c 65 66 74 7d 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 3e 61 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 34 70 78 7d 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 2b 6c 69 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 32 70 78 7d 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 2e 61 63 74 69 76 65 3e 61 2c 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 2e 61 63 74 69 76 65 3e 61 3a 66 6f 63 75 73 2c 2e 6e 61 76 2d 70 69 6c 6c 73 3e 6c 69 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 33 33 37 61 62 37 7d 2e 6e 61 76 2d 73 74 61 63 6b 65 64 3e 6c 69 7b 66 6c 6f 61 74 3a Data Ascii: 8000ottom-color:#fff}}.nav-pills>li{float:left}.nav-pills>li>a{border-radius:4px}.nav-pills>li+li{margin-left:2px}.nav-pills>li.active>a,.nav-pills>li.active>a:focus,.nav-pills>li.active>a:hover{color:#fff;background-color:#337ab7}.nav-stacked>li{float:

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	299	IN	Data Raw: 20 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 3e 6c 69 3e 61 3a 66 6f 63 75 73 2c 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 6c 69 3e 61 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 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 6e 61 76 7b 66 6c 6f 61 74 3a 6c 65 66 74 3b 6d 61 72 67 69 6e 3a 30 7d 2e 6e 61 76 62 61 72 2d 6e 61 76 3e 6c 69 7b 66 6c 6f 61 74 3a 6c 65 66 74 7d 2e 6e 61 76 62 61 72 2d 6e 61 76 3e 6c 69 3e 61 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 31 35 70 78 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 35 70 78 7d 7d 2e 6e 61 76 62 61 72 2d 66 6f 72 6d 7b 70 61 64 64 69 6e 67 3a 31 30 Data Ascii: .dropdown-menu>li>a:focus,.navbar-nav .open .dropdown-menu>li>a:hover{background-image:none}}@media (min-width:768px){.navbar-nav{float:left;margin:0}.navbar-nav>li{float:left}.navbar-nav>li>a{padding-top:15px;padding-bottom:15px}}.navbar-form{padding:10
2022-06-30 20:27:53 UTC	303	IN	Data Raw: 65 66 61 75 6c 74 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 2e 6e 61 76 62 61 72 2d 64 65 66 61 75 6c 74 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 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 63 63 63 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 7d 2e 6e 61 76 62 61 72 2d 64 65 66 61 75 6c 74 20 2e 6e 61 76 62 61 72 2d 6c 69 6e 6b 7b 63 6f 6c 6f 72 3a 23 37 37 37 7d 2e 6e 61 76 62 61 72 2d 64 65 66 61 75 6c 74 20 2e 6e 61 76 62 61 72 2d 6c 69 6e 6b 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 33 33 33 7d 2e 6e 61 Data Ascii: efault .navbar-nav .open .dropdown-menu>.disabled>a:focus,.navbar-default .navbar-nav .open .dropdown-menu>.disabled>a:hover{color:#ccc;background-color:transparent}}.navbar-default .navbar-link{color:#777}.navbar-default .navbar-link:hover{color:#333}.na
2022-06-30 20:27:53 UTC	307	IN	Data Raw: 6c 6f 72 3a 23 33 33 37 61 62 37 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 33 37 61 62 37 7d 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 61 2c 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 61 3a 66 6f 63 75 73 2c 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 61 3a 68 6f 76 65 72 2c 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 73 70 61 6e 2c 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 73 70 61 6e 3a 66 6f 63 75 73 2c 2e 70 61 67 69 6e 61 74 69 6f 6e 3e 2e 64 69 73 61 62 6c 65 64 3e 73 70 61 6e 3a 68 6f 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 Data Ascii: lor:#337ab7;border-color:#337ab7}.pagination>.disabled>a,.pagination>.disabled>a:focus,.pagination>.disabled>a:hover,.pagination>.disabled>span,.pagination>.disabled>span:focus,.pagination>.disabled>span:hover{color:#777;cursor:not-allowed;background-colo
2022-06-30 20:27:53 UTC	311	IN	Data Raw: 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 30 70 78 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 7d 2e 61 6c 65 72 74 20 68 34 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 7d 2e 61 6c 65 72 74 20 2e 61 6c 65 72 74 2d 6c 69 6e 6b 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 7d 2e 61 6c 65 72 74 3e 70 2c 2e 61 6c 65 72 74 3e 75 6c 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 61 6c 65 72 74 3e 70 2b 70 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 70 78 7d 2e 61 6c 65 72 74 2d 64 69 73 6d 69 73 73 61 62 6c 65 2c 2e 61 6c 65 72 74 2d 64 69 73 6d 69 73 73 69 62 6c 65 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 33 35 70 78 Data Ascii: margin-bottom:20px;border:1px solid transparent;border-radius:4px}.alert h4{margin-top:0;color:inherit}.alert .alert-link{font-weight:700}.alert>p,.alert>ul{margin-bottom:0}.alert>p+p{margin-top:5px}.alert-dismissable,.alert-dismissible{padding-right:35px
2022-06-30 20:27:53 UTC	315	IN	Data Raw: 2c 32 35 35 2c 32 35 35 2c 2e 31 35 29 20 32 35 25 2c 74 72 61 6e 73 70 61 72 65 6e 74 20 32 35 25 2c 74 72 61 6e 73 70 61 72 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 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 34 35 64 65 67 2c 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 31 35 29 20 32 35 25 2c 74 72 61 6e 73 70 61 72 65 6e 74 20 32 35 25 2c 74 72 61 6e 73 70 61 72 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 Data Ascii: ,255,255,.15) 25%,transparent 25%,transparent 50%,rgba(255,255,255,.15) 50%,rgba(255,255,255,.15) 75%,transparent 75%,transparent);background-image:linear-gradient(45deg,rgba(255,255,255,.15) 25%,transparent 25%,transparent 50%,rgba(255,255,255,.15) 50%,r
2022-06-30 20:27:53 UTC	319	IN	Data Raw: 72 3a 23 33 63 37 36 33 64 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 63 37 36 33 64 7d 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 69 6e 66 6f 7b 63 6f 6c 6f 72 3a 23 33 31 37 30 38 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 39 65 64 66 37 7d 61 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 69 6e 66 6f 2c 62 75 74 74 6f 6e 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 69 6e 66 6f 7b 63 6f 6c 6f 72 3a 23 33 31 37 30 38 66 7d 61 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 69 6e 66 6f 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 62 75 74 74 6f 6e 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 69 6e 66 6f 20 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 2d 68 65 61 64 Data Ascii: r:#3c763d;border-color:#3c763d}.list-group-item-info{color:#31708f;background-color:#d9edf7}a.list-group-item-info,button.list-group-item-info{color:#31708f}a.list-group-item-info .list-group-item-heading,button.list-group-item-info .list-group-item-headi
2022-06-30 20:27:53 UTC	323	IN	Data Raw: 2e 74 61 62 6c 65 3a 66 69 72 73 74 2d 63 68 69 6c 64 3e 74 62 6f 64 79 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 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 6c 61 73 74 2d 63 68 69 6c 64 3e 74 61 62 6c 65 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 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 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 62 6f 64 79 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 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 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 62 6f 64 79 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 68 65 61 64 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 3a 6c 61 73 74 2d 63 68 Data Ascii: .table:first-child>tbody:first-child>tr:first-child,.panel>.table-responsive:first-child>.table:first-child>thead:first-child>tr:first-child,.panel>.table:first-child>tbody:first-child>tr:first-child,.panel>.table:first-child>thead:first-child>tr:first-ch
2022-06-30 20:27:53 UTC	326	IN	Data Raw: 35 35 65 64 0d 0a 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 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 74 61 62 6c 65 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 66 6f 6f 74 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 3a 6c 61 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 6c 61 73 74 2d 63 68 69 6c 64 3e 2e 74 61 62 6c 65 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 66 6f 6f 74 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 3a 6c 61 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 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 66 6f 6f 74 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 74 72 3a 6c 61 73 74 2d 63 Data Ascii: 55edst-child,.panel>.table-responsive:last-child>.table:last-child>tfoot:last-child>tr:last-child td:last-child,.panel>.table-responsive:last-child>.table:last-child>tfoot:last-child>tr:last-child th:last-child,.panel>.table:last-child>tbody:last-child>

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	331	IN	Data Raw: 33 33 37 61 62 37 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 7d 2e 70 61 6e 65 6c 2d 70 72 69 6d 61 72 79 3e 2e 70 61 6e 65 6c 2d 66 6f 6f 74 65 72 2b 2e 70 61 6e 65 6c 2d 63 6f 6c 6c 61 70 73 65 3e 2e 70 61 6e 65 6c 2d 62 6f 64 79 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 33 33 37 61 62 37 7d 2e 70 61 6e 65 6c 2d 73 75 63 63 65 73 73 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 36 65 39 63 36 7d 2e 70 61 6e 65 6c 2d 73 75 63 63 65 73 73 3e 2e 70 61 6e 65 6c 2d 68 65 61 64 69 6e 67 7b 63 6f 6c 6f 72 3a 23 33 63 37 36 33 64 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 66 66 30 64 38 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 36 65 39 63 36 7d 2e 70 61 6e 65 6c 2d 73 75 63 63 65 73 73 3e Data Ascii: 337ab7;background-color:#fff}.panel-primary>.panel-footer+.panel-collapse>.panel-body{border-bottom-color:#337ab7}.panel-success{border-color:#d6e9c6}.panel-success>.panel-heading{color:#3c763d;background-color:#dff0d8;border-color:#d6e9c6}.panel-success>
2022-06-30 20:27:53 UTC	335	IN	Data Raw: 69 6e 2d 6c 65 66 74 3a 30 7d 2e 6d 6f 64 61 6c 2d 73 63 72 6f 6c 6c 62 61 72 2d 6d 65 61 73 75 72 65 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 2d 39 39 39 39 70 78 3b 77 69 64 74 68 3a 35 30 70 78 3b 68 65 69 67 68 74 3a 35 30 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 73 63 72 6f 6c 6c 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 6d 6f 64 61 6c 2d 64 69 61 6c 6f 67 7b 77 69 64 74 68 3a 36 30 30 70 78 3b 6d 61 72 67 69 6e 3a 33 30 70 78 20 61 75 74 6f 7d 2e 6d 6f 64 61 6c 2d 63 6f 6e 74 65 6e 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 35 70 78 20 31 35 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 35 70 78 20 31 35 70 78 20 72 Data Ascii: in-left:0}.modal-scrollbar-measure{position:absolute;top:-9999px;width:50px;height:50px;overflow:scroll}@media (min-width:768px){.modal-dialog{width:600px;margin:30px auto}.modal-content{-webkit-box-shadow:0 5px 15px rgba(0,0,0,.5);box-shadow:0 5px 15px r
2022-06-30 20:27:53 UTC	339	IN	Data Raw: 69 67 68 74 2d 77 69 64 74 68 3a 30 3b 62 6f 72 64 65 72 2d 6c 65 66 74 2d 63 6f 6c 6f 72 3a 23 66 66 66 7d 2e 63 61 72 6f 75 73 65 6c 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 2e 63 61 72 6f 75 73 65 6c 2d 69 6e 6e 65 72 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 77 69 64 74 68 3a 31 30 30 25 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 2e 63 61 72 6f 75 73 65 6c 2d 69 6e 6e 65 72 3e 2e 69 74 65 6d 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 6e 6f 6e 65 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 2e 36 73 20 65 61 73 65 2d 69 6e 2d 6f 75 74 20 6c 65 66 74 3b 2d 6f 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 2e 36 73 20 65 61 73 65 2d 69 6e 2d 6f 75 74 20 6c 65 66 74 3b 74 72 Data Ascii: ight-width:0;border-left-color:#fff}.carousel{position:relative}.carousel-inner{position:relative;width:100%;overflow:hidden}.carousel-inner>.item{position:relative;display:none;-webkit-transition:.6s ease-in-out left;-o-transition:.6s ease-in-out left;tr
2022-06-30 20:27:53 UTC	343	IN	Data Raw: 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 20 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 6c 65 66 74 2c 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 20 2e 67 6c 79 70 68 69 63 6f 6e 2d 63 68 65 76 72 6f 6e 2d 72 69 67 68 74 2c 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 20 2e 69 63 6f 6e 2d 6e 65 78 74 2c 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 20 2e 69 63 6f 6e 2d 70 72 65 76 7b 77 69 64 74 68 3a 33 30 70 78 3b 68 65 69 67 68 74 3a 33 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 33 30 70 78 7d 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 20 2e 67 6c 79 70 68 69 63 6f 6e 2d Data Ascii: creen and (min-width:768px){.carousel-control .glyphicon-chevron-left,.carousel-control .glyphicon-chevron-right,.carousel-control .icon-next,.carousel-control .icon-prev{width:30px;height:30px;margin-top:-10px;font-size:30px}.carousel-control .glyphicon-
2022-06-30 20:27:53 UTC	347	IN	Data Raw: 39 31 70 78 29 7b 2e 68 69 64 64 65 6e 2d 73 6d 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 39 39 32 70 78 29 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 31 31 39 39 70 78 29 7b 2e 68 69 64 64 65 6e 2d 6d 64 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 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 68 69 64 64 65 6e 2d 6c 67 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 7d 2e 76 69 73 69 62 6c 65 2d 70 72 69 6e 74 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 40 6d 65 64 69 61 20 70 72 69 6e 74 7b 2e 76 69 73 69 62 6c 65 2d 70 72 69 6e 74 7b 64 69 73 70 Data Ascii: 91px){.hidden-sm{display:none!important}}@media (min-width:992px) and (max-width:1199px){.hidden-md{display:none!important}}@media (min-width:1200px){.hidden-lg{display:none!important}}.visible-print{display:none!important}@media print{.visible-print{disp
2022-06-30 20:27:53 UTC	348	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49786	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 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
2022-06-30 20:27:53 UTC	96	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:53 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: 107368 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: 7239a52d4e52909c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 20:27:53 UTC	97	IN	Data Raw: 31 34 36 65 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: 146e/*! * 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
2022-06-30 20:27:53 UTC	97	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 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
2022-06-30 20:27:53 UTC	100	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]*$)/,""));var g=a("#"===f?[]:f);b&&b.preventDefault(),g.length||(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?g.one("bsTransitionEnd",c).emula
2022-06-30 20:27:53 UTC	103	IN	Data Raw: 70 75 74 22 29 3b 22 72 61 64 69 6f 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 3f 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 26 26 28 61 3d 21 31 29 2c 62 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 22 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 61 64 64 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 29 3a 22 63 68 65 63 6b 62 6f 78 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 26 26 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 21 3d 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 61 73 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 26 26 28 61 21 3d 21 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 74 6f 67 67 6c 65 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 Data Ascii: put");"radio"==c.prop("type")?(c.prop("checked")&&(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&(c.prop("checked")!==this.$element.hasClass("active")&&(a=!1),this.$element.toggleClass("active"
2022-06-30 20:27:53 UTC	108	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
2022-06-30 20:27:53 UTC	112	IN	Data Raw: 37 63 34 37 0d 0a 21 31 29 2c 74 68 69 73 2e 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 Data Ascii: 7c47!1),this.interval&&clearInterval(this.interval),this.options.interval&&!this.paused&&(this.interval=setI nterval(a.proxy(this.next,this),this.options.interval)),this},c.prototype.getItemIndex=function(a){return this.$items=a. parent().children(".item"
2022-06-30 20:27:53 UTC	114	IN	Data Raw: 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 29 72 65 74 75 72 6e 20 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 21 31 3b 76 61 72 20 6a 3d 66 5b 30 5d 2c 6b 3d 61 2e 45 76 65 6e 74 28 22 73 6c 69 64 65 2e 62 73 2e 63 61 72 6f 75 73 65 6c 22 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 6a 2c 64 69 72 65 63 74 69 6f 6e 3a 68 7d 29 3b 69 66 28 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 74 72 69 67 67 65 72 28 6b 29 2c 21 6b 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 69 66 28 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 21 30 2c 67 26 26 74 68 69 73 2e 70 61 75 73 65 28 29 2c 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 2e 6c 65 6e 67 74 68 29 7b 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 22 Data Ascii: Class("active"))return this.sliding=!1;var j=f[0],k=a.Event("slide.bs.carousel",{relatedTarget:j,direction:h});if(this .$element.trigger(k),!k.isDefaultPrevented()){if(this.sliding=!0,g&&this.pause(),this.$indicators.length){this.$indicato rs.find(".active"
2022-06-30 20:27:53 UTC	120	IN	Data Raw: 22 63 6c 69 63 6b 2e 62 73 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 28 6a 51 75 65 72 79 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 Data Ascii: "click.bs.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("hr
2022-06-30 20:27:53 UTC	124	IN	Data Raw: 69 67 67 65 72 28 66 29 2c 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 2c 21 30 29 3b 76 61 72 20 67 3d 74 68 69 73 2e 64 69 6d 65 6e 73 69 6f 6e 28 29 3b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 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 Data Ascii: igger(f),!f.isDefaultPrevented()){e&&e.length&&(c.call(e,"hide"),b||e.data("bs.collapse",null));var g=this.d imension();this.$element.removeClass("collapse").addClass("collapsing")[g](0).attr("aria-expanded",!0),this.$trigger.rem oveClass("collapsed").attr(
2022-06-30 20:27:53 UTC	126	IN	Data Raw: 65 2e 74 6f 67 67 6c 65 3d 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 Data Ascii: e.toggle=function(){this[this.$element.hasClass("in")?"hide":"show"]()},d.prototype.getParent=function(){return a(this.options.parent).find('[data-toggle="collapse"][data-parent="'+this.options.parent+'"]').each(a.proxy(function(c,d){var e=a(d);this.addAr
2022-06-30 20:27:53 UTC	129	IN	Data Raw: 6f 77 6e 22 2c 66 29 29 29 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 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 Data Ascii: own",f))))))))}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=f unction(b){a(b).on("click.b
2022-06-30 20:27:53 UTC	134	IN	Data Raw: 64 72 6f 70 64 6f 77 6e 3d 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 Data Ascii: dropdown=d,a.fn.dropdown.Constructor=g,a.fn.dropdown.noConflict=function(){return a.fn.dropdown=h, this},a(document).on("click.bs.dropdown.data-api",c).on("click.bs.dropdown.data-api",".dropdown form",function(a){a.stop Propagation()}).on("click.bs.dropdown
2022-06-30 20:27:53 UTC	136	IN	Data Raw: 2e 74 72 69 67 67 65 72 28 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 Data Ascii: .trigger(e),this.isShown||e.isDefaultPrevented()||(this.isShown=!0,this.checkScrollbar(),this.setScrollbar() ,this.$body.addClass("modal-open"),this.escape(),this.resize(),this.$element.on("click.dismiss.bs.modal",'[data-dismiss= "modal"]',a.proxy(this.hide

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	140	IN	Data Raw: 72 6f 78 79 28 74 68 69 73 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 Data Ascii: roxy(this.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.$element[0]===a.target||t
2022-06-30 20:27:53 UTC	145	IN	Data Raw: 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3d 21 31 29 3a 76 6f 69 64 28 61 2e 74 61 72 67 65 74 3d 3d 3d 61 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 26 26 28 22 73 74 61 74 69 63 22 3d 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 62 61 63 6b 64 72 6f 70 3f 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 2e 66 6f 63 75 73 28 29 3a 74 68 69 73 2e 68 69 64 65 28 29 29 7d 2c 74 68 69 73 29 29 2c 66 26 26 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 5b 30 5d 2e 6f 66 66 73 65 74 57 69 64 74 68 2c 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 2e 61 64 64 43 6c 61 73 73 28 22 69 6e 22 29 2c 21 62 29 72 65 74 75 72 6e 3b 66 3f 74 68 69 73 2e 24 62 61 63 6b 64 72 6f 70 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 62 29 2e 65 6d 75 6c 61 74 65 54 72 61 Data Ascii: ackdropClick=!1):void(a.target===a.currentTarget&&("static"==this.options.backdrop?this.$element[0].focus():this.hide()))},this)),f&&this.$backdrop[0].offsetWidth,this.$backdrop.addClass("in"),!b)return;f?this.$backdrop.one("bsTransitionEnd",b).emulateTra
2022-06-30 20:27:53 UTC	150	IN	Data Raw: 64 69 6e 67 52 69 67 68 74 7c 7c 22 22 2c 74 68 69 73 2e 62 6f 64 79 49 73 4f 76 65 72 66 6c 6f 77 69 6e 67 26 26 74 68 69 73 2e 24 62 6f 64 79 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 61 2b 74 68 69 73 2e 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 72 65 73 65 74 53 63 72 6f 6c 6c 62 61 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 24 62 6f 64 79 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 74 68 69 73 2e 6f 72 69 67 69 6e 61 6c 42 6f 64 79 50 61 64 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 6d 65 61 73 75 72 65 53 63 72 6f 6c 6c 62 61 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 Data Ascii: dingRight||"",this.bodyIsOverflowing&&this.$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("
2022-06-30 20:27:53 UTC	156	IN	Data Raw: 22 2c 63 2e 54 52 41 4e 53 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 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 Data Ascii: ",c.TRANSITION_DURATION=150,c.DEFAULTS={animation:!0,placement:"top",selector:!1,template:' ',trigger:"hover focus",title:"",delay:0,html:!1,contain
2022-06-30 20:27:53 UTC	160	IN	Data Raw: 74 6f 74 79 70 65 2e 67 65 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 Data Ascii: totype.getDefaults=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=
2022-06-30 20:27:53 UTC	164	IN	Data Raw: 69 6d 65 6f 75 74 29 2c 63 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 Data Ascii: imeout),c.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()&&thi
2022-06-30 20:27:53 UTC	170	IN	Data Raw: 74 61 74 65 3b 65 2e 24 65 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 Data Ascii: tate;e.$element.trigger("shown.bs."+e.type),e.hoverState=null,"out"==a&&e.leave(e)};a.support.transition&&this.$tip.hasClass("fade")?f.one("bsTransitionEnd",q).emulateTransitionEnd(c.TRANSITION_DURATION):q()}},c.prototype.applyPlacement=function(b,c){var
2022-06-30 20:27:53 UTC	174	IN	Data Raw: 73 2e 24 65 6c 65 6d 65 6e 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 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 Data Ascii: s.$element.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=t

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	181	IN	Data Raw: 6f 6e 28 74 68 69 73 2e 24 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 Data Ascii: on(this.$viewport);if(/right|left/.test(a)){var h=b.top-f-g.scroll,i=b.top+f-g.scroll+d;h<g.top?e.top=g.top-h:i>g.top+g.height&&(e.top=g.top+g.height-i)}else{var j=b.left-f,k=b.left+f+c;j<g.left?e.left=g.left-j:k>g.right&&(e.left=g.left+g.width-k)}return
2022-06-30 20:27:53 UTC	183	IN	Data Raw: 6d 65 6f 75 74 28 74 68 69 73 2e 74 69 6d 65 6f 75 74 29 2c 74 68 69 73 2e 68 69 64 65 28 66 75 6e 63 74 69 6f 6e 28 29 7b 61 2e 24 65 6c 65 6d 65 6e 74 2e 6f 66 66 28 22 2e 22 2b 61 2e 74 79 70 65 29 2e 72 65 6d 6f 76 65 44 61 74 61 28 22 62 73 2e 22 2b 61 2e 74 79 70 65 29 2c 61 2e 24 74 69 70 26 26 61 2e 24 74 69 70 2e 64 65 74 61 63 68 28 29 2c 61 2e 24 74 69 70 3d 6e 75 6c 6c 2c 61 2e 24 61 72 72 6f 77 3d 6e 75 6c 6c 2c 61 2e 24 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 7d 29 7d 3b 76 61 72 20 64 3d 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 3b 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 3d 62 2c 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 63 2c 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 2e 6e 6f Data Ascii: meout(this.timeout),this.hide(function(){a.$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.no
2022-06-30 20:27:53 UTC	184	IN	Data Raw: 22 29 2c 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 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 5b 30 5d 29 7c 7c 28 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 74 6d 6c 28 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 63 61 6c 6c 28 74 68 69 73 2c 61 29 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 Data Ascii: "),a.find(".popover-title").html()||a.find(".popover-title").hide()},c.prototype.hasContent=function(){return this.getTitle()||this.getContent()},c.prototype.getContent=function(){var a=this.$element,b=this.options;return a.attr("data-content")||("functio
2022-06-30 20:27:53 UTC	185	IN	Data Raw: 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 74 61 72 67 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 73 63 72 6f 6c 6c 48 65 69 67 68 74 3d 74 68 69 73 2e 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 61 2e 69 73 57 69 6e 64 6f 77 28 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 5b 30 5d 29 7c 7c 28 63 3d 22 70 6f 73 69 74 69 6f 6e 22 2c 64 3d 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 73 63 72 6f 6c 6c 54 6f 70 28 29 29 2c 74 68 69 73 2e 24 62 6f 64 79 2e 66 69 6e 64 28 74 68 69 73 2e 73 65 6c 65 63 74 6f 72 29 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 61 28 74 68 69 73 29 2c 65 3d 62 2e 64 61 74 61 28 22 74 61 72 67 65 74 22 29 7c 7c 62 2e 61 74 74 72 28 22 68 72 65 66 22 29 2c 66 3d 2f 5e 23 2e 2f 2e 74 65 73 Data Ascii: ets=[],this.targets=[],this.scrollHeight=this.getScrollHeight(),a.isWindow(this.$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=/^#./.tes
2022-06-30 20:27:53 UTC	187	IN	Data Raw: 3d 62 2c 61 2e 66 6e 2e 73 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 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 Data Ascii: =b,a.fn.scrollspy.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){retur
2022-06-30 20:27:53 UTC	188	IN	Data Raw: 64 65 22 29 2c 62 2e 70 61 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 24 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 Data Ascii: de"),b.parent(".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").l
2022-06-30 20:27:53 UTC	189	IN	Data Raw: 66 73 65 74 28 29 2c 67 3d 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 3b 69 66 28 22 62 6f 74 74 6f 6d 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 Data Ascii: fset(),g=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!=
2022-06-30 20:27:53 UTC	191	IN	Data Raw: 66 69 78 3d 62 2c 61 2e 66 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 Data Ascii: fix=b,a.fn.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.offset
2022-06-30 20:27:53 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	192.168.2.5	49790	104.17.24.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	93	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
2022-06-30 20:27:53 UTC	191	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:53 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: 629157 Expires: Tue, 20 Jun 2023 20:27:53 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=OYYc8iMAOXaRevNcCxIKOKPmAUSMhO%2BcaU4fdPyDU22ECTO3vrxYSo3G99lq13WAESvntrd3elSldKtvKuRQ73kc7ti%2BrbkDLs0XFVJAkrUwSAkGEXOF%2FvhNIYhlc2omUAoeaPzT"}],"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: 7239a52d6eb39055-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 20:27:53 UTC	192	IN	Data Raw: 37 62 62 31 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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	196	IN	Data Raw: 74 61 72 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 30 36 22 3b 0a 7d 0a 2e 66 61 2d 75 73 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 30 37 22 3b 0a 7d 0a 2e 66 61 2d 66 69 6c 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 30 30 38 22 3b 0a 7d 0a 2e 66 61 2d 74 68 2d 6c 61 72 67 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 30 39 22 3b 0a 7d 0a 2e 66 61 2d 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 30 30 61 22 3b 0a 7d 0a 2e 66 61 2d 74 68 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 30 62 22 3b 0a 7d 0a 2e 66 61 2d 63 68 65 63 6b 3a 62 65 66 Data Ascii: tar-o:before { content: "\f006";}.fa-user:before { content: "\f007";}.fa-film:before { content: "\f008";}.fa-th-large:before { content: "\f009";}.fa-th:before { content: "\f00a";}.fa-th-list:before { content: "\f00b";}.fa-check:bef
2022-06-30 20:27:53 UTC	198	IN	Data Raw: 36 22 3b 0a 7d 0a 2e 66 61 2d 76 6f 6c 75 6d 65 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 32 37 22 3b 0a 7d 0a 2e 66 61 2d 76 6f 6c 75 6d 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 30 32 38 22 3b 0a 7d 0a 2e 66 61 2d 71 72 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 30 32 39 22 3b 0a 7d 0a 2e 66 61 2d 62 61 72 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 30 32 61 22 3b 0a 7d 0a 2e 66 61 2d 74 61 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 30 32 62 22 3b 0a 7d 0a 2e 66 61 2d 74 61 67 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 Data Ascii: 6";}.fa-volume-down:before { content: "\f027";}.fa-volume-up:before { content: "\f028";}.fa-qrcode:before { content: "\f029";}.fa-barcode:before { content: "\f02a";}.fa-tag:before { content: "\f02b";}.fa-tags:before { content: "\f0
2022-06-30 20:27:53 UTC	199	IN	Data Raw: 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 34 35 22 3b 0a 7d 0a 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 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 34 36 22 3b 0a 7d 0a 2e 66 61 2d 61 72 72 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 30 34 37 22 3b 0a 7d 0a 2e 66 61 2d 73 74 65 70 2d 62 61 63 6b 77 61 72 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 34 38 22 3b 0a 7d 0a 2e 66 61 2d 66 61 73 74 2d 62 61 63 6b 77 61 72 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 34 39 22 3b 0a 7d 0a 2e 66 61 2d 62 61 63 6b 77 61 72 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 34 61 Data Ascii: e { content: "\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
2022-06-30 20:27:53 UTC	200	IN	Data Raw: 20 22 5c 66 30 36 34 22 3b 0a 7d 0a 2e 66 61 2d 65 78 70 61 6e 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 36 35 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 6d 70 72 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 30 36 36 22 3b 0a 7d 0a 2e 66 61 2d 70 6c 75 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 36 37 22 3b 0a 7d 0a 2e 66 61 2d 6d 69 6e 75 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 36 38 22 3b 0a 7d 0a 2e 66 61 2d 61 73 74 65 72 69 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 36 39 22 3b 0a 7d 0a 2e 66 61 2d 65 78 63 6c 61 6d 61 74 69 6f 6e 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 20 7b 0a Data Ascii: "\f064";}.fa-expand:before { content: "\f065";}.fa-compress:before { content: "\f066";}.fa-plus:before { content: "\f067";}.fa-minus:before { content: "\f068";}.fa-asterisk:before { content: "\f069";}.fa-exclamation-circle:before {
2022-06-30 20:27:53 UTC	202	IN	Data Raw: 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 30 38 34 22 3b 0a 7d 0a 2e 66 61 2d 67 65 61 72 73 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 63 6f 67 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 38 35 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 6d 6d 65 6e 74 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 38 36 22 3b 0a 7d 0a 2e 66 61 2d 74 68 75 6d 62 73 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 38 37 22 3b 0a 7d 0a 2e 66 61 2d 74 68 75 6d 62 73 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 38 38 22 3b 0a 7d 0a 2e 66 61 2d 73 74 61 72 2d 68 61 6c 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 Data Ascii: content: "\f084";}.fa-gears:before,.fa-cogs:before { content: "\f085";}.fa-comments:before { content: "\f086";}.fa-thumbs-o-up:before { content: "\f087";}.fa-thumbs-o-down:before { content: "\f088";}.fa-star-half:before { content: "\f
2022-06-30 20:27:53 UTC	203	IN	Data Raw: 6e 64 2d 6f 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 30 61 34 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 2d 6f 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 30 61 35 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 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 61 36 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 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 61 37 22 3b 0a 7d 0a 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 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 30 61 38 22 3b 0a 7d 0a 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 2d 72 69 67 68 Data Ascii: nd-o-right:before { content: "\f0a4";}.fa-hand-o-left:before { content: "\f0a5";}.fa-hand-o-up:before { content: "\f0a6";}.fa-hand-o-down:before { content: "\f0a7";}.fa-arrow-circle-left:before { content: "\f0a8";}.fa-arrow-circle-righ
2022-06-30 20:27:53 UTC	204	IN	Data Raw: 63 64 22 3b 0a 7d 0a 2e 66 61 2d 74 61 62 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 63 65 22 3b 0a 7d 0a 2e 66 61 2d 6d 61 67 69 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 30 22 3b 0a 7d 0a 2e 66 61 2d 74 72 75 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 30 64 31 22 3b 0a 7d 0a 2e 66 61 2d 70 69 6e 74 65 72 65 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 64 32 22 3b 0a 7d 0a 2e 66 61 2d 70 69 6e 74 65 72 65 73 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 30 64 33 22 3b 0a 7d 0a 2e 66 61 2d 67 6f 6f 67 6c 65 2d 70 6c 75 73 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 Data Ascii: cd";}.fa-table:before { content: "\f0ce";}.fa-magic:before { content: "\f0d0";}.fa-truck:before { content: "\f0d1";}.fa-pinterest:before { content: "\f0d2";}.fa-pinterest-square:before { content: "\f0d3";}.fa-google-plus-square:befor
2022-06-30 20:27:53 UTC	206	IN	Data Raw: 6c 69 67 68 74 62 75 6c 62 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 65 62 22 3b 0a 7d 0a 2e 66 61 2d 65 78 63 68 61 6e 67 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 63 22 3b 0a 7d 0a 2e 66 61 2d 63 6c 6f 75 64 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 65 64 22 3b 0a 7d 0a 2e 66 61 2d 63 6c 6f 75 64 2d 75 70 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 65 65 22 3b 0a 7d 0a 2e 66 61 2d 75 73 65 72 2d 6d 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 66 30 22 3b 0a 7d 0a 2e 66 61 2d 73 74 65 74 68 6f 73 63 6f 70 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 Data Ascii: lightbulb-o:before { content: "\f0eb";}.fa-exchange:before { content: "\f0ec";}.fa-cloud-download:before { content: "\f0ed";}.fa-cloud-upload:before { content: "\f0ee";}.fa-user-md:before { content: "\f0f0";}.fa-stethoscope:before {
2022-06-30 20:27:53 UTC	207	IN	Data Raw: 7d 0a 2e 66 61 2d 6d 6f 62 69 6c 65 2d 70 68 6f 6e 65 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 6d 6f 62 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 30 62 22 3b 0a 7d 0a 2e 66 61 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 31 30 63 22 3b 0a 7d 0a 2e 66 61 2d 71 75 6f 74 65 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 30 64 22 3b 0a 7d 0a 2e 66 61 2d 71 75 6f 74 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 65 22 3b 0a 7d 0a 2e 66 61 2d 73 70 69 6e 6e 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 31 31 30 22 3b 0a 7d 0a 2e 66 61 2d 63 69 Data Ascii: }.fa-mobile-phone:before,.fa-mobile:before { content: "\f10b";}.fa-circle-o:before { content: "\f10c";}.fa-quote-left:before { content: "\f10d";}.fa-quote-right:before { content: "\f10e";}.fa-spinner:before { content: "\f110";}.fa-ci

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	208	IN	Data Raw: 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 32 61 22 3b 0a 7d 0a 2e 66 61 2d 73 75 70 65 72 73 63 72 69 70 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 32 62 22 3b 0a 7d 0a 2e 66 61 2d 73 75 62 73 63 72 69 70 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 32 63 22 3b 0a 7d 0a 2e 66 61 2d 65 72 61 73 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 31 32 64 22 3b 0a 7d 0a 2e 66 61 2d 70 75 7a 7a 6c 65 2d 70 69 65 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 32 65 22 3b 0a 7d 0a 2e 66 61 2d 6d 69 63 72 6f 70 68 6f 6e 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 33 30 22 3b 0a 7d 0a 2e 66 61 Data Ascii: { content: "\f12a";}.fa-superscript:before { content: "\f12b";}.fa-subscript:before { content: "\f12c";}.fa-eraser:before { content: "\f12d";}.fa-puzzle-piece:before { content: "\f12e";}.fa-microphone:before { content: "\f130";}.fa
2022-06-30 20:27:53 UTC	210	IN	Data Raw: 34 39 22 3b 0a 7d 0a 2e 66 61 2d 63 68 65 63 6b 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 34 61 22 3b 0a 7d 0a 2e 66 61 2d 70 65 6e 63 69 6c 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 34 62 22 3b 0a 7d 0a 2e 66 61 2d 65 78 74 65 72 6e 61 6c 2d 6c 69 6e 6b 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 34 63 22 3b 0a 7d 0a 2e 66 61 2d 73 68 61 72 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 34 64 22 3b 0a 7d 0a 2e 66 61 2d 63 6f 6d 70 61 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 31 34 65 22 3b 0a 7d 0a 2e 66 61 2d Data Ascii: 49";}.fa-check-square:before { content: "\f14a";}.fa-pencil-square:before { content: "\f14b";}.fa-external-link-square:before { content: "\f14c";}.fa-share-square:before { content: "\f14d";}.fa-compass:before { content: "\f14e";}.fa-
2022-06-30 20:27:53 UTC	211	IN	Data Raw: 61 2d 74 68 75 6d 62 73 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 36 34 22 3b 0a 7d 0a 2e 66 61 2d 74 68 75 6d 62 73 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 31 36 35 22 3b 0a 7d 0a 2e 66 61 2d 79 6f 75 74 75 62 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 36 36 22 3b 0a 7d 0a 2e 66 61 2d 79 6f 75 74 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 31 36 37 22 3b 0a 7d 0a 2e 66 61 2d 78 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 31 36 38 22 3b 0a 7d 0a 2e 66 61 2d 78 69 6e 67 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 Data Ascii: a-thumbs-up:before { content: "\f164";}.fa-thumbs-down:before { content: "\f165";}.fa-youtube-square:before { content: "\f166";}.fa-youtube:before { content: "\f167";}.fa-xing:before { content: "\f168";}.fa-xing-square:before { conte
2022-06-30 20:27:53 UTC	212	IN	Data Raw: 0a 2e 66 61 2d 67 72 61 74 69 70 61 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 38 34 22 3b 0a 7d 0a 2e 66 61 2d 73 75 6e 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 38 35 22 3b 0a 7d 0a 2e 66 61 2d 6d 6f 6f 6e 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 38 36 22 3b 0a 7d 0a 2e 66 61 2d 61 72 63 68 69 76 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 38 37 22 3b 0a 7d 0a 2e 66 61 2d 62 75 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 31 38 38 22 3b 0a 7d 0a 2e 66 61 2d 76 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 38 39 22 3b 0a 7d 0a 2e 66 61 2d 77 65 69 Data Ascii: .fa-gratipay:before { content: "\f184";}.fa-sun-o:before { content: "\f185";}.fa-moon-o:before { content: "\f186";}.fa-archive:before { content: "\f187";}.fa-bug:before { content: "\f188";}.fa-vk:before { content: "\f189";}.fa-wei
2022-06-30 20:27:53 UTC	214	IN	Data Raw: 74 65 6e 74 3a 20 22 5c 66 31 61 31 22 3b 0a 7d 0a 2e 66 61 2d 72 65 64 64 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 61 32 22 3b 0a 7d 0a 2e 66 61 2d 73 74 75 6d 62 6c 65 75 70 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 31 61 33 22 3b 0a 7d 0a 2e 66 61 2d 73 74 75 6d 62 6c 65 75 70 6f 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 31 61 34 22 3b 0a 7d 0a 2e 66 61 2d 64 65 6c 69 63 69 6f 75 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 61 35 22 3b 0a 7d 0a 2e 66 61 2d 64 69 67 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 31 61 36 22 3b 0a 7d 0a 2e 66 61 Data Ascii: tent: "\f1a1";}.fa-reddit-square:before { content: "\f1a2";}.fa-stumbleupon-circle:before { content: "\f1a3";}.fa-stumbleupon:before { content: "\f1a4";}.fa-delicious:before { content: "\f1a5";}.fa-digg:before { content: "\f1a6";}.fa
2022-06-30 20:27:53 UTC	215	IN	Data Raw: 0a 7d 0a 2e 66 61 2d 66 69 6c 65 2d 77 6f 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 31 63 32 22 3b 0a 7d 0a 2e 66 61 2d 66 69 6c 65 2d 65 78 63 65 6c 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 63 33 22 3b 0a 7d 0a 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 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 31 63 34 22 3b 0a 7d 0a 2e 66 61 2d 66 69 6c 65 2d 70 68 6f 74 6f 2d 6f 3a 62 65 66 6f 72 65 2c 0a 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 0a 2e 66 61 2d 66 69 6c 65 2d 69 6d 61 67 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 63 35 22 3b 0a 7d 0a 2e 66 61 2d Data Ascii: }.fa-file-word-o:before { content: "\f1c2";}.fa-file-excel-o:before { 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-
2022-06-30 20:27:53 UTC	217	IN	Data Raw: 6f 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 70 61 70 65 72 2d 70 6c 61 6e 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 64 39 22 3b 0a 7d 0a 2e 66 61 2d 68 69 73 74 6f 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 64 61 22 3b 0a 7d 0a 2e 66 61 2d 63 69 72 63 6c 65 2d 74 68 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 31 64 62 22 3b 0a 7d 0a 2e 66 61 2d 68 65 61 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 31 64 63 22 3b 0a 7d 0a 2e 66 61 2d 70 61 72 61 67 72 61 70 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 64 64 22 3b 0a 7d 0a 2e 66 61 2d 73 6c 69 64 65 72 73 3a 62 65 66 6f 72 65 20 Data Ascii: o:before,.fa-paper-plane-o:before { content: "\f1d9";}.fa-history:before { content: "\f1da";}.fa-circle-thin:before { content: "\f1db";}.fa-header:before { content: "\f1dc";}.fa-paragraph:before { content: "\f1dd";}.fa-sliders:before
2022-06-30 20:27:53 UTC	218	IN	Data Raw: 0a 2e 66 61 2d 63 6f 70 79 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 66 39 22 3b 0a 7d 0a 2e 66 61 2d 61 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 66 61 22 3b 0a 7d 0a 2e 66 61 2d 65 79 65 64 72 6f 70 70 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 31 66 62 22 3b 0a 7d 0a 2e 66 61 2d 70 61 69 6e 74 2d 62 72 75 73 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 66 63 22 3b 0a 7d 0a 2e 66 61 2d 62 69 72 74 68 64 61 79 2d 63 61 6b 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 66 64 22 3b 0a 7d 0a 2e 66 61 2d 61 72 65 61 2d 63 68 61 72 74 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e Data Ascii: .fa-copyright:before { content: "\f1f9";}.fa-at:before { content: "\f1fa";}.fa-eyedropper:before { content: "\f1fb";}.fa-paint-brush:before { content: "\f1fc";}.fa-birthday-cake:before { content: "\f1fd";}.fa-area-chart:before { con
2022-06-30 20:27:53 UTC	223	IN	Data Raw: 66 32 31 38 22 3b 0a 7d 0a 2e 66 61 2d 64 69 61 6d 6f 6e 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 31 39 22 3b 0a 7d 0a 2e 66 61 2d 73 68 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 32 31 61 22 3b 0a 7d 0a 2e 66 61 2d 75 73 65 72 2d 73 65 63 72 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 31 62 22 3b 0a 7d 0a 2e 66 61 2d 6d 6f 74 6f 72 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 32 31 63 22 3b 0a 7d 0a 2e 66 61 2d 73 74 72 65 65 74 2d 76 69 65 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 31 64 22 3b 0a 7d 0a 2e 66 61 2d 68 65 61 72 74 62 65 61 74 3a 62 65 66 6f 72 65 20 7b 0a Data Ascii: f218";}.fa-diamond:before { content: "\f219";}.fa-ship:before { content: "\f21a";}.fa-user-secret:before { content: "\f21b";}.fa-motorcycle:before { content: "\f21c";}.fa-street-view:before { content: "\f21d";}.fa-heartbeat:before {

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	225	IN	Data Raw: 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 33 61 22 3b 0a 7d 0a 2e 66 61 2d 79 63 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 79 2d 63 6f 6d 62 69 6e 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 32 33 62 22 3b 0a 7d 0a 2e 66 61 2d 6f 70 74 69 6e 2d 6d 6f 6e 73 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 33 63 22 3b 0a 7d 0a 2e 66 61 2d 6f 70 65 6e 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 32 33 64 22 3b 0a 7d 0a 2e 66 61 2d 65 78 70 65 64 69 74 65 64 73 73 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 65 22 3b 0a 7d 0a 2e 66 61 2d 62 61 74 74 65 72 79 2d 34 3a 62 65 66 6f 72 65 2c 0a 2e 66 Data Ascii: re { content: "\f23a";}.fa-yc:before,.fa-y-combinator:before { content: "\f23b";}.fa-optin-monster:before { content: "\f23c";}.fa-opencart:before { content: "\f23d";}.fa-expeditedssl:before { content: "\f23e";}.fa-battery-4:before,.f
2022-06-30 20:27:53 UTC	226	IN	Data Raw: 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 35 34 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 2d 67 72 61 62 2d 6f 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 68 61 6e 64 2d 72 6f 63 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 32 35 35 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 2d 73 74 6f 70 2d 6f 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 68 61 6e 64 2d 70 61 70 65 72 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 35 36 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 2d 73 63 69 73 73 6f 72 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 32 35 37 22 3b 0a 7d 0a 2e 66 61 2d 68 61 6e 64 2d 6c 69 7a 61 72 64 2d 6f 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e Data Ascii: fore { content: "\f254";}.fa-hand-grab-o:before,.fa-hand-rock-o:before { content: "\f255";}.fa-hand-stop-o :before,.fa-hand-paper-o:before { content: "\f256";}.fa-hand-scissors-o:before { content: "\f257";}.fa-hand-lizard-o:before { con
2022-06-30 20:27:53 UTC	227	IN	Data Raw: 31 36 37 35 0d 0a 7d 0a 2e 66 61 2d 61 6d 61 7a 6f 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 32 37 30 22 3b 0a 7d 0a 2e 66 61 2d 63 61 6c 65 6e 64 61 72 2d 70 6c 75 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 32 37 31 22 3b 0a 7d 0a 2e 66 61 2d 63 61 6c 65 6e 64 61 72 2d 6d 69 6e 75 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 32 37 32 22 3b 0a 7d 0a 2e 66 61 2d 63 61 6c 65 6e 64 61 72 2d 74 69 6d 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 32 37 33 22 3b 0a 7d 0a 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 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 37 34 22 3b 0a Data Ascii: 1675}.fa-amazon:before { content: "\f270";}.fa-calendar-plus-o:before { content: "\f271";}.fa-calendar-minus-o:before { content: "\f272";}.fa-calendar-times-o:before { content: "\f273";}.fa-calendar-check-o:before { content: "\f274";
2022-06-30 20:27:53 UTC	228	IN	Data Raw: 3b 0a 7d 0a 2e 66 61 2d 73 68 6f 70 70 69 6e 67 2d 62 61 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 39 30 22 3b 0a 7d 0a 2e 66 61 2d 73 68 6f 70 70 69 6e 67 2d 62 61 73 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 39 31 22 3b 0a 7d 0a 2e 66 61 2d 68 61 73 68 74 61 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 39 32 22 3b 0a 7d 0a 2e 66 61 2d 62 6c 75 65 74 6f 6f 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 39 33 22 3b 0a 7d 0a 2e 66 61 2d 62 6c 75 65 74 6f 6f 74 68 2d 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 39 34 22 3b 0a 7d 0a 2e 66 61 2d 70 65 72 63 65 6e 74 3a 62 65 66 6f 72 Data Ascii: ;}.fa-shopping-bag:before { content: "\f290";}.fa-shopping-basket:before { content: "\f291";}.fa-hashtag:before { content: "\f292";}.fa-bluetooth:before { content: "\f293";}.fa-bluetooth-b:before { content: "\f294";}.fa-percent:befor
2022-06-30 20:27:53 UTC	230	IN	Data Raw: 6f 6e 74 65 6e 74 3a 20 22 5c 66 32 61 62 22 3b 0a 7d 0a 2e 66 61 2d 73 6e 61 70 63 68 61 74 2d 67 68 6f 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 32 61 63 22 3b 0a 7d 0a 2e 66 61 2d 73 6e 61 70 63 68 61 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 32 61 64 22 3b 0a 7d 0a 2e 66 61 2d 70 69 65 64 2d 70 69 70 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 61 65 22 3b 0a 7d 0a 2e 66 61 2d 66 69 72 73 74 2d 6f 72 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 32 62 30 22 3b 0a 7d 0a 2e 66 61 2d 79 6f 61 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 32 62 31 22 3b 0a 7d 0a 2e Data Ascii: ontent: "\f2ab";}.fa-snapchat-ghost:before { content: "\f2ac";}.fa-snapchat-square:before { content: "\f2ad";}.fa-pied-piper:before { content: "\f2ae";}.fa-first-order:before { content: "\f2b0";}.fa-yoast:before { content: "\f2b1";}.
2022-06-30 20:27:53 UTC	231	IN	Data Raw: 6d 6f 6d 65 74 65 72 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 66 75 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 32 63 37 22 3b 0a 7d 0a 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 74 68 72 65 65 2d 71 75 61 72 74 65 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 32 63 38 22 3b 0a 7d 0a 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 32 3a 62 65 66 6f 72 65 2c 0a 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 68 61 6c 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 63 39 22 3b 0a 7d 0a 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 31 3a 62 65 66 Data Ascii: mometer:before,.fa-thermometer-full:before { content: "\f2c7";}.fa-thermometer-3:before,.fa-thermometer-three-quarters:before { content: "\f2c8";}.fa-thermometer-2:before,.fa-thermometer-half:before { content: "\f2c9";}.fa-th ermometer-1:bef
2022-06-30 20:27:53 UTC	232	IN	Data Raw: 74 65 3b 0a 20 20 77 69 64 74 68 3a 20 31 70 78 3b 0a 20 20 68 65 69 67 68 74 3a 20 31 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 2d 31 70 78 3b 0a 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 20 20 63 6c 69 70 3a 20 72 65 63 74 28 30 2c 20 30 2c 20 30 2c 20 30 29 3b 0a 20 20 62 6f 72 64 65 72 3a 20 30 3b 0a 7d 0a 2e 73 72 2d 6f 6e 6c 79 2d 66 6f 63 75 73 61 62 6c 65 3a 61 63 74 69 76 65 2c 0a 2e 73 72 2d 6f 6e 6c 79 2d 66 6f 63 75 73 61 62 6c 65 3a 66 6f 63 75 73 20 7b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 73 74 61 74 69 63 3b 0a 20 20 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 20 20 68 65 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 6f 76 65 72 66 6c 6f 77 3a 20 76 Data Ascii: te; width: 1px; height: 1px; padding: 0; margin: -1px; overflow: hidden; clip: rect(0, 0, 0, 0); border: 0;}.sr-only-focusable:active,.sr-only-focusable:focus { position: static; width: auto; height: auto; margin: 0; overflow: v
2022-06-30 20:27:53 UTC	233	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49794	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 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
2022-06-30 20:27:53 UTC	233	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:53 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: 7e7b81dd14f3258c35786fb02c0e17ca CDN-Cache: HIT CF-Cache-Status: HIT Age: 290191 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: 7239a52d6e925b92-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 20:27:53 UTC	234	IN	Data Raw: 31 66 32 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 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: 1f26/*! * 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
2022-06-30 20:27:53 UTC	234	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
2022-06-30 20:27:53 UTC	235	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 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
2022-06-30 20:27:53 UTC	237	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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	239	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 2e 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 61 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
2022-06-30 20:27:53 UTC	241	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 65 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
2022-06-30 20:27:53 UTC	242	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 62 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 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
2022-06-30 20:27:53 UTC	244	IN	Data Raw: 35 39 66 32 0d 0a 32 22 7d 2e 66 61 2d 63 61 6d 65 72 61 2d 72 65 74 72 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 33 22 7d 2e 66 61 2d 6b 65 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 34 22 7d 2e 66 61 2d 67 65 61 72 73 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 63 6f 67 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 35 22 7d 2e 66 61 2d 63 6f 6d 6d 65 6e 74 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 36 22 7d 2e 66 61 2d 74 68 75 6d 62 73 2d 6f 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 37 22 7d 2e 66 61 2d 74 68 75 6d 62 73 2d 6f 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 38 38 22 7d 2e 66 61 2d 73 74 61 72 2d 68 Data Ascii: 59f22"}.fa-camera-retro:before{content:"\f083"}.fa-key:before{content:"\f084"}.fa-gears:before,.fa-cogs:before{content:"\f085"}.fa-comments:before{content:"\f086"}.fa-thumbs-o-up:before{content:"\f087"}.fa-thumbs-o-down:before{content:"\f088"}.fa-star-h
2022-06-30 20:27:53 UTC	246	IN	Data Raw: 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 38 22 7d 2e 66 61 2d 61 72 72 6f 77 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 30 61 39 22 7d 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 61 22 7d 2e 66 61 2d 61 72 72 6f 77 2d 63 69 72 63 6c 65 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 62 22 7d 2e 66 61 2d 67 6c 6f 62 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 63 22 7d 2e 66 61 2d 77 72 65 6e 63 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 64 22 7d 2e 66 61 2d 74 61 73 6b 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 61 65 22 7d 2e 66 Data Ascii: re{content:"\f0a8"}.fa-arrow-circle-right:before{content:"\f0a9"}.fa-arrow-circle-up:before{content:"\f0aa"}.fa-arrow-circle-down:before{content:"\f0ab"}.fa-globe:before{content:"\f0ac"}.fa-wrench:before{content:"\f0ad"}.fa-tasks:before{content:"\f0ae"}.f
2022-06-30 20:27:53 UTC	248	IN	Data Raw: 6e 74 3a 22 5c 66 30 64 39 22 7d 2e 66 61 2d 63 61 72 65 74 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 30 64 61 22 7d 2e 66 61 2d 63 6f 6c 75 6d 6e 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 62 22 7d 2e 66 61 2d 75 6e 73 6f 72 74 65 64 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 73 6f 72 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 63 22 7d 2e 66 61 2d 73 6f 72 74 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 73 6f 72 74 2d 61 73 63 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 64 22 7d 2e 66 61 2d 73 6f 72 74 2d 75 70 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 73 6f 72 74 2d 61 73 63 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 65 22 7d 2e 66 61 2d 65 Data Ascii: nt:"\f0d9"}.fa-caret-right:before{content:"\f0da"}.fa-columns:before{content:"\f0db"}.fa-unsorted:before,.fa-sort:before{content:"\f0dc"}.fa-sort-down:before,.fa-sort-desc:before{content:"\f0dd"}.fa-sort-up:before,.fa-sort-asc:before{content:"\f0de"}.fa-e
2022-06-30 20:27:53 UTC	250	IN	Data Raw: 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 66 64 22 7d 2e 66 61 2d 70 6c 75 73 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 66 65 22 7d 2e 66 61 2d 61 6e 67 6c 65 2d 64 6f 75 62 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 30 30 22 7d 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 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 31 22 7d 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 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 32 22 7d 2e 66 61 2d 61 6e 67 6c 65 2d 64 6f 75 62 6c 65 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 30 33 22 7d 2e 66 61 2d 61 6e 67 6c Data Ascii: quare: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"}.fa-angle-double-down:before{content:"\f103"}.fa-angl
2022-06-30 20:27:53 UTC	253	IN	Data Raw: 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 33 22 7d 2e 66 61 2d 6c 6f 63 61 74 69 6f 6e 2d 61 72 72 6f 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 34 22 7d 2e 66 61 2d 63 72 6f 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 35 22 7d 2e 66 61 2d 63 6f 64 65 2d 66 6f 72 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 36 22 7d 2e 66 61 2d 75 6e 6c 69 6e 6b 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 63 68 61 69 6e 2d 62 72 6f 6b 65 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 37 22 7d 2e 66 61 2d 71 75 65 73 74 69 6f 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 38 22 7d 2e 66 61 2d 69 6e 66 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 32 39 22 7d 2e Data Ascii: {content:"\f123"}.fa-location-arrow:before{content:"\f124"}.fa-crop:before{content:"\f125"}.fa-code-fork:before{content:"\f126"}.fa-unlink:before,.fa-chain-broken:before{content:"\f127"}.fa-question:before{content:"\f128"}.fa-info:before{content:"\f129"}.

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	254	IN	Data Raw: 66 31 34 38 22 7d 2e 66 61 2d 6c 65 76 65 6c 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 39 22 7d 2e 66 61 2d 63 68 65 63 6b 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 34 61 22 7d 2e 66 61 2d 70 65 6e 63 69 6c 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 34 62 22 7d 2e 66 61 2d 65 78 74 65 72 6e 61 6c 2d 6c 69 6e 6b 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 34 63 22 7d 2e 66 61 2d 73 68 61 72 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 31 34 64 22 7d 2e 66 61 2d 63 6f 6d 70 61 73 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 65 22 7d 2e 66 61 2d 74 6f 67 Data Ascii: f148"}.fa-level-down:before{content:"\f149"}.fa-check-square:before{content:"\f14a"}.fa-pencil-square:before{content:"\f14b"}.fa-external-link-square:before{content:"\f14c"}.fa-share-square:before{content:"\f14d"}.fa-compass:before{content:"\f14e"}.fa-tog
2022-06-30 20:27:53 UTC	257	IN	Data Raw: 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 38 22 7d 2e 66 61 2d 78 69 6e 67 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 36 39 22 7d 2e 66 61 2d 79 6f 75 74 75 62 65 2d 70 6c 61 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 61 22 7d 2e 66 61 2d 64 72 6f 70 62 6f 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 62 22 7d 2e 66 61 2d 73 74 61 63 6b 2d 6f 76 65 72 66 6c 6f 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 63 22 7d 2e 66 61 2d 69 6e 73 74 61 67 72 61 6d 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 64 22 7d 2e 66 61 2d 66 6c 69 63 6b 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 65 22 7d 2e 66 61 2d 61 64 6e 3a 62 65 66 6f 72 Data Ascii: ontent:"\f168"}.fa-xing-square:before{content:"\f169"}.fa-youtube-play:before{content:"\f16a"}.fa-dropbox:before{content:"\f16b"}.fa-stack-overflow:before{content:"\f16c"}.fa-instagram:before{content:"\f16d"}.fa-flickr:before{content:"\f16e"}.fa-adn:befor
2022-06-30 20:27:53 UTC	260	IN	Data Raw: 65 2d 6f 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 39 30 22 7d 2e 66 61 2d 74 6f 67 67 6c 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 63 61 72 65 74 2d 73 71 75 61 72 65 2d 6f 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 39 31 22 7d 2e 66 61 2d 64 6f 74 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 39 32 22 7d 2e 66 61 2d 77 68 65 65 6c 63 68 61 69 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 33 22 7d 2e 66 61 2d 76 69 6d 65 6f 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 39 34 22 7d 2e 66 61 2d 74 75 72 6b 69 73 68 2d 6c 69 72 61 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 74 72 79 3a 62 65 66 Data Ascii: e-o-left:before{content:"\f190"}.fa-toggle-left:before,.fa-caret-square-o-left:before{content:"\f191"}.fa-dot-circle-o:before{content:"\f192"}.fa-wheelchair:before{content:"\f193"}.fa-vimeo-square:before{content:"\f194"}.fa-turkish-lira:before,.fa-try:bef
2022-06-30 20:27:53 UTC	265	IN	Data Raw: 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 62 34 22 7d 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 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 62 35 22 7d 2e 66 61 2d 73 74 65 61 6d 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 62 36 22 7d 2e 66 61 2d 73 74 65 61 6d 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 62 37 22 7d 2e 66 61 2d 72 65 63 79 63 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 62 38 22 7d 2e 66 61 2d 61 75 74 6f 6d 6f 62 69 6c 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 63 61 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 62 39 22 7d 2e 66 61 2d 63 61 62 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 74 61 78 69 3a 62 65 66 Data Ascii: e: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:before,.fa-car:before{content:"\f1b9"}.fa-cab:before,.fa-taxi:bef
2022-06-30 20:27:53 UTC	268	IN	Data Raw: 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 64 33 22 7d 2e 66 61 2d 79 2d 63 6f 6d 62 69 6e 61 74 6f 72 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 79 63 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 68 61 63 6b 65 72 2d 6e 65 77 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 64 34 22 7d 2e 66 61 2d 74 65 6e 63 65 6e 74 2d 77 65 69 62 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 64 35 22 7d 2e 66 61 2d 71 71 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 64 36 22 7d 2e 66 61 2d 77 65 63 68 61 74 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 77 65 69 78 69 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 64 37 22 7d 2e 66 61 2d 73 65 6e 64 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 70 61 Data Ascii: re{content:"\f1d3"}.fa-y-combinator-square:before,.fa-yc-square:before,.fa-hacker-news:before{content:"\f1d4"}.fa-tencent-weibo:before{content:"\f1d5"}.fa-qq:before{content:"\f1d6"}.fa-wechat:before,.fa-weixin:before{content:"\f1d7"}.fa-send:before,.fa-pa
2022-06-30 20:27:53 UTC	272	IN	Data Raw: 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 37 22 7d 2e 66 61 2d 74 72 61 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 38 22 7d 2e 66 61 2d 63 6f 70 79 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 66 39 22 7d 2e 66 61 2d 61 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 61 22 7d 2e 66 61 2d 65 79 65 64 72 6f 70 70 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 62 22 7d 2e 66 61 2d 70 61 69 6e 74 2d 62 72 75 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 63 22 7d 2e 66 61 2d 62 69 72 74 68 64 61 79 2d 63 61 6b 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 66 64 22 7d 2e 66 61 2d 61 72 65 61 2d 63 68 61 72 74 Data Ascii: before{content:"\f1f7"}.fa-trash:before{content:"\f1f8"}.fa-copyright:before{content:"\f1f9"}.fa-at:before{content:"\f1fa"}.fa-eyedropper:before{content:"\f1fb"}.fa-paint-brush:before{content:"\f1fc"}.fa-birthday-cake:before{content:"\f1fd"}.fa-area-chart
2022-06-30 20:27:53 UTC	274	IN	Data Raw: 32 31 64 22 7d 2e 66 61 2d 68 65 61 72 74 62 65 61 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 31 65 22 7d 2e 66 61 2d 76 65 6e 75 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 32 31 22 7d 2e 66 61 2d 6d 61 72 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 32 22 7d 2e 66 61 2d 6d 65 72 63 75 72 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 32 33 22 7d 2e 66 61 2d 69 6e 74 65 72 73 65 78 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 74 72 61 6e 73 67 65 6e 64 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 32 34 22 7d 2e 66 61 2d 74 72 61 6e 73 67 65 6e 64 65 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 32 35 22 7d 2e 66 61 2d 76 65 6e 75 73 2d 64 Data Ascii: 21d"}.fa-heartbeat:before{content:"\f21e"}.fa-venus:before{content:"\f221"}.fa-mars:before{content:"\f222"}.fa-mercury:before{content:"\f223"}.fa-intersex:before,.fa-transgender:before{content:"\f224"}.fa-transgender-alt:before{content:"\f225"}.fa-venus-d
2022-06-30 20:27:53 UTC	277	IN	Data Raw: 65 2c 2e 66 61 2d 62 61 74 74 65 72 79 2d 71 75 61 72 74 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 34 33 22 7d 2e 66 61 2d 62 61 74 74 65 72 79 2d 30 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 62 61 74 74 65 72 79 2d 65 6d 70 74 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 34 34 22 7d 2e 66 61 2d 6d 6f 75 73 65 2d 70 6f 69 6e 74 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 34 35 22 7d 2e 66 61 2d 69 2d 63 75 72 73 6f 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 34 36 22 7d 2e 66 61 2d 6f 62 6a 65 63 74 2d 67 72 6f 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 34 37 22 7d 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 7b 63 6f 6e 74 65 Data Ascii: e,.fa-battery-quarter:before{content:"\f243"}.fa-battery-0:before,.fa-battery-empty:before{content:"\f244"}.fa-mouse-pointer:before{content:"\f245"}.fa-i-cursor:before{content:"\f246"}.fa-object-group:before{content:"\f247"}.fa-object-ungroup:before{conte

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	280	IN	Data Raw: 64 6e 6f 6b 6c 61 73 73 6e 69 6b 69 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 32 36 34 22 7d 2e 66 61 2d 67 65 74 2d 70 6f 63 6b 65 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 35 22 7d 2e 66 61 2d 77 69 6b 69 70 65 64 69 61 2d 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 36 22 7d 2e 66 61 2d 73 61 66 61 72 69 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 37 22 7d 2e 66 61 2d 63 68 72 6f 6d 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 38 22 7d 2e 66 61 2d 66 69 72 65 66 6f 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 39 22 7d 2e 66 61 2d 6f 70 65 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 36 61 22 Data Ascii: dnoklassniki-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:"\f269"}.fa-opera:before{content:"\f26a"
2022-06-30 20:27:53 UTC	281	IN	Data Raw: 6e 74 65 6e 74 3a 22 5c 66 32 38 61 22 7d 2e 66 61 2d 70 61 75 73 65 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 38 62 22 7d 2e 66 61 2d 70 61 75 73 65 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 38 63 22 7d 2e 66 61 2d 73 74 6f 70 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 38 64 22 7d 2e 66 61 2d 73 74 6f 70 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 38 65 22 7d 2e 66 61 2d 73 68 6f 70 70 69 6e 67 2d 62 61 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 39 30 22 7d 2e 66 61 2d 73 68 6f 70 70 69 6e 67 2d 62 61 73 6b 65 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 Data Ascii: ntent:"\f28a"}.fa-pause-circle:before{content:"\f28b"}.fa-pause-circle-o:before{content:"\f28c"}.fa-stop-circle:before{content:"\f28d"}.fa-stop-circle-o:before{content:"\f28e"}.fa-shopping-bag:before{content:"\f290"}.fa-shopping-basket:before{content:"\f2
2022-06-30 20:27:53 UTC	283	IN	Data Raw: 74 65 6e 74 3a 22 5c 66 32 61 63 22 7d 2e 66 61 2d 73 6e 61 70 63 68 61 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 32 61 64 22 7d 2e 66 61 2d 70 69 65 64 2d 70 69 70 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 61 65 22 7d 2e 66 61 2d 66 69 72 73 74 2d 6f 72 64 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 30 22 7d 2e 66 61 2d 79 6f 61 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 31 22 7d 2e 66 61 2d 74 68 65 6d 65 69 73 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 32 22 7d 2e 66 61 2d 67 6f 6f 67 6c 65 2d 70 6c 75 73 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 67 6f 6f 67 6c 65 2d 70 6c 75 73 2d 6f 66 66 69 63 69 Data Ascii: tent:"\f2ac"}.fa-snapchat-square:before{content:"\f2ad"}.fa-pied-piper:before{content:"\f2ae"}.fa-first-order:before{content:"\f2b0"}.fa-yoast:before{content:"\f2b1"}.fa-themeisle:before{content:"\f2b2"}.fa-google-plus-circle:before,.fa-google-plus-offici
2022-06-30 20:27:53 UTC	284	IN	Data Raw: 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 61 22 7d 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 30 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 74 68 65 72 6d 6f 6d 65 74 65 72 2d 65 6d 70 74 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 63 22 7d 2e 66 61 2d 74 68 74 75 62 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 73 31 35 3a 62 65 66 6f 72 65 2c 2e 66 61 2d 62 61 74 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 64 22 7d 2e 66 61 2d 70 6f 64 63 61 73 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 65 22 7d 2e 66 61 2d 77 69 6e 64 6f 77 2d 6d 61 78 69 6d 69 7a 65 3a 62 65 66 6f 72 65 Data Ascii: :before{content:"\f2ca"}.fa-thermometer-0:before,.fa-thermometer-empty:before{content:"\f2cb"}.fa-shower:before{content:"\f2cc"}.fa-bathtub:before,.fa-s15:before,.fa-bath:before{content:"\f2cd"}.fa-podcast:before{content:"\f2ce"}.fa-window-maximize:before
2022-06-30 20:27:53 UTC	285	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49791	104.17.24.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	94	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
2022-06-30 20:27:53 UTC	238	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 20:27:53 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: 3007183 Expires: Tue, 20 Jun 2023 20:27:53 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BAsCHEm43szFppRIAJdc9RtBPlpQ0woQlnc6lK5uh9T%2Bf2gINhOsdKIGCHC%2Bx08XaG2wO%2Bruyh5dIpVEjUmQD6zSYD9qNCww2EqDNUEDtlc790WAqYy4k1JYi88XYnE3VELilJV7"}],"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: 7239a52d6d7c5c32-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 20:27:53 UTC	239	IN	Data Raw: 39 36 35 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 26 Data Ascii: 965/* 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&&
2022-06-30 20:27:53 UTC	243	IN	Data Raw: 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 7d 66 75 Data Ascii: ()})(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}fu
2022-06-30 20:27:53 UTC	247	IN	Data Raw: 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 6f 5d 7d Data Ascii: ction 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[o]}
2022-06-30 20:27:53 UTC	249	IN	Data Raw: 34 36 61 61 0d 0a 65 69 67 68 74 27 3d 3d 3d 65 3f 27 42 6f 74 74 6f 6d 27 3a 27 52 69 67 68 74 27 29 5d 3a 30 29 7d 66 75 6e 63 74 69 6f 6e 20 68 28 29 7b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2c 74 3d 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 6f 3d 69 65 28 31 30 29 26 26 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 74 29 3b 72 65 74 75 72 6e 7b 68 65 69 67 68 74 3a 6d 28 27 48 65 69 67 68 74 27 2c 65 2c 74 2c 6f 29 2c 77 69 64 74 68 3a 6d 28 27 57 69 64 74 68 27 2c 65 2c 74 2c 6f 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 63 28 65 29 7b 72 65 74 75 72 6e 20 64 65 28 7b 7d 2c 65 2c 7b 72 69 67 68 74 3a 65 2e 6c 65 66 74 2b 65 2e 77 69 64 74 68 2c 62 6f 74 74 6f 6d 3a 65 2e 74 6f 70 2b 65 2e 68 65 69 67 Data Ascii: 46aaeight'===e?'Bottom':'Right')]:0)}function h(){var e=document.body,t=document.documentElement,o=ie(10)&&getComputedStyle(t);return{height:m('Height',e,t,o),width:m('Width',e,t,o)}}function c(e){return de({},e,{right:e.left+e.width,bottom:e.top+e.heig
2022-06-30 20:27:53 UTC	252	IN	Data Raw: 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 26 26 61 72 67 75 6d 65 6e 74 73 5b 31 5d 2c 6f 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 6e 3d 75 28 65 2c 6f 29 2c 69 3d 51 28 6f 2e 63 6c 69 65 6e 74 57 69 64 74 68 2c 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 57 69 64 74 68 7c 7c 30 29 2c 72 3d 51 28 6f 2e 63 6c 69 65 6e 74 48 65 69 67 68 74 2c 77 69 6e 64 6f 77 2e 69 6e 6e 65 72 48 65 69 67 68 74 7c 7c 30 29 2c 70 3d 74 3f 30 3a 61 28 6f 29 2c 73 3d 74 3f 30 3a 61 28 6f 2c 27 6c 65 66 74 27 29 2c 64 3d 7b 74 6f 70 3a 70 2d 6e 2e 74 6f 70 2b 6e 2e 6d 61 72 67 69 6e 54 6f 70 2c 6c 65 66 74 3a 73 2d 6e 2e 6c 65 66 74 2b 6e 2e 6d 61 72 67 69 6e 4c 65 66 Data Ascii: ents.length&&void 0!==arguments[1]&&arguments[1],o=e.ownerDocument.documentElement,n=u(e,o),i=Q(o.clientWidth,window.innerWidth||0),r=Q(o.clientHeight,window.innerHeight||0),p=t?0:a(o),s=t?0:a(o,'left'),d={top:p-n.top+n.marginTop,left:s-n.left+n.marginLef

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	256	IN	Data Raw: 77 69 64 74 68 3a 70 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 70 2e 62 6f 74 74 6f 6d 2d 74 2e 62 6f 74 74 6f 6d 7d 2c 6c 65 66 74 3a 7b 77 69 64 74 68 3a 74 2e 6c 65 66 74 2d 70 2e 6c 65 66 74 2c 68 65 69 67 68 74 3a 70 2e 68 65 69 67 68 74 7d 7d 2c 64 3d 4f 62 6a 65 63 74 2e 6b 65 79 73 28 73 29 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 64 65 28 7b 6b 65 79 3a 65 7d 2c 73 5b 65 5d 2c 7b 61 72 65 61 3a 76 28 73 5b 65 5d 29 7d 29 7d 29 2e 73 6f 72 74 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 74 2e 61 72 65 61 2d 65 2e 61 72 65 61 7d 29 2c 61 3d 64 2e 66 69 6c 74 65 72 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 2e 77 69 64 74 68 2c 6e 3d 65 2e 68 65 69 67 68 74 3b 72 65 74 75 72 6e 20 Data Ascii: width:p.width,height:p.bottom-t.bottom},left:{width:t.left-p.left,height:p.height}},d=Object.keys(s).map(function(e){return de({key:e},s[e],{area:v(s[e])})}).sort(function(e,t){return t.area-e.area}),a=d.filter(function(e){var t=e.width,n=e.height;return
2022-06-30 20:27:53 UTC	258	IN	Data Raw: 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 74 29 7b 74 5b 27 66 75 6e 63 74 69 6f 6e 27 5d 26 26 63 6f 6e 73 6f 6c 65 2e 77 61 72 6e 28 27 60 6d 6f 64 69 66 69 65 72 2e 66 75 6e 63 74 69 6f 6e 60 20 69 73 20 64 65 70 72 65 63 61 74 65 64 2c 20 75 73 65 20 60 6d 6f 64 69 66 69 65 72 2e 66 6e 60 21 27 29 3b 76 61 72 20 6e 3d 74 5b 27 66 75 6e 63 74 69 6f 6e 27 5d 7c 7c 74 2e 66 6e 3b 74 2e 65 6e 61 62 6c 65 64 26 26 65 28 6e 29 26 26 28 6f 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 63 28 6f 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 29 2c 6f 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 3d 63 28 6f 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 29 2c 6f 3d 6e 28 6f 2c 74 29 29 7d 29 2c 6f 7d 66 75 6e 63 Data Ascii: eturn i.forEach(function(t){t['function']&&console.warn(`modifier.function` is deprecated, use `modifier.fn`!');var n=t['function']||t.fn;t.enabled&&e(n)&&(o.offsets.popper=c(o.offsets.popper),o.offsets.reference=c(o.offsets.reference),o=n(o,t))}),o}func
2022-06-30 20:27:53 UTC	261	IN	Data Raw: 29 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 70 6f 73 69 74 69 6f 6e 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 74 6f 70 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 6c 65 66 74 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 72 69 67 68 74 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 62 6f 74 74 6f 6d 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 77 69 6c 6c 43 68 61 6e 67 65 3d 27 27 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 5b 57 28 27 74 72 61 6e 73 66 6f 72 6d 27 29 5d 3d 27 27 29 2c 74 68 69 73 2e 64 69 73 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 6f 70 74 69 6f 6e 73 2e 72 65 6d 6f 76 Data Ascii:),this.popper.style.position='',this.popper.style.top='',this.popper.style.left='',this.popper.style.right='',this.popper.style.bottom='',this.popper.style.willChange='',this.popper.style[W('transform')]='',this.disableEventListeners(),this.options.remov
2022-06-30 20:27:53 UTC	262	IN	Data Raw: 2c 27 62 6f 74 74 6f 6d 27 2c 27 6c 65 66 74 27 5d 2e 69 6e 64 65 78 4f 66 28 6f 29 26 26 55 28 74 5b 6f 5d 29 26 26 28 6e 3d 27 70 78 27 29 2c 65 2e 73 74 79 6c 65 5b 6f 5d 3d 74 5b 6f 5d 2b 6e 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 6a 28 65 2c 74 29 7b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 74 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 6f 29 7b 76 61 72 20 6e 3d 74 5b 6f 5d 3b 21 31 3d 3d 3d 6e 3f 65 2e 72 65 6d 6f 76 65 41 74 74 72 69 62 75 74 65 28 6f 29 3a 65 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 6f 2c 74 5b 6f 5d 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 71 28 65 2c 74 2c 6f 29 7b 76 61 72 20 6e 3d 44 28 65 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 65 2e 6e 61 6d 65 3b 72 65 74 75 72 6e 20 6f 3d 3d 3d 74 7d 29 2c 69 3d 21 21 Data Ascii: ,'bottom','left'].indexOf(o)&&U(t[o])&&(n='px'),e.style[o]=t[o]+n})}function j(e,t){Object.keys(t).forEach(function(o){var n=t[o];!1===n?e.removeAttribute(o):e.setAttribute(o,t[o])})}function q(e,t,o){var n=D(e,function(e){var o=e.name;return o===t}),i=!!
2022-06-30 20:27:53 UTC	264	IN	Data Raw: 63 6f 6d 6d 61 20 28 2c 29 20 69 6e 73 74 65 61 64 2e 27 29 3b 76 61 72 20 64 3d 2f 5c 73 2a 2c 5c 73 2a 7c 5c 73 2b 2f 2c 61 3d 2d 31 3d 3d 3d 73 3f 5b 70 5d 3a 5b 70 2e 73 6c 69 63 65 28 30 2c 73 29 2e 63 6f 6e 63 61 74 28 5b 70 5b 73 5d 2e 73 70 6c 69 74 28 64 29 5b 30 5d 5d 29 2c 5b 70 5b 73 5d 2e 73 70 6c 69 74 28 64 29 5b 31 5d 5d 2e 63 6f 6e 63 61 74 28 70 2e 73 6c 69 63 65 28 73 2b 31 29 29 5d 3b 72 65 74 75 72 6e 20 61 3d 61 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 76 61 72 20 69 3d 28 31 3d 3d 3d 6e 3f 21 72 3a 72 29 3f 27 68 65 69 67 68 74 27 3a 27 77 69 64 74 68 27 2c 70 3d 21 31 3b 72 65 74 75 72 6e 20 65 2e 72 65 64 75 63 65 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 27 27 3d 3d 3d 65 5b 65 2e 6c 65 6e 67 Data Ascii: comma (,) instead.');var d=/\s*,\s*|\s+/,a=-1===s?[p]:[p.slice(0,s).concat([p[s].split(d)[0]]),[p[s].split(d)[1]]].concat(p.slice(s+1))];return a=a.map(function(e,n){var i=(1===n?!r:r)?'height':'width',p=!1;return e.reduce(function(e,t){return''===e[e.leng
2022-06-30 20:27:53 UTC	266	IN	Data Raw: 3d 65 3f 6e 65 5b 65 5d 3d 2d 31 21 3d 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 27 54 72 69 64 65 6e 74 27 29 3a 27 31 30 27 3d 3d 3d 65 3f 6e 65 5b 65 5d 3d 2d 31 21 3d 3d 6e 61 76 69 67 61 74 6f 72 2e 61 70 70 56 65 72 73 69 6f 6e 2e 69 6e 64 65 78 4f 66 28 27 4d 53 49 45 20 31 30 27 29 3a 27 61 6c 6c 27 3d 3d 3d 65 3f 6e 65 5b 65 5d 3d 2d 31 21 3d 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 27 54 72 69 64 65 6e 74 27 29 7c 7c 2d 31 21 3d 3d 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 27 4d 53 49 45 27 29 3a 76 6f 69 64 20 30 2c 6e 65 2e 61 6c 6c 3d 6e 65 2e 61 6c 6c 7c 7c 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6e 65 29 2e 73 6f Data Ascii: =e?ne[e]=-1!==navigator.userAgent.indexOf('Trident'):'10'===e?ne[e]=-1!==navigator.appVersion.indexOf('MSIE 10'):'all'===e?ne[e]=-1!==navigator.userAgent.indexOf('Trident')||-1!==navigator.userAgent.indexOf('MSIE'):void 0,ne.all=ne.all||Object.keys(ne).so
2022-06-30 20:27:53 UTC	269	IN	Data Raw: 74 68 69 73 2e 75 70 64 61 74 65 2e 62 69 6e 64 28 74 68 69 73 29 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 64 65 28 7b 7d 2c 74 2e 44 65 66 61 75 6c 74 73 2c 72 29 2c 74 68 69 73 2e 73 74 61 74 65 3d 7b 69 73 44 65 73 74 72 6f 79 65 64 3a 21 31 2c 69 73 43 72 65 61 74 65 64 3a 21 31 2c 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 3a 5b 5d 7d 2c 74 68 69 73 2e 72 65 66 65 72 65 6e 63 65 3d 6f 26 26 6f 2e 6a 71 75 65 72 79 3f 6f 5b 30 5d 3a 6f 2c 74 68 69 73 2e 70 6f 70 70 65 72 3d 6e 26 26 6e 2e 6a 71 75 65 72 79 3f 6e 5b 30 5d 3a 6e 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6d 6f 64 69 66 69 65 72 73 3d 7b 7d 2c 4f 62 6a 65 63 74 2e 6b 65 79 73 28 64 65 28 7b 7d 2c 74 2e 44 65 66 61 75 6c 74 73 2e 6d 6f 64 69 66 69 65 72 73 2c 72 2e 6d 6f 64 69 66 69 65 72 Data Ascii: this.update.bind(this)),this.options=de({},t.Defaults,r),this.state={isDestroyed:!1,isCreated:!1,scrollParents:[]},this.reference=o&&o.jquery?o[0]:o,this.popper=n&&n.jquery?n[0]:n,this.options.modifiers={},Object.keys(de({},t.Defaults.modifiers,r.modifier
2022-06-30 20:27:53 UTC	270	IN	Data Raw: 70 6f 70 70 65 72 2c 73 3d 2d 31 21 3d 3d 5b 27 62 6f 74 74 6f 6d 27 2c 27 74 6f 70 27 5d 2e 69 6e 64 65 78 4f 66 28 6f 29 2c 64 3d 73 3f 27 6c 65 66 74 27 3a 27 74 6f 70 27 2c 61 3d 73 3f 27 77 69 64 74 68 27 3a 27 68 65 69 67 68 74 27 2c 6c 3d 7b 73 74 61 72 74 3a 73 65 28 7b 7d 2c 64 2c 72 5b 64 5d 29 2c 65 6e 64 3a 73 65 28 7b 7d 2c 64 2c 72 5b 64 5d 2b 72 5b 61 5d 2d 70 5b 61 5d 29 7d 3b 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 64 65 28 7b 7d 2c 70 2c 6c 5b 6e 5d 29 7d 72 65 74 75 72 6e 20 65 7d 7d 2c 6f 66 66 73 65 74 3a 7b 6f 72 64 65 72 3a 32 30 30 2c 65 6e 61 62 6c 65 64 3a 21 30 2c 66 6e 3a 5f 2c 6f 66 66 73 65 74 3a 30 7d 2c 70 72 65 76 65 6e 74 4f 76 65 72 66 6c 6f 77 3a 7b 6f 72 64 65 72 3a 33 30 30 2c 65 6e 61 62 6c 65 64 3a 21 30 Data Ascii: popper,s=-1!==['bottom','top'].indexOf(o),d=s?'left':'top',a=s?'width':'height',l={start:se({},d,r[d]),end:se({},d,r[d]+r[a]-p[a])};e.offsets.popper=de({},p,l[n])}return e}},offset:{order:200,enabled:!0,fn:_,offset:0},preventOverflow:{order:300,enabled:!0

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	273	IN	Data Raw: 72 6f 77 27 2c 27 6b 65 65 70 54 6f 67 65 74 68 65 72 27 29 29 72 65 74 75 72 6e 20 65 3b 76 61 72 20 69 3d 6f 2e 65 6c 65 6d 65 6e 74 3b 69 66 28 27 73 74 72 69 6e 67 27 3d 3d 74 79 70 65 6f 66 20 69 29 7b 69 66 28 69 3d 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 69 29 2c 21 69 29 72 65 74 75 72 6e 20 65 3b 7d 65 6c 73 65 20 69 66 28 21 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2e 63 6f 6e 74 61 69 6e 73 28 69 29 29 72 65 74 75 72 6e 20 63 6f 6e 73 6f 6c 65 2e 77 61 72 6e 28 27 57 41 52 4e 49 4e 47 3a 20 60 61 72 72 6f 77 2e 65 6c 65 6d 65 6e 74 60 20 6d 75 73 74 20 62 65 20 63 68 69 6c 64 20 6f 66 20 69 74 73 20 70 6f 70 70 65 72 20 65 6c 65 6d 65 6e 74 21 27 29 2c 65 3b 76 61 72 20 72 3d 65 Data Ascii: row','keepTogether'))return e;var i=o.element;if('string'==typeof i){if(i=e.instance.popper.querySelector(i),!i)return e;}else if(!e.instance.popper.contains(i))return console.warn('WARNING: `arrow.element` must be child of its popper element!'),e;var r=e
2022-06-30 20:27:53 UTC	276	IN	Data Raw: 75 72 6e 20 65 3b 6e 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 2c 69 3d 53 28 6e 29 3b 76 61 72 20 61 3d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 6c 3d 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 66 3d 4a 2c 6d 3d 27 6c 65 66 74 27 3d 3d 3d 6e 26 26 66 28 61 2e 72 69 67 68 74 29 3e 66 28 6c 2e 6c 65 66 74 29 7c 7c 27 72 69 67 68 74 27 3d 3d 3d 6e 26 26 66 28 61 2e 6c 65 66 74 29 3c 66 28 6c 2e 72 69 67 68 74 29 7c 7c 27 74 6f 70 27 3d 3d 3d 6e 26 26 66 28 61 2e 62 6f 74 74 6f 6d 29 3e 66 28 6c 2e 74 6f 70 29 7c 7c 27 62 6f 74 74 6f 6d 27 3d 3d 3d 6e 26 26 66 28 61 2e 74 6f 70 29 3c 66 28 6c 2e 62 6f 74 74 6f 6d 29 2c 68 3d 66 28 61 2e 6c 65 66 74 29 3c 66 28 6f 2e 6c 65 66 74 29 2c 63 3d 66 28 Data Ascii: urn e;n=e.placement.split('-')[0],i=S(n);var a=e.offsets.popper,l=e.offsets.reference,f=J,m='left'===n&&f(a.right)>f(l.left)||'right'===n&&f(a.left)<f(l.right)||'top'===n&&f(a.bottom)>f(l.top)||'bottom'===n&&f(a.top)<f(l.bottom),h=f(a.left)<f(o.left),c=f(
2022-06-30 20:27:53 UTC	278	IN	Data Raw: 29 72 65 74 75 72 6e 20 65 3b 65 2e 68 69 64 65 3d 21 30 2c 65 2e 61 74 74 72 69 62 75 74 65 73 5b 27 78 2d 6f 75 74 2d 6f 66 2d 62 6f 75 6e 64 61 72 69 65 73 27 5d 3d 27 27 7d 65 6c 73 65 7b 69 66 28 21 31 3d 3d 3d 65 2e 68 69 64 65 29 72 65 74 75 72 6e 20 65 3b 65 2e 68 69 64 65 3d 21 31 2c 65 2e 61 74 74 72 69 62 75 74 65 73 5b 27 78 2d 6f 75 74 2d 6f 66 2d 62 6f 75 6e 64 61 72 69 65 73 27 5d 3d 21 31 7d 72 65 74 75 72 6e 20 65 7d 7d 2c 63 6f 6d 70 75 74 65 53 74 79 6c 65 3a 7b 6f 72 64 65 72 3a 38 35 30 2c 65 6e 61 62 6c 65 64 3a 21 30 2c 66 6e 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6f 3d 74 2e 78 2c 6e 3d 74 2e 79 2c 69 3d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 70 3d 44 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 Data Ascii:)return e;e.hide=!0,e.attributes['x-out-of-boundaries']='';}else{if(!1===e.hide)return e;e.hide=!1,e.attributes['x-out-of-boundaries']=!1}return e}},computeStyle:{order:850,enabled:!0,fn:function(e,t){var o=t.x,n=t.y,i=e.offsets.popper,p=D(e.instance.modif
2022-06-30 20:27:53 UTC	280	IN	Data Raw: 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 2c 6e 2c 69 29 7b 76 61 72 20 72 3d 4f 28 69 2c 74 2c 65 2c 6f 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 29 2c 70 3d 78 28 6f 2e 70 6c 61 63 65 6d 65 6e 74 2c 72 2c 74 2c 65 2c 6f 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6c 69 70 2e 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 2c 6f 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6c 69 70 2e 70 61 64 64 69 6e 67 29 3b 72 65 74 75 72 6e 20 74 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 27 78 2d 70 6c 61 63 65 6d 65 6e 74 27 2c 70 29 2c 59 28 74 2c 7b 70 6f 73 69 74 69 6f 6e 3a 6f 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 7d 29 2c 6f 7d 2c 67 70 75 41 63 63 65 6c 65 72 61 74 69 6f 6e 3a 76 6f 69 64 20 30 7d 7d 7d 2c 6d Data Ascii: :function(e,t,o,n,i){var r=O(i,t,e,o.positionFixed),p=x(o.placement,r,t,e,o.modifiers.flip.boundariesElement,o.modifiers.flip.padding);return t.setAttribute('x-placement',p),Y(t,{position:o.positionFixed?'fixed':'absolute'}),o},gpuAcceleration:void 0}}},m
2022-06-30 20:27:53 UTC	281	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

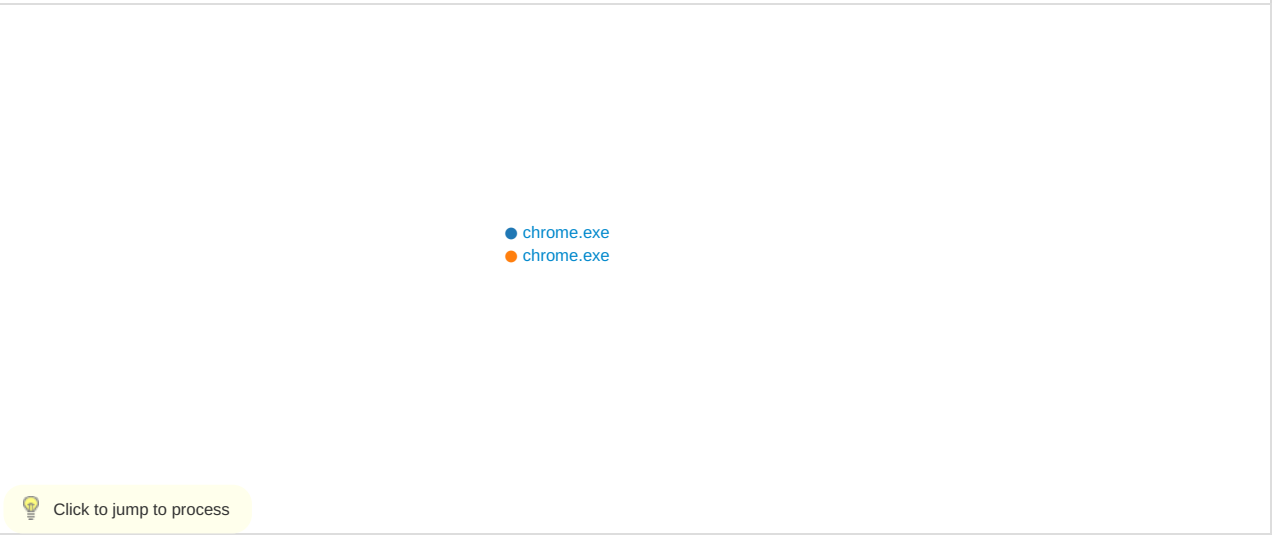
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49792	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	95	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
2022-06-30 20:27:53 UTC	216	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: 160327 Cache-Control: public, max-age=604800 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:27:53 GMT Etag: 0x8D64101507E84BD Last-Modified: Fri, 02 Nov 2018 20:25:22 GMT Server: ECAcc (muc/3369) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5f096bc0-c01e-0068-5d4a-8b7b59000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:27:53 UTC	220	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: **1416**, Parent PID: **5544**

General

Target ID:	1
Start time:	22:27:44
Start date:	30/06/2022
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#*peter.boyd@southside.com*
Imagebase:	0x7ff6a7220000
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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6120**, Parent PID: **1416**

General

Target ID:	3
Start time:	22:27:46
Start date:	30/06/2022
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=1596,15411392373280957286,14155618800222134520,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1916 /prefetch:8
Imagebase:	0x7ff6a7220000
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