

ID: 655224
Cookbook: browseurl.jbs
Time: 18:41:32
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9 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
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 9
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 13
Joe Sandbox View / Context 13
IPs 13
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\086dda27-f745-44b8-94ab-ba8b6ac61b32.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\30b0081c-bdb9-4e20-9da2-b9d71b90d53c.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\5ecad9ab-3e42-45be-b945-e911d4b6f84f.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\6c6a0a2f-a887-4066-b512-65cb3e77fc9d.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\731254e2-7898-4d5d-bb22-6d2909cf2801.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\94aae6bc-374c-4115-a4c7-edd0075d992b.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\1df751d8-d58f-4cc2-91af-afc1f2a0a7af.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1f1d84e3-6e92-4d48-84d6-b3daf31d9a84.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\26c64c90-d440-4d06-992f-05567e6e720a.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\342d06f8-becd-4196-ae18-f29cd9961fb9.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\539f4c29-0538-49fc-90ee-d20ac32635ba.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62a275ec-5489-4b19-9458-c013e7b1974b.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\633358e7-c7f3-4f89-8d83-94ce757453a9.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63b8ac16-cd70-47d8-9cc4-a2966b7e5414.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9e2b98f2-a0b2-49bb-a0bb-da60df2d9536.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\000001.dbtmp 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\CURRENT (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\MANIFEST-000001 21

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\6b006fd1-2d16-41e3-af96-3f08c2d9df9a.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\df65693d-31b6-4c80-b26d-d65c02a3e5be.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b5ba8a12-ab39-4364-b5c0-8fa8fd010a19.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d83903ff-e649-4d9f-bbf2-ba112ab04227.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir2912_265036453\Ruleset Data 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\c50c5c5f-72c3-4d69-9527-c4a53ec79026.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\d522c0ee-6c80-4905-96d1-8ed746da792d.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\f0236d04-1c65-4778-83b9-40c8ea6c4aac.tmp 28
C:\Users\user\AppData\Local\Temp\2912_1837665677\Filtering Rules 28
C:\Users\user\AppData\Local\Temp\2912_1837665677\LICENSE.txt 29
C:\Users\user\AppData\Local\Temp\2912_1837665677_metadata\verified_contents.json 29
C:\Users\user\AppData\Local\Temp\2912_1837665677\manifest.fingerprint 29
C:\Users\user\AppData\Local\Temp\2912_1837665677\manifest.json 30
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_pnacl_json 30
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 30
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 30
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 31
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 31
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 31
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 32
C:\Users\user\AppData\Local\Temp\2912_742143674\Recovery.crx3 32
C:\Users\user\AppData\Local\Temp\2912_742143674_metadata\verified_contents.json 32
C:\Users\user\AppData\Local\Temp\2912_742143674\manifest.fingerprint 33
C:\Users\user\AppData\Local\Temp\2912_742143674\manifest.json 33
C:\Users\user\AppData\Local\Temp\4b81576d-c52b-449b-96ab-b87469f2c343.tmp 33
C:\Users\user\AppData\Local\Temp\e1462bfa-6d0d-414d-956a-e46a1cffcf59.tmp 34
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\bg\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ca\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\cs\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\da\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\de\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\el\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\en\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\en_GB\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\es\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\es_419\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\et\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\fi\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\fil\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\fr\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\hi\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\hr\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\hu\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\id\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\it\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ja\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ko\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\lt\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\lv\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\nb\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\nl\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pl\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pt_BR\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pt_PT\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ro\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ru\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sk\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sl\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sr\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sv\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\th\messages.json 45
C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\tr\messages.json 45
Static File Info 45
Network Behavior 46

Network Port Distribution 46
TCP Packets 46
UDP Packets 48
DNS Queries 48
DNS Answers 49
HTTP Request Dependency Graph 51
HTTPS Proxied Packets 51
Statistics 113
Behavior 113
System Behavior 113
Analysis Process: chrome.exePID: 2912, Parent PID: 988 113
General 113
File Activities 113
Registry Activities 113
Key Value Modified 114
Analysis Process: chrome.exePID: 5892, Parent PID: 2912 114
General 114
File Activities 114
Disassembly 114

Copyright Joe Security LLC 2022

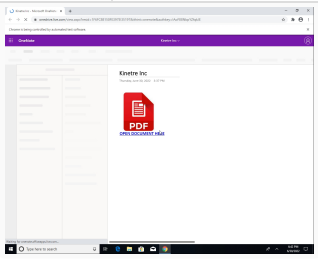
Windows Analysis Report

https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9

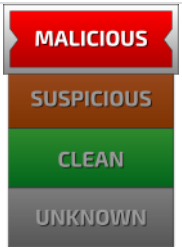
Overview

General Information

Sample URL:	http://https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9
Analysis ID:	655224
Infos:	



Detection



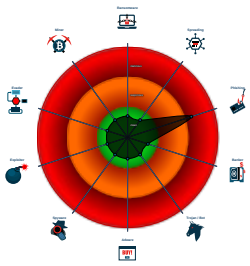
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish7
- Antivirus detection for URL or domain
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2912 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5892 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1516,9226078963959691659,212244689140897862 9,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
38924.3.pages.csv	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing

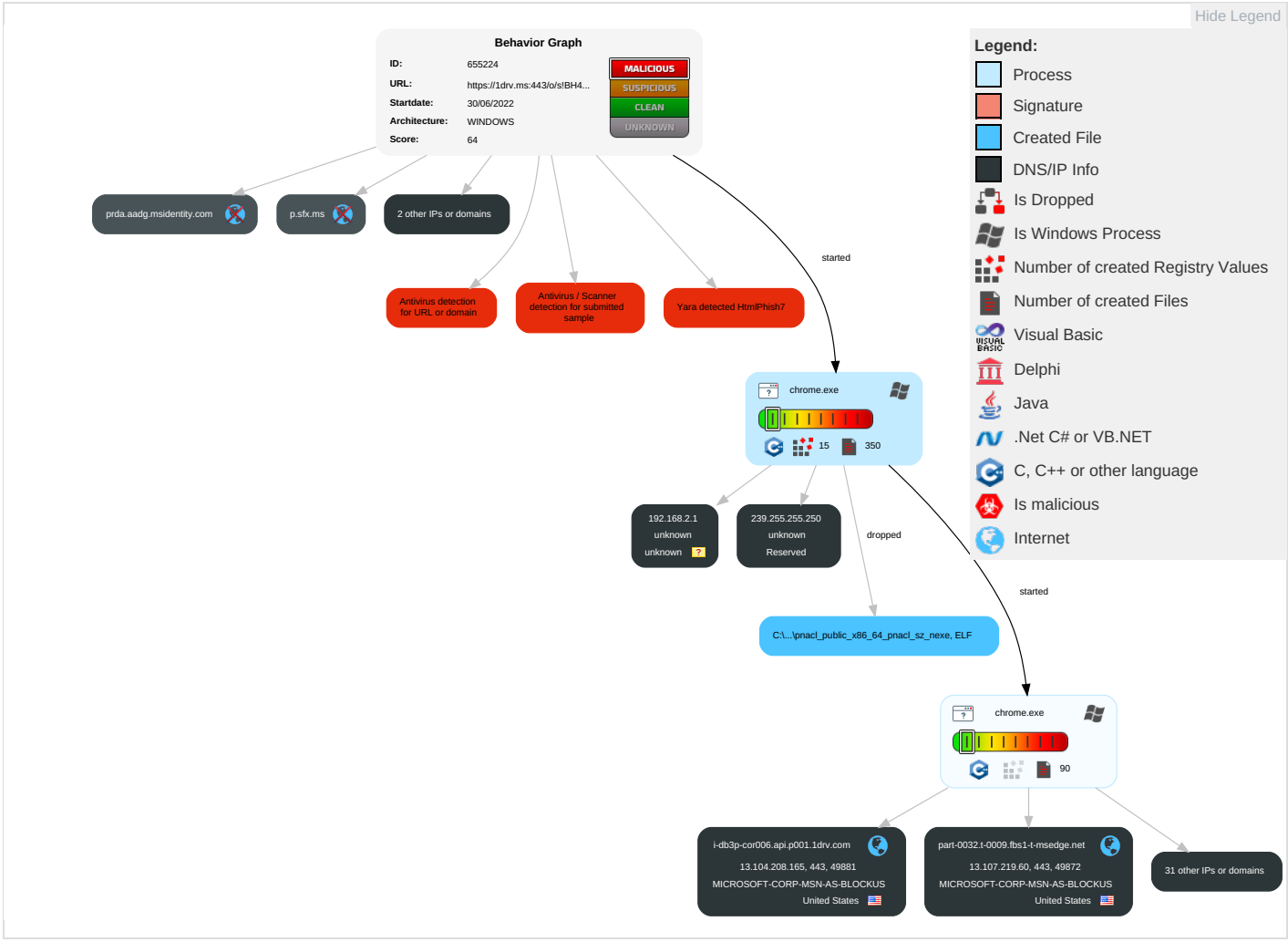


Yara detected HtmlPhish7

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
Valid Accounts	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

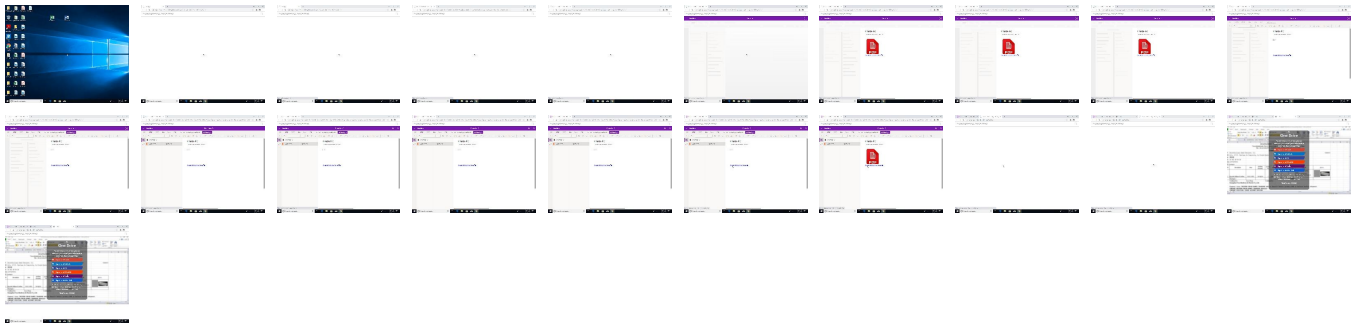
Behavior Graph

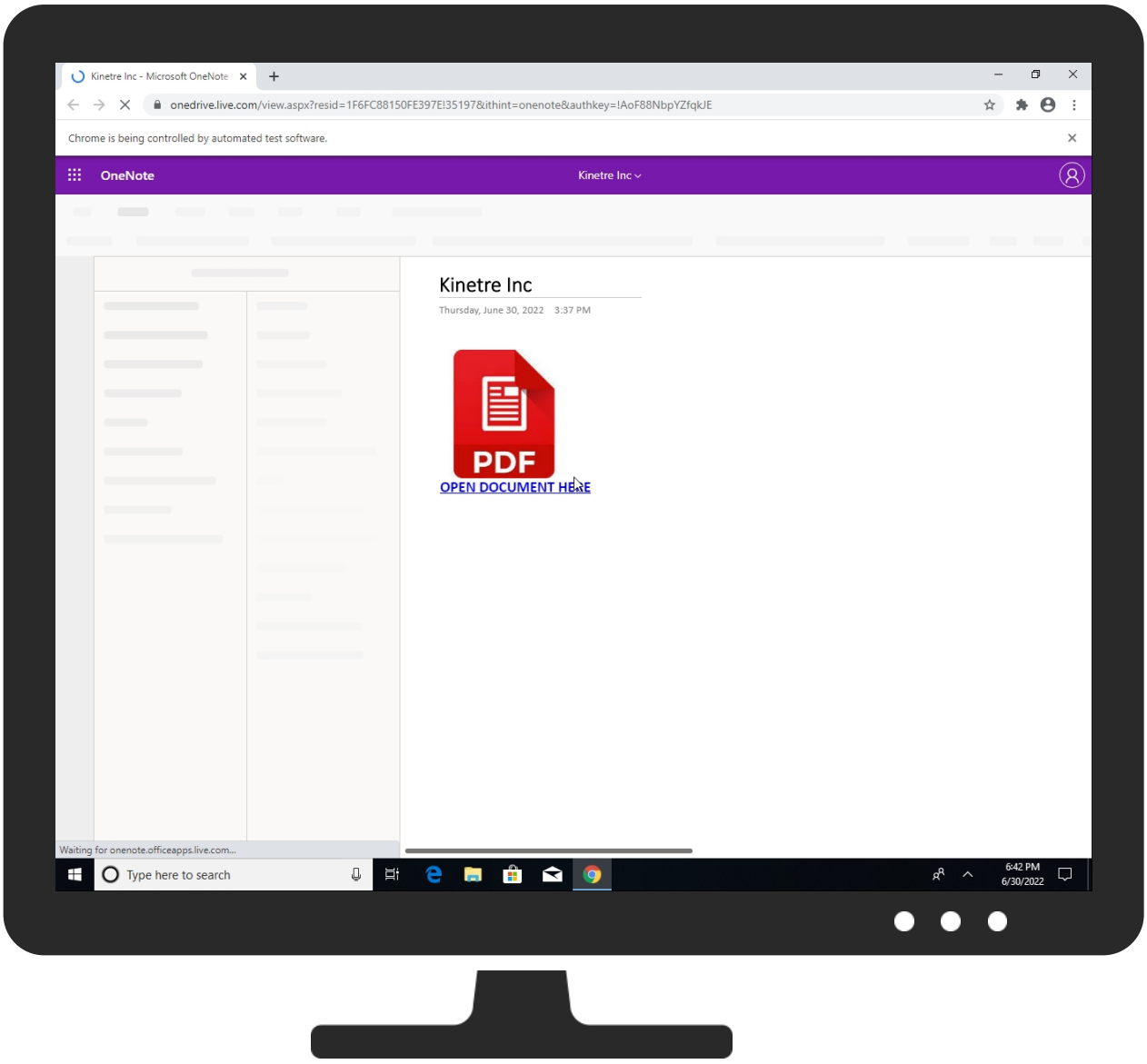


Screenshots

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://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9	1%	Virustotal		Browse
http://https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9	0%	Avira URL Cloud	safe	
http://https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com/redir?resid=1F6FC88150FE397E%2135197&authkey=%21AoF88NbpYZfqkJE&page=View&wd=target%28Quick%20Notes.one%7C5d7d8a2d-e7c2-4f4c-8bbd-8958bcaab581%2FKinetre%20Inc%7C98a50910-a8d3-4348-9fa8-39684459cbc8%2F%29&wdorigin=NavigationUrl	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://verbena-woolly-clutch.glitch.me/toy.htm	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://onedrive.live.com/view.aspx?resid=1F6FC88150FE397E!35197&ithint=onenote&authkey=!AoF88NbpYZfqkJE	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	
http://https://amcdn.msftauth.net/me?partner=OneNoteOnline&version=10.21153.1&market=EN-US&wrapperId=suiteshell	0%	Virustotal		Browse
http://https://amcdn.msftauth.net/me?partner=OneNoteOnline&version=10.21153.1&market=EN-US&wrapperId=suiteshell	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
b-0016.b-msedge.net	13.107.6.171	true	false		unknown
gstaticadssl.l.google.com	142.251.36.227	true	false		high
accounts.google.com	142.251.36.205	true	false		high
dual-a-0001.a-msedge.net	204.79.197.200	true	false		unknown
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
clients.l.google.com	142.251.36.238	true	false		high
i-db3p-cor006.api.p001.1drv.com	13.104.208.165	true	false		high
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		unknown
1drv.ms	13.107.42.12	true	false		high
verbena-woolly-clutch.glitch.me	52.22.91.148	true	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
c.live.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
p.sfx.ms	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false		unknown
spoprod-a.akamaihd.net	unknown	unknown	false		high
www.onenote.com	unknown	unknown	false		high
messaging.engagement.office.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://verbena-woolly-clutch.glitch.me/favicon.ico	false		high
http://https://1drv.ms/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9	false		high
http://https://onedrive.live.com/redir?resid=1F6FC88150FE397E%2135197&authkey=%21AoF88NbpYZfqkJE&page=View&wd=target%28Quick%20Notes.one%7C5d7d8a2d-e7c2-4f4c-8bbd-8958bcaab581%2FKinetre%20Inc%7C98a50910-a8d3-4348-9fa8-39684459cbc8%2F%29&wdorigin=NavigationUrl	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high

Copyright Joe Security LLC 2022

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	false		high
http://https://verbena-woolly-clutch.glitch.me/toy.htm	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://verbena-woolly-clutch.glitch.me/toy.htm	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://onedrive.live.com/view.aspx?resid=1F6FC88150FE397E!35197&ithint=onenote&authkey=!AoF88NbpYZfqkJE	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	false		high
http://https://verbena-woolly-clutch.glitch.me/css/hover.css	false		high
http://https://amcdn.msftauth.net/me?partner=OneNoteOnline&version=10.21153.1&market=EN-US&wrapperId=suiteshell	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high

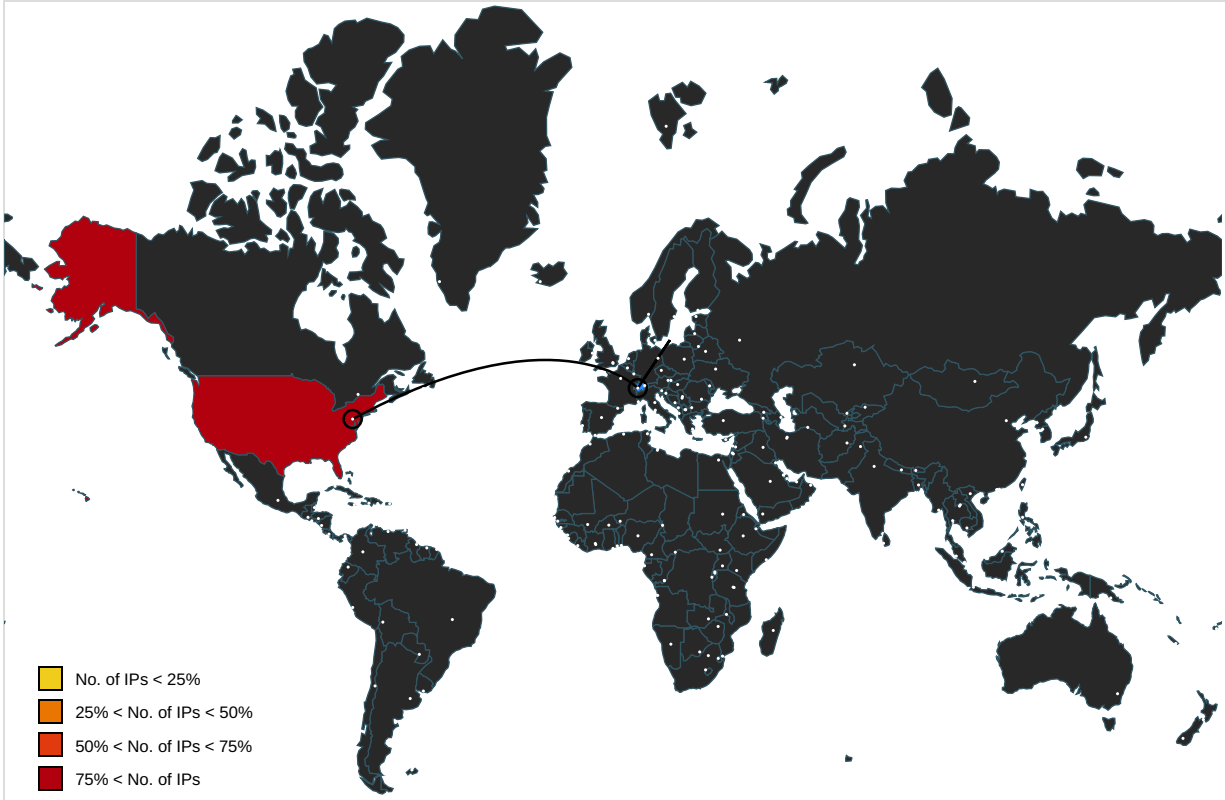
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 6b006fd1-2d16-41e3-af96-3f08c2d9df9a.tmp.1.dr, df65693d-31b6-4c80-b26d-d65c02a3e5be.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.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_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://onedrive.live.com/redir?resid=1F6FC88150FE397E	History Provider Cache.0.dr	false		high
http://https://onedrive.live.com/view.aspx?resid=1F6FC88150FE397E	History Provider Cache.0.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://easylist.to/)	LICENSE.txt.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr	false		high
http://https://creativecommons.org/compatiblelicenses	LICENSE.txt.0.dr	false		high
http://https://www.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://github.com/easylist)	LICENSE.txt.0.dr	false		high
http://https://creativecommons.org/.	LICENSE.txt.0.dr	false		high
http://https://accounts.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://1drv.ms/o/s	History Provider Cache.0.dr	false		high
http://https://clients2.googleusercontent.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://apis.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://spoprod-a.akamaihd.net	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr	false		high

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://clients2.google.com	633358e7-c7f3-4f89-8d83-94ce757453a9.tmp.1.dr, 539f4c29-0538-49fc-90ee-d20ac32635ba.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.219.60	part-0032.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
204.79.197.200	dual-a-0001.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.36.227	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
13.107.6.171	b-0016.b-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.104.208.165	i-db3p-cor006.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.22.91.148	verbena-woolly-clutch.glitch.me	United States		14618	AMAZON-AESUS	false
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
13.107.42.12	1drv.ms	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

Copyright Joe Security LLC 2022

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655224
Start date and time: 30/06/202218:41:32	2022-06-30 18:41:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9
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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@32/119@21/14
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://verbena-woolly-clutch.glitch.me/toy.htm

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.36.206, 142.251.36.195, 74.125.104.71, 13.107.42.13, 34.104.35.123, 80.67.82.209, 80.67.82.219, 13.81.118.91, 23.35.237.204, 52.109.88.115, 52.109.32.24, 51.104.15.252, 23.35.236.56, 142.251.36.170, 23.35.236.59, 52.111.236.5, 51.105.71.137, 20.234.93.27, 52.109.88.2, 20.190.159.4, 20.190.159.2, 20.190.159.73, 20.190.159.0, 20.190.159.71, 40.126.31.73, 20.190.159.23, 20.190.159.64, 152.199.19.160, 23.203.67.116, 23.203.68.253, 40.126.32.136, 40.126.32.74, 40.126.32.76, 20.190.160.14, 40.126.32.140, 20.190.160.22, 40.126.32.68, 40.126.32.134, 69.16.175.42, 69.16.175.10, 172.217.16.170, 104.18.22.52, 104.18.23.52, 142.251.37.10, 172.67.150.137, 104.21.30.41, 142.251.36.240, 142.251.37.16, 172.217.16.176, 142.251.36.176, 142.251.36.208, 20.189.173.5, 20.44.10.123, 52.242.101.226
- Excluded domains from analysis (whitelisted): odwebp.trafficmanager.net, e2682.g.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, ka-f.fontawesome.com.cdn.cloudflare.net, storage.googleapis.com, prod-azurecdn-akamai-iris.azureedge.net, c1-wildcard.cdn.office.net-c.edgekey.net.globalredir.akadns.net, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, browser.events.data.trafficmanager.net, res-1.cdn.office.net, appsforoffice.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, cdn.onenote.net.edgekey.net, onedscolprduks03.uksouth.cloudapp.azure.com, prod-campaignaggregator.omexexternallfb.office.net.akadns.net, star-azurefd-prod.trafficmanager.net, login.live.com, r2---sn-4g5lznlz.gvt1.com, update.googleapis.com, officeclient.microsoft.com, www.gstatic.com, onenoteonlinesync.onenote.trafficmanager.net, westeurope0-odwebp.cloudapp.net, global-entry-afdthirdparty-fallback.trafficmanager.net, www.bing.com, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, ajax.googleapis.c
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- 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\086dda27-f745-44b8-94ab-ba8b6ac61b32.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724

Entropy (8bit):	3.751153150705699
Encrypted:	false
SSDEEP:	384:7/rM8uh3CytofNErFvg83/M+HHy7GrOrZ+wexvCGi5r1AmRmNOsEwfOOi8NB1cFd:NWhJ2G37keX6cWAvfCQKa081w
MD5:	2A987A659BC9042D1A5091102F5F0F6B
SHA1:	93C197298EFE4C8334FE3CB135A498D8744BB0D1
SHA-256:	1D7FD55E928F00592662846D1F3D8FF7C5A9CF37E11774F6C59C38D7296AD7BA
SHA-512:	B351F14BC008CE4C8482346DC4A4952BC679379C2032BE2932AB16B9A5EF9917EC9EBB9EA9456E735360399ACB230658DD937DAD38484B3A3713CA692C6548B2
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\30b0081c-bdb9-4e20-9da2-b9d71b90d53c.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):	205939
Entropy (8bit):	6.0427949815655335
Encrypted:	false
SSDEEP:	6144:tY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:uSFNwtzR7o5okKor
MD5:	57A385104ED6A1CD25C0099590C3E517
SHA1:	934F8D89C9CFA3A18A717616ABBA4C0FC32B91D6
SHA-256:	4F7DD1FEB3CBCB490F476D5DCFB5CD4EE5E325725C82883C866741226A8F0280
SHA-512:	80E0E21F9A8BEFA496E11C33A620A2604010F5EBB5E3D53361AFFA02B3E87C0F9A8F4F5FA44B4B8BC6A6BF894727F6123A9B4A5214C517C846158073837F9D65
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639140338"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ecad9ab-3e42-45be-b945-e911d4b6f84f.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):	206134
Entropy (8bit):	6.043307722866735
Encrypted:	false
SSDEEP:	6144:TY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:kSFNwtzR7o5okKor
MD5:	E27EB258B1AC78C1E46965F0A34C6519
SHA1:	9EA708B3602D0B35F779B72E4373DBA5EC1A971C
SHA-256:	383E2E0D749AE807CAE0CFAA22EA59F37F1182204957C511AAE720D7141FBC75
SHA-512:	143A38A4412EC94654CCA652AC9442A39AF56D6F1B55D3475E61BCDEB5C854E06CA61F2644D1A7E2FED76B5FD666F1A082ACF6EB444E4387360DA82C17B2BA06
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639140338"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6c6a0a2f-a887-4066-b512-65cb3e77fc9d.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):	214380
Entropy (8bit):	6.070652256296569
Encrypted:	false
SSDEEP:	6144:/LY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:/sSFNwtzR7o5okKor
MD5:	D68654F988A06576F477172359937508
SHA1:	EA5817523D8CD6C65FB39DC1830B691514FD0FAC
SHA-256:	3212D2BCCA2FA0842A0814D11715A43F876768B344E257BCF8471F5E20B293F1
SHA-512:	E513ADA067B6ACFF84FB01EC50120CECE9670127B31369DEA8B4B0FE0E2D06794551EDF0A352590329F076BFC85F613AF28C45CDA9BD0E5414C3B24F8374F8E
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\731254e2-7898-4d5d-bb22-6d2909cf2801.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7518868909215723
Encrypted:	false
SSDEEP:	384:l/rM8uh32lyUVZrofNErFvg83/M+HHy7GrOrZ+wexvCGi5r1AmRmNOsEwfOOi8NW:J6WhJ2G37keX6cWAvfCQKa081O
MD5:	624DF0F2C0640E8D6FA1561CFDDBA45C
SHA1:	63D5A58CB8F3F88E0C15139E8D5141737BCFC229
SHA-256:	28EFD86E5D0B6C4F59AB79AA178A0EDEFDEAD6A35D5C7BB56938A501BA847397
SHA-512:	8CD8EB9FD64AAD9B95B5DED36190D75991FBB921E2A09E4CA601476307A5970402E75A75773098F60D28476A3FE45E7A45A90F315323F664AACD66624856C57F
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\94aae6bc-374c-4115-a4c7-edd0075d992b.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):	206031
Entropy (8bit):	6.043040423424427
Encrypted:	false
SSDEEP:	6144:nY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:YSFNwtzR7o5okKor
MD5:	031C79AD08C0904442D3A62A5377238D
SHA1:	D1C4817C0D08B22734186D285FEB99285C398A96
SHA-256:	F352EDDFD3650041C645390FB5132CF889D7F69DD3FD04A1C7F7EBDDCC864697
SHA-512:	0F17C70182EAE3F891E1B4B3DEB6A6485C57BD31CE55F16FBAF2A66361E1B21B1D7581E514F902CEDF88E7F09540339F479228A6AF489D56D924FDB986EAC9F2
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639140338"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1df751d8-d58f-4cc2-91af-afc1f2a0a7af.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):	19792
Entropy (8bit):	5.563646878220393
Encrypted:	false
SSDEEP:	384:zRmtlLlKWXo1kXqKf/pUZNCgVLH2HfDRrUZHGKMQQH/324G:kLlno1kXqKf/pUZNCgVLH2HfFrU9GKQ8
MD5:	28FF252997F6FE6EE9BF5B365B5BA6A3
SHA1:	C3425D441B353FB7925A99A08DA165F961401103
SHA-256:	3D64739F7EFEF134502BC87FED321656793C68E64D1A78F10918CD189260E3B9
SHA-512:	2226DDF65387825123557EF8BFF3700B7FA086B65598967FAF0A2A636EF91DE2F752C3E6C4C710B6D7EE2D3BC6A4D56D38DFE6B64A23080EE5F79B1F93B72F7B
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":"13301113354966212","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\1f1d84e3-6e92-4d48-84d6-b3daf31d9a84.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):	5.573668581482286
Encrypted:	false
SSDEEP:	384:zRmtwLlKWXo1kXqKf/pUZNCgVLH2HfDRrU2FQQHK24f:zLlno1kXqKf/pUZNCgVLH2HfFrU2m2k
MD5:	75AA153659E8C26150324C5E661F6B5F
SHA1:	20C9CD448DD3204CE01C8593ABA5B948EF739516
SHA-256:	1580491742DE5D29F42EADD97FA534FBC3F7487120866F21BEF848AD37158B24
SHA-512:	E43C7B322D0BDA278DF19193673AB77C869B455901CA35AF196F41B58D14A45F72E44D9752C6415F411A536F7C0D58543AE0F54D08DC31DE2FD79E188DA806C
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":"13301113354966212","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\26c64c90-d440-4d06-992f-05567e6e720a.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):	5199
Entropy (8bit):	4.982928387719534
Encrypted:	false
SSDEEP:	96:nuCqAc/1pcKI3kok0JCKL8MkDjtbOTQVuwn:nuCqf1pcJ4KBkDR
MD5:	F043CE7EAB4C43D3C455BA8D1B87118B
SHA1:	205FF6C1FAE02395B6CF25257733F06103E1C6FC
SHA-256:	233AF15700EB5A823DF98CA52D70C3E160DD1D5CFF9ADD774A6511088D0FCDF0
SHA-512:	71A10F7B00EA31D95729F9623FDC1478D047B315DEE3E24D00BB5B5EFAA1C1BCBE2460BF9342BCB47C715A322FDFE61A47AC97A2C3860821A0B5614B1EDE93 82
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301113355787309","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

Size (bytes):	5136
Entropy (8bit):	4.9797728235862735
Encrypted:	false
SSDEEP:	96:nuC4f/1pcKI3hok0JCKL8LkW1pbOTQVuwn:nuC01pci4K+kWv
MD5:	2AC551F3457AAB52BB7F3E7D6F780EBE
SHA1:	A86359F4F13C43EFBA0E0A77265FBA4D4F973938
SHA-256:	CCD3B33CC10C7523F653613ECB90B6AD0AC3C90337D29ABB2CAAE8BB3E960273
SHA-512:	7C3EA8A864CF015A660DF02346673DEAD0F26DC763C882E42AA7F01D974AB8241F6788D9B287039B3B9234A0DAF6CF50C0536161B819A38C9E042D4DD721056
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301113355787309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.576235776951924
Encrypted:	false
SSDEEP:	384:zRmtlLlKWXo1kXqKf/pUZNCgVLH2HfDRrUCMQQHd9+24+:kLlno1kXqKf/pUZNCgVLH2HfFrUCe9+8
MD5:	F411552C7A4009FDA4BD1C09BD1A78C8
SHA1:	7CE75DF2CD9996199E28494C5AB1F33825EEA758
SHA-256:	03001EE489E389ED5F2707186046973D13A1EAB6F6FC675C3FE8B0931D152E1C
SHA-512:	C9A50145B8E838E24403608C8A9EE477E2DAAB31F998957AD519129A67F4A2D1E2E0F5C025FDE753F97778CBCB5BEAD593D2D3B9A48777CD8BDA1CD1D553E B6
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:mh t: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":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13301113354966212","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\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","w ifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI="," DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7C MjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+ wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vW LQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhl zuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.335017817514775
Encrypted:	false
SSDEEP:	6:2j9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVRJSJZmwYVRPS9VkwOWXp+N23iKKN:O4va5KkTXfchI3FUt7J/oSD5f5KkTXfE
MD5:	C58CE02CDFF6C3E4AE7128AF7526FC0A
SHA1:	6D3EC87B435F673F499DABEC2138BE855023D6CA
SHA-256:	3E5816024A2E05173A3E1AC4AEEB9F9BCB7741A6F2B54B9F0283FC90026257CF
SHA-512:	35E88E3E422860FCEEF9A7F2367E1B7CB3939D1478C736F5098408B68FC333587A282B87F690A997899C192247EEE323A98543710AB546F6D1DB3201A6D3A094
Malicious:	false
Reputation:	low
Preview:	2022/06/30-18:42:56.967 1428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-18:42:56.971 1428 Recovering log #3.2022/06/30-18:42:56.977 1428 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.335017817514775
Encrypted:	false
SSDEEP:	6:2j9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVRJSJZmwYVRPS9VkwOWXp+N23iKKN:O4va5KkTXfchI3FUt7J/oSD5f5KkTXfE
MD5:	C58CE02CDFF6C3E4AE7128AF7526FC0A
SHA1:	6D3EC87B435F673F499DABEC2138BE855023D6CA
SHA-256:	3E5816024A2E05173A3E1AC4AEEB9F9BCB7741A6F2B54B9F0283FC90026257CF
SHA-512:	35E88E3E422860FCEEF9A7F2367E1B7CB3939D1478C736F5098408B68FC333587A282B87F690A997899C192247EEE323A98543710AB546F6D1DB3201A6D3A094
Malicious:	false
Reputation:	low
Preview:	2022/06/30-18:42:56.967 1428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-18:42:56.971 1428 Recovering log #3.2022/06/30-18:42:56.977 1428 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):	2270
Entropy (8bit):	6.104248999871066
Encrypted:	false
SSDEEP:	48:DVvPoLSWU9iOd1eAkTyLK+HiRbEh+fEh+VKIScTzEcShwmi:Zoc9PqNTyLK+alVBScTbShwmi
MD5:	D575ADC7573A556F05C30752057BD84F
SHA1:	4223757AE555260AF85878B0D38064B0FCFAEF9F
SHA-256:	8B6F37FC81B9C70401AFE413C76DE401529CE6947D4F8592BBEA1E9843EE3068
SHA-512:	1DAE01CC9D813DFA662B2D81DEBAC0FB79190A7CBC138D0F4C67D52084C93D28B473A97AEFDC07DF550C5C09E3E1A96F07246572484AEC66936F852D25A77F98
Malicious:	false
Reputation:	low
Preview:	.....".....1f6fc88150fe397e..35197..aof88nbpyzfqkje..aspx..authkey..com..https..inc..ithint..kinetre..live..microsoft..onedrive..onenote..online..resid..view..2..wdo..1drv..9..at..bh45..e..lcbyg8fgpj9gxzw1ulhl..ms..o..qqkq..s..yveguvzg9es2pfokugiefw..redir*.....1drv.....1f6fc88150fe397e.....2.....35197.....9.....aof88nbpyzfqkje.....aspx.....at.....authkey.....bh45.....com.....e.....https.....inc.....ithint.....kinetre.....lcbyg8fgpj9gxzw1ulhl.....live.....microsoft.....ms.....o.....onedrive.....onenote.....online.....qqkq.....redir.....resid.....s.....view.....wdo.....yveguvzg9es2pfokugiefw..2...$.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\000001.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false

SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\CURRENT (copy)

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_onenote.officeapps.live.com_0.indexeddb.leveldb\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	........idb_cmp1.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent 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):	2708
Entropy (8bit):	4.898465958139244
Encrypted:	false
SSDEEP:	48:Y2TntwXGDH3qyvz5sfGs5RLsQSasuKsRMHRsGRsKO7sC6MqsAxbD:JTnOXGDHa+zUHSs7Gd9OT6MixH
MD5:	5C6163AE61E0E96B4958BB9C137B8F8B
SHA1:	D2DDE6449374D83135EF26D7E7812BAE866C0380
SHA-256:	EC069FCC0C0AE7B6E4B24FA311C72B3D3847557E76F23CF2EB35B47815F98F99
SHA-512:	645053150CA914D01342590949A200ED6093940ECC78D2F283DDDBB5797318101AF79E1BEA6BEC8AAB2308593EF79F808471C9A2F89F33954A856D61E9AD49EE
Malicious:	false
Reputation:	low

Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13303705359297926","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13303705359339022","port":443,"protocol_str":"

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):	5226
Entropy (8bit):	4.987055089789741
Encrypted:	false
SSDEEP:	96:nuCqAm/1pcKI3kok0JCKL8MkDjQbOTQVuwn:nuCqT1pcJ4KBkDW
MD5:	AA588E94012F01381DB570DD10E8F9E3
SHA1:	D00E8E1375313BBA43FA36A49250424B7C67D754
SHA-256:	560274792FCE3C727F237F5BD327DDD8E29303FF305FDAB066F315E0CE89A0DC
SHA-512:	A002AA717EF5B705DB77D5C71CC1D2E749F2963465DB34E71C25D0497CAF3CCC604349581D24A87C1C9A4C551764216E23B7247A5F21EA3AE5256EE9CBDC09C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301113355787309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low
Preview:	....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low

Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\df65693d-31b6-4c80-b26d-d65c02a3e5be.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b5ba8a12-ab39-4364-b5c0-8fa8fd010a19.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):	5226
Entropy (8bit):	4.987055089789741
Encrypted:	false
SSDEEP:	96:nuCqAm/1pcKI3kok0JCKL8MkDjQbOTQVuwn:nuCqT1pcJ4KBkDW
MD5:	AA588E94012F01381DB570DD10E8F9E3
SHA1:	D00E8E1375313BBA43FA36A49250424B7C67D754
SHA-256:	560274792FCE3C727F237F5BD327DDD8E29303FF305FDAB066F315E0CE89A0DC
SHA-512:	A002AA717EF5B705DB77D5C71CC1D2E749F2963465DB34E71C25D0497CAF3CCC604349581D24A87C1C9A4C551764216E23B7247A5F21EA3AE5256EE9CBDC09C
Malicious:	false
Reputation:	low

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301113355787309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206134
Entropy (8bit):	6.043307722866735
Encrypted:	false
SSDEEP:	6144:TY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:kSFNwtzR7o5okKor
MD5:	E27EB258B1AC78C1E46965F0A34C6519
SHA1:	9EA708B3602D0B35F779B72E4373DBA5EC1A971C
SHA-256:	383E2E0D749AE807CAE0CFAA22EA59F37F1182204957C511AAE720D7141FBC75
SHA-512:	143A38A4412EC94654CCA652AC9442A39AF56D6F1B55D3475E61BCDEB5C854E06CA61F2644D1A7E2FED76B5FD666F1A082ACF6EB444E4387360DA82C17B2BA06
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639140338"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

Size (bytes):	95428
Entropy (8bit):	3.7514178850400683
Encrypted:	false
SSDEEP:	384:V/rM8uh32lyUVZrofNErFvg83/M+HHy7GrOrZ+wexvCGi5r1AmR9XNOsEwfOOi8W:Z6WhJ2GA7keX6cWAvfCQKa0810
MD5:	29286FDCBF6C9E6AD2B91286C89CF073
SHA1:	642E888DD932680D0D5272BBD19B0E66825BBA6C
SHA-256:	A339F22D0EBC1EBAE8856D3DF7EFC8E613B3309AADF803C0A7E78EAB6D8124EF
SHA-512:	D0098A25A136FBCF9281352E55AEED7F5226FA6DF78BBAF3FDFCA40B65D53BC8DCA549413FA917D7112BD7D2AED4F5B45ACB3E8FB82EA32BD3940798BA4CD251
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir2912_265036453\Ruleset Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150056
Entropy (8bit):	4.8588214550289095
Encrypted:	false
SSDEEP:	3072:P8C4uHgjBz+BZKEZZ3F0Sl03PzpDL7UI09QEwNyfe:P8C5go1U6IYeH
MD5:	C56FF16BF9B9FC0002C0128DD0BD763D
SHA1:	5048CFDBAC5D7AAAD345BAE08E66E8C4E803CA02
SHA-256:	404AA48D274C3A8FEC3145858E00279D01E0C37A5304218E191C0156E4DE00FF
SHA-512:	D993A324F5D9A1FC4FB3131252F48679750081D996295C994E2DCA4E84F2DECF7E90AF6766EFEDC2CEFC6B66194FFF38181C9E9CE45346BEEB8B3A09CE66BB73
Malicious:	false
Reputation:	low
Preview:	.....[..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....|...`...D..... .....'.....ozama.....*...'.....g.bat.....&.. .'.....onwod.....`....'.....ennab.....'.....nozam.....(.....geips.....P...((.....rekoj.....@(.....lgoog.....X(.....uotpo.....+..p(.....lreko.....d...h(.....Y..... .....Y...Y..pY..TY..8Y...Y...Y...Y...Y...Y...X...Y...Y...Y...Y...X..|Y..xY...X..pY..xX..hY..XX..`Y..\Y..4X..TY..PY..LY..HY..DY..@Y...X..8Y...W..0Y...W..(Y...W.. Y...Y...Y.. .Y...Y...Y...Y...Y...Y...X...X...X...X..PW..4W...X...X...X...X...W...X...X...X...X...V...X...V...V...X...X...X...xV...X...X...X...X...X...X...X...X...X..|X..4V..tX..pX..lX..hX..dX...V...U..XX ...U..PX..LX...U..DX..@X..<X..8X..xU..\U..@U..(X..$X.. X...X...X...X...U...X...X...X...X...T...T...T...T...W...W...W...W...W...W...W...W...W...LT...W...W...W...W.. T...W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\c50c5c5f-72c3-4d69-9527-c4a53ec79026.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):	214380
Entropy (8bit):	6.070652128323124
Encrypted:	false
SSDEEP:	6144:scY3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:sZSFNwtzR7o5okKor
MD5:	2DE2BD63404A285F91EE8402C2F669DD
SHA1:	995BAA969C1DEEF1EE7A03AE79F4CBD5AB2A75EE
SHA-256:	5B3151BA828BFF53B76503671065E14FCD7FDF63E7793CBB6BFD829320AEB025
SHA-512:	AF7C592B2AC49A918853C7025AF529AC8E8AE1929FFCA825DB0BCCAABDC2B6E5D9E6C7191260FCA8DEF60E6F28854E27C74A8754238D552319817E5308A2D14A
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639140338"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d522c0ee-6c80-4905-96d1-8ed746da792d.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):	214379
Entropy (8bit):	6.070652655874212
Encrypted:	false
SSDEEP:	6144:/7Y3CFrBwtnztpWK7o5Q4xJqk5aqfIlUOoSiuRM:/8SFNwtzR7o5okKor
MD5:	60991BA0331480DF31F1915FEF544C7B
SHA1:	A2E02AA8E76409EE9338D9501BF4B1990AB41C13
SHA-256:	0013F555C2CBD7FB493FDA9DB1C14F001C7A9F5B610926940F9FF4789A802651
SHA-512:	89C3C3DFD7CFC981959D970F52A23624997BE04FF8BB5AA68F978E30FC13A5DDB8DAC5B28E2E820A9EFAAC824AADD8DF6F9675A6E1B5E37E853456EAD63FC2C2
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":1.656639757584938e+12,"network":1.656607359e+12,"ticks":117564482.0,"uncertainty":4635451.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\f0236d04-1c65-4778-83b9-40c8ea6c4aac.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7514178850400683
Encrypted:	false
SSDEEP:	384:V/rM8uh32lyUVZrofNErFvg83/M+HHy7GrOrZ+wexvCGi5r1AmR9XNOsEwfOOi8W:Z6WhJ2GA7keX6cWAvfCQKa0810
MD5:	29286FDCBF6C9E6AD2B91286C89CF073
SHA1:	642E888DD932680D0D5272BBD19B0E66825BBA6C
SHA-256:	A339F22D0EBC1EBAE8856D3DF7EFC8E613B3309AADF803C0A7E78EAB6D8124EF
SHA-512:	D0098A25A136FBCF9281352E55AEED7F5226FA6DF78BBAF3FDFCA40B65D53BC8DCA549413FA917D7112BD7D2AED4F5B45ACB3E8FB82EA32BD3940798BA4CD251
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....`8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\2912_1837665677\Filtering Rules

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97968
Entropy (8bit):	5.489893397464442
Encrypted:	false
SSDEEP:	1536:ojHlFMJw9iI9Yh9FHc6cPC3CpBHTrDo630a8Q78xRAQudDv4NZ/p2GuN+BO1:6FMJw9v9efHc6cPCURDR30EYnAQuJANw
MD5:	3846A25BC9191585763E06550798BAB1
SHA1:	F43D903B13AB969E2276E304795CE164F22F893C
SHA-256:	C7D5D133E8F995D3E4D5B68F28BE0D7B1F290DFBD1502E0EC260142325FA8F88
SHA-512:	6B1E1776DE4B4B7D7BD7E6252F555AD84CC689EFE1F3920B3ACFE23DE65212254FC219E0A530037A5EA819894BC2F5B85ECFC0ADDEE9AF3163393AA32F97BA44
Malicious:	false
Reputation:	low
Preview:	.....0.8.@.R.-728x90.....0.8.@.R.adtdp.com^.....0.8.@.R.yomeno.xyz^.:.....*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....0.8.@.R.uwoapte e.com^.8.....*...safeway.com0.8.@.R.fwcdn2.com/js/embed-feed.js.....0.8.@.R._468_60..3.....0.8.@.R#/wp-content/plugins/wp-super-popup/.9.....0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....0.8.@.R..adbutler-.....0.8.@.R.adrecover.com^.....0.8.@.R.hdbcode.com^.?.....*...google.com0.8.@.R!developers.google.com/google-ads/.-.....*...konograma.com..0.8.@.R./adserver.....*...vk.com0.8.@.R.vk.me/css/al/ads.css.,.....0.8.@.R.mysmth.net/nForum/*/ADAgent_.....0.8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.E.....*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.(.....0.8.@.R.looker.com/api/internal/.#.....0.8.@.R.broadstreetads.com^.....0.8.@.R./banner.cgi?.....*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net

C:\Users\user\AppData\Local\Temp\2912_1837665677\LICENSE.txt	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454E
Malicious:	false
Reputation:	low
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\2912_1837665677_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):	1529
Entropy (8bit):	5.993915630498445
Encrypted:	false
SSDEEP:	24:pZRj/flTHYfcl5kYbKqLjeT3azkaoX1pF/kSYYRVHbo0doXxOB6G6QL3foQ3QL5D:p/h4ElBbKdTakak1pFcSfRV7o0dkx8L4
MD5:	6B2EDD2D0C16E5D77BD2C3E4AE88C95F
SHA1:	BC82982FA8A04FA6FD9F17DA03D443A57E0F78D4
SHA-256:	CA0F5F75FC56FBEDA7522B2C83707A451D01760F417C497A37C70554E290B737
SHA-512:	533026A33030795ABF24B6E78D26763734D98CA74BFA4FAC2073EFAD0BB5CA1C38E7036BEAF17E6ABBFE56CF968E80EB3CA3CFD23AEEC10CE1280E8DB1C4078C
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJMTF90X0NkWWRYUnpMSHJBZ3hmUW5tcENTaXlkWEtzVVlJZnZjLTR0czRBIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJIn0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6Imo4MmhRZGhaa0MwMjFWOEZ1MHUtMExvMnVJdXI5SzdFem5JcHE3WHd2YlkifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMzYuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"VM_rIA1uXuXjbhz_uZ8uQp9F3FfgEgGTjCXL08Q_jrGXXH-Yty1DqAw4yzWsadeOjVRozUf_7kBrYJ2U8Y8slircdLRbrqJejQeyyrJx4HFT8qgZEb60YHdsOd76C57YzF5dXErpjT7_FkWA41lTxLQvdWbACMO0DE7uOHO9mZx5pM98Ni9GsM_yxJbRSyDZWa8BdPHErfMuO6YE6D8tbnYTr2tXcMV9p2ZEAFMiso2B-6DSr

C:\Users\user\AppData\Local\Temp\2912_1837665677\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9458563396006063
Encrypted:	false
SSDEEP:	3:SWllBTGVn1VJ8U1hRGGpWdTdSATn:SWNT+eKhRR4dTVT
MD5:	991F44CE02222E783A1FEFE4187727CE
SHA1:	9855D1CA0338ADCD5829C3260BF7FAAF88A23509
SHA-256:	58704ADE087671AA1226BC9CEC1719F5B80B90C571EF747812A64458BBEA0F50
SHA-512:	C2616426939B235620A22B24A9BEC6D4F7DBB695C812F1784A4C95B41E53A21F371A6C440177CFABDE47E203EB83269F9013FC75C6D758EA6FDFE7B52B4A554E
Malicious:	false
Reputation:	low
Preview:	1.34ff2e9d7a7ce81c5d760d4b0f4b59a0237dd5db0d1e84ccd5103a30687eac17

C:\Users\user\AppData\Local\Temp\2912_1837665677\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.563301657145084
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS1Avn:F6VlMZWuMt5SKPS1Avn
MD5:	47B89067C397B3EABBD04E6FC4008B71
SHA1:	7B4E623806D7EA8BFCD2FE6836A21E50C9F9340E
SHA-256:	8FCDA141D859902D36D55F05BB4BBED0BA36B88BABF4AEC4CE7229ABB5F0BDB6
SHA-512:	FDA1CE8EB24A05F65E8132248EEF96C422E5AA2D3254B590FBFD3FCB2016E3B7F6E4B53702D88E1695D4BEC0175F72EB4256CDAA2FF72DDF4390D480D04BA373
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.36.0".}.

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_pnacl_json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271CE
Malicious:	false
Reputation:	low
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A15840
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff.....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<....f.....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped

Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl...x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

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

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....__pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t''..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive

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

C:\Users\user\AppData\Local\Temp\2912_2145922573_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`... ...@...@.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\2912_742143674\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FCAF
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.....S'.....2.{.....'....+.'.."..Y.x.ISa...)....H.&92..?!..~..F.5."...n,.B.-|\.)..(.....]G..j.-M)...C.....o&L..0.K.....UtP.&.N..;..^w/a{}v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0.."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8.....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..('e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Users\user\AppData\Local\Temp\2912_742143674_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):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	48:p/hii6zkvVI1Jip2qRNHvakuQkCNFxdsGwmBKkgum91:Rz0kv6cNvaYNFwSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F0FE
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxIiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZgQvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8qlRy7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZdkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\2912_742143674\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675
Encrypted:	false
SSDEEP:	3:SpOXzxlQ4BdPWfDL9c:SpOjDQFfVc
MD5:	2AE14F91312C4E8034366B09D49D5B18
SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Reputation:	low
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\2912_742143674\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\4b81576d-c52b-449b-96ab-b87469f2c343.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\e1462bfa-6d0d-414d-956a-e46a1cffcf59.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\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_dir2912_1000190791\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_dir2912_1000190791\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_dir2912_1000190791\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_u navailable": {.. "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 comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\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:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80 552

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "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 trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\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:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4 0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "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_dir2912_1000190791\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "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_dir2912_1000190791\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
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_dir2912_1000190791\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_dir2912_1000190791\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 transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\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:	dropped
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_unavailable": {.. "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_dir2912_1000190791\CRX_INSTALL_locales\fi\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):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\fr\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):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . unr.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\hi\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):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "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_dir2912_1000190791\CRX_INSTALL_locales\hr\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):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 96E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\hu\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):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604

Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\it\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):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ja\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):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
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_dir2912_1000190791\CRX_INSTALL_locales\ko\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):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF

SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
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_dir2912_1000190791\CRX_INSTALL_locales\lt\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):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\lv\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):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\nb\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):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB5

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXl8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pl\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):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pt_BR\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):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\pt_PT\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):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 24
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ro\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):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\ru\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):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_u navailable": {.. "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_dir2912_1000190791\CRX_INSTALL_locales\sk\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):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59D
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": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sl\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):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC09D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\sr\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):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
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_dir2912_1000190791\CRX_INSTALL_locales\sv\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):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA687 52E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavai lable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2912_1000190791\CRX_INSTALL_locales\th\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):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	24:1HEKa1dDa1/WYp6UFi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
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_dir2912_1000190791\CRX_INSTALL_locales\tr\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):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "craw_a pp_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavail able": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 18:42:38.200994968 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.201028109 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.201109886 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.202316999 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.202368021 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.202431917 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.203073978 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.203111887 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.203186989 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.203439951 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:38.203464985 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:38.203563929 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:38.204581022 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.204597950 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.204973936 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.205033064 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.205277920 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.205312967 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.205688953 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:38.205718040 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:38.267792940 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:38.268413067 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:38.268439054 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:38.269860983 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:38.269927025 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:38.282392025 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.282749891 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.282782078 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.283112049 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.283184052 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.283993959 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:38.284070015 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:38.285701036 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.286509037 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.287919044 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.287965059 CEST	443	49741	13.107.42.12	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 18:42:38.288163900 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.288202047 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.288718939 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.288728952 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.288820982 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.289083004 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.289956093 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.290035963 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:38.290256977 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:38.290327072 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.061733961 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:39.062096119 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.062405109 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.062763929 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.063081980 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:39.063409090 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.063416958 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.063739061 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.064558983 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:39.064595938 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.064760923 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.064804077 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.065078020 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:39.065119028 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.102060080 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.102129936 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:39.102157116 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.102199078 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.102251053 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:39.103456974 CEST	49743	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:39.103485107 CEST	443	49743	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:39.119364023 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.119522095 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.135848045 CEST	49744	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.135875940 CEST	443	49744	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.138686895 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.138758898 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:39.138782978 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.138958931 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.139019966 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:39.150733948 CEST	49745	443	192.168.2.3	142.251.36.205
Jun 30, 2022 18:42:39.150758028 CEST	443	49745	142.251.36.205	192.168.2.3
Jun 30, 2022 18:42:39.189656973 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:39.189682007 CEST	443	49741	13.107.42.12	192.168.2.3
Jun 30, 2022 18:42:39.289735079 CEST	49741	443	192.168.2.3	13.107.42.12
Jun 30, 2022 18:42:42.922713041 CEST	49767	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.922771931 CEST	443	49767	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:42.922852039 CEST	49767	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923032045 CEST	49768	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923065901 CEST	443	49768	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:42.923144102 CEST	49768	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923330069 CEST	49769	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923383951 CEST	443	49769	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:42.923464060 CEST	49769	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923603058 CEST	49767	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923635006 CEST	443	49767	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:42.923804998 CEST	49768	443	192.168.2.3	13.107.6.171
Jun 30, 2022 18:42:42.923830032 CEST	443	49768	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:42.923949003 CEST	49769	443	192.168.2.3	13.107.6.171

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 18:42:42.923985004 CEST	443	49769	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:43.024696112 CEST	443	49767	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:43.024843931 CEST	443	49768	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:43.024888992 CEST	443	49769	13.107.6.171	192.168.2.3
Jun 30, 2022 18:42:43.025150061 CEST	49767	443	192.168.2.3	13.107.6.171

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 18:42:38.164534092 CEST	65358	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:38.168430090 CEST	49873	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:38.171451092 CEST	53802	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:38.185444117 CEST	53	49873	8.8.8.8	192.168.2.3
Jun 30, 2022 18:42:38.191809893 CEST	53	65358	8.8.8.8	192.168.2.3
Jun 30, 2022 18:42:38.196875095 CEST	53	53802	8.8.8.8	192.168.2.3
Jun 30, 2022 18:42:39.157346010 CEST	63548	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:41.987354040 CEST	61380	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:41.991329908 CEST	63146	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:43.303570032 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.335694075 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.338148117 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.370574951 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.370620012 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.370657921 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.370695114 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.374321938 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.375873089 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.413094044 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.413450956 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.457186937 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.459332943 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.459487915 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.469233990 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.484523058 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.485019922 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.485053062 CEST	443	58626	142.251.36.238	192.168.2.3
Jun 30, 2022 18:42:43.485728979 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.511033058 CEST	58626	443	192.168.2.3	142.251.36.238
Jun 30, 2022 18:42:43.587486029 CEST	52810	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:51.708564043 CEST	64996	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:57.199040890 CEST	63861	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:57.697922945 CEST	49723	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:58.218815088 CEST	52581	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:59.027538061 CEST	56639	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:59.199142933 CEST	50450	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:42:59.496953011 CEST	62724	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:11.410109997 CEST	61877	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:11.431724072 CEST	53	61877	8.8.8.8	192.168.2.3
Jun 30, 2022 18:43:12.546941042 CEST	64412	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:12.548346043 CEST	51779	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:12.550493956 CEST	54205	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:12.567298889 CEST	53	51779	8.8.8.8	192.168.2.3
Jun 30, 2022 18:43:12.853821039 CEST	58497	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:43:12.874304056 CEST	53	58497	8.8.8.8	192.168.2.3
Jun 30, 2022 18:43:12.920520067 CEST	62701	53	192.168.2.3	8.8.8.8
Jun 30, 2022 18:44:02.248027086 CEST	51994	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 18:42:38.164534092 CEST	192.168.2.3	8.8.8.8	0xf378	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:38.168430090 CEST	192.168.2.3	8.8.8.8	0x145f	Standard query (0)	1drv.ms	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:38.171451092 CEST	192.168.2.3	8.8.8.8	0x6a2	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:39.157346010 CEST	192.168.2.3	8.8.8.8	0xc1ff	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:41.987354040 CEST	192.168.2.3	8.8.8.8	0xb6f3	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:41.991329908 CEST	192.168.2.3	8.8.8.8	0x5c0a	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:43.587486029 CEST	192.168.2.3	8.8.8.8	0x8b39	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:51.708564043 CEST	192.168.2.3	8.8.8.8	0x5436	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:57.199040890 CEST	192.168.2.3	8.8.8.8	0x8f13	Standard query (0)	messaging.engagement.office.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:57.697922945 CEST	192.168.2.3	8.8.8.8	0xb438	Standard query (0)	c.live.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:58.218815088 CEST	192.168.2.3	8.8.8.8	0xd21b	Standard query (0)	amcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:59.027538061 CEST	192.168.2.3	8.8.8.8	0x246	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:59.199142933 CEST	192.168.2.3	8.8.8.8	0x9cdb	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:59.496953011 CEST	192.168.2.3	8.8.8.8	0x3c65	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:11.410109997 CEST	192.168.2.3	8.8.8.8	0x3c87	Standard query (0)	verbena-woolly-clutch.glitch.me	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.546941042 CEST	192.168.2.3	8.8.8.8	0x4dbf	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.548346043 CEST	192.168.2.3	8.8.8.8	0x47da	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.550493956 CEST	192.168.2.3	8.8.8.8	0xbf11	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.853821039 CEST	192.168.2.3	8.8.8.8	0x28ee	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.920520067 CEST	192.168.2.3	8.8.8.8	0x1f61	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jun 30, 2022 18:44:02.248027086 CEST	192.168.2.3	8.8.8.8	0xfb34	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 18:42:38.185444117 CEST	8.8.8.8	192.168.2.3	0x145f	No error (0)	1drv.ms		13.107.42.12	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:38.191809893 CEST	8.8.8.8	192.168.2.3	0xf378	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:38.191809893 CEST	8.8.8.8	192.168.2.3	0xf378	No error (0)	clients.l.google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:38.196875095 CEST	8.8.8.8	192.168.2.3	0x6a2	No error (0)	accounts.google.com		142.251.36.205	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:39.177510977 CEST	8.8.8.8	192.168.2.3	0xc1ff	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:42.008594036 CEST	8.8.8.8	192.168.2.3	0xb6f3	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:42.030064106 CEST	8.8.8.8	192.168.2.3	0x5c0a	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:42.921627998 CEST	8.8.8.8	192.168.2.3	0xb751	No error (0)	onenote.wac.trafficmanager.net.b-0016.b-msedge.net	b-0016.b-msedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 18:42:42.921627998 CEST	8.8.8.8	192.168.2.3	0xb751	No error (0)	b-0016.b-msedge.net		13.107.6.171	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:43.616445065 CEST	8.8.8.8	192.168.2.3	0x8b39	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:51.727365017 CEST	8.8.8.8	192.168.2.3	0x5436	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:57.226531029 CEST	8.8.8.8	192.168.2.3	0x8f13	No error (0)	messaging.engagement.office.com	prod-campaignaggregator.omexexternallfb.office.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:57.723500967 CEST	8.8.8.8	192.168.2.3	0xb438	No error (0)	c.live.com	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:57.723500967 CEST	8.8.8.8	192.168.2.3	0xb438	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	No error (0)	amcdn.msftauth.net	mecontrol-prod.azurefd.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	No error (0)	mecontrol-prod.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	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 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:58.252754927 CEST	8.8.8.8	192.168.2.3	0xd21b	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:58.426589966 CEST	8.8.8.8	192.168.2.3	0xf7f5	No error (0)	c-bing-com.a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:58.426589966 CEST	8.8.8.8	192.168.2.3	0xf7f5	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:58.426589966 CEST	8.8.8.8	192.168.2.3	0xf7f5	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:59.046216965 CEST	8.8.8.8	192.168.2.3	0x246	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:59.046216965 CEST	8.8.8.8	192.168.2.3	0x246	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:59.046216965 CEST	8.8.8.8	192.168.2.3	0x246	No error (0)	db3pcor006-com.be.1drv.com	i-db3p-cor006.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:59.046216965 CEST	8.8.8.8	192.168.2.3	0x246	No error (0)	i-db3p-cor006.api.p001.1drv.com		13.104.208.165	A (IP address)	IN (0x0001)
Jun 30, 2022 18:42:59.224668980 CEST	8.8.8.8	192.168.2.3	0x9cdb	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:59.386162996 CEST	8.8.8.8	192.168.2.3	0x6d48	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:42:59.517972946 CEST	8.8.8.8	192.168.2.3	0x3c65	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:09.738847017 CEST	8.8.8.8	192.168.2.3	0x9171	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:11.431724072 CEST	8.8.8.8	192.168.2.3	0x3c87	No error (0)	verbena-woolly-clutch.glitch.me		52.22.91.148	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:11.431724072 CEST	8.8.8.8	192.168.2.3	0x3c87	No error (0)	verbena-woolly-clutch.glitch.me		35.175.8.217	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:11.431724072 CEST	8.8.8.8	192.168.2.3	0x3c87	No error (0)	verbena-woolly-clutch.glitch.me		52.201.197.170	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 18:43:11.431724072 CEST	8.8.8.8	192.168.2.3	0x3c87	No error (0)	verbena-woolly-clutch.glitch.me		52.3.67.232	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.563955069 CEST	8.8.8.8	192.168.2.3	0x4dbf	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:12.567298889 CEST	8.8.8.8	192.168.2.3	0x47da	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.567298889 CEST	8.8.8.8	192.168.2.3	0x47da	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.572022915 CEST	8.8.8.8	192.168.2.3	0xbf11	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:12.870739937 CEST	8.8.8.8	192.168.2.3	0xd41e	No error (0)	gstaticadssl.l.google.com		142.251.36.227	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.874304056 CEST	8.8.8.8	192.168.2.3	0x28ee	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.874304056 CEST	8.8.8.8	192.168.2.3	0x28ee	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)
Jun 30, 2022 18:43:12.942642927 CEST	8.8.8.8	192.168.2.3	0x1f61	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:47.880269051 CEST	8.8.8.8	192.168.2.3	0x2b10	No error (0)	onenote.wac.trafficmanager.net.b-0016.b-msedge.net	b-0016.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 18:43:47.880269051 CEST	8.8.8.8	192.168.2.3	0x2b10	No error (0)	b-0016.b-msedge.net		13.107.6.171	A (IP address)	IN (0x0001)
Jun 30, 2022 18:44:02.276420116 CEST	8.8.8.8	192.168.2.3	0xfb34	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- 1drv.ms
- clients2.google.com
- https:
  - onenote.officeapps.live.com
  - amcdn.msftauth.net
  - c.bing.com
  - storage.live.com
  - verbena-woolly-clutch.glitch.me
  - maxcdn.bootstrapcdn.com
  - cdnjs.cloudflare.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49745	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:39 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

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:39 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-06-30 16:42:39 UTC	4	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 30 Jun 2022 16:42:39 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-ddEZLQE_6QAY_1BUIonZIQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-ddEZLQE_6QAY_1BUIonZIQ' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin 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=* 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 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 16:42:39 UTC	5	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-06-30 16:42:39 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	13.107.42.12	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:39 UTC	0	OUT	GET /o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9 HTTP/1.1 Host: 1drv.ms Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:42:39 UTC	3	IN	HTTP/1.1 301 Moved Permanently Location: https://onedrive.live.com/redir?resid=1F6FC88150FE397E!35197&authkey=!AoF88NbpYZfqkJE&ithint=onenote&e=yvEgUVzG9ES2PfoKuGIEfw&at=9 X-MSNSERVER: AM4PPF2F3C280BE Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: BTY3lSiBDE26i9K3ynfdwg.0 X-AsmVersion: UNKNOWN; 19.946.620.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 6727003FAD084753A3A3A3D81E131661 Ref B: FRAEDGE1312 Ref C: 2022-06-30T16:42:39Z Date: Thu, 30 Jun 2022 16:42:38 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49790	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:44 UTC	278	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":3,"MsSinceStart":862,"Value":"Get cells response received:200","Type":"BootLogs"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:45 UTC	281	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":4,"MsSinceStart":868,"Value":"Launching FastView from entry point WacBootGetCells","Type":"BootLogs"},{"Index":5,"MsSinceStart":871,"Value":"RecordContentDisplayed","Type":"BootPhaseCompleted"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:45 UTC	283	OUT	POST /o/OneNoteS2SHandler.ashx?action=educationuser&WOPIsrc=https%3A%2F%2Fwopi%2Eonedrive%2Ecom%2Fwopi%2Ffolders%2F1F6FC88150FE397E%2135197&access_token=4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF%2DynTSOSveEi0XEaPSoAexqp7%2D12GLVzZG1WjgR%2DaZoeDjLwtY20zVT5%2DXDPGmWP14AVg&access_token_ttl=1658421761813 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 haep: 1 X-WacFrontEnd: AM4PEPF00006B54 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync Content-Type: application/x-www-form-urlencoded; charset=UTF-8 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 X-Requested-With: XMLHttpRequest X-UserType: WOPI X-xhr: 1 X-IsCoauthSession: false X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:45 UTC	285	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":6,"MsSinceStart":2359,"Value":"SplashScreenShown","Type":"BootPhaseCompleted"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:51 UTC	288	OUT	GET /o/GetImage.ashx?&WOPIsrc=https%3A%2F%2Fwopi%2Eonedrive%2Ecom%2Fwopi%2Ffiles%2F1F6FC88150FE397E%2135199&access_token=4wpOZfRrABcyXY4FJ0rgBz2V4z1L7vFQI10PJ%5FJNhBPOJfHXO%5FtxF5Xpte3oLpRjEw2j0n7aG1SmfzD1yTc5YUTbFU3TAQKAQRZpxLVZ%5FFGBPB17bmmVXmW8%2DXmT2g7MBJUd%5Fu4GMZmdWmWWaVsRfMEw&access_token_ttl=1658421761813&ObjectDataBlobId=%7B964778b5-12c8-4a0e-843d-7c7be63d40bc%7D%7B1%7D&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&build=16.0.15417.41022&waccluster=PNL1&wdwacuseragent=MSWACONSync&DataUrlEnabled=true HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive haep: 1 X-WacFrontEnd: AM4PEPF00006B54 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync 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 X-Requested-With: XMLHttpRequest X-UserType: WOPI X-xhr: 1 X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8lJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:10 UTC	511	IN	Data Raw: 4e 58 69 37 78 4a 4e 34 78 38 55 61 31 72 4e 31 4c 35 74 31 66 33 4d 30 7a 66 56 6e 33 62 66 2f 41 42 37 62 2f 77 41 42 72 78 63 30 78 63 73 4e 43 4d 49 66 61 50 31 62 77 39 34 66 77 2b 63 34 79 72 69 4d 58 48 6d 68 53 35 66 64 2f 6d 6b 2f 68 76 35 61 4d 69 31 7a 78 4a 71 76 69 36 2b 6e 76 64 57 31 47 62 55 4c 36 54 37 38 30 31 79 58 50 36 2f 64 58 2f 5a 72 4f 70 31 46 66 46 50 58 56 6e 39 57 30 36 63 4b 56 4e 55 36 61 73 68 74 46 4f 6f 70 47 6f 32 69 6e 55 55 41 4e 6f 6f 6f 6f 41 4b 4b 4b 4b 41 43 69 69 69 67 44 70 2f 68 4c 38 66 64 64 2b 41 66 78 45 47 72 61 56 4e 39 70 30 75 66 79 30 76 74 4d 64 39 73 4d 38 58 2f 41 4c 4b 36 2f 77 41 50 39 33 2f 64 33 4c 58 36 6e 2f 44 48 34 71 36 46 38 57 76 42 31 6a 34 6b 30 43 37 45 74 6e 63 66 49 38 5a 47 4a 4c 64 Data Ascii: NXi7xJN4x8Ua1rN1L5t1f3M0zfVn3bf/AB7b/wABrxc0xcsNCMIfaP1bw94fw+c4yriMXHmhS5fd/mk/hv5aMi1z xJqvi6+nvdW1GbUL6T7801yXP6/dX/ZrOp1FfFPXVn9W06cKVNU6ashtFOopGo2inUUANoooAKKKKACiiigDp/hL8 fdd+AfxEGraVN9p0ufy0vtMd9sM8X/ALK6/wAP93/d3LX6n/DH4q6F8WvB1j4k0C7EtncfI8ZGJLd
2022-06-30 16:43:10 UTC	519	IN	Data Raw: 4f 41 55 55 55 55 41 46 46 46 46 41 46 44 56 2f 2b 51 62 66 66 39 63 6d 2f 77 44 51 61 2f 44 46 37 36 48 37 52 2f 72 66 34 2f 38 41 32 61 76 33 4e 31 62 2f 41 4a 42 74 39 2f 31 78 62 2f 30 47 76 77 59 6b 2f 77 43 57 2f 77 44 77 4b 76 6b 4f 49 50 38 41 6c 31 38 2f 30 50 36 46 38 4a 36 6e 4a 48 47 2f 39 75 66 2b 33 47 76 39 75 67 2f 35 36 30 66 62 6f 50 38 41 6e 72 57 54 52 58 79 4a 2b 2f 38 41 74 35 6d 74 39 75 67 2f 35 36 30 66 62 6f 50 2b 65 74 5a 4e 4e 6f 44 36 31 49 32 50 74 30 48 2f 41 44 31 6f 2b 33 51 66 38 39 61 78 36 4b 42 2f 57 57 62 48 32 36 44 2f 41 4a 36 30 66 62 6f 50 2b 65 74 59 39 4f 6f 44 36 31 49 31 76 74 30 48 2f 50 57 6a 37 64 42 2f 7a 31 72 48 6f 6f 44 36 77 7a 59 2b 33 51 2f 38 39 66 38 41 30 4b 6a 37 64 44 2f 7a 31 2f 38 41 51 71 78 Data Ascii: OAUUUUAFFFFAFDV/+Qbff9cm/wDQa/DF76H7R/rf4/8A2av3N1b/AJBt9/1xb/0GvwYk/wCW/wDwKv kOIP8Al18/0P6F8J6nJHG/9uf+3Gv9ug/560fboP8AnrWTRXyJ+/8At5mt9ug/560fboP+etZNNoD61I2Pt0H/AD1o +3Qf89ax6KB/WWbH26D/AJ60fboP+etY9OoD61I1vt0H/PWj7dB/z1rHooD6wzY+3Q/89f8A0Kj7dD/z1/8AQqx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49814	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:51 UTC	290	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":7,"MsSinceStart":8127,"Value":"RecordAppInteractive","Type":"BootPhaseCompleted"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E =P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCooki e=00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000
2022-06-30 16:42:51 UTC	291	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 3b9ef0f5-7597-458f-b64d-b85009eb7ab0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF0000695E X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF0000695E X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_excelslice_control,afd_onenoteslice_control,afd_wacinfra4 ,afd_wacinfra5 X-MSEdge-Ref: Ref A: 930FE8F0AFE8404287250C9A34175D1C Ref B: AM3EDGE0220 Ref C: 2022-06-30T16:42:51Z Date: Thu, 30 Jun 2022 16:42:51 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49827	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:52 UTC	292	OUT	POST /o/RemoteTelemetry.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 125 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:53 UTC	294	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 15479 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E =P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCooki e=0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000
2022-06-30 16:42:53 UTC	296	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 37 36 35 39 36 32 2c 22 4c 22 3a 5b 7b 22 47 22 3a 32 30 30 32 35 36 37 39 2c 22 54 22 3a 2d 33 32 32 2c 22 4d 22 3a 22 53 65 74 41 70 70 49 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 53 74 61 74 75 73 3a 20 61 70 70 43 74 6f 72 53 74 61 72 74 69 6e 67 22 2c 22 43 22 3a 33 30 36 2c 22 44 22 3a 35 30 7d 2c 7 b 22 47 22 3a 35 39 32 34 38 37 38 39 32 2c 22 54 22 3a 2d 32 35 33 2c 22 4d 22 3a 22 49 73 48 6f 73 74 46 72 61 6d 65 54 72 75 73 74 65 64 3a 32 22 2c 22 43 22 3a 33 30 36 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 33 39 30 38 39 31 31 33 2c 22 54 22 3a 2d 32 34 36 2c 22 4d 22 3a 22 53 53 45 44 3a 73 74 61 72 74 73 65 73 73 69 6f 6e 20 69 6e 66 6f 20 73 65 6e 74 20 74 6f 20 4f 74 65 6c 22 2c 22 43 22 3a 33 30 36 2c 22 44 Data Ascii: {"T":1656639765962,"L":[{"G":20025679,"T":-322,"M":"SetAppInitializationStatus: appCtorStarting","C":306,"D" :50},{"G":592487892,"T":-253,"M":"IsHostFrameTrusted:2","C":306,"D":50},{"G":39089113,"T":-246,"M":"SSED:start session info sent to Otel","C":306,"D
2022-06-30 16:42:53 UTC	311	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 5d61ba41-3754-446c-9c60-aed51533a092 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006021 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X- bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006021 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_visioslice,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 3327F7E3739D4CD0A8C6327764CE0AB0 Ref B: AMS04EDGE2911 Ref C: 2022-06-30T16:42:5 3Z Date: Thu, 30 Jun 2022 16:42:52 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49829	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:53 UTC	313	OUT	POST /o/RemoteUls.ashx?usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&officeserverversion=16.0.15417.41022 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 4871 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:54 UTC	321	OUT	GET /o/App_Scripts/Acl/Acl1033.js HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49743	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:39 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:42:39 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-aJbZGsmIZ_8p602p-Mgkxg' '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 16:42:39 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5659 X-Daystart: 34959 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 16:42:39 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 33 34 39 35 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" protocol="2.0" server="prod"><daystart elapsed_days="5659" elapsed_seconds="34959"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-06-30 16:42:39 UTC	3	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="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-06-30 16:42:39 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49864	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:57 UTC	342	OUT	POST /o/RemoteTelemetry.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 27992 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	372	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 52564 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E =P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCooki e=00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000; ShCLSessionID=1656639775607_0.6675230212797223; BP=l=SDX.Skydrive& FR=&ST=
2022-06-30 16:42:58 UTC	373	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 37 37 33 31 38 34 2c 22 4c 22 3a 5b 7b 22 47 22 3a 34 31 35 34 33 33 38 30 2c 22 54 22 3a 33 34 2c 22 4d 22 3a 22 46 69 6e 69 73 68 65 64 20 72 65 6e 64 65 72 69 6e 67 20 64 65 6c 61 79 65 64 20 6f 75 74 6c 69 6e 65 73 20 70 6f 73 74 2d 62 6f 6f 74 22 2c 22 43 22 3a 33 33 39 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 35 31 34 30 31 38 30 32 2c 22 54 22 3a 33 35 2c 22 4d 22 3a 22 52 65 73 70 6f 6e 73 65 20 72 65 61 64 79 20 66 6f 72 20 68 74 74 70 73 3a 2f 2f 6f 66 66 69 63 65 63 6c 69 65 6e 74 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 6 3 6f 6e 66 69 67 31 36 3f 66 6c 69 67 68 74 73 3d 43 6c 69 65 6e 74 2e 52 65 73 6f 75 72 63 65 53 65 72 76 69 63 65 34 48 69 64 64 65 6e 56 32 26 73 65 72 76 69 63 65 73 3d 52 65 73 6f Data Ascii: {"T":1656639773184,"L":[{"G":41543380,"T":34,"M":"Finished rendering delayed outlines post-boot","C":339,"D" :50},{"G":51401802,"T":35,"M":"Response ready for https://officeclient.microsoft.com/config16?flights=Client.ResourceSer vice4HiddenV2&services=Reso
2022-06-30 16:42:58 UTC	389	OUT	Data Raw: 65 6e 74 5c 22 2c 5c 22 6b 65 79 5c 22 3a 5c 22 53 75 69 74 65 48 65 61 64 65 72 3a 46 69 72 73 74 52 65 6e 64 65 72 2d 53 75 69 74 65 48 65 61 64 65 72 3a 43 6f 6e 73 74 72 75 63 74 6f 72 5c 22 2c 5c 22 73 74 61 72 74 54 69 6d 65 5c 22 3a 31 31 39 31 36 2e 38 33 35 30 30 30 30 30 30 30 30 30 36 2c 5c 22 65 6e 64 54 69 6d 65 5c 22 3a 31 33 30 30 30 2e 35 39 30 30 30 30 30 30 30 30 30 30 32 2c 5c 22 64 75 72 61 74 69 6f 6e 4d 73 5c 22 3a 31 30 38 34 7d 22 2c 22 43 22 3a 33 34 30 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 35 39 35 38 35 35 31 38 32 2c 22 54 22 3a 32 39 32 31 2c 22 4d 22 3a 22 52 65 61 63 74 48 65 61 64 65 72 20 66 69 72 73 74 20 72 65 6e 64 65 72 20 74 69 6d 65 3a 20 31 30 38 34 20 6d 73 22 2c 22 43 22 3a 33 34 30 2c 22 44 22 3a 35 30 7d 2c 7b 22 Data Ascii: ent\",\"key\":\"SuiteHeader:FirstRender-SuiteHeader:Constructor\",\"startTime\":11916.835000000006 ,\"endTime\":13000.590000000002,\"durationMs\":1084}","C":340,"D":50},{"G":595855182,"T":2921,"M":"ReactHeader first render time: 1084 ms","C":340,"D":50},{"
2022-06-30 16:42:58 UTC	405	OUT	Data Raw: 74 61 72 74 5c 22 3a 5c 22 30 5c 22 2c 5c 22 52 65 64 69 72 65 63 74 45 6e 64 5c 22 3a 5c 22 30 5c 22 2c 5c 22 46 65 74 63 68 53 74 61 72 74 5c 22 3a 5c 22 32 39 34 32 2e 33 39 5c 22 2c 5c 22 44 6f 6d 61 69 6e 4c 6f 6f 6b 75 70 53 74 61 72 74 5c 22 3a 5c 22 33 37 38 33 2e 33 5c 22 2c 5c 22 44 6f 6d 61 69 6e 4c 6f 6f 6b 75 70 45 6e 64 5c 22 3a 5c 22 33 37 38 33 2e 33 32 5c 22 2c 5c 22 43 6f 6e 6e 65 63 74 53 74 61 72 74 5c 22 3a 5c 22 33 37 38 33 2e 33 32 5c 22 2c 5c 22 43 6f 6e 6e 65 63 74 45 6e 64 5c 22 3a 5c 22 34 33 34 36 2e 32 31 5c 22 2c 5c 22 53 65 63 75 72 65 43 6f 6e 6e 65 63 74 69 6f 6e 53 74 61 72 74 5c 22 3a 5c 22 33 37 38 36 2e 30 33 5c 22 2c 5c 22 52 65 71 75 65 73 74 53 74 61 7 2 74 5c 22 3a 5c 22 34 33 34 37 2e 33 34 35 5c 22 2c 5c 22 52 65 Data Ascii: tart\":\"0\",\"RedirectEnd\":\"0\",\"FetchStart\":\"2942.39\",\"DomainLookupStart\":\"3783.3\",\"DomainLooku pEnd\":\"3783.32\",\"ConnectStart\":\"3783.32\",\"ConnectEnd\":\"4346.21\",\"SecureConnectionStart\":\"3786.03\",\"Reque stStart\":\"4347.345\",\"Re
2022-06-30 16:42:58 UTC	421	OUT	Data Raw: 65 76 69 65 77 43 72 69 74 69 71 75 65 73 46 69 6c 74 65 72 2e 46 69 6c 74 65 72 69 6e 67 42 65 66 6f 72 65 49 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 2c 4f 66 66 69 63 65 2e 44 6f 63 73 2e 53 68 61 72 65 64 43 6f 6d 6d 65 6e 74 73 2e 43 6f 6d 6d 69 74 43 6f 6d 6d 65 6e 74 2c 4f 66 66 69 63 65 2e 44 6f 63 73 2e 53 68 61 72 65 64 43 6f 6d 6d 65 6e 74 73 2e 44 69 73 63 61 72 64 44 72 61 66 74 41 73 79 6e 63 5c 22 2c 5c 22 74 61 73 6b 44 75 72 61 74 69 6f 6e 4c 6f 67 46 72 65 71 75 65 6e 63 79 5c 22 3a 32 30 2c 5c 22 74 61 73 6b 44 75 72 61 74 69 6f 6e 4c 6f 67 54 68 72 65 73 68 6f 6c 64 5c 22 3a 31 30 30 2c 5c 22 72 65 70 6f 72 74 54 61 73 6b 44 65 74 61 69 6c 73 5c 22 3a 66 61 6c 73 65 7d 22 2 c 22 43 22 3a 32 32 35 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a Data Ascii: eviewCritiquesFilter.FilteringBeforeInitialization,Office.Docs.SharedComments.CommitComment,Office .Docs.SharedComments.DiscardDraftAsync\",\"taskDurationLogFrequency\":20,\"taskDurationLogThreshold\":100,\"re portTaskDetails\":false}","C":225,"D":50},{"G":

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	425	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 32889ec7-d3f4-42c7-9f27-43f9ee517248 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006B53 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006B53 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: B46F706468DC4F608C3BD047912E3CCC Ref B: AM3EDGE0321 Ref C: 2022-06-30T16:42:58Z Date: Thu, 30 Jun 2022 16:42:57 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49872	13.107.219.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	426	OUT	GET /me?partner=OneNoteOnline&version=10.21153.1&market=EN-US&wrapperId=suiteshell HTTP/1.1 Host: amcdn.msftauth.net Connection: keep-alive Origin: https://onenote.officeapps.live.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://onenote.officeapps.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:42:58 UTC	429	IN	HTTP/1.1 200 OK Cache-Control: public, no-transform, max-age=43200 Content-Length: 29999 Content-Type: application/javascript Expires: Fri, 01 Jul 2022 04:42:58 GMT X-Cache: CONFIG_NOCACHE X-Content-Type-Options: nosniff Access-Control-Allow-Origin: * X-UA-Compatible: IE=edge Strict-Transport-Security: max-age=31536000; includeSubDomains X-Azure-Ref-OriginShield: 0ktK9YgAAAADA+KC+C3zsQKGdaFbS7qrgQU1TMDRFREdFMTgwNgBlYWM1ZjQ5Zi1lMDJkLTRmNDEtYjBhNi0yZDUwZjlmY2Y4NGE= X-Azure-Ref: 0ktK9YgAAAAB2WyagFUPTTIVpBfzu8qKTRlJBMjMxMDUwNDE4MDQ3ADlmZTZjM2YxLTE3MTgtNGE5My05MjU1LTYzY2QzZjhjYTVhYg== Date: Thu, 30 Jun 2022 16:42:57 GMT Connection: close
2022-06-30 16:42:58 UTC	430	IN	Data Raw: 77 69 6e 64 6f 77 2e 4d 53 41 3d 77 69 6e 64 6f 77 2e 4d 53 41 7c 7c 7b 7d 3b 77 69 6e 64 6f 77 2e 4d 53 41 2e 4d 65 43 6f 6e 74 72 6f 6c 3d 77 69 6e 64 6f 77 2e 4d 53 41 2e 4d 65 43 6f 6e 74 72 6f 6c 7c 7c 7b 7d 3b 77 69 6e 64 6f 77 2e 4d 53 41 2e 4d 65 43 6f 6e 74 72 6f 6c 2e 43 6f 6e 66 69 67 3d 7b 22 76 65 72 22 3a 22 31 30 2e 32 32 31 30 38 2e 32 22 2c 22 6d 6b 74 22 3a 22 65 6e 2d 55 53 22 2c 22 70 74 6e 22 3a 22 6f 6e 65 6e 6f 74 65 6f 6e 6c 69 6e 65 22 2c 22 67 66 78 22 3a 22 68 74 74 70 73 3a 2f 2f 61 6d 63 64 6e 2e 6d 73 66 74 61 75 74 68 2e 6e 65 74 22 2c 22 64 62 67 22 3a 66 61 6c 73 65 2c 22 61 61 64 22 3a 74 72 75 65 2c 22 69 6e 74 22 3a 66 61 6c 73 65 2c 22 70 78 79 22 3a 74 72 75 65 2c 22 6d 73 54 78 74 22 3a 66 61 6c 73 65 2c 22 72 77 64 Data Ascii: window.MSA=window.MSA||{};window.MSA.MeControl=window.MSA.MeControl||{};window.MSA.MeControl.Config={"ver":"10.22108.2","mkt":"en-US","ptn":"onenoteonline","gfx":"https://amcdn.msftauth.net","dbg":false,"aad":true,"int":false,"pxy":true,"msTxt":false,"rwd

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	433	IN	Data Raw: 63 65 2e 6e 6f 77 28 29 7d 2c 68 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 70 2e 70 65 72 66 6f 72 6d 61 6e 63 65 26 26 70 2e 70 65 72 66 6f 72 6d 61 6e 63 65 2e 67 65 74 45 6e 74 72 69 65 73 3f 77 69 6e 64 6f 77 2e 70 65 72 66 6f 72 6d 61 6e 63 65 2e 67 65 74 45 6e 74 72 69 65 73 28 29 3a 5b 5d 7d 2c 79 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 70 2e 6c 6f 63 61 74 69 6f 6e 7d 3b 76 61 72 20 65 3d 70 2e 72 65 71 75 65 73 74 41 6e 69 6d 61 74 69 6f 6e 46 72 61 6d 65 3f 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 70 2e 72 65 71 75 65 73 74 41 6e 69 6d 61 74 69 6f 6e 46 72 61 6d 65 28 65 29 7d 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 Data Ascii: ce.now()},h=function(){return p.performance&&p.performance.getEntries?window.performance.getEntries():[]},y=function(){return p.location};var e=p.requestAnimationFrame?function(e){return p.requestAnimationFrame(e)}:function(e){return setTimeout(function()
2022-06-30 16:42:58 UTC	441	IN	Data Raw: 7d 29 7d 63 61 74 63 68 28 65 29 7b 69 66 28 74 29 72 65 74 75 72 6e 3b 74 3d 21 30 2c 55 65 28 6e 2c 65 29 7d 7d 4d 65 2e 70 72 6f 74 6f 74 79 70 65 2e 63 61 74 63 68 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 74 68 65 6e 28 6e 75 6c 6c 2c 65 29 7d 2c 4d 65 2e 70 72 6f 74 6f 74 79 70 65 2e 74 68 65 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 76 61 72 20 74 3d 6e 65 77 20 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 28 50 65 29 3b 72 65 74 75 72 6e 20 4f 65 28 74 68 69 73 2c 6e 65 77 20 5f 65 28 65 2c 6e 2c 74 29 29 2c 74 7d 2c 4d 65 2e 70 72 6f 74 6f 74 79 70 65 2e 66 69 6e 61 6c 6c 79 3d 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 76 61 72 20 74 3d 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3b 72 65 74 75 72 6e 20 74 Data Ascii: }}}catch(e){if(t)return;t=!0,Ue(n,e)}}Me.prototype.catch=function(e){return this.then(null,e)},Me.prototype.then=function(e,n){var t=new this.constructor(Pe);return Oe(this,new _e(e,n,t)),t},Me.prototype.finally=function(n){var t=this.constructor;return t
2022-06-30 16:42:58 UTC	445	IN	Data Raw: 29 7b 76 61 72 20 65 3d 75 28 29 2c 6e 3d 22 42 75 6e 64 6c 65 20 64 6f 77 6e 6c 6f 61 64 20 74 69 6d 65 64 20 6f 75 74 22 3b 6e 6e 28 73 2c 65 2c 63 2c 21 30 2c 6e 29 2c 61 28 41 28 6e 2b 22 3a 20 22 2b 73 2b 22 20 28 22 2b 63 2b 22 29 22 2c 21 30 29 29 7d 2c 6d 2e 43 6f 6e 66 69 67 2e 74 69 6d 65 6f 75 74 4d 73 29 3b 66 75 6e 63 74 69 6f 6e 20 75 28 29 7b 72 65 74 75 72 6e 20 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 72 29 2c 74 26 26 28 74 2e 6f 6e 65 72 72 6f 72 3d 74 2e 6f 6e 6c 6f 61 64 3d 76 6f 69 64 20 30 2c 74 3d 76 6f 69 64 20 30 29 2c 67 28 29 2d 65 7d 74 2e 6f 6e 6c 6f 61 64 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 75 28 29 3b 65 6e 28 29 3b 76 61 72 20 6e 3d 4b 65 28 73 29 2c 72 3d 6e 26 26 6e 2e 65 78 70 6f 72 74 73 3b 69 66 28 Data Ascii: }{var e=u(),n="Bundle download timed out";nn(s,e,c,!0,n),a(A(n+": "+s+" ("+c+")",!0))},m.Config.timeoutMs);function u(){return clearTimeout(r),t&&(t.onerror=t.onload=void 0,t=void 0),g()-e}t.onload=function(e){var t=u();en();var n=Ke(s),r=n&&n.exports;if(
2022-06-30 16:42:58 UTC	453	IN	Data Raw: 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 6e 75 6c 6c 21 3d 65 2e 6d 65 6d 62 65 72 4e 61 6d 65 26 26 30 3c 65 2e 6d 65 6d 62 65 72 4e 61 6d 65 2e 6c 65 6e 67 74 68 7d 28 65 29 3b 63 61 73 22 6d 73 61 22 3a 63 61 73 65 22 6d 73 61 46 65 64 22 3a 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 6e 75 6c 6c 21 3d 65 2e 6d 65 6d 62 65 72 4e 61 6d 65 26 26 30 3c 65 2e 6d 65 6d 62 65 72 4e 61 6d 65 2e 6c 65 6e 67 74 68 7d 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 53 6e 28 65 29 7b 69 66 28 62 6e 28 65 29 29 73 77 69 74 63 68 28 65 2e 69 64 70 29 7b 63 61 73 65 22 61 61 64 22 3a 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 7b 74 79 70 65 3a 22 61 61 64 22 2c 61 75 74 68 65 6e 74 Data Ascii: tion(e){return e&&null!=e.memberName&&0<e.memberName.length}(e);case"msa":case"msaFed":return function(e){return e&&null!=e.memberName&&0<e.memberName.length}(e)}}function Sn(e){if(bn(e))switch(e.idp){case"aad":return function(e){return{type:"aad",authent

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49873	204.79.197.200	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	427	OUT	GET /c.gif?DI=15347&wlxid=a94776a0-ee2a-458a-9854-05b95ebe50e6&reqid=002b179adb0&csiperf=ANON%3D%26NL%3D0%26TP%3D0%26CL%3DRDE42AAC93A338%26MA%3Den-US%26B%3D0.0.0%26TR%3DNA%252ANA%252A%253ASDX.Skydrive%252AWac.view.F.U.%26PLT%3D17047%26IR%3D1%26EX%3D0%26L.h%3D1987%26L.bc%3D2132%26L.ac%3D2132%26L.f%3D2304%26L.sjs%3D16442%26L.ttg%3D10992%26C.st%3D1656639760502%26N.domIn%3D2304%26N.tcp%3D73%26N.req%3D1590%26N.resp%3D33%26N.navType%3D0%26N.redirectCount%3D0&r=0.26911081202565157&CtsSyncId=DA428D9AB9444AF192DAC7E040F48A7F&RedC=c.live.com&MXFR=210011B4A40D624F14CA0067A00D667C HTTP/1.1 Host: c.bing.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: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	428	IN	HTTP/1.1 302 Redirect Cache-Control: private, no-cache, proxy-revalidate, no-store Pragma: no-cache Location: https://c.live.com/c.gif?DI=15347&wlxid=a94776a0-ee2a-458a-9854-05b95ebe50e6&reqid=002b179adb0&csiperf=ANON%3D%26NL%3D0%26TP%3D0%26CL%3DRDE42AAC93A338%26MA%3Den-US%26B%3D0.0.0%26TR%3DNA%252ANA%252A%253ASDX.Skydrive%252AWac.view.F.U.%26PLT%3D17047%26IR%3D1%26EX%3D0%26L.h%3D1987%26L.bc%3D2132%26L.ac%3D2132%26L.f%3D2304%26L.sjs%3D16442%26L.ttg%3D10992%26C.st%3D1656639760502%26N.domIn%3D2304%26N.tcp%3D73%26N.req%3D1590%26N.resp%3D33%26N.navType%3D0%26N.redirectCount%3D0&r=0.26911081202565157&CtsSyncId=DA428D9AB9444AF192DAC7E040F48A7F&MUID=210011B4A40D624F14CA0067A00D667C P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" Set-Cookie: MUID=210011B4A40D624F14CA0067A00D667C; domain=.bing.com; expires=Tue, 25-Jul-2023 16:42:58 GMT; path=/; SameSite=None; Secure; Priority=High; Set-Cookie: SRM_B=210011B4A40D624F14CA0067A00D667C; domain=c.bing.com; expires=Tue, 25-Jul-2023 16:42:58 GMT; path=/; SameSite=None; Secure; Set-Cookie: SRM_L=210011B4A40D624F14CA0067A00D667C; domain=c.bing.com; expires=Tue, 25-Jul-2023 16:42:58 GMT; path=/; SameSite=None; Secure; X-Powered-By: ASP.NET X-Cache: CONFIG_NOCACHE Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: AAB04858CEFA4D6696D3ADB366684A00 Ref B: FRAEDGE1210 Ref C: 2022-06-30T16:42:58Z Date: Thu, 30 Jun 2022 16:42:58 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49877	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	459	OUT	GET /o/AddinServiceHandler.ashx?action=laststoreupdate&app=4&lc=EN-US&WOPIsrc=https%3A%2F%2Fwopi%2Eonedrive%2Ecom%2Fwopi%2Ffolders%2F1F6FC88150FE397E%2135197&access_token=4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF%2DynTSOSveEi0XEaPSoAexqp7%2D12GLVzZG1WjgR%2DaZoeDjLwtY20zVT5%2DXDPGmWP14AVg&access_token_ttl=1658421761813 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive haep: 1 X-WacFrontEnd: AM4PEPF00006B54 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync 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 X-Requested-With: XMLHttpRequest X-UserType: WOPI X-xhr: 1 X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:58 UTC	461	IN	HTTP/1.1 403 Forbidden Cache-Control: private Content-Length: 1233 Content-Type: text/html P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 8c75f87c-e98a-45f3-a97f-6626d22dd69c X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006961 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 X-OFFICEFD: AM4PEPF00006961 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 59A74E99FA8641E288D31293CEBB9B15 Ref B: AMS04EDGE2021 Ref C: 2022-06-30T16:42:58Z Date: Thu, 30 Jun 2022 16:42:58 GMT Connection: close
2022-06-30 16:42:58 UTC	462	IN	Data Raw: 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 53 74 72 69 63 74 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 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 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 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 2d 20 46 6f 72 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>403 - For

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49881	13.104.208.165	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:59 UTC	463	OUT	GET /mydata/myprofile/expressionprofile/profilephoto:UserTileStatic,UserTileSmall/MeControlMediumUserTile?ck=1&ex=24&fofoff=1&sc=1656639779208 HTTP/1.1 Host: storage.live.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-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://onenote.officeapps.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8lJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; BP=l=SDX.Skydrive&FR=&ST=; MUID=210011B4A40D624F14CA0067A00D667C
2022-06-30 16:42:59 UTC	464	IN	HTTP/1.1 302 Found Content-Length: 0 Location: https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1656607379&rver=7.3.6962.0&wp=MBI_SSL&wreply=https:%2F%2Fstorage.live.com%2Fstorageservice%2Fpassport%2Fauth.aspx%3Fsru%3Dhttps:%252f%252fstorage.live.com%252fmydata%252fmyprofile%252fexpressionprofile%252fprofilephoto:UserTileStatic%252cUserTileSmall%252fMeControlMediumUserTile&lc=1033&id=63539 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DB3PPF7E67C5F62 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: A1280UtBz0umO86hn7Y4KQ.0 X-QosStats: {"ApiId":0,"ResultType":2,"SourcePropertyId":0,"TargetPropertyId":42} X-ThrowSite: 4212.9205 X-ClientErrorCode: PassportAuthFail X-ErrorCodeChain: Unauthenticated X-AsmVersion: UNKNOWN; 19.934.602.2009 Date: Thu, 30 Jun 2022 16:42:58 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49924	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:05 UTC	466	OUT	GET /o/error/error.html?aspxerrorpath=/o/OneNoteS2SHandler.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive haep: 1 X-WacFrontEnd: AM4PEPF00006B54 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync 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 X-Requested-With: XMLHttpRequest X-UserType: WOPI X-xhr: 1 X-IsCoauthSession: false X-WacCluster: PNL1 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:05 UTC	472	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 34397 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1 033&data=1033; BIGipCookie=0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000; ShCLSessionID=1656639775607_0.6 675230212797223; BP=l=SDX.Skydrive&FR=&ST=; MUID=210011B4A40D624F14CA0067A00D667C; xidseq=4; E=P:tcNhmbda2og=:PJLCcxjKwQVUWFIETez3k69O9vOeDWpicKYwq8SBqKA=:F; wlidperf=latency=238
2022-06-30 16:43:05 UTC	474	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 37 37 38 32 35 38 2c 22 4c 22 3a 5b 7b 22 47 22 3a 34 31 35 30 32 35 35 36 2c 22 54 22 3a 31 2c 22 4d 22 3a 22 4e 6f 20 76 61 6c 75 65 73 20 69 6e 20 6d 65 73 73 61 67 65 22 2c 22 43 22 3a 32 30 34 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 35 39 34 38 39 32 39 32 38 2c 22 54 22 3a 34 37 2c 22 4d 22 3a 22 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 66 75 6e 63 74 69 6f 6e 45 78 65 63 75 74 69 6f 6e 5c 22 2c 5c 22 6b 65 79 5c 22 3a 5c 22 53 74 61 74 75 73 42 61 72 3a 72 65 6e 64 65 72 4f 6e 65 4e 6f 74 65 53 74 61 74 75 73 42 61 72 5c 22 2c 5c 22 73 74 61 72 74 54 69 6d 65 5c 22 3a 31 35 31 37 35 2e 31 34 39 39 39 39 39 39 38 39 2c 5c 22 65 6e 64 54 69 6d 65 5c 22 3a 31 35 32 30 33 2e 30 37 39 39 39 39 39 39 39 38 35 2c Data Ascii: {"T":1656639778258,"L":[{"G":41502556,"T":1,"M":"No values in message","C":204,"D":50},{"G":594892 928,"T":47,"M":"{\"type\":\"functionExecution\",\"key\":\"StatusBar:renderOneNoteStatusBar\",\"startTime\":15175.1499999 99989,\"endTime\":15203.079999999985,
2022-06-30 16:43:05 UTC	490	OUT	Data Raw: 43 22 3a 33 37 31 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 32 30 30 33 30 32 33 36 2c 22 54 22 3a 34 39 38 2c 22 4d 22 3a 22 41 70 70 73 46 6f 72 4f 66 66 69 63 65 50 61 63 6b 61 67 65 3a 3a 49 6e 69 74 3a 20 4f 6e 65 4e 6f 74 65 41 70 70 73 46 6f 72 4f 66 66 69 63 65 49 6e 74 65 67 72 61 74 69 6f 6e 4d 61 6e 61 67 65 72 20 49 6e 69 74 69 61 6c 69 7a 65 22 2c 22 43 22 3a 33 37 31 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 32 30 30 33 30 32 33 37 2c 22 54 22 3a 34 39 39 2c 22 4d 22 3a 22 4f 6e 65 4e 6f 74 65 41 70 70 73 46 6f 72 4f 66 66 69 63 65 55 49 41 63 74 6f 72 3a 3a 52 65 67 69 73 74 65 72 41 63 74 69 6f 6e 73 22 2c 22 43 22 3a 33 37 31 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 34 32 39 30 35 38 38 2c 22 54 22 3a 35 31 31 2c 22 4d 22 3a 22 43 72 65 Data Ascii: C":371,"D":50},{"G":20030236,"T":498,"M":"AppsForOfficePackage::Init: OneNoteAppsForOfficeIntegrat ionManager Initialize","C":371,"D":50},{"G":20030237,"T":499,"M":"OneNoteAppsForOfficeUIActor::RegisterActions ","C":371,"D":50},{"G":4290588,"T":511,"M":"Cre
2022-06-30 16:43:05 UTC	506	OUT	Data Raw: 63 74 69 76 69 74 79 53 74 61 72 74 54 69 6d 65 20 53 75 69 74 65 55 73 61 67 65 4e 50 53 22 2c 22 43 22 3a 33 35 36 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 33 37 37 35 34 35 30 31 2c 22 54 22 3a 35 36 38 31 2c 22 4d 22 3a 22 53 49 46 42 3a 20 4c 6f 67 41 63 74 69 76 69 74 79 53 74 61 72 74 49 6e 74 65 72 6e 61 6c 20 41 70 70 55 73 61 67 65 4e 4c 51 53 22 2c 22 43 22 3a 33 35 36 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 33 37 38 35 36 32 36 30 2c 22 54 22 3a 35 36 38 31 2c 22 4d 22 3a 22 42 46 43 4f 43 56 2e 43 61 6c 6c 69 6e 67 20 4f 43 56 27 73 20 6c 6f 67 41 63 74 69 76 69 74 79 53 74 61 72 74 54 69 6d 65 20 41 70 70 55 73 61 67 65 4e 4c 51 53 22 2c 22 43 22 3a 33 35 36 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 33 37 37 35 34 35 30 31 2c 22 54 22 3a Data Ascii: ctivityStartTime SuiteUsageNPS","C":356,"D":50},{"G":37754501,"T":5681,"M":"SIFB: LogActivityStartInternal A ppUsageNLQS","C":356,"D":50},{"G":37856260,"T":5681,"M":"BFCOCV.Calling OCV's logActivityStartTime A ppUsageNLQS","C":356,"D":50},{"G":37754501,"T":

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:05 UTC	508	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 20355dc0-daf4-4bf0-b7ef-7b5136f995f5 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF0000695D X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF0000695D X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 4437499449C2483F86F3D155B4B4D308 Ref B: AM3EDGE0109 Ref C: 2022-06-30T16:43:05Z Date: Thu, 30 Jun 2022 16:43:05 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49942	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:11 UTC	524	OUT	GET /toy.htm HTTP/1.1 Host: verbena-woolly-clutch.glitch.me Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:12 UTC	525	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 16:43:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 77224 Connection: close x-amz-id-2: eeFSay+AawTmlC71PPnAEqZQimR6MuHMQXPG6G8MXYcyBFUdBsKXauH5rhz0Ghe3XASzPS1gYyw= x-amz-request-id: K3BGWZJZ84XTKF0Z last-modified: Tue, 28 Jun 2022 11:12:48 GMT etag: "49e28388e15f2554c9b456faf7eb2f27" cache-control: no-cache x-amz-version-id: TZHib0m1dTZVgsFhvlyHpkF7J4OLqBMI accept-ranges: bytes server: AmazonS3
2022-06-30 16:43:12 UTC	525	IN	Data Raw: 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 32 2e 32 2e 34 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 31 2e 31 2e 6d 69 6e 2e 6a 73 22 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 33 2e 31 2e 6a 73 22 20 69 6e 74 65 Data Ascii: <!doctype html><html lang="en"><head> <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> <script src="https://code.jquery.com/jquery-3.1.1.min.js"> <script src="https://code.jquery.com/jquery-3.3.1.js" inte

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	541	IN	Data Raw: 67 34 6a 49 39 49 6b 41 41 41 79 50 4d 50 55 4e 41 41 41 43 44 7a 44 6b 4c 6c 53 78 73 64 78 73 56 69 77 6f 51 41 53 41 41 41 53 53 41 43 44 7a 54 49 2b 57 50 4d 42 41 49 41 42 36 68 38 37 46 54 31 35 65 49 38 36 75 41 7a 4b 6e 43 59 6d 4b 5a 47 52 42 39 34 66 70 70 36 4e 64 6f 41 41 41 4b 6c 44 51 6b 41 41 41 67 6f 58 4a 41 41 42 55 38 33 54 48 57 52 62 4e 41 45 35 76 6f 47 34 42 79 48 4b 65 6d 57 41 41 41 41 41 41 41 41 41 41 4f 49 78 50 53 4a 41 41 41 41 41 41 49 50 4e 4e 6a 74 41 41 41 41 41 41 42 42 35 70 71 64 70 49 41 41 4f 45 78 50 54 4a 41 4b 6e 6c 48 65 64 41 41 41 41 42 42 78 47 52 36 52 49 41 41 42 6b 65 59 65 6f 61 41 41 41 45 48 6b 6e 6c 45 6c 43 44 71 50 5a 4f 67 74 46 53 4b 6b 45 6c 51 53 53 43 78 49 41 41 42 42 35 70 6b 66 4c 48 6d 45 41 67 41 Data Ascii: g4jI9IkAAAyPMPUNAAACDzDkLlSxsdxsViwoQASAAASSACDzTI+WPMBAIAB6h87FT15eI86uAzKnCY mKZGRB94fpp6NdoAAAKlDQkAAAgoXJAABU83THWRbNAE5voG4ByHKemWAAAAAAAAAAAOIxPSJAAAAAIP NNjtAAAAABB5pqdpIAAOExPTJAKnlHedAAABBxGR6RIAABkeYeoaAAAEHknlElCDqPZOgtFSKkElQSSCxIAABB5pkf LHmEAgA
2022-06-30 16:43:12 UTC	541	IN	Data Raw: 77 75 70 72 46 7a 51 67 35 6a 41 34 30 38 38 38 38 38 6b 2b 6f 30 2f 53 7a 30 44 74 41 41 41 42 55 6f 61 45 67 41 41 45 46 43 35 49 41 41 4b 6e 6d 36 5a 61 7a 42 62 4e 41 45 35 76 6f 47 34 42 79 48 4b 65 6d 57 41 41 41 41 41 41 41 41 41 41 41 4f 49 78 50 53 4a 41 41 41 41 41 41 49 50 4e 4e 6a 74 41 41 41 41 41 42 42 35 70 71 64 70 49 41 41 4f 45 78 50 54 4a 41 4b 6e 6c 48 65 64 41 41 41 42 42 78 47 52 36 52 49 41 41 42 6b 65 59 65 6f 61 41 41 41 45 48 6b 48 68 69 49 4e 4b 67 75 44 73 42 7a 4a 64 72 42 4b 6d 70 41 42 71 65 32 64 6f 41 42 49 49 50 4e 4d 6a 35 59 38 73 45 45 6b 45 67 48 71 48 69 52 55 37 31 6b 72 46 54 55 30 49 4a 4c 49 4b 6e 67 6d 32 6e 36 49 65 67 64 6f 41 41 41 4b 6c 44 51 6b 41 41 41 67 6f 58 4a 41 41 42 55 38 33 54 4c 57 59 4c 5a 6f 41 6e Data Ascii: wuprFzQg5jA4088888k+o0/Sz0DtAAABUoaEgAAEFC5IAAKnm6ZazBbNAE5voG4ByHKemWAAAAAAAA AAAOIxPSJAAAAAIPNNjtAAAAABB5pqdpIAAOExPTJAKnlHedAAABBxGR6RIAABkeYeoaAAAEHkHhiINKguDsBzJdrB KmpABqe2doABIIPNMj5Y8sEEkEgHqHiRU71krFTU0IJLIKngm2n6IegdoAAAKlDQkAAAgoXJAABU83TLWYLZoAn
2022-06-30 16:43:12 UTC	550	IN	Data Raw: 6b 42 73 56 75 74 35 61 48 6d 4a 4a 67 42 79 43 32 49 6d 41 66 42 38 68 5a 71 58 7a 30 55 68 4a 72 46 49 45 41 4a 72 31 41 51 4d 6d 5a 6b 52 48 42 4c 71 30 36 74 49 6f 67 6b 47 54 4d 7a 4d 7a 4d 7a 67 67 41 46 77 63 55 42 30 6b 35 38 38 79 4e 66 4a 49 6a 38 6e 78 79 6d 2b 52 58 54 5a 73 66 4e 61 70 41 63 48 43 54 6c 4e 35 6e 6e 73 6d 4c 59 41 44 48 41 47 77 41 62 46 41 4d 4e 6a 67 42 42 41 69 51 59 76 69 34 71 59 69 51 55 32 71 51 66 44 34 35 6c 32 71 77 77 75 2b 31 4a 77 52 55 6d 52 48 77 39 46 79 52 42 46 71 33 52 41 4d 64 6b 39 46 6e 35 2f 6d 50 6d 53 48 6b 2b 57 69 62 43 66 34 6a 34 4a 52 52 30 4a 49 47 4b 38 54 57 78 67 55 79 61 79 57 74 6d 55 45 6b 69 66 4d 34 66 44 48 4d 34 36 67 63 4a 48 6d 63 6d 63 69 50 69 5a 69 49 77 54 41 63 50 6b 54 41 62 42 77 Data Ascii: kBsVut5aHmJJgByC2ImAfB8hZqXz0UhJrFIEAJr1AQMmZkRHBLq06tIogkGTMzMzMzggAFwcUB0k58 8yNfJlj8nxym+RXTZsfNapAcHCTlN5nnsmLYADHAGwAbFAMNjgBBAiQYvi4qYiQU2qQfD45l2qwu+1JwRUmRHw9FyR BFq3RAMdk9Fn5/mPmSHk+WibCf4j4JRR0JIGK8TWxgUyayWtmUEkifM4fDHM46gcJHmcmciPiZilwTAcPkTAbBw
2022-06-30 16:43:12 UTC	559	IN	Data Raw: 78 48 34 56 4e 30 4a 47 48 48 49 6f 4f 56 50 52 59 72 59 37 55 37 57 72 30 35 33 54 77 66 52 52 65 73 31 48 79 67 76 55 6e 79 4b 6a 78 7a 33 4d 48 4b 35 6c 58 53 54 35 6d 70 39 6a 59 48 37 47 77 6e 37 47 77 50 77 4e 67 59 48 30 48 42 77 50 77 48 42 77 6e 34 6a 38 42 2b 4a 73 44 2f 57 62 43 66 36 6a 59 54 38 54 59 47 42 2b 41 2f 41 66 64 54 42 78 66 45 66 68 78 6c 57 2b 42 6a 6c 4d 37 63 47 6e 6e 4a 34 37 49 6f 31 5a 74 6f 65 4e 75 49 6a 64 69 44 73 69 6a 56 46 6d 33 54 66 4e 7a 4e 50 50 51 63 41 73 6b 6b 30 5a 45 2b 77 34 48 37 47 77 6e 37 47 77 50 77 4e 67 59 48 30 48 42 77 50 77 48 42 77 6e 34 6a 38 42 2b 4a 73 44 2f 57 62 43 66 36 6a 59 54 38 54 59 47 42 2b 41 2f 41 66 64 54 42 78 66 45 63 73 62 4e 4a 63 4b 4a 43 6a 7a 6c 4a 49 6c 30 67 6a 42 6b 74 Data Ascii: xH4VN0JGHHIoOVPRYrY7U7Wr053TwfRRes1HygvUnyKjxz3MHK5lXST5mp9jYH7Gwn7GwPwNgYH0HB wPwHBwn4j8B+JsD/WbCf6jYT8TYGB+A/AfdTBxfEfhxlW+BjlM7cGnnJ47Io1ZtoeNuIjdiDsijVFm3TfNzNPPQcAs kk0ZE+w4H7Gwn7GwPwNgYH0HBwPwHBwn4j8B+JsD/WbCf6jYT8TYGB+A/AfdTBxfEcsbNJcKJCCjzlJIl0gjBkt
2022-06-30 16:43:12 UTC	575	IN	Data Raw: 45 7a 56 48 41 51 68 43 45 49 51 68 43 45 49 51 68 43 45 49

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49941	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	559	OUT	GET /css/hover.css HTTP/1.1 Host: verbena-woolly-clutch.glitch.me Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:12 UTC	744	IN	HTTP/1.1 404 Not Found Date: Thu, 30 Jun 2022 16:43:12 GMT Content-Length: 3672 Connection: close Cache-Control: max-age=0
2022-06-30 16:43:12 UTC	744	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 6c 6c 2c 20 79 6f 75 20 66 6f 75 6e 64 20 61 20 67 6c 69 74 63 68 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6c 6f 75 64 2e 77 65 62 74 79 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Well, you found a glitch.</title> <meta name="viewport" content="initial-scale=1, width=device-width"> <link rel="stylesheet" type="text/css" href ="https://cloud.webty

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49767	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	5	OUT	POST /o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 1473 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: https://onedrive.live.com Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8lJu1vdQXlP/bseSGMwIgEJuQSe1c=:F
2022-06-30 16:42:43 UTC	6	OUT	Data Raw: 61 63 63 65 73 73 5f 74 6f 6b 65 6e 3d 34 77 6f 53 6a 31 7a 44 6d 44 36 6a 57 6d 6a 48 42 4e 31 78 53 43 30 6c 55 4e 75 67 68 63 66 31 54 57 30 46 69 43 61 77 62 70 4c 4e 77 67 59 6a 45 38 70 47 4f 7a 72 68 51 48 73 73 6a 64 44 54 4e 4b 38 4a 6e 32 31 43 70 5a 31 75 33 53 62 4b 49 51 73 46 2d 79 6e 54 53 4f 53 76 65 45 69 30 58 45 61 50 53 6f 41 65 78 71 70 37 2d 31 32 47 4c 56 7a 5a 47 31 57 6a 67 52 2d 61 5a 6f 65 44 6a 4c 77 74 59 32 30 7a 56 54 35 2d 58 44 50 47 6d 57 50 31 34 41 56 67 26 61 63 63 65 73 73 5f 74 6f 6b 65 6e 5f 74 74 6c 3d 31 36 35 38 34 32 31 37 36 31 38 31 33 26 66 69 6c 65 4e 61 6d 65 3d 4b 69 6e 65 74 72 65 2b 49 6e 63 26 66 69 6c 65 53 69 7a 65 3d 34 31 30 32 32 26 6f 77 6e 65 72 5f 69 64 3d 31 66 36 66 63 38 38 31 35 30 66 65 33 Data Ascii: access_token=4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg&access_token_ttl=1658421761813&fileName=Kinetre+Inc&fileSize=41022&owner_id=1f6fc88150fe3

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	15	IN	HTTP/1.1 200 OK Cache-Control: no-cache, no-store Pragma: no-cache Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Expires: -1 P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: DcLcid=ui=1033&data=1033; expires=Fri, 30-Sep-2022 16:42:43 GMT; path=/; samesite=none; secure; HttpOnly Set-Cookie: DcLcid=ui=1033&data=1033; expires=Fri, 30-Sep-2022 16:42:43 GMT; path=/; samesite=none; secure; HttpOnly Set-Cookie: BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	31	IN	Data Raw: 32 30 30 30 0d 0a 61 76 65 3b 61 6e 69 6d 61 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 6c 69 6e 65 61 72 3b 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 61 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 6c 69 6e 65 61 72 3b 61 6e 69 6d 61 74 69 6f 6e 2d 69 74 65 72 61 74 69 6f 6e 2d 63 6f 75 6e 74 3a 69 6e 66 69 6e 69 74 65 3b 7d 20 2e 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 42 6f 78 55 6e 69 74 20 7b 68 65 69 67 68 74 3a 32 31 36 70 78 3b 77 69 64 74 68 3a 34 31 36 70 78 3b 7d 20 2e 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 52 74 6c 20 7b 7a 2d 69 6e 64 65 78 3a 20 2d 31 3b 20 6c 65 66 74 3a 20 30 70 78 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 20 40 6b 65 79 66 72 61 6d 65 73 20 61 6e 69 6d 61 74 65 57 61 76 65 20 7b 30 25 7b Data Ascii: 2000ave;animation-timing-function:linear;-webkit-animation-timing-function:linear;animation-iteration-count: infinite;} .skeletalCanvasBoxUnit {height:216px;width:416px;} .skeletalCanvasRtl {z-index: -1; left: 0px !important;} @k eyframes animateWave {0%{
2022-06-30 16:42:43 UTC	39	IN	Data Raw: 32 30 30 30 0d 0a 74 2d 66 61 6d 69 6c 79 3a 27 53 65 67 6f 65 20 55 49 27 2c 27 53 65 67 6f 65 20 55 49 20 57 65 62 20 28 57 65 73 74 20 45 75 72 6f 70 65 61 6e 29 27 2c 27 53 65 67 6f 65 20 55 49 27 2c 2d 61 70 70 6c 65 2d 73 79 73 74 65 6d 2c 42 6c 69 6e 6b 4d 61 63 53 79 73 74 65 6d 46 6f 6e 74 2c 52 6f 62 6f 74 6f 2c 27 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 27 2c 73 61 6e 73 2d 73 65 72 69 66 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 3b 74 65 78 74 2d 6f 76 65 72 66 6c 6f 77 3a 65 6c 6c 69 70 73 69 73 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 2e 4d 6f 64 65 72 6e 55 58 48 65 61 64 65 72 50 6c 61 63 65 68 6f 6c 64 65 72 20 2e 64 6f 63 75 6d 65 6e 74 54 69 74 6c 65 2d 37 31 7b 63 6f 6c 6f 72 3a 23 36 31 36 31 36 31 7d 2e 56 Data Ascii: 2000t-family:'Segoe UI','Segoe UI Web (West European)','Segoe UI',-apple-system,BlinkMacSystemFont ,Roboto,'Helvetica Neue',sans-serif;white-space:nowrap;text-overflow:ellipsis;overflow:hidden}.ModernUXHeaderP laceholder .documentTitle-71{color:#616161}.V
2022-06-30 16:42:43 UTC	47	IN	Data Raw: 32 30 30 30 0d 0a 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 73 6b 65 6c 65 74 61 6c 53 4c 52 52 69 62 62 6f 6e 4e 65 77 56 69 73 75 61 6c 42 6f 78 22 20 72 6f 6c 65 3d 22 70 72 65 73 65 6e 74 61 74 69 6f 6e 22 20 73 74 79 6c 65 3d 22 6c 65 66 74 3a 31 32 36 39 70 78 3b 77 69 64 74 68 3a 31 32 36 70 78 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 69 64 3d 22 53 6b 65 6c 65 74 61 6c 4e 61 76 69 67 61 74 69 6f 6e 52 69 62 62 6f 6e 22 20 63 6c 61 73 73 3d 22 73 6b 65 6c 65 74 61 6c 50 6f 73 69 74 69 6f 6e 52 65 77 72 69 74 65 4e 61 76 70 61 6e 65 22 20 72 6f 6c 65 3d 22 70 72 65 73 65 6e 74 61 74 69 6f 6e 22 3e 3c 73 70 61 6e 20 69 64 3d 22 53 6b 65 6c 65 74 61 6c 4e 61 76 70 61 6e 65 54 61 62 22 20 63 6c Data Ascii: 2000<span id="SkeletalNavpaneTab" cl
2022-06-30 16:42:43 UTC	55	IN	Data Raw: 32 30 30 30 0d 0a 73 73 3d 22 73 6b 65 6c 65 74 61 6c 55 6e 69 74 20 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 4c 6f 6e 67 55 6e 69 74 20 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 46 69 72 73 74 43 6f 6c 75 6d 6e 55 6e 69 74 22 20 72 6f 6c 65 3d 22 70 72 65 73 65 6e 74 61 74 69 6f 6e 22 20 73 74 79 6c 65 3d 22 74 6f 70 3a 36 31 38 70 78 3b 61 6e 69 6d 61 74 69 6f 6e 2d 64 65 6c 61 79 3a 32 2e 33 35 34 73 3b 61 6e 69 6d 61 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 34 73 3b 77 69 64 74 68 3a 33 39 38 70 78 22 3e 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 73 6b 65 6c 65 74 61 6c 55 6e 69 74 20 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 42 6f 78 55 6e 69 74 20 73 6b 65 6c 65 74 61 6c 43 61 6e 76 61 73 53 65 63 6f 6e 64 43 6f 6c 75 6d 6e 55 6e Data Ascii: 2000ss="skeletalUnit skeletalCanvasLongUnit skeletalCanvasFirstColumnUnit" role="presentation" sty le="top:618px;animation-delay:2.354s;animation-duration:4s;width:398px"><span class="skeletalUnit skele talCanvasBoxUnit skeletalCanvasSecondColumnUn
2022-06-30 16:42:43 UTC	63	IN	Data Raw: 32 30 30 30 0d 0a 30 30 32 66 27 2c 43 6f 6d 6d 6f 6e 53 63 72 69 70 74 73 42 61 73 65 3a 20 27 41 70 70 5f 53 63 72 69 70 74 73 5c 75 30 30 32 66 27 2c 43 6f 6d 6d 6f 6e 53 63 72 69 70 74 73 4c 63 69 64 42 61 73 65 3a 20 27 41 70 70 5f 53 63 72 69 70 74 73 5c 75 30 30 32 66 31 30 33 33 5c 75 30 30 32 66 27 2c 53 68 6f 77 53 65 73 73 69 6f 6e 49 64 4f 6e 45 72 72 6f 72 3a 20 27 66 61 6c 73 65 27 2c 57 61 63 50 65 72 66 4f 62 73 65 72 76 65 72 45 6e 74 72 69 65 73 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 53 74 61 74 69 63 43 6f 6e 74 65 6e 74 48 6f 73 74 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 63 31 2d 6f 6e 65 6e 6f 74 65 2d 31 35 2e 63 64 6e 2e 6f 66 66 69 63 65 2e 6e 65 74 3a 34 34 33 5c 75 30 30 32 66 6f 5c 75 30 30 Data Ascii: 2000002f',CommonScriptsBase: 'App_Scripts\u002f',CommonScriptsLcidBase: 'App_Scripts\u002f1033\u00 2f',ShowSessionIdOnError: 'false',WacPerfObserverEntriesIsEnabled: 'true',StaticContentHost: 'https:\u002f\u002fc1- onenote-15.cdn.office.net:443\u002fo\u00
2022-06-30 16:42:43 UTC	71	IN	Data Raw: 31 31 38 65 0d 0a 49 6e 74 6c 2e 6a 73 27 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 64 65 66 65 72 20 6f 6e 6c 6f 61 64 3d 27 67 5f 6a 73 4c 54 20 3d 20 6e 65 77 20 44 61 74 65 28 29 3b 69 66 20 28 70 65 72 66 6f 72 6d 61 6e 63 65 20 26 26 20 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6d 61 72 6b 29 20 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6d 61 72 6b 28 22 67 5f 6a 73 4c 54 22 29 3b 67 5f 6a 73 4c 54 48 69 67 68 68 52 65 73 54 69 6d 65 5b 22 68 74 74 70 73 3a 2f 2f 63 31 2d 6f 6e 65 6e 6f 74 65 2d 31 35 2e 63 64 6e 2e 6f 66 66 69 63 65 2e 6e 65 74 3a 34 34 33 2f 6f 2f 73 2f 68 33 39 43 46 33 33 45 46 35 46 32 44 41 30 33 45 5f 41 70 70 5f 53 63 72 69 70 74 73 2f 31 30 33 33 2f 43 6f 6d 6d 6f 6e 49 6e 74 6c 2e 6a 73 22 5d 3d 68 69 67 Data Ascii: 118eIntl.js' type='text/javascript' defer onload='g_jsLT = new Date();if (performance && performance.mark) p erformance.mark("g_jsLT");g_jsLTHighhResTime["https://c1-onenote-15.cdn.office.net:443/o/s/h39CF33EF5F2DA03E_A pp_Scripts/1033/CommonIntl.js"]=hig
2022-06-30 16:42:43 UTC	76	IN	Data Raw: 66 63 37 0d 0a 3c 66 6f 72 6d 20 6d 65 74 68 6f 64 3d 22 70 6f 73 74 22 20 61 63 74 69 6f 6e 3d 22 2f 22 20 69 64 3d 22 66 6f 72 6d 31 22 20 6f 6e 73 75 62 6d 69 74 3d 22 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 22 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 69 6e 68 65 72 69 74 22 3e 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 73 70 4e 65 74 48 69 64 64 65 6e 22 3e 0d 0a 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 6e 61 6d 65 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 22 20 69 64 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 22 20 76 61 6c 75 65 3d 22 22 20 2f 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 41 70 70 6c 69 63 61 74 69 6f 6e 43 6f 6e 74 61 69 6e 65 72 22 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 69 6e 68 65 72 69 74 Data Ascii: fc7<form method="post" action="/" id="form1" onsubmit="return false;" style="height:inherit"> <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="" /> <div id="Applic ationContainer" style="height:inherit
2022-06-30 16:42:43 UTC	80	IN	Data Raw: 32 30 30 30 0d 0a 32 32 4c 6f 63 61 74 69 6f 6e 53 74 61 74 65 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 41 61 72 67 61 75 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4c 6f 63 61 74 69 6f 6e 43 6f 75 6e 74 72 79 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 53 77 69 74 7a 65 72 6c 61 6e 64 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 48 6f 73 74 53 65 73 73 69 6f 6e 49 64 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 6d 6e 66 68 79 7a 4c 43 64 6b 4f 54 57 52 53 5c 75 30 30 32 66 68 55 75 4e 6b 41 2e 30 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 53 74 61 72 74 54 69 6d 65 55 74 63 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 32 30 32 32 2d 30 36 2d 33 30 54 31 36 3a 34 32 3a 34 33 2e 30 38 32 34 36 36 32 5a 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4d 61 63 68 69 6e 65 4e 61 6d 65 5c 75 30 30 32 Data Ascii: 200022LocationState\u0022:\u0022Aargau\u0022,\u0022LocationCountry\u0022:\u0022Switzerland\u0022,\ u0022HostSessionId\u0022:\u0022mnfhyzLCdkOTWRS\u002fhUuNkA.0\u0022,\u0022StartTimeUtc\u0022:\u00222022- 06-30T16:42:43.0824662Z\u0022,\u0022MachineName\u002

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	88	IN	Data Raw: 31 30 33 32 0d 0a 27 2c 4f 6e 65 4e 6f 74 65 54 77 6f 50 61 6e 65 4e 61 76 50 61 6e 65 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 43 6f 6e 66 69 72 6d 61 74 69 6f 6e 44 69 61 6c 6f 67 46 6f 72 44 65 6c 65 74 65 50 61 67 65 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 4f 6e 65 4e 6f 74 65 43 73 73 50 6f 73 69 74 69 6f 6e 52 65 77 72 69 74 65 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 4f 6e 65 4e 6f 74 65 44 72 61 67 48 61 6e 64 6c 65 73 43 6f 6c 6c 61 70 73 65 49 73 45 6e 61 62 6c 65 64 3a 20 27 66 61 6c 73 65 27 2c 4f 6e 65 4e 6f 74 65 4c 65 67 61 63 79 48 65 61 64 65 72 52 65 6e 64 65 72 69 6e 67 44 69 73 61 62 6c 65 64 3a 20 27 66 61 6c 73 65 27 2c 4f 6e 65 4e 6f 74 65 52 65 6e 64 65 72 46 61 73 74 56 69 65 77 4f 6e 53 6b Data Ascii: 1032',OneNoteTwoPaneNavPaneIsEnabled: 'true',ConfirmationDialogForDeletePageIsEnabled: 'true',OneNoteCssPositionRewriteIsEnabled: 'true',OneNoteDragHandlesCollapseIsEnabled: 'false',OneNoteLegacyHeaderRenderingDisabled: 'false',OneNoteRenderFastViewOnSk
2022-06-30 16:42:43 UTC	92	IN	Data Raw: 32 30 30 30 0d 0a 72 75 65 27 2c 41 70 70 53 77 69 74 63 68 65 72 46 61 6c 6c 62 61 63 6b 55 72 6c 3a 20 27 27 2c 41 70 70 53 77 69 74 63 68 65 72 52 65 64 69 72 65 63 74 55 72 6c 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 77 77 77 2e 6f 66 66 69 63 65 2e 63 6f 6d 27 2c 41 72 69 61 45 6e 64 70 6f 69 6e 74 54 61 72 67 65 74 3a 20 27 50 55 42 4c 49 43 27 2c 41 72 69 61 45 6e 76 53 70 65 63 69 66 69 63 45 6e 64 50 6f 69 6e 74 45 6e 61 62 6c 65 64 3a 20 27 66 61 6c 73 65 27 2c 41 72 69 61 4c 6f 67 67 69 6e 67 49 73 45 6e 61 62 6c 65 64 3a 20 27 54 72 75 65 27 2c 41 72 69 61 4f 6e 65 43 6f 6c 6c 65 63 74 6f 72 55 72 6c 43 6c 69 65 6e 74 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 62 72 6f 77 73 65 72 2e 65 76 65 6e 74 73 Data Ascii: 2000rue',AppSwitcherFallbackUrl: '',AppSwitcherRedirectUrl: 'https:\u002f\u002fwww.office.com',AriaEndpointTarget: 'PUBLIC',AriaEnvSpecificEndPointEnabled: 'false',AriaLoggingIsEnabled: 'True',AriaOneCollectorUrlClient: 'https:\u002f\u002fbrowser.events
2022-06-30 16:42:43 UTC	100	IN	Data Raw: 32 30 30 30 0d 0a 6f 6e 65 6e 6f 74 65 2d 31 35 2e 63 64 6e 2e 6f 66 66 69 63 65 2e 6e 65 74 3a 34 34 33 5c 75 30 30 32 66 6f 5c 75 30 30 32 66 73 5c 75 30 30 32 66 68 38 33 41 30 31 45 36 43 38 36 42 31 30 41 31 42 5f 41 70 70 5f 53 63 72 69 70 74 73 5c 75 30 30 32 66 68 65 61 6c 74 68 53 6d 61 6c 6c 4f 66 66 6c 69 6e 65 2e 77 6f 72 6b 65 72 2e 6d 69 6e 2e 6a 73 27 2c 48 65 61 6c 74 68 54 65 6c 65 6d 65 74 72 79 53 79 73 74 65 6d 48 65 61 72 74 62 65 61 74 49 6e 74 65 72 76 61 6c 4d 73 3a 20 27 33 30 30 30 30 30 27 2c 48 65 61 6c 74 68 54 65 6c 65 6d 65 74 72 79 53 79 73 74 65 6d 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 48 65 61 6c 74 68 54 65 6c 65 6d 65 74 72 79 53 79 73 74 65 6d 4c 6f 67 67 65 72 4d 61 78 49 6e 74 65 72 76 61 6c 4d 73 3a Data Ascii: 2000onenote-15.cdn.office.net:443\u002fo\u002fs\u002fh83A01E6C86B10A1B_App_Scripts\u002fhealthSmallOffline.worker.min.js',HealthTelemetrySystemHeartbeatIntervalMs: '300000',HealthTelemetrySystemIsEnabled: 'true',HealthTelemetrySystemLoggerMaxIntervalMs:
2022-06-30 16:42:43 UTC	108	IN	Data Raw: 32 30 30 30 0d 0a 72 75 65 27 2c 4f 74 65 6c 4c 69 62 72 61 72 79 43 72 61 73 68 53 75 70 72 65 73 73 69 6f 6e 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 4f 74 65 6c 4d 69 6e 53 69 6e 6b 45 76 65 6e 74 4c 69 6d 69 74 3a 20 27 35 30 30 27 2c 4f 74 65 6c 50 69 6e 67 43 6f 6c 6c 65 63 74 6f 72 45 6e 64 70 6f 69 6e 74 3a 20 27 46 61 6c 73 65 27 2c 4f 74 65 6c 50 69 6e 67 43 6f 6c 6c 65 63 74 6f 72 50 69 6e 67 55 72 6c 3a 20 27 54 72 75 65 27 2c 4f 74 65 6c 50 69 70 65 6c 69 6e 65 41 70 70 65 6e 64 41 6c 77 61 79 73 4f 6e 4d 65 74 61 64 61 74 61 54 6f 45 76 65 72 79 45 76 65 6e 74 3a 20 27 54 72 75 65 27 2c 4f 74 65 6c 50 69 70 65 6c 69 6e 65 45 76 65 6e 74 55 70 6c 6f 61 64 46 72 65 71 75 65 6e 63 79 3a 20 27 32 30 30 30 27 2c 4f 74 65 6c 50 69 70 Data Ascii: 2000rue',OtelLibraryCrashSupressionIsEnabled: 'true',OtelMinSinkEventLimit: '500',OtelPingCollectorEndpoint: 'False',OtelPingCollectorPingUrl: 'True',OtelPipelineAppendAlwaysOnMetadataToEveryEvent: 'True',OtelPipelineEventUploadFrequency: '2000',OtelPip
2022-06-30 16:42:43 UTC	116	IN	Data Raw: 32 30 30 30 0d 0a 69 65 73 49 73 45 6e 61 62 6c 65 64 3a 20 27 66 61 6c 73 65 27 2c 57 61 63 41 70 70 6c 79 44 65 66 61 75 6c 74 50 6f 6c 69 63 79 4c 61 62 65 6c 49 73 45 6e 61 62 6c 65 64 3a 20 27 54 72 75 65 27 2c 57 61 63 41 70 70 6c 79 4d 61 6e 75 61 6c 50 6f 6c 69 63 79 4c 61 62 65 6c 49 73 45 6e 61 62 6c 65 64 3a 20 27 54 72 75 65 27 2c 57 41 43 41 72 69 61 45 76 65 6e 74 4e 61 6d 65 73 54 6f 42 65 53 75 70 70 72 65 73 73 65 64 43 6f 6d 6d 61 53 65 70 61 72 61 74 65 64 3a 20 27 4f 66 66 69 63 65 2e 54 65 6c 6c 4d 65 2e 54 65 6c 6c 4d 65 57 41 43 2e 51 75 65 72 79 52 65 73 70 6f 6e 73 65 2c 4f 66 66 69 63 65 2e 57 6f 72 64 2e 4f 6e 6c 69 6e 65 2e 48 65 61 6c 74 68 2e 4b 70 69 2e 53 61 66 65 4c 69 6e 6b 73 47 65 74 50 6f 6c 69 63 79 2c 4f 66 66 69 63 Data Ascii: 2000iesIsEnabled: 'false',WacApplyDefaultPolicyLabelIsEnabled: 'True',WacApplyManualPolicyLabelIsEnabled: 'True',WACAriaEventNamesToBeSuppressedCommaSeparated: 'Office.TellMe.TellMeWAC.QueryResponse,Office.Word.Online.Health.Kpi.SafeLinksGetPolicy,Offic
2022-06-30 16:42:43 UTC	124	IN	Data Raw: 32 30 30 30 0d 0a 65 73 73 4f 70 65 72 61 74 69 6f 6e 54 69 6d 65 6f 75 74 3a 20 27 33 30 30 30 27 2c 43 6c 69 70 61 72 74 49 6e 73 65 72 74 45 6e 61 62 6c 65 64 3a 20 27 46 61 6c 73 65 27 2c 43 6f 41 75 74 68 4c 61 74 65 6e 63 79 42 72 6f 6b 65 6e 53 6c 6f 77 54 61 72 67 65 74 56 61 6c 75 65 3a 20 27 35 30 30 30 27 2c 43 6f 41 75 74 68 4c 61 74 65 6e 63 79 42 72 6f 6b 65 6e 53 6c 6f 77 54 68 72 65 73 68 6f 6c 64 50 65 72 63 65 6e 74 69 6c 65 3a 20 27 39 35 27 2c 43 6f 41 75 74 68 4c 61 74 65 6e 63 79 53 6c 6f 77 54 61 72 67 65 74 56 61 6c 75 65 3a 20 27 33 30 30 30 27 2c 43 6f 41 75 74 68 4c 61 74 65 6e 63 79 53 6c 6f 77 54 68 72 65 73 68 6f 6c 64 50 65 72 63 65 6e 74 69 6c 65 3a 20 27 39 35 27 2c 44 65 6c 61 79 49 6e 69 74 4e 6f 6e 43 6f 72 65 53 6c 69 Data Ascii: 2000essOperationTimeout: '3000',ClipartInsertEnabled: 'False',CoAuthLatencyBrokenSlowTargetValue: '5000',CoAuthLatencyBrokenSlowThresholdPercentile: '95',CoAuthLatencySlowTargetValue: '3000',CoAuthLatencySlowThresholdPercentile: '95',DelayInitNonCoreSli
2022-06-30 16:42:43 UTC	132	IN	Data Raw: 32 30 30 30 0d 0a 61 6e 69 66 65 73 74 3f 74 65 6e 61 6e 74 3d 39 31 38 38 30 34 30 64 2d 36 63 36 37 2d 34 63 35 62 2d 62 31 31 32 2d 33 36 61 33 30 34 62 36 36 64 61 64 27 2c 4f 6e 65 4e 6f 74 65 43 6c 61 73 73 4e 6f 74 65 62 6f 6f 6b 54 65 61 6d 73 4d 61 6e 69 66 65 73 74 4c 6f 63 61 74 69 6f 6e 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 77 77 77 2e 6f 6e 65 6e 6f 74 65 2e 63 6f 6d 5c 75 30 30 32 66 6f 66 66 69 63 65 61 64 64 69 6e 73 5c 75 30 30 32 66 63 6c 61 73 73 6e 6f 74 65 62 6f 6f 6b 5c 75 30 30 32 66 6d 61 6e 69 66 65 73 74 5c 75 30 30 32 66 74 65 61 6d 73 3f 74 65 6e 61 6e 74 3d 39 31 38 38 30 34 30 64 2d 36 63 36 37 2d 34 63 35 62 2d 62 31 31 32 2d 33 36 61 33 30 34 62 36 36 64 61 64 27 2c 4f 6e 65 4e 6f 74 65 4c 69 76 65 Data Ascii: 2000anifest?tenant=9188040d-6c67-4c5b-b112-36a304b66dad',OneNoteClassNotebookTeamsManifestLocation: 'https:\u002f\u002fwww.onenote.com\u002fofficeaddins\u002fclassnotebook\u002fmanifest\u002fteams?tenant=9188040d-6c67-4c5b-b112-36a304b66dad',OneNoteLive
2022-06-30 16:42:43 UTC	140	IN	Data Raw: 32 30 30 30 0d 0a 65 4e 6f 74 65 54 65 61 6d 73 52 65 74 72 79 53 79 6e 63 44 65 6c 61 79 49 6e 4d 73 3a 20 27 35 30 30 27 2c 4f 6e 65 4e 6f 74 65 56 61 6c 69 64 61 74 65 47 72 61 70 68 52 65 76 69 73 69 6f 6e 73 3a 20 27 74 72 75 65 27 2c 4f 6e 65 4e 6f 74 65 43 6f 6e 74 65 6e 74 53 79 6e 63 46 44 4f 43 61 63 68 65 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 4f 6e 65 4e 6f 74 65 43 6f 6e 74 65 6e 74 53 79 6e 63 46 44 4f 43 61 63 68 65 56 65 72 73 69 6f 6e 3a 20 27 31 27 2c 4f 6e 65 4e 6f 74 65 56 69 65 77 4d 6f 64 65 49 6e 6c 69 6e 65 45 64 69 74 45 6e 61 62 6c 65 64 3a 20 27 46 61 6c 73 65 27 2c 4f 6e 65 4e 6f 74 65 45 6e 73 75 72 65 52 65 66 72 65 73 68 4f 6e 42 6f 6f 74 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 4f 6e 65 4e 6f 74 Data Ascii: 2000eNoteTeamsRetrySyncDelayInMs: '500',OneNoteValidateGraphRevisions: 'true',OneNoteContentSyncFDOCacheIsEnabled: 'true',OneNoteContentSyncFDOCacheVersion: '1',OneNoteViewModeInlineEditEnabled: 'False',OneNoteEnsureRefreshOnBootIsEnabled: 'true',OneNot

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	148	IN	Data Raw: 32 30 30 30 0d 0a 3b 73 68 73 68 61 38 32 36 3b 73 68 61 63 39 33 33 3b 73 68 73 68 61 38 34 31 63 66 3b 73 68 73 6d 61 34 36 30 3b 68 69 65 68 38 31 31 31 3b 32 34 68 64 33 39 38 32 3b 77 6f 72 64 66 6c 6f 6f 64 67 61 74 65 66 6c 69 67 68 74 31 34 3b 39 61 65 61 33 31 39 31 3b 66 67 61 64 6d 69 6e 3b 66 72 73 68 61 72 65 64 63 61 6e 61 72 79 63 66 3b 73 68 61 72 65 64 63 61 6e 61 72 79 3b 75 73 65 73 68 65 6c 6c 73 65 72 76 69 63 65 66 6f 72 75 73 65 72 63 6f 6e 73 65 6e 74 67 72 6f 75 70 3b 73 68 75 73 65 39 34 35 3b 73 68 75 73 65 32 39 34 3b 73 68 73 75 70 38 34 38 3b 73 68 61 72 65 39 36 34 3b 73 68 73 68 6f 36 36 34 3b 73 68 61 6c 6c 38 31 30 3b 69 65 73 6f 66 74 62 6c 6f 63 6b 3b 73 68 61 72 65 64 64 6f 63 6f 77 6e 65 72 63 61 6e 61 72 79 3b 64 Data Ascii: 2000;shsha826;shacc933;shsha841cf;shsma460;hieh8111;24hd3982;wordfloodgateflight14;9aea3191;fgadmin;frsharedcanarycf;sharedcanary;useshellserviceforuserconsentgroup;shuse945;shuse294;shsup848;share964;shsho664;shall810;iesoftblock;shareddocownercanary;d
2022-06-30 16:42:43 UTC	156	IN	Data Raw: 32 30 30 30 0d 0a 6e 74 55 49 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 54 72 75 65 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4d 69 63 72 6f 73 6f 66 74 2e 4f 66 66 69 63 65 2e 53 68 61 72 65 64 4f 6e 6c 69 6e 65 2e 53 4d 42 55 73 65 72 4c 69 63 65 6e 73 69 6e 67 45 6e 61 62 6c 65 64 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 54 72 75 65 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4d 69 63 72 6f 73 6f 66 74 2e 4f 66 66 69 63 65 2e 53 68 61 72 65 64 4f 6e 6c 69 6e 65 2e 46 6c 6f 6f 64 67 61 74 65 50 72 6f 6d 70 74 41 75 74 6f 44 69 73 6d 69 73 73 45 6e 75 6d 5c 75 30 30 32 32 3a 5c 75 30 30 32 32 34 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4d 69 63 72 6f 73 6f 66 74 2e 4f 66 66 69 63 65 2e 53 68 61 72 65 64 4f 6e 6c 69 6e 65 2e 46 6c 6f 6f 64 67 61 74 65 47 6f 76 65 72 6e Data Ascii: 2000ntUI\u0022:\u0022True\u0022,\u0022Microsoft.Office.SharedOnline.SMBUserLicensingEnabled\u0022:\u0022True\u0022,\u0022Microsoft.Office.SharedOnline.FloodgatePromptAutoDismissEnum\u0022:\u00224\u0022,\u0022Microsoft.Office.SharedOnline.FloodgateGovern
2022-06-30 16:42:43 UTC	164	IN	Data Raw: 32 30 30 30 0d 0a 30 30 32 32 2c 5c 75 30 30 32 32 45 78 63 65 6c 4c 61 72 67 65 46 69 6c 65 4f 70 65 6e 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 45 78 63 65 6c 50 6f 77 65 72 51 75 65 72 79 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 4f 6c 6b 4f 72 67 45 78 70 6c 6f 72 65 72 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 49 6e 76 61 6c 69 64 46 65 61 74 75 72 65 5c 75 30 30 32 32 5d 27 2c 41 70 70 43 61 74 61 6c 6f 67 55 72 6c 3a 20 27 27 2c 41 70 70 6c 69 65 64 50 6f 6c 69 63 79 49 64 3a 20 27 27 2c 41 70 70 72 6f 76 65 64 41 64 64 49 6e 73 3a 20 27 5b 5c 75 30 30 32 32 57 41 32 30 30 30 30 31 32 31 36 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 57 41 32 30 30 30 30 31 36 31 37 5c 75 30 30 32 32 2c 5c 75 30 30 32 32 57 41 31 30 34 33 38 30 30 35 30 5c 75 30 30 32 32 2c 5c Data Ascii: 20000022,\u0022ExcelLargeFileOpen\u0022,\u0022ExcelPowerQuery\u0022,\u0022OlkOrgExplorer\u0022,\u0022InvalidFeature\u0022]',AppCatalogUrl: '',AppliedPolicyId: '',ApprovedAddIns: '[\u0022WA200001216\u0022,\u0022WA200001617\u0022,\u0022WA104380050\u0022,\
2022-06-30 16:42:43 UTC	172	IN	Data Raw: 32 30 30 30 0d 0a 65 61 72 63 68 49 73 45 6e 61 62 6c 65 64 3a 20 27 74 72 75 65 27 2c 54 65 6c 6c 4d 65 53 65 72 76 69 63 65 49 6e 74 45 6e 64 70 6f 69 6e 74 46 6f 72 53 65 61 72 63 68 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 74 65 6c 65 6d 65 74 72 79 2e 6f 66 66 69 63 65 2e 6e 65 74 5c 75 30 30 32 66 74 65 6c 6c 6d 65 73 65 72 76 69 63 65 5c 75 30 30 32 66 61 70 69 5c 75 30 30 32 66 73 75 67 67 65 73 74 69 6f 6e 73 27 2c 54 65 6c 6c 4d 65 53 65 72 76 69 63 65 50 72 6f 64 45 6e 64 70 6f 69 6e 74 46 6f 72 53 65 61 72 63 68 3a 20 27 68 74 74 70 73 3a 5c 75 30 30 32 66 5c 75 30 30 32 66 74 65 6c 65 6d 65 73 65 72 76 69 63 65 2e 6f 73 69 2e 6f 66 66 69 63 65 2e 6e 65 74 5c 75 30 30 32 66 74 65 6c 6c Data Ascii: 2000earchIsEnabled: 'true',TellMeServiceIntEndpointForSearch: 'https:\u002f\u002ftellmeservice.osi.office-int.net\u002ftellmeservice\u002fapi\u002fsuggestions',TellMeServiceProdEndpointForSearch: 'https:\u002f\u002ftellmeservice.osi.office.net\u002ftell
2022-06-30 16:42:43 UTC	180	IN	Data Raw: 32 30 30 30 0d 0a 30 32 66 73 5c 75 30 30 32 66 31 36 31 35 34 31 37 34 31 30 32 32 5f 72 65 73 6f 75 72 63 65 73 5c 75 30 30 32 66 31 30 33 33 5c 75 30 30 32 66 77 61 70 73 77 2e 70 6e 67 3f 62 3d 31 36 30 31 35 34 31 37 34 31 30 32 32 5c 75 30 30 32 37 20 63 6c 61 73 73 3d 5c 75 30 30 32 37 77 61 70 73 77 5f 4f 44 43 5f 54 69 6c 65 50 65 6f 70 6c 65 5f 31 31 30 78 31 31 30 78 33 32 5c 75 30 30 32 37 20 72 6f 6c 65 3d 5c 75 30 30 32 37 70 72 65 73 65 6e 74 61 74 69 6f 6e 5c 75 30 30 32 37 20 74 69 74 6c 65 3d 5c 75 30 30 32 37 5c 75 30 30 32 37 5c 75 30 30 33 65 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 09 5c 75 30 30 33 63 73 70 61 6e 20 63 6c 61 73 73 3d 5c 75 30 30 32 37 73 77 54 69 6c 65 54 65 78 74 20 41 70 70 5c 75 30 30 33 65 5c 72 5c 6e 09 09 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 09 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e Data Ascii: 200002fs\u002f161541741022_resources\u002f1033\u002fwapsw.png?b=1601541741022\u0027 class=\u0027wapsw_ODC_TilePeople_110x110x32\u0027 role=\u0027presentation\u0027 title=\u0027\u0027\u003e\u003c\u002fspan\u003e\r\n\u003cspan class=\u0027swTileText App
2022-06-30 16:42:43 UTC	188	IN	Data Raw: 37 65 37 0d 0a 75 30 30 32 37 20 72 6f 6c 65 3d 5c 75 30 30 32 37 70 72 65 73 65 6e 74 61 74 69 6f 6e 5c 75 30 30 32 37 20 74 69 74 6c 65 3d 5c 75 30 30 32 37 5c 75 30 30 32 37 5c 75 30 30 33 65 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 09 5c 75 30 30 33 63 73 70 61 6e 20 63 6c 61 73 73 3d 5c 75 30 30 32 37 73 77 54 69 6c 65 54 65 78 74 20 41 70 70 54 69 6c 65 55 49 46 6f 6e 74 5c 75 30 30 32 37 5c 75 30 30 33 65 46 6c 6f 77 5c 75 30 30 33 63 5c 75 30 30 32 66 73 70 61 6e 5c 75 30 30 33 65 5c 72 5c 6e 09 5c 75 30 30 33 63 5c 75 30 30 32 66 61 5c 75 30 30 33 65 5c 72 5c 6e 5c 75 30 30 33 63 5c 75 30 30 32 66 6c 69 5c 75 30 30 33 65 5c 72 5c 6e 09 5c 75 30 30 33 63 5c 75 30 30 32 66 75 6c 5c 75 30 30 33 65 5c 72 5c 6e Data Ascii: 7e7u0027 role=\u0027presentation\u0027 title=\u0027\u0027\u003e\u003c\u002fspan\u003e\r\n\u003cspan class=\u0027swTileText AppTileUIFont\u0027\u003eFlow\u003c\u002fspan\u003e\r\n\u003c\u002fa\u003e\r\n\u003c\u002fli\u003e\r\n\u003c\u002ful\u003e\r\n
2022-06-30 16:42:43 UTC	190	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49945	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	601	OUT	GET /bootstrap/4.0.0/css/bootstrap.min.css HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://verbena-woolly-clutch.glitch.me 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://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:12 UTC	601	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 16:43:12 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 22:04:04 GMT CDN-CachedAt: 06/09/2022 14:01:47 CDN-EdgeStorageId: 756 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: b80d6707600152fe100493eda241d493 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: 72385c0bfaa39040-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 16:43:12 UTC	602	IN	Data Raw: 33 63 31 0d 0a 2f 2a 21 0a 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 30 2e 30 20 28 68 74 74 70 73 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 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 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 3a 72 6f 6f 74 7b 2d 2d 62 6c 75 65 3a 23 30 30 37 62 66 66 3b 2d 2d 69 6e 64 69 67 6f 3a 23 36 36 31 30 66 Data Ascii: 3c1/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors * Copyright 2011-2018 Twitter, Inc. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */:root{--blue:#007bff;--indigo:#6610f
2022-06-30 16:43:12 UTC	603	IN	Data Raw: 79 61 6e 3a 23 31 37 61 32 62 38 3b 2d 2d 77 68 69 74 65 3a 23 66 66 66 3b 2d 2d 67 72 61 79 3a 23 36 63 37 35 37 64 3b 2d 2d 67 72 61 79 2d 64 61 72 6b 3a 23 33 34 33 61 34 30 3b 2d 2d 70 72 69 6d 61 72 79 3a 23 30 30 37 62 66 66 3b 2d 2d 73 65 63 6f 6e 64 61 72 79 3a 23 36 63 37 35 37 64 3b 2d 2d 73 75 63 63 65 73 73 3a 23 32 38 61 37 34 35 3b 2d 2d 69 6e 66 6f 3a 23 31 37 61 32 62 38 3b 2d 2d 77 61 72 6e 69 6e 67 3a 23 66 66 63 31 30 37 3b 2d 2d 64 61 6e 67 65 72 3a 23 64 63 33 35 34 35 3b 2d 2d 6c 69 67 68 74 3a 23 66 38 66 39 66 61 3b 2d 2d 64 61 72 6b 3a 23 33 34 33 61 34 30 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 78 73 3a 30 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 73 6d 3a 35 37 36 70 78 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 6d 64 3a 37 36 Data Ascii: yan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:76
2022-06-30 16:43:12 UTC	603	IN	Data Raw: 37 66 66 39 0d 0a 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 73 61 6e 73 2d 73 65 72 69 66 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 31 35 3b 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 31 30 30 25 3b 2d 6d 73 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 31 30 30 25 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 73 63 72 6f 6c 6c 62 61 72 3b 2d 77 65 62 6b 69 74 2d 74 61 70 2d 68 69 67 68 6c 69 67 68 74 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 40 2d 6d 73 2d 76 69 65 77 70 6f 72 74 7b 77 69 64 74 68 3a 64 65 76 69 63 65 2d 77 69 64 74 68 7d 61 72 74 69 63 6c 65 2c 61 73 69 64 65 2c 64 69 61 6c 6f 67 2c 66 69 67 63 61 70 74 Data Ascii: 7ff9sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-ms-overflow-style:scrollbar;-webkit-tap-highlight-color:transparent}@-ms-viewport{width:device-width}article,aside,dialog,figcapt
2022-06-30 16:43:12 UTC	605	IN	Data Raw: 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 2d 73 6b 69 70 3a 6f 62 6a 65 63 74 73 7d 61 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 30 30 35 36 62 33 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 7d 61 3a 6e 6f 74 28 5b 68 72 65 66 5d 29 3a 6e 6f 74 28 5b 74 61 62 69 6e 64 65 78 5d 29 7b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 3a 6e 6f 74 28 5b 68 72 65 66 5d 29 3a 6e 6f 74 28 5b 74 61 62 69 6e 64 65 78 5d 29 3a 66 6f 63 75 73 2c 61 3a 6e 6f 74 28 5b 68 72 65 66 5d 29 3a 6e 6f 74 28 5b 74 61 62 69 6e 64 65 78 5d 29 3a 68 6f 76 65 72 Data Ascii: none;background-color:transparent;-webkit-text-decoration-skip:objects}a:hover{color:#0056b3;text-decoration:underline}a:not([href]):not([tabindex]){color:inherit;text-decoration:none}a:not([href]):not([tabindex]):focus,a:not([href]):not([tabindex]):hover

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	606	IN	Data Raw: 64 61 74 65 74 69 6d 65 2d 6c 6f 63 61 6c 5d 2c 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 74 69 6d 65 5d 7b 2d 77 65 62 6b 69 74 2d 61 70 70 65 61 72 61 6e 63 65 3a 6c 69 73 74 62 6f 78 7d 74 65 78 74 61 72 65 61 7b 6f 76 65 72 66 6c 6f 77 3a 61 75 74 6f 3b 72 65 73 69 7a 65 3a 76 65 72 74 69 63 61 6c 7d 66 69 65 6c 64 73 65 74 7b 6d 69 6e 2d 77 69 64 74 68 3a 30 3b 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 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 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 2e 35 72 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e Data Ascii: datetime-local],input[type=month],input[type=time]{-webkit-appearance:listbox}textarea{overflow:auto;resize:vertical}fieldset{min-width:0;padding:0;margin:0;border:0}legend{display:block;width:100%;max-width:100%;padding:0;margin-bottom:.5rem;font-size:1.
2022-06-30 16:43:12 UTC	607	IN	Data Raw: 69 6e 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 62 6f 72 64 65 72 3a 30 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 29 7d 2e 73 6d 61 6c 6c 2c 73 6d 61 6c 6c 7b 66 6f 6e 74 2d 73 69 7a 65 3a 38 30 25 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 7d 2e 6d 61 72 6b 2c 6d 61 72 6b 7b 70 61 64 64 69 6e 67 3a 2e 32 65 6d 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 63 66 38 65 33 7d 2e 6c 69 73 74 2d 75 6e 73 74 79 6c 65 64 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 7d 2e 6c 69 73 74 2d 69 6e 6c 69 6e 65 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 6e 6f 6e 65 7d 2e 6c 69 73 74 2d 69 6e 6c 69 6e 65 2d Data Ascii: in-bottom:1rem;border:0;border-top:1px solid rgba(0,0,0,.1)}.small,small{font-size:80%;font-weight:400}.mark,mark{padding:.2em;background-color:#fcf8e3}.list-unstyled{padding-left:0;list-style:none}.list-inline{padding-left:0;list-style:none}.list-inline-
2022-06-30 16:43:12 UTC	609	IN	Data Raw: 74 3a 31 35 70 78 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 61 75 74 6f 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 61 75 74 6f 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 35 37 36 70 78 29 7b 2e 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 78 2d 77 69 64 74 68 3a 35 34 30 70 78 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 78 2d 77 69 64 74 68 3a 37 32 30 70 78 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 7b 2e 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 78 2d 77 69 64 74 68 3a 39 36 30 70 78 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 32 30 30 70 78 29 7b 2e 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 78 2d 77 69 64 74 68 3a 31 31 34 30 70 78 7d Data Ascii: t:15px;margin-right:auto;margin-left:auto}@media (min-width:576px){.container{max-width:540px}}@media (min-width:768px){.container{max-width:720px}}@media (min-width:992px){.container{max-width:960px}}@media (min-width:1200px){.container{max-width:1140px}
2022-06-30 16:43:12 UTC	610	IN	Data Raw: 6c 65 78 2d 70 72 65 66 65 72 72 65 64 2d 73 69 7a 65 3a 30 3b 66 6c 65 78 2d 62 61 73 69 73 3a 30 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 31 3b 2d 6d 73 2d 66 6c 65 78 2d 70 6f 73 69 74 69 76 65 3a 31 3b 66 6c 65 78 2d 67 72 6f 77 3a 31 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 2e 63 6f 6c 2d 61 75 74 6f 3b 66 6c 65 78 3a 30 20 30 20 61 75 74 6f 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 7d 2e 63 6f 6c 2d 31 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 38 2e 33 33 33 33 33 33 33 25 3b 66 6c 65 78 3a 30 20 30 20 38 2e 33 33 33 33 33 33 33 25 3b Data Ascii: lex-preferred-size:0;flex-basis:0;-webkit-box-flex:1;-ms-flex-positive:1;flex-grow:1;max-width:100%}.col-auto{-webkit-box-flex:0;-ms-flex:0 0 auto;flex:0 0 auto;width:auto;max-width:none}.col-1{-webkit-box-flex:0;-ms-flex:0 0 8.333333%;flex:0 0 8.333333%;
2022-06-30 16:43:12 UTC	611	IN	Data Raw: 31 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 30 3b 6f 72 64 65 72 3a 30 7d 2e 6f 72 64 65 72 2d 31 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 32 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 31 3b 6f 72 64 65 72 3a 31 7d 2e 6f 72 64 65 72 2d 32 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 33 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 32 3b 6f 72 64 65 72 3a 32 7d 2e 6f 72 64 65 72 2d 33 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 34 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 33 3b 6f 72 64 65 72 3a 33 7d 2e 6f 72 64 65 72 2d 34 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 35 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 34 3b 6f 72 64 65 72 3a 34 7d 2e 6f 72 64 65 72 2d 35 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 36 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 35 3b 6f 72 64 65 72 3a 35 7d 2e 6f 72 64 65 72 2d 72 65 76 65 72 73 65 3a 6e 6f 6e 65 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 36 3b 6f 72 66 Data Ascii: 1;-ms-flex-order:0;order:0}.order-1{-webkit-box-ordinal-group:2;-ms-flex-order:1;order:1}.order-2{-webkit-box-ordinal-group:3;-ms-flex-order:2;order:2}.order-3{-webkit-box-ordinal-group:4;-ms-flex-order:3;order:3}.order-4{-webkit-box-ordinal-group:5;-ms-f
2022-06-30 16:43:12 UTC	613	IN	Data Raw: 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 38 2e 33 33 33 33 33 33 25 3b 66 6c 65 78 3a 30 20 30 20 38 2e 33 33 33 33 33 33 25 3b 6d 61 78 2d 77 69 64 74 68 3a 38 2e 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 73 6d 2d 32 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 31 36 2e 36 36 36 36 36 37 25 3b 66 6c 65 78 3a 30 20 30 20 31 36 2e 36 36 36 36 36 37 25 3b 6d 61 78 2d 77 69 64 74 68 3a 31 36 2e 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 73 6d 2d 33 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 6d 61 78 2d 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 6d 61 78 2d 77 69 64 74 68 3a

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	617	IN	Data Raw: 72 64 65 72 3a 33 7d 2e 6f 72 64 65 72 2d 6d 64 2d 34 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 35 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 34 3b 6f 72 64 65 72 3a 34 7d 2e 6f 72 64 65 72 2d 6d 64 2d 35 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 36 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 35 3b 6f 72 64 65 72 3a 35 7d 2e 6f 72 64 65 72 2d 6d 64 2d 36 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 37 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 36 3b 6f 72 64 65 72 3a 36 7d 2e 6f 72 64 65 72 2d 6d 64 2d 37 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 38 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 Data Ascii: rder:3}.order-md-4{-webkit-box-ordinal-group:5;-ms-flex-order:4;order:4}.order-md-5{-webkit-box-ordinal-group:6;-ms-flex-order:5;order:5}.order-md-6{-webkit-box-ordinal-group:7;-ms-flex-order:6;order:6}.order-md-7{-webkit-box-ordinal-group:8;-ms-flex-orde
2022-06-30 16:43:12 UTC	618	IN	Data Raw: 20 31 36 2e 36 36 36 36 36 37 25 3b 66 6c 65 78 3a 30 20 30 20 31 36 2e 36 36 36 36 36 37 25 3b 6d 61 78 2d 77 69 64 74 68 3a 31 36 2e 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 33 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 6d 61 78 2d 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 6c 67 2d 34 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 20 30 20 33 33 2e 33 33 33 33 33 33 25 3b 66 6c 65 78 3a 30 20 30 20 33 33 2e 33 33 33 33 33 33 25 3b 6d 61 78 2d 77 69 64 74 68 3a 33 33 2e 33 33 33 33 33 33 25 3b 6d 61 78 2d 77 69 64 74 68 3a 33 33 2e 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 6d 64 2d 35 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 35 3b 6f 72 64 65 72 3a 35 7d 2e 6f 72 64 65 72 2d 6d 64 2d 36 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 36 3b 6f 72 64 65 72 3a 36 7d 2e 6f 72 64 65 72 2d 6d 64 2d 37 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 37 3b 2d 6d 73 2d 66 6c Data Ascii: 16.666667%;flex:0 0 16.666667%;max-width:16.666667%}.col-lg-3{-webkit-box-flex:0;-ms-flex:0 0 25%;flex:0 0 25%;max-width:25%}.col-lg-4{-webkit-box-flex:0;-ms-flex:0 0 33.333333%;flex:0 0 33.333333%;max-width:33.333333%}.col-lg-5{-webkit-box-flex:0;-ms-fl
2022-06-30 16:43:12 UTC	619	IN	Data Raw: 65 72 3a 34 3b 6f 72 64 65 72 3a 34 7d 2e 6f 72 64 65 72 2d 6c 67 2d 35 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 36 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 35 3b 6f 72 64 65 72 3a 35 7d 2e 6f 72 64 65 72 2d 6c 67 2d 36 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 65 72 3a 37 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 36 3b 6f 72 64 65 72 3a 36 7d 2e 6f 72 64 65 72 2d 6c 67 2d 37 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 38 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 37 3b 6f 72 64 65 72 3a 37 7d 2e 6f 72 64 65 72 2d 6c 67 2d 38 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 39 3b 2d 6d 73 2d 66 6c 65 Data Ascii: er:4;order:4}.order-lg-5{-webkit-box-ordinal-group:6;-ms-flex-order:5;order:5}.order-lg-6{-webkit-box-ordinal-group:7;-ms-flex-order:6;order:6}.order-lg-7{-webkit-box-ordinal-group:8;-ms-flex-order:7;order:7}.order-lg-8{-webkit-box-ordinal-group:9;-ms-fle
2022-06-30 16:43:12 UTC	621	IN	Data Raw: 78 6c 2d 33 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 66 6c 65 78 3a 30 20 30 20 32 35 25 3b 6d 61 78 2d 77 69 64 74 68 3a 32 35 25 7d 2e 63 6f 6c 2d 78 6c 2d 34 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 33 33 2e 33 33 33 33 33 33 25 3b 66 6c 65 78 3a 30 20 30 20 33 33 2e 33 33 33 33 33 33 25 3b 6d 61 78 2d 77 69 64 74 68 3a 33 33 2e 33 33 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 6c 2d 35 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 34 31 2e 36 36 36 36 36 37 25 3b 66 6c 65 78 3a 30 20 30 20 34 31 2e 36 36 36 36 36 37 25 3b 6d 61 78 2d 77 69 64 74 68 3a 34 31 2e 36 36 36 36 36 37 25 Data Ascii: xl-3{-webkit-box-flex:0;-ms-flex:0 0 25%;flex:0 0 25%;max-width:25%}.col-xl-4{-webkit-box-flex:0;-ms-flex:0 0 33.333333%;flex:0 0 33.333333%;max-width:33.333333%}.col-xl-5{-webkit-box-flex:0;-ms-flex:0 0 41.666667%;flex:0 0 41.666667%;max-width:41.666667%
2022-06-30 16:43:12 UTC	622	IN	Data Raw: 6c 65 78 2d 6f 72 64 65 72 3a 35 3b 6f 72 64 65 72 3a 35 7d 2e 6f 72 64 65 72 2d 78 6c 2d 36 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 37 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 36 3b 6f 72 64 65 72 3a 36 7d 2e 6f 72 64 65 72 2d 78 6c 2d 37 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 38 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 37 3b 6f 72 64 65 72 3a 37 7d 2e 6f 72 64 65 72 2d 78 6c 2d 38 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 39 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 38 3b 6f 72 64 65 72 3a 38 7d 2e 6f 72 64 65 72 2d 78 6c 2d 39 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 31 30 Data Ascii: lex-order:5;order:5}.order-xl-6{-webkit-box-ordinal-group:7;-ms-flex-order:6;order:6}.order-xl-7{-webkit-box-ordinal-group:8;-ms-flex-order:7;order:7}.order-xl-8{-webkit-box-ordinal-group:9;-ms-flex-order:8;order:8}.order-xl-9{-webkit-box-ordinal-group:10
2022-06-30 16:43:12 UTC	623	IN	Data Raw: 20 74 68 65 61 64 20 74 64 2c 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 20 74 68 65 61 64 20 74 68 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 77 69 64 74 68 3a 32 70 78 7d 2e 74 61 62 6c 65 2d 73 74 72 69 70 65 64 20 74 62 6f 64 79 20 74 72 3a 6e 74 68 2d 6f 66 2d 74 79 70 65 28 6f 64 64 29 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 35 29 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 74 62 6f 64 79 20 74 72 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 7d 2e 74 61 62 6c 65 2d 70 72 69 6d 61 72 79 2c 2e 74 61 62 6c 65 2d 70 72 69 6d 61 72 79 3e 74 64 2c 2e 74 61 62 6c 65 2d 70 72 69 6d 61 72 79 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e Data Ascii: thead td,.table-bordered thead th{border-bottom-width:2px}.table-striped tbody tr:nth-of-type(odd){background-color:rgba(0,0,0,.05)}.table-hover tbody tr:hover{background-color:rgba(0,0,0,.075)}.table-primary,.table-primary>td,.table-primary>th{backgroun
2022-06-30 16:43:12 UTC	625	IN	Data Raw: 67 65 72 2c 2e 74 61 62 6c 65 2d 64 61 6e 67 65 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 64 61 6e 67 65 72 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 35 63 36 63 62 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 64 61 6e 67 65 72 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 31 62 30 62 37 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 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 20 2e 74 61 62 6c 65 2d 64 61 6e 67 65 72 3a 68 6f 76 65 72 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 31 62 30 62 37 7d 2e 74 61 62 6c 65 2d 6c 69 67 68 74 2c 2e 74 61 62 6c 65 2d 6c 69 67 68 74 3e 74 64 2c 2e 74 61 62 6c 65 2d 6c Data Ascii: ger,.table-danger>td,.table-danger>th{background-color:#f5c6cb}.table-hover .table-danger:hover{background-color:#f1b0b7}.table-hover .table-danger:hover>td,.table-hover .table-danger:hover>th{background-color:#f1b0b7}.table-light,.table-light>td,.table-l
2022-06-30 16:43:12 UTC	626	IN	Data Raw: 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 30 37 35 29 7d 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 37 35 2e 39 38 70 78 29 7b 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 2d 73 6d 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 6f 76 65 72 66 6c 6f 77 2d 78 3a 61 75 74 6f 3b 2d 77 65 62 6b 69 74 2d 6f 76 65 72 66 6c 6f 77 2d 73 63 72 6f 6c 6c 69 6e 67 3a 74 6f 75 63 68 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 2d 73 6d 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 7b 62 6f 72 64 65 72 3a 30 7d 7d 40 6d 65 64 69 61 20 28 6d 61 78 Data Ascii: -color:rgba(255,255,255,.075)}@media (max-width:575.98px){.table-responsive-sm{display:block;width:100%;overflow-x:auto;-webkit-overflow-scrolling:touch;-ms-overflow-style:-ms-autohiding-scrollbar}.table-responsive-sm>.table-bordered{border:0}}@media (max

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	627	IN	Data Raw: 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 3a 30 7d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 66 6f 63 75 73 7b 63 6f 6c 6f 72 3a 23 34 39 35 30 35 37 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6f 72 3a 23 66 66 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 38 30 62 64 66 66 3b 6f 75 74 6c 69 6e 65 3a 30 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 30 2c 31 32 33 2c 32 35 35 2c 2e 32 35 29 7d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 3a 2d 77 65 62 6b 69 74 2d 69 6e 70 75 74 2d 70 6c 61 63 65 68 6f 6c 64 65 72 7b 63 6f 6c 6f 72 3a 23 36 63 37 35 37 64 3b 6f 70 61 63 69 74 79 3a 31 7d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 3a 2d 6d 6f 7a 2d 70 6c 61 63 65 68 6f Data Ascii: round-color:transparent;border:0}.form-control:focus{color:#495057;background-color:#fff;border-color:#80bdf f;outline:0;box-shadow:0 0 0 .2rem rgba(0,123,255,.25)}.form-control::-webkit-input-placeholder{color:#6c757d;opacity:1} .form-control::-moz-placeho
2022-06-30 16:43:12 UTC	629	IN	Data Raw: 6c 61 69 6e 74 65 78 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 73 6d 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 70 6c 61 69 6e 74 65 78 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 3e 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 70 6c 61 69 6e 74 65 78 74 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 3e 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 70 6c 61 69 6e 74 65 78 74 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 74 65 78 74 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 70 72 65 70 65 6e 64 Data Ascii: laintext.form-control-sm,.input-group-lg>.form-control-plaintext.form-control,.input-group-lg>.input-group-a ppend>.form-control-plaintext.btn,.input-group-lg>.input-group-append>.form-control-plaintext.input-group-text,.input-gr oup-lg>.input-group-prepend
2022-06-30 16:43:12 UTC	630	IN	Data Raw: 5d 29 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 73 65 6c 65 63 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 6e 6f 74 28 5b 73 69 7a 65 5d 29 3a 6e 6f 74 28 5b 6d 75 6c 74 69 70 6c 65 5d 29 2c 73 65 6c 65 63 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 73 6d 3a 6e 6f 74 28 5b 73 69 7a 65 5d 29 3a 6e 6f 74 28 5b 6d 75 6c 74 69 70 6c 65 5d 29 7b 68 65 69 67 68 74 3a 63 61 6c 63 28 31 2e 38 31 32 35 72 65 6d 20 2b 20 32 70 78 29 7d 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 67 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 2e 69 6e 70 Data Ascii:]),.input-group-sm>select.form-control:not([size]):not([multiple]),select.form-control-sm:not([size]):not([multiple]) {height:calc(1.8125rem + 2px)}.form-control-lg,.input-group-lg>.form-control,.input-group-lg>.input-group-append>.btn,.in put-group-lg>.inp
2022-06-30 16:43:12 UTC	631	IN	Data Raw: 73 61 62 6c 65 64 7e 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 6c 61 62 65 6c 7b 63 6f 6c 6f 72 3a 23 36 63 37 35 37 64 7d 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 6c 61 62 65 6c 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 6c 69 6e 65 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 69 6e 6c 69 6e 65 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 66 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 3b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 3b 6d 61 72 67 69 6e 2d 72 Data Ascii: sabled~.form-check-label{color:#6c757d}.form-check-label{margin-bottom:0}.form-check-inline{display:-webkit-inline-box;display:-ms-inline-flexbox;display:inline-flex;-webkit-box-align:center;-ms-flex-align:center;align-items:cen ter;padding-left:0;margin-r
2022-06-30 16:43:12 UTC	633	IN	Data Raw: 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 6c 61 62 65 6c 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 3a 76 61 6c 69 64 7e 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 6c 61 62 65 6c 7b 63 6f 6c 6f 72 3a 23 32 38 61 37 34 35 7d 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 3a 76 61 6c 69 64 7e Data Ascii: {display:block}.form-check-input.is-valid~.form-check-label,.was-validated .form-check-input:valid~.form-check-label{color:#28a745}.form-check-input.is-valid~.valid-feedback,.form-check-input.is-valid~.valid-tooltip,.was-validated .form-check-input:valid~
2022-06-30 16:43:12 UTC	634	IN	Data Raw: 69 6c 65 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 3a 76 61 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 7d 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 3a Data Ascii: ile-input.is-valid~.custom-file-label::before,.was-validated .custom-file-input:valid~.custom-file-label::be fore{border-color:inherit}.custom-file-input.is-valid~.valid-feedback,.custom-file-input.is-valid~.valid-tooltip,.was-validated .c ustom-file-input:
2022-06-30 16:43:12 UTC	635	IN	Data Raw: 38 30 30 30 0d 0a 2e 69 6e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2e 69 73 2d 69 6e 76 61 6c 69 64 7e 2e 69 6e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 3a 69 6e 76 61 6c 69 64 7e 2e 69 6e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 3a 69 6e 76 61 6c 69 64 7e 2e 69 6e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 3a 69 6e 76 61 6c 69 64 7e 2e 69 6e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 66 6f 72 6d 2d 63 6f Data Ascii: 8000.invalid-feedback,.form-control.is-invalid~.invalid-tooltip,.was-validated .custom-select:invalid~.invalid-feedback,.was-validated .custom-select:invalid~.invalid-tooltip,.was-validated .form-control:invalid~.invalid-feedback,.was-validated .form-co
2022-06-30 16:43:12 UTC	637	IN	Data Raw: 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 2e 69 73 2d 69 6e 76 61 6c 69 64 3a 66 6f 63 75 73 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 69 6e 76 61 6c 69 64 3a 66 6f 63 75 73 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 31 70 78 20 23 66 66 66 2c 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 32 35 29 7d 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 2e 69 73 2d 69 6e 76 61 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 6c 61 62 65 6c 2c 2e 77 61 73 2d Data Ascii: -control-input.is-invalid:focus~.custom-control-label::before,.was-validated .custom-control-input:invalid:f ocus~.custom-control-label::before{box-shadow:0 0 0 1px #fff,0 0 0 .2rem rgba(220,53,69,.25)}.custom-file-input.is-inval id~.custom-file-label,.was-

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	638	IN	Data Raw: 65 72 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 66 6f 72 6d 2d 67 72 6f 75 70 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 61 75 74 6f 3b 66 6c 65 78 3a 30 20 30 20 61 75 74 6f 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 2d 6d 73 2d 66 6c 65 78 2d 66 6c 6f 77 3a 72 6f 77 20 77 72 61 70 3b 66 6c 65 78 2d 66 6c 6f 77 3a 72 6f 77 20 77 72 61 70 3b 2d 77 65 62 6b 69 Data Ascii: er;margin-bottom:0}.form-inline .form-group{display:-webkit-box;display:-ms-flexbox;display:flex;-webkit-box-flex:0;-ms-flex:0 0 auto;flex:0 0 auto;-webkit-box-orient:horizontal;-webkit-box-direction:normal;-ms-flex-flow:row wrap;flex-flow:row wrap;-webki
2022-06-30 16:43:12 UTC	639	IN	Data Raw: 61 73 65 2d 69 6e 2d 6f 75 74 2c 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 20 2e 31 35 73 20 65 61 73 65 2d 69 6e 2d 6f 75 74 2c 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 2e 31 35 73 20 65 61 73 65 2d 69 6e 2d 6f 75 74 2c 62 6f 78 2d 73 68 61 64 6f 77 20 2e 31 35 73 20 65 61 73 65 2d 69 6e 2d 6f 75 74 7d 2e 62 74 6e 3a 66 6f 63 75 73 2c 2e 62 74 6e 3a 68 6f 76 65 72 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 2e 62 74 6e 2e 66 6f 63 75 73 2c 2e 62 74 6e 3a 66 6f 63 75 73 7b 6f 75 74 6c 69 6e 65 3a 30 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 30 2c 31 32 33 2c 32 35 35 2c 2e 32 35 29 7d 2e 62 74 6e 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 3a 64 69 73 61 62 6c 65 64 7b 6f 70 61 63 69 74 Data Ascii: ase-in-out,background-color .15s ease-in-out,border-color .15s ease-in-out,box-shadow .15s ease-in-out}.btn:focus,.btn:hover{text-decoration:none}.btn.focus,.btn:focus{outline:0;box-shadow:0 0 0 .2rem rgba(0,123,255,.25)}.btn.disabled,.btn:disabled{opacit
2022-06-30 16:43:12 UTC	641	IN	Data Raw: 6f 6e 64 61 72 79 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 31 30 38 2c 31 31 37 2c 31 32 35 2c 2e 35 29 7d 2e 62 74 6e 2d 73 65 63 6f 6e 64 61 72 79 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 73 65 63 6f 6e 64 61 72 79 3a 64 69 73 61 62 6c 65 64 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 36 63 37 35 37 64 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 36 63 37 35 37 64 7d 2e 62 74 6e 2d 73 65 63 6f 6e 64 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 73 65 63 6f 6e 64 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c Data Ascii: ondary:focus{box-shadow:0 0 0 .2rem rgba(108,117,125,.5)}.btn-secondary.disabled,.btn-secondary:disabled{color:#fff;background-color:#6c757d;border-color:#6c757d}.btn-secondary:not(:disabled):not(.disabled).active,.btn-secondary:not(:disabled):not(.disabl
2022-06-30 16:43:12 UTC	642	IN	Data Raw: 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 31 33 38 34 39 36 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 31 31 37 61 38 62 7d 2e 62 74 6e 2d 69 6e 66 6f 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 69 6e 66 6f 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 33 2c 31 36 32 2c 31 38 34 2c 2e 35 29 7d 2e 62 74 6e 2d 69 6e 66 6f 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 69 6e 66 6f 3a 64 69 73 61 62 6c 65 64 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 31 37 61 32 62 38 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 31 37 61 32 62 38 7d 2e 62 74 6e 2d 69 6e 66 6f 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 Data Ascii: f;background-color:#138496;border-color:#117a8b}.btn-info.focus,.btn-info:focus{box-shadow:0 0 0 .2rem rgba(23,162,184,.5)}.btn-info.disabled,.btn-info:disabled{color:#fff;background-color:#17a2b8;border-color:#17a2b8}.btn-info:not(:disabled):not(.disable
2022-06-30 16:43:12 UTC	643	IN	Data Raw: 63 6f 6c 6f 72 3a 23 64 63 33 35 34 35 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 38 32 33 33 33 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 62 64 32 31 33 30 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 35 29 7d 2e 62 74 6e 2d 64 61 6e 67 65 72 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 64 61 6e 67 65 72 3a 64 69 73 61 62 6c 65 64 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 63 33 35 34 35 3b 62 6f 72 64 65 72 2d 63 6f 6c Data Ascii: color:#dc3545}.btn-danger:hover{color:#fff;background-color:#c82333;border-color:#bd2130}.btn-danger.focus,.btn-danger:focus{box-shadow:0 0 0 .2rem rgba(220,53,69,.5)}.btn-danger.disabled,.btn-danger:disabled{color:#fff;background-color:#dc3545;border-col
2022-06-30 16:43:12 UTC	645	IN	Data Raw: 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 33 34 33 61 34 30 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 34 33 61 34 30 7d 2e 62 74 6e 2d 64 61 72 6b 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 32 33 32 37 32 62 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 31 64 32 31 32 34 7d 2e 62 74 6e 2d 64 61 72 6b 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 64 61 72 6b 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 35 32 2c 35 38 2c 36 34 2c 2e 35 29 7d 2e 62 74 6e 2d 64 61 72 6b 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 64 61 72 6b 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e Data Ascii: #fff;background-color:#343a40;border-color:#343a40}.btn-dark:hover{color:#fff;background-color:#23272b;border-color:#1d2124}.btn-dark.focus,.btn-dark:focus{box-shadow:0 0 0 .2rem rgba(52,58,64,.5)}.btn-dark.disabled,.btn-dark:disabled{color:#fff;backgroun
2022-06-30 16:43:12 UTC	646	IN	Data Raw: 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 72 79 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 30 2c 31 32 33 2c 32 35 35 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 65 63 6f 6e 64 61 72 79 7b 63 6f 6c 6f 72 3a 23 36 63 37 35 37 64 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 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 23 36 63 37 35 37 64 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 65 63 6f 6e 64 61 72 79 3a 68 6f 76 65 72 7b 63 Data Ascii: (.disabled):active:focus,.show>.btn-outline-primary.dropdown-toggle:focus{box-shadow:0 0 0 .2rem rgba(0,123,255,.5)}.btn-outline-secondary{color:#6c757d;background-color:transparent;background-image:none;border-color:#6c757d}.btn-outline-secondary:hover{c
2022-06-30 16:43:12 UTC	647	IN	Data Raw: 6e 65 2d 73 75 63 63 65 73 73 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 75 63 63 65 73 73 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 75 63 63 65 73 73 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 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 32 38 61 37 34 35 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 32 38 61 37 34 35 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 75 63 63 65 73 73 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 Data Ascii: ne-success:not(:disabled):not(.disabled).active,.btn-outline-success:not(:disabled):not(.disabled):active,.show>.btn-outline-success.dropdown-toggle{color:#fff;background-color:#28a745;border-color:#28a745}.btn-outline-success:not(:disabled):not(.disabled

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	649	IN	Data Raw: 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 77 61 72 6e 69 6e 67 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 77 61 72 6e 69 6e 67 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 35 35 2c 31 39 33 2c 37 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 77 61 72 6e 69 6e 67 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 77 61 72 6e 69 6e 67 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 77 61 Data Ascii: round-color:#ffc107;border-color:#ffc107}.btn-outline-warning.focus,.btn-outline-warning:focus{box-shadow:0 0 0 .2rem rgba(255,193,7,.5)}.btn-outline-warning.disabled,.btn-outline-warning:disabled{color:#ffc107;background-color: transparent}.btn-outline-wa
2022-06-30 16:43:12 UTC	650	IN	Data Raw: 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 6e 67 65 72 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 6c 69 67 68 74 7b 63 6f 6c 6f 72 3a 23 66 38 66 39 66 61 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 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 23 66 38 66 39 66 61 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 6c 69 67 68 74 3a 68 6f 76 65 72 7b 63 6f 6c Data Ascii: ed):not(.disabled):active:focus,.show>.btn-outline-danger.dropdown-toggle:focus{box-shadow:0 0 0 .2rem rgba(220,53,69,.5)}.btn-outline-light{color:#f8f9fa;background-color:transparent;background-image:none;border-color :#f8f9fa}.btn-outline-light:hover{col
2022-06-30 16:43:12 UTC	651	IN	Data Raw: 6e 65 2d 64 61 72 6b 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 72 6b 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 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 34 33 61 34 30 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 34 33 61 34 30 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 72 6b 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 72 6b 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 Data Ascii: ne-dark:not(:disabled):not(.disabled):active,.show>.btn-outline-dark.dropdown-toggle{color:#fff;background-c olor:#343a40;border-color:#343a40}.btn-outline-dark:not(:disabled):not(.disabled).active:focus,.btn-outline-dark:not(:di sabled):not(.disabled):acti
2022-06-30 16:43:12 UTC	653	IN	Data Raw: 69 76 65 7d 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 3a 61 66 74 65 72 7b 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 30 3b 68 65 69 67 68 74 3a 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2e 32 35 35 65 6d 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 2e 32 35 35 65 6d 3b 63 6f 6e 74 65 6e 74 3a 22 22 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 2e 33 65 6d 20 73 6f 6c 69 64 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 2e 33 65 6d 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 62 6f 74 74 6f 6d 3a 30 3b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 2e 33 65 6d 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 65 6d 70 74 79 3a 3a 61 66 74 65 Data Ascii: ive}.dropdown-toggle::after{display:inline-block;width:0;height:0;margin-left:.255em;vertical-align:.255em;c ontent:"";border-top:.3em solid;border-right:.3em solid transparent;border-bottom:0;border-left:.3em solid transparent}. dropdown-toggle:empty::afte
2022-06-30 16:43:12 UTC	654	IN	Data Raw: 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 3a 61 66 74 65 72 7b 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 30 3b 68 65 69 67 68 74 3a 30 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2e 32 35 35 65 6d 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 2e 32 35 35 65 6d 3b 63 6f 6e 74 65 6e 74 3a 22 22 7d 2e 64 72 6f 70 6c 65 66 74 20 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 3a 61 66 74 65 72 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 2e 64 72 6f 70 6c 65 66 74 20 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 3a 62 65 66 6f 72 65 7b 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 30 3b 68 65 69 67 68 74 3a 30 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2e 32 35 35 65 6d 3b 76 65 Data Ascii: dropdown-toggle::after{display:inline-block;width:0;height:0;margin-left:.255em;vertical-align:.255em;conten t:""}.dropleft .dropdown-toggle::after{display:none}.dropleft .dropdown-toggle::before{display:inline-block;width:0;heig ht:0;margin-right:.255em;ve
2022-06-30 16:43:12 UTC	655	IN	Data Raw: 2c 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 31 20 61 75 74 6f 3b 66 6c 65 78 3a 30 20 31 20 61 75 74 6f 7d 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 3a 68 6f 76 65 72 2c 2e 62 74 6e 2d 67 72 6f 75 70 3e 2e 62 74 6e 3a 68 6f 76 65 72 7b 7a 2d 69 6e 64 65 78 3a 31 7d 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 3a 61 63 74 69 76 65 2c 2e 62 74 6e 2d 67 72 6f 75 70 2d 76 65 72 74 69 63 61 6c 3e 2e 62 74 6e 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 67 72 6f 75 70 3e Data Ascii: ,.btn-group>.btn{position:relative;-webkit-box-flex:0;-ms-flex:0 1 auto;flex:0 1 auto}.btn-group-vertical>.b tn:hover,.btn-group>.btn:hover{z-index:1}.btn-group-vertical>.btn.active,.btn-group-vertical>.btn:active,.btn-group-vert ical>.btn:focus,.btn-group>
2022-06-30 16:43:12 UTC	659	IN	Data Raw: 62 65 66 6f 72 65 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 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 6c 65 66 74 2d 72 61 64 69 75 73 3a 30 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 70 72 65 70 65 6e 64 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 20 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 70 72 65 70 65 6e 64 20 2e 62 74 6e 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7a 2d 69 6e 64 65 78 3a 32 7d 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 20 2e 62 Data Ascii: before{border-top-left-radius:0;border-bottom-left-radius:0}.input-group-append,.input-group-prepend{display:-webkit-box;display:-ms-flexbox;display:flex}.input-group-append .btn,.input-group-prepend .btn{position:relative;z-ind ex:2}.input-group-append .b
2022-06-30 16:43:12 UTC	664	IN	Data Raw: 32 35 35 2c 2e 35 29 7d 2e 63 75 73 74 6f 6d 2d 72 61 64 69 6f 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 35 30 25 7d 2e 63 75 73 74 6f 6d 2d 72 61 64 69 6f 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 63 68 65 63 6b 65 64 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 7d 2e 63 75 73 74 6f 6d 2d 72 61 64 69 6f 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 63 68 65 63 6b 65 64 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 61 66 74 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d Data Ascii: 255,.5)}.custom-radio .custom-control-label::before{border-radius:50%}.custom-radio .custom-control-input:ch ecked~.custom-control-label::before{background-color:#007bff}.custom-radio .custom-control-input:checked~.custom-control-label::after{background-im

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	667	IN	Data Raw: 38 30 30 30 0d 0a 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 31 3b 2d 6d 73 2d 66 6c 65 78 2d 70 6f 73 69 74 69 76 65 3a 31 3b 66 6c 65 78 2d 67 72 6f 77 3a 31 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 7d 2e 74 61 62 2d 63 6f 6e 74 65 6e 74 3e 2e 74 61 62 2d 70 61 6e 65 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 2e 74 61 62 2d 63 6f 6e 74 65 6e 74 3e 2e 61 63 74 69 76 65 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 6e 61 76 62 61 72 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 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 6d 73 2d 66 6c 65 78 2d 77 72 61 70 3a 77 72 61 70 3b 66 6c 65 78 2d 77 72 61 70 3a 77 Data Ascii: 8000-webkit-box-flex:1;-ms-flex-positive:1;flex-grow:1;text-align:center}.tab-content>.tab-pane{display:none}.tab-content>.active{display:block}.navbar{position:relative;display:-webkit-box;display:-ms-flexbox;display:flex;-ms-flex-wrap:wrap;flex-wrap:w
2022-06-30 16:43:12 UTC	671	IN	Data Raw: 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 2d 6d 73 2d 66 6c 65 78 2d 66 6c 6f 77 3a 72 6f 77 20 6e 6f 77 72 61 70 3b 66 6c 65 78 2d 66 6c 6f 77 3a 72 6f 77 20 6e 6f 77 72 61 70 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 73 74 61 72 74 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 73 74 61 72 74 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 66 6c 65 78 2d 73 74 61 72 74 7d 2e 6e 61 76 62 61 72 2d 65 78 70 61 6e 64 2d 6c 67 20 2e 6e 61 76 62 61 72 2d 6e 61 76 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 Data Ascii: rizontal;-webkit-box-direction:normal;-ms-flex-flow:row nowrap;flex-flow:row nowrap;-webkit-box-pack:start;-ms-flex-pack:start;justify-content:flex-start}.navbar-expand-lg .navbar-nav{-webkit-box-orient:horizontal;-webkit-box-direction:normal;-ms-flex-dir
2022-06-30 16:43:12 UTC	676	IN	Data Raw: 69 6e 6b 3a 66 6f 63 75 73 2c 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6e 61 76 2d 6c 69 6e 6b 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 37 35 29 7d 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6e 61 76 2d 6c 69 6e 6b 2e 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 2e 32 35 29 7d 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 61 63 74 69 76 65 3e 2e 6e 61 76 2d 6c 69 6e 6b 2c 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 72 2d 6e 61 76 20 2e 6e 61 76 2d 6c 69 6e 6b 2c 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 72 2d 64 61 72 6b 20 2e 6e 61 76 62 61 Data Ascii: ink:focus,.navbar-dark .navbar-nav .nav-link:hover{color:rgba(255,255,255,.75)}.navbar-dark .navbar-nav .nav-link.disabled{color:rgba(255,255,255,.25)}.navbar-dark .navbar-nav .active>.nav-link,.navbar-dark .navbar-nav .nav-link .active,.navbar-dark .navba
2022-06-30 16:43:12 UTC	680	IN	Data Raw: 63 68 69 6c 64 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 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 6c 65 66 74 2d 72 61 64 69 75 73 3a 30 7d 2e 63 61 72 64 2d 67 72 6f 75 70 3e 2e 63 61 72 64 3a 6c 61 73 74 2d 63 68 69 6c 64 20 2e 63 61 72 64 2d 68 65 61 64 65 72 2c 2e 63 61 72 64 2d 67 72 6f 75 70 3e 2e 63 61 72 64 3a 6c 61 73 74 2d 63 68 69 6c 64 20 2e 63 61 72 64 2d 66 6f 6f 74 65 72 2c 2e 63 61 72 64 2d 67 72 6f 75 70 3e 2e 63 61 72 64 3a 6c 61 73 74 2d 63 68 69 6c 64 20 2e 63 61 72 64 2d 69 6d 67 2d 62 6f 74 74 6f Data Ascii: child{border-top-left-radius:0;border-bottom-left-radius:0}.card-group>.card:last-child .card-header,.card-group>.card:last-child .card-img-top{border-top-left-radius:0}.card-group>.card:last-child .card-footer,.card-group>.card:last-child .card-img-botto
2022-06-30 16:43:12 UTC	684	IN	Data Raw: 32 62 38 7d 2e 62 61 64 67 65 2d 69 6e 66 6f 5b 68 72 65 66 5d 3a 66 6f 63 75 73 2c 2e 62 61 64 67 65 2d 69 6e 66 6f 5b 68 72 65 66 5d 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 31 31 37 61 38 62 7d 2e 62 61 64 67 65 2d 77 61 72 6e 69 6e 67 7b 63 6f 6c 6f 72 3a 23 32 31 32 35 32 39 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 7d 2e 62 61 64 67 65 2d 77 61 72 6e 69 6e 67 5b 68 72 65 66 5d 3a 66 6f 63 75 73 2c 2e 62 61 64 67 65 2d 77 61 72 6e 69 6e 67 5b 68 72 65 66 5d 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 32 31 32 35 32 39 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 62 61 63 Data Ascii: 2b8}.badge-info[href]:focus,.badge-info[href]:hover{color:#fff;text-decoration:none;background-color:#117a8b}.badge-warning{color:#212529;background-color:#ffc107}.badge-warning[href]:focus,.badge-warning[href]:hover{color:#212529;text-decoration:none;bac
2022-06-30 16:43:12 UTC	688	IN	Data Raw: 70 61 64 64 69 6e 67 3a 2e 37 35 72 65 6d 20 31 2e 32 35 72 65 6d 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 2d 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 32 35 29 7d 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 3a 66 69 72 73 74 2d 63 68 69 6c 64 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 74 2d 72 61 64 69 75 73 3a 2e 32 35 72 65 6d 3b 62 6f 72 64 65 72 2d 74 6f 70 2d 72 69 67 68 74 2d 72 61 64 69 75 73 3a 2e 32 35 72 65 6d 7d 2e 6c 69 73 74 2d 67 72 6f 75 70 2d 69 74 65 6d 3a 6c 61 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 72 69 67 68 74 2d 72 61 64 Data Ascii: padding:.75rem 1.25rem;margin-bottom:-1px;background-color:#fff;border:1px solid rgba(0,0,0,.125)}.list-group-item:first-child{border-top-left-radius:.25rem;border-top-right-radius:.25rem}.list-group-item:last-child{margin-bottom:0;border-bottom-right-rad
2022-06-30 16:43:12 UTC	692	IN	Data Raw: 30 29 7d 2e 6d 6f 64 61 6c 2d 64 69 61 6c 6f 67 2d 63 65 6e 74 65 72 65 64 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 63 61 6c 63 28 31 30 30 25 20 2d 20 28 2e 35 72 65 6d 20 2a 20 32 29 29 7d 2e 6d 6f 64 61 6c 2d 63 6f 6e 74 65 6e 74 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 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 Data Ascii: 0)}.modal-dialog-centered{display:-webkit-box;display:-ms-flexbox;display:flex;-webkit-box-align:center;-ms-flex-align:center;align-items:center;min-height:calc(100% - (.5rem * 2))}.modal-content{position:relative;display:-webkit-box;display:-ms-flexbox;d
2022-06-30 16:43:12 UTC	696	IN	Data Raw: 6e 65 3b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 6e 6f 6e 65 3b 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 6e 6f 72 6d 61 6c 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 6e 6f 72 6d 61 6c 3b 77 6f 72 64 2d 73 70 61 63 69 6e 67 3a 6e 6f 72 6d 61 6c 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 72 6d 61 6c 3b 6c 69 6e 65 2d 62 72 65 61 6b 3a 61 75 74 6f 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 37 35 72 65 6d 3b 77 6f 72 64 2d 77 72 61 70 3a 62 72 65 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 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6c 69 70 3a 70 61 64 64 69 6e 67 2d 62 6f 78 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 32 29 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 2e 33 Data Ascii: ne;text-transform:none;letter-spacing:normal;word-break:normal;word-spacing:normal;white-space:normal;line-break:auto;font-size:.875rem;word-wrap:break-word;background-color:#fff;background-clip:padding-box;border:1px solid rgba(0,0,0,.2);border-radius:.3

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	699	IN	Data Raw: 38 30 30 30 0d 0a 66 74 20 2e 61 72 72 6f 77 3a 3a 61 66 74 65 72 7b 72 69 67 68 74 3a 31 70 78 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 70 6f 70 6f 76 65 72 2d 68 65 61 64 65 72 7b 70 61 64 64 69 6e 67 3a 2e 35 72 65 6d 20 2e 37 35 72 65 6d 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 72 65 6d 3b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 37 66 37 66 37 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 65 62 65 62 65 62 3b 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 74 2d 72 61 64 69 75 73 3a 63 61 6c 63 28 2e 33 72 65 6d 20 2d 20 31 70 78 29 3b 62 6f 72 64 65 72 2d 74 6f 70 2d 72 69 67 68 74 2d 72 61 Data Ascii: 8000ft .arrow::after{right:1px;border-left-color:#fff}.popover-header{padding:.5rem .75rem;margin-bottom:0;font-size:1rem;color:inherit;background-color:#f7f7f7;border-bottom:1px solid #ebebeb;border-top-left-radius:calc(.3rem - 1px);border-top-right-ra
2022-06-30 16:43:12 UTC	703	IN	Data Raw: 74 65 78 74 2d 62 6f 74 74 6f 6d 7b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 65 78 74 2d 62 6f 74 74 6f 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 74 65 78 74 2d 74 6f 70 7b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 74 65 78 74 2d 74 6f 70 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 62 67 2d 70 72 69 6d 61 72 79 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 21 69 6d 70 6f 72 74 61 6e 74 7d 61 2e 62 67 2d 70 72 69 6d 61 72 79 3a 66 6f 63 75 73 2c 61 2e 62 67 2d 70 72 69 6d 61 72 79 3a 68 6f 76 65 72 2c 62 75 74 74 6f 6e 2e 62 67 2d 70 72 69 6d 61 72 79 3a 66 6f 63 75 73 2c 62 75 74 74 6f 6e 2e 62 67 2d 70 72 69 6d 61 72 79 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 30 30 36 32 63 Data Ascii: text-bottom{vertical-align:text-bottom!important}.align-text-top{vertical-align:text-top!important}.bg-primary{background-color:#007bff!important}a.bg-primary:focus,a.bg-primary:hover,button.bg-primary:focus,button.bg-primary:hover{background-color:#0062c
2022-06-30 16:43:12 UTC	708	IN	Data Raw: 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 64 2d 6d 64 2d 66 6c 65 78 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 64 2d 6d 64 2d 69 6e 6c 69 6e 65 2d 66 6c 65 78 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 69 6e 6c 69 6e 65 2d 62 6f 78 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 69 6e 6c 69 6e 65 2d 66 6c 65 78 62 6f 78 21 69 6d 70 6f 72 74 61 6e 74 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 66 6c 65 78 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 7b 2e 64 Data Ascii: !important}.d-md-flex{display:-webkit-box!important;display:-ms-flexbox!important;display:flex!important}.d-md-inline-flex{display:-webkit-inline-box!important;display:-ms-inline-flexbox!important;display:inline-flex!important}}@media (min-width:992px){.d
2022-06-30 16:43:12 UTC	712	IN	Data Raw: 78 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 69 74 65 6d 73 2d 73 74 72 65 74 63 68 7b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 63 6f 6e 74 65 6e 74 2d 73 74 61 72 74 7b 2d 6d 73 2d 66 6c 65 78 2d 6c 69 6e 65 2d 70 61 63 6b 3a 73 74 61 Data Ascii: x-align:baseline!important;-ms-flex-align:baseline!important;align-items:baseline!important}.align-items-stretch{-webkit-box-align:stretch!important;-ms-flex-align:stretch!important;align-items:stretch!important}.align-content-start{-ms-flex-line-pack:sta
2022-06-30 16:43:12 UTC	716	IN	Data Raw: 64 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 73 65 6c 66 2d 73 6d 2d 63 65 6e 74 65 72 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 73 65 6c 66 2d 73 6d 2d 62 61 73 65 6c 69 6e 65 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 73 65 6c 66 2d 73 6d 2d 73 74 72 65 74 63 68 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 6e 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c Data Ascii: d!important}.align-self-sm-center{-ms-flex-item-align:center!important;align-self:center!important}.align-self-sm-baseline{-ms-flex-item-align:baseline!important;align-self:baseline!important}.align-self-sm-stretch{-ms-flex-item-align:stretch!important;al
2022-06-30 16:43:12 UTC	720	IN	Data Raw: 2e 66 6c 65 78 2d 6c 67 2d 77 72 61 70 7b 2d 6d 73 2d 66 6c 65 78 2d 77 72 61 70 3a 77 72 61 70 21 69 6d 70 6f 72 74 61 6e 74 3b 66 6c 65 78 2d 77 72 61 70 3a 77 72 61 70 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 66 6c 65 78 2d 6c 67 2d 6e 6f 77 72 61 70 7b 2d 6d 73 2d 66 6c 65 78 2d 77 72 61 70 3a 6e 6f 77 72 61 70 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 66 6c 65 78 2d 6c 67 2d 77 72 61 70 2d 72 65 76 65 72 73 65 7b 2d 6d 73 2d 66 6c 65 78 2d 77 72 61 70 3a 77 72 61 70 2d 72 65 76 65 72 73 65 21 69 6d 70 6f 72 74 61 6e 74 3b 66 6c 65 78 2d 77 72 61 70 3a 77 72 61 70 2d 72 65 76 65 72 73 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 2d 6c 67 2d 73 Data Ascii: .flex-lg-wrap{-ms-flex-wrap:wrap!important;flex-wrap:wrap!important}.flex-lg-nowrap{-ms-flex-wrap:nowrap!important;flex-wrap:nowrap!important}.flex-lg-wrap-reverse{-ms-flex-wrap:wrap-reverse!important;flex-wrap:wrap-reverse!important}.justify-content-lg-s
2022-06-30 16:43:12 UTC	724	IN	Data Raw: 62 6f 78 2d 61 6c 69 67 6e 3a 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 66 6c 65 78 2d 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 69 74 65 6d 73 2d 78 6c 2d 63 65 6e 74 65 72 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 69 74 65 6d 73 2d 78 6c 2d 62 61 73 65 6c 69 6e 65 7b 2d 77 65 Data Ascii: box-align:end!important;-ms-flex-align:end!important;align-items:flex-end!important}.align-items-xl-center{-webkit-box-align:center!important;-ms-flex-align:center!important;align-items:center!important}.align-items-xl-baseline{-webkit-box-align:baseline!
2022-06-30 16:43:12 UTC	728	IN	Data Raw: 2e 6d 6c 2d 34 2c 2e 6d 78 2d 34 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 2d 35 7b 6d 61 72 67 69 6e 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 74 2d 35 2c 2e 6d 79 2d 35 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 72 2d 35 2c 2e 6d 78 2d 35 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 62 2d 35 2c 2e 6d 79 2d 35 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 6c 2d 35 2c 2e 6d 78 2d 35 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 2d 30 7b 70 61 64 64 69 6e 67 3a 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 74 2d Data Ascii: .ml-4,.mx-4{margin-left:1.5rem!important}.m-5{margin:3rem!important}.mt-5,.my-5{margin-top:3rem!important}.mr-5,.mx-5{margin-right:3rem!important}.mb-5,.my-5{margin-bottom:3rem!important}.ml-5,.mx-5{margin-left:3rem!important}.p-0{padding:0!important}.pt-

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	731	IN	Data Raw: 33 32 33 33 0d 0a 72 74 61 6e 74 7d 2e 70 72 2d 73 6d 2d 31 2c 2e 70 78 2d 73 6d 2d 31 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 62 2d 73 6d 2d 31 2c 2e 70 79 2d 73 6d 2d 31 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6 c 2d 73 6d 2d 31 2c 2e 70 78 2d 73 6d 2d 31 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 2d 73 6d 2d 32 7b 70 61 64 64 69 6e 67 3a 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 74 2d 73 6d 2d 32 2c 2e 70 79 2d 73 6d 2d 32 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 72 2d 73 6d 2d 32 2c 2e 70 78 2d 73 6d 2d 32 7b Data Ascii: 3233rtant}.pr-sm-1,.px-sm-1{padding-right:.25rem!important}.pb-sm-1,.py-sm-1{padding-bottom:.25rem !important}.pl-sm-1,.px-sm-1{padding-left:.25rem!important}.p-sm-2{padding:.5rem!important}.pt-sm-2,.py-sm-2{padding-top:.5rem!important}.pr-sm-2,.px-sm-2{
2022-06-30 16:43:12 UTC	735	IN	Data Raw: 74 61 6e 74 7d 2e 6d 72 2d 6c 67 2d 30 2c 2e 6d 78 2d 6c 67 2d 30 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 62 2d 6c 67 2d 30 2c 2e 6d 79 2d 6c 67 2d 30 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 6c 2d 6c 67 2d 30 2c 2e 6d 78 2d 6c 67 2d 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 2d 6c 67 2d 31 7b 6d 61 72 67 69 6e 3a 2e 32 35 72 6 5 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 74 2d 6c 67 2d 31 2c 2e 6d 79 2d 6c 67 2d 31 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 72 2d 6c 67 2d 31 2c 2e 6d 78 2d 6c 67 2d 31 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 Data Ascii: tant}.mr-lg-0,.mx-lg-0{margin-right:0!important}.mb-lg-0,.my-lg-0{margin-bottom:0!important}.ml-lg-0,.mx-lg-0{margin-left:0!important}.m-lg-1{margin:.25rem!important}.mt-lg-1,.my-lg-1{margin-top:.25rem!important}.mr-lg-1,.mx-lg-1{margin-right:.25rem!impor
2022-06-30 16:43:12 UTC	740	IN	Data Raw: 6d 70 6f 72 74 61 6e 74 7d 2e 70 6c 2d 78 6c 2d 30 2c 2e 70 78 2d 78 6c 2d 30 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 2d 78 6c 2d 31 7b 70 61 64 64 69 6e 67 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 74 2d 78 6c 2d 31 2c 2e 70 79 2d 78 6c 2d 31 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 72 2d 78 6c 2d 31 2c 2e 70 78 2d 78 6c 2d 31 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 62 2d 78 6c 2d 31 2c 2e 70 79 2d 78 6c 2d 31 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6c 2d 78 6c 2d 31 2c 2e 70 78 2d 78 6c 2d 31 7b 70 61 64 64 69 6e Data Ascii: mportant}.pl-xl-0,.px-xl-0{padding-left:0!important}.p-xl-1{padding:.25rem!important}.pt-xl-1,.py-xl-1{padding-top:.25rem!important}.pr-xl-1,.px-xl-1{padding-right:.25rem!important}.pb-xl-1,.py-xl-1{padding-bottom:.25rem!important}.pl-xl-1,.px-xl-1{paddin
2022-06-30 16:43:12 UTC	744	IN	Data Raw: 7d 2e 74 61 62 6c 65 20 74 64 2c 2e 74 61 62 6c 65 20 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 20 74 64 2c 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 20 74 68 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 64 64 21 69 6d 70 6f 72 74 61 6e 74 7d 7d 0a 2f 2a 23 20 73 6f 75 72 63 65 4d 61 70 70 69 6e 67 55 52 4c 3d 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 2e 6d 61 70 20 2a 2f 0d 0a Data Ascii: }.table td,.table th{background-color:#fff!important}.table-bordered td,.table-bordered th{border:1px solid #ddd!important}}/*# sourceMappingURL=bootstrap.min.css.map */
2022-06-30 16:43:12 UTC	744	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49952	104.18.11.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	748	OUT	GET /bootstrap/4.0.0/js/bootstrap.min.js HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://verbena-woolly-clutch.glitch.me User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	768	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 16:43:12 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/"14d449eb8876fa55e1ef3c2cc52b0c17" Last-Modified: Mon, 25 Jan 2021 22:04:04 GMT CDN-CachedAt: 03/10/2022 17:24:53 CDN-ProxyVer: 1.02 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True CDN-EdgeStorageId: 860 CDN-Status: 200 timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-RequestId: a0274657e9a1cb74a0c66cf1589a94dd 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: 72385c0e1dddbb71-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 16:43:13 UTC	769	IN	Data Raw: 37 62 62 66 0d 0a 2f 2a 21 0a 20 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 30 2e 30 20 28 68 74 74 70 73 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 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 67 72 61 70 68 73 2f 63 6f 6e 74 72 69 62 75 74 6f 72 73 29 0a 20 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 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 74 Data Ascii: 7bbf/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors) * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */!function(t
2022-06-30 16:43:13 UTC	770	IN	Data Raw: 28 65 78 70 6f 72 74 73 2c 72 65 71 75 69 72 65 28 22 6a 71 75 65 72 79 22 29 2c 72 65 71 75 69 72 65 28 22 70 6f 70 70 65 72 2e 6a 73 22 29 29 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 5b 22 65 78 70 6f 72 74 73 22 2c 22 6a 71 75 65 72 79 22 2c 22 70 6f 70 70 65 72 2e 6a 73 22 5d 2c 65 29 3a 65 28 74 2e 62 6f 6f 74 73 74 72 61 70 3d 7b 7d 2c 74 2e 6a 51 75 65 72 79 2c 74 2e 50 6f 70 70 65 72 29 7d 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 69 28 74 2c 65 29 7b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 65 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 69 3d 65 5b 6e 5d Data Ascii: (exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n]
2022-06-30 16:43:13 UTC	771	IN	Data Raw: 75 6c 6c 7d 63 61 74 63 68 28 74 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 7d 2c 72 65 66 6c 6f 77 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 74 2e 6f 66 66 73 65 74 48 65 69 67 68 74 7d 2c 74 72 69 67 67 65 72 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 74 28 6e 29 2e 74 72 69 67 67 65 72 28 65 2e 65 6e 64 29 7d 2c 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 42 6f 6f 6c 65 61 6e 28 65 29 7d 2c 69 73 45 6c 65 6d 65 6e 74 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 28 74 5b 30 5d 7c 7c 74 29 2e 6e 6f 64 65 54 79 70 65 7d 2c 74 79 70 65 43 68 65 63 6b 43 6f 6e 66 69 67 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b Data Ascii: ull}catch(t){return null}},reflow:function(t){return t.offsetHeight},triggerTransitionEnd:function(n){t(n).trigger(e.end)},supportsTransitionEnd:function(){return Boolean(e)},isElement:function(t){return(t[0]||t).nodeType},typeCheckConfig:function(t,e,n){
2022-06-30 16:43:13 UTC	772	IN	Data Raw: 65 74 75 72 6e 20 65 26 26 28 6e 3d 6f 28 65 29 5b 30 5d 29 2c 6e 7c 7c 28 6e 3d 6f 28 74 29 2e 63 6c 6f 73 65 73 74 28 22 2e 22 2b 66 29 5b 30 5d 29 2c 6e 7d 2c 65 2e 5f 74 72 69 67 67 65 72 43 6c 6f 73 65 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 6f 2e 45 76 65 6e 74 28 75 2e 43 4c 4f 53 45 29 3b 72 65 74 75 72 6e 20 6f 28 74 29 2e 74 72 69 67 67 65 72 28 65 29 2c 65 2e 5f 72 65 6d 6f 76 65 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 6f 28 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 29 2c 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 6f 28 74 29 2e 68 61 73 43 6c 61 73 73 28 64 29 3f 6f 28 74 29 2e 6f 6e 65 28 50 2e 54 52 41 4e Data Ascii: eturn e&&(n=o(e)[0]),n||(n=o(t).closest("."+f)[0]),n},e._triggerCloseEvent=function(t){var e=o.Event(u.CLOSE);return o(t).trigger(e),e},e._removeElement=function(t){var e=this;o(t).removeClass(_),P.supportsTransitionEnd()&&o(t).hasClass(d)?o(t).one(P.TRAN
2022-06-30 16:43:13 UTC	774	IN	Data Raw: 69 6f 22 3d 3d 3d 69 2e 74 79 70 65 29 69 66 28 69 2e 63 68 65 63 6b 65 64 26 26 70 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 43 29 29 74 3d 21 31 3b 65 6c 73 65 7b 76 61 72 20 73 3d 70 28 6e 29 2e 66 69 6e 64 28 77 29 5b 30 5d 3b 73 26 26 70 28 73 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 43 29 7d 69 66 28 74 29 7b 69 66 28 69 2e 68 61 73 41 74 74 72 69 62 75 74 65 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 6e 2e 68 61 73 41 74 74 72 69 62 75 74 65 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 69 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c 65 64 22 29 7c 7c 6e 2e 63 6c 61 73 73 4c 69 73 74 2e 63 6f 6e 74 61 69 6e 73 28 22 64 69 73 61 62 6c 65 64 22 29 29 72 65 74 75 72 6e 3b 69 2e 63 68 65 Data Ascii: io"===i.type)if(i.checked&&p(this._element).hasClass(C))t=!1;else{var s=p(n).find(w)[0];s&&p(s).removeClass(C)}if(t){if(i.hasAttribute("disabled")||n.hasAttribute("disabled")||i.classList.contains("disabled")||n.classList.contains("disabled"))return;i.che

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	775	IN	Data Raw: 70 72 65 76 22 2c 75 3d 22 6c 65 66 74 22 2c 66 3d 22 72 69 67 68 74 22 2c 64 3d 7b 53 4c 49 44 45 3a 22 73 6c 69 64 65 22 2b 69 2c 53 4c 49 44 3a 22 73 6c 69 64 22 2b 69 2c 4b 45 59 44 4f 57 4e 3a 22 6b 65 79 64 6f 77 6e 22 2b 69 2c 4d 4f 55 53 45 45 4e 54 45 52 3a 22 6d 6f 75 73 65 65 6e 74 65 72 22 2b 69 2c 4d 4f 55 53 45 4c 45 41 56 45 3a 22 6d 6f 75 73 65 6c 65 61 76 65 22 2b 69 2c 54 4f 55 43 48 45 4e 44 3a 22 74 6f 75 63 68 65 6e 64 22 2b 69 2c 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 3a 22 6c 6f 61 64 22 2b 69 2b 22 2e 64 61 74 61 2d 61 70 69 22 2c 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 3a 22 63 6c 69 63 6b 22 2b 69 2b 22 2e 64 61 74 61 2d 61 70 69 22 7d 2c 5f 3d 22 63 61 72 6f 75 73 65 6c 22 2c 67 3d 22 61 63 74 69 76 65 22 2c 70 3d 22 73 6c 69 Data Ascii: prev",u="left",f="right",d={SLIDE:"slide"+i,SLID:"slid"+i,KEYDOWN:"keydown"+i,MOUSEENTER:"mouseenter"+i,MOUSELEAVE:"mouseleave"+i,TOUCHEND:"touchend"+i,LOAD_DATA_API:"load"+i+".data-api",CLICK_DATA_API:"click"+i+".data-api"},_="carousel",g="active",p="sli
2022-06-30 16:43:13 UTC	776	IN	Data Raw: 6c 7d 2c 43 2e 63 79 63 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 7c 7c 28 74 68 69 73 2e 5f 69 73 50 61 75 73 65 64 3d 21 31 29 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 26 26 28 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 29 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 29 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 69 6e 74 65 72 76 61 6c 26 26 21 74 68 69 73 2e 5f 69 73 50 61 75 73 65 64 26 26 28 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 73 65 74 49 6e 74 65 72 76 61 6c 28 28 64 6f 63 75 6d 65 6e 74 2e 76 69 73 69 62 69 6c 69 74 79 53 74 61 74 65 3f 74 68 69 73 2e 6e 65 78 74 57 68 65 6e 56 69 73 69 62 6c 65 3a 74 68 69 73 2e 6e 65 78 74 29 2e 62 69 6e 64 28 74 68 69 73 29 2c 74 68 69 73 Data Ascii: l},C.cycle=function(t){t||(this._isPaused=!1),this._interval&&(clearInterval(this._interval),this._interval=null),this._config.interval&&!this._isPaused&&(this._interval=setInterval((document.visibilityState?this.nextWhenVisible:this.next).bind(this),this
2022-06-30 16:43:13 UTC	778	IN	Data Raw: 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 2e 63 79 63 6c 65 28 74 29 7d 2c 35 30 30 2b 65 2e 5f 63 6f 6e 66 69 67 2e 69 6e 74 65 72 76 61 6c 29 7d 29 29 7d 2c 43 2e 5f 6b 65 79 64 6f 77 6e 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 21 2f 69 6e 70 75 74 7c 74 65 78 74 61 72 65 61 2f 69 2e 74 65 73 74 28 74 2e 74 61 72 67 65 74 2e 74 61 67 4e 61 6d 65 29 29 73 77 69 74 63 68 28 74 2e 77 68 69 63 68 29 7b 63 61 73 65 20 33 37 3a 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 74 68 69 73 2e 70 72 65 76 28 29 3b 62 72 65 61 6b 3b 63 61 73 65 20 33 39 3a 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 74 68 69 73 2e 6e 65 78 74 28 29 7d 7d 2c 43 2e 5f 67 65 74 49 74 65 6d 49 6e 64 65 78 3d 66 75 6e 63 Data Ascii: meout(function(t){return e.cycle(t)},500+e._config.interval)}))},C._keydown=function(t){if(!/input|textarea/i.test(t.target.tagName))switch(t.which){case 37:t.preventDefault(),this.prev();break;case 39:t.preventDefault(),this.next()}},C._getItemIndex=func
2022-06-30 16:43:13 UTC	779	IN	Data Raw: 26 26 61 26 26 63 29 7b 74 68 69 73 2e 5f 69 73 53 6c 69 64 69 6e 67 3d 21 30 2c 43 26 26 74 68 69 73 2e 70 61 75 73 65 28 29 2c 74 68 69 73 2e 5f 73 65 74 41 63 74 69 76 65 49 6e 64 69 63 61 74 6f 72 45 6c 65 6d 65 6e 74 28 63 29 3b 76 61 72 20 49 3d 74 2e 45 76 65 6e 74 28 64 2e 53 4c 49 44 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 63 2c 64 69 72 65 63 74 69 6f 6e 3a 72 2c 66 72 6f 6d 3a 6c 2c 74 6f 3a 5f 7d 29 3b 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 70 29 3f 28 74 28 63 29 2e 61 64 64 43 6c 61 73 73 28 73 29 2c 50 2e 72 65 66 6c 6f 77 28 63 29 2c 74 28 61 29 2e 61 64 64 43 6c 61 73 73 28 69 29 2c 74 28 63 29 2e 61 64 64 43 6c Data Ascii: &&a&&c){this._isSliding=!0,C&&this.pause(),this._setActiveIndicatorElement(c);var I=t.Event(d.SLID,{relatedTarget:c,direction:r,from:l,to:_});P.supportsTransitionEnd()&&t(this._element).hasClass(p)?(t(c).addClass(s),P.reflow(c),t(a).addClass(i),t(c).addCl
2022-06-30 16:43:13 UTC	780	IN	Data Raw: 20 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 64 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 79 2e 44 41 54 41 5f 53 4c 49 44 45 2c 43 2e 5f 64 61 74 61 41 70 69 43 6c 69 63 6b 48 61 6e 64 6c 65 72 29 2c 74 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 64 2e 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 79 2e 44 41 54 41 5f 52 49 44 45 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 28 74 68 69 73 29 3b 43 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 65 2c 65 2e 64 61 74 61 28 29 29 7d 29 2c 74 2e 66 6e 5b 65 5d 3d 43 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 5b 65 5d 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 43 2c 74 2e 66 6e 5b 65 5d 2e 6e 6f 43 Data Ascii: t(document).on(d.CLICK_DATA_API,y.DATA_SLIDE,C._dataApiClickHandler),t(window).on(d.LOAD_DATA_API,function(){t(y.DATA_RIDE).each(function(){var e=t(this);C._jQueryInterface.call(e,e.data())})}),t.fn[e]=C._jQueryInterface,t.fn[e].Constructor=C,t.fn[e].noC
2022-06-30 16:43:13 UTC	782	IN	Data Raw: 73 68 6f 77 28 29 7d 2c 6f 2e 73 68 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 2c 73 2c 72 3d 74 68 69 73 3b 69 66 28 21 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 26 26 21 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 63 29 26 26 28 74 68 69 73 2e 5f 70 61 72 65 6e 74 26 26 30 3d 3d 3d 28 65 3d 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 74 68 69 73 2e 5f 70 61 72 65 6e 74 29 2e 66 69 6e 64 28 70 2e 41 43 54 49 56 45 53 29 2e 66 69 6c 74 65 72 28 27 5b 64 61 74 61 2d 70 61 72 65 6e 74 3d 22 27 2b 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 70 61 72 65 6e 74 2b 27 22 5d 27 29 29 2e 6c 65 6e 67 74 68 26 26 28 65 3d 6e 75 6c 6c 29 2c 21 28 65 26 26 28 73 3d 74 28 65 29 2e 6e 6f 74 28 74 68 69 73 Data Ascii: show()},o.show=function(){var e,s,r=this;if(!this._isTransitioning&&!t(this._element).hasClass(c)&&(this._parent&&0===(e=t.makeArray(t(this._parent).find(p.ACTIVES).filter('[data-parent="'+this._config.parent+'"]'))).length&&(e=null),!(e&&(s=t(e).not(this
2022-06-30 16:43:13 UTC	783	IN	Data Raw: 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 2e 6c 65 6e 67 74 68 3e 30 29 66 6f 72 28 76 61 72 20 73 3d 30 3b 73 3c 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 2e 6c 65 6e 67 74 68 3b 73 2b 2b 29 7b 76 61 72 20 72 3d 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 5b 73 5d 2c 6f 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 72 29 3b 69 66 28 6e 75 6c 6c 21 3d 3d 6f 29 74 28 6f 29 2e 68 61 73 43 6c 61 73 73 28 63 29 7c 7c 74 28 72 29 2e 61 64 64 43 6c 61 73 73 28 64 29 2e 61 74 74 72 28 22 61 72 69 61 2d 65 78 70 61 6e 64 65 64 22 2c 21 31 29 7d 74 68 69 73 2e 73 65 74 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 28 21 30 29 3b 76 61 72 20 61 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 65 2e 73 65 74 54 72 61 6e 73 Data Ascii: his._triggerArray.length>0)for(var s=0;s<this._triggerArray.length;s++){var r=this._triggerArray[s],o=P.getSelectorFromElement(r);if(null!==o)t(o).hasClass(c)||t(r).addClass(d).attr("aria-expanded",!1)}this.setTransitioning(!0);var a=function(){e.setTrans
2022-06-30 16:43:13 UTC	784	IN	Data Raw: 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6e 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 65 29 3b 72 65 74 75 72 6e 20 6e 3f 74 28 6e 29 5b 30 5d 3a 6e 75 6c 6c 7d 2c 69 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 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 73 3d 74 28 74 68 69 73 29 2c 6f 3d 73 2e 64 61 74 61 28 6e 29 2c 6c 3d 72 28 7b 7d 2c 61 2c 73 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 29 3b 69 66 28 21 6f 26 26 6c 2e 74 6f 67 67 6c 65 26 26 2f 73 68 6f 77 7c 68 69 64 65 2f 2e 74 65 73 74 28 65 29 26 26 28 6c 2e 74 6f 67 67 6c 65 3d 21 31 29 2c 6f 7c 7c 28 6f 3d 6e 65 77 Data Ascii: unction(e){var n=P.getSelectorFromElement(e);return n?t(n)[0]:null},i._jQueryInterface=function(e){return this.each(function(){var s=t(this),o=s.data(n),l=r({},a,s.data(),"object"==typeof e&&e);if(!o&&l.toggle&&/show|hide/.test(e)&&(l.toggle=!1),o||(o=new

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	786	IN	Data Raw: 20 2e 64 72 6f 70 64 6f 77 6e 2d 69 74 65 6d 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 22 2c 41 3d 22 74 6f 70 2d 73 74 61 72 74 22 2c 62 3d 22 74 6f 70 2d 65 6e 64 22 2c 44 3d 22 62 6f 74 74 6f 6d 2d 73 74 61 72 74 22 2c 53 3d 22 62 6f 74 74 6f 6d 2d 65 6e 64 22 2c 77 3d 22 72 69 67 68 74 2d 73 74 61 72 74 22 2c 4e 3d 22 6c 65 66 74 2d 73 74 61 72 74 22 2c 4f 3d 7b 6f 66 66 73 65 74 3a 30 2c 66 6c 69 70 3a 21 30 2c 62 6f 75 6e 64 61 72 79 3a 22 73 63 72 6f 6c 6c 50 61 72 65 6e 74 22 7d 2c 6b 3d 7b 6f 66 66 73 65 74 3a 22 28 6e 75 6d 62 65 72 7c 73 74 72 69 6e 67 7c 66 75 6e 63 74 69 6f 6e 29 22 2c 66 6c 69 70 3a 22 62 6f 6f 6c 65 61 6e 22 2c 62 6f 75 6e 64 61 72 79 3a 22 28 73 74 72 69 6e 67 7c 65 6c 65 6d 65 6e 74 29 22 7d 2c 4c 3d 66 75 6e 63 74 69 Data Ascii: .dropdown-item:not(.disabled)",A="top-start",b="top-end",D="bottom-start",S="bottom-end",w="right-start",N="left-start",O={offset:0,flip:!0,boundary:"scrollParent"},k={offset:"(number|string|function)",flip:"boolean",boundary:"(string|element)"},L=functi
2022-06-30 16:43:13 UTC	787	IN	Data Raw: 28 29 7b 74 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 69 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 6f 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 6d 65 6e 75 3d 6e 75 6c 6c 2c 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 28 74 68 69 73 2e 5f 70 6f 70 70 65 72 2e 64 65 73 74 72 6f 79 28 29 2c 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 6e 75 6c 6c 29 7d 2c 6c 2e 75 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 69 6e 4e 61 76 62 61 72 3d 74 68 69 73 2e 5f 64 65 74 65 63 74 4e 61 76 62 61 72 28 29 2c 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 74 68 69 73 2e 5f 70 6f 70 70 65 72 2e 73 63 68 65 64 75 6c 65 Data Ascii: (){t.removeData(this._element,i),t(this._element).off(o),this._element=null,this._menu=null,null!==this._popper&&(this._popper.destroy(),this._popper=null)},l.update=function(){this._inNavbar=this._detectNavbar(),null!==this._popper&&this._popper.schedule
2022-06-30 16:43:13 UTC	788	IN	Data Raw: 61 72 20 6e 3d 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 29 3b 69 66 28 6e 7c 7c 28 6e 3d 6e 65 77 20 61 28 74 68 69 73 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 3f 65 3a 6e 75 6c 6c 29 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 2c 6e 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6e 5b 65 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 64 20 22 27 2b 65 2b 27 22 27 29 3b 6e 5b 65 5d 28 29 7d 7d 29 7d 2c 61 2e 5f 63 6c 65 61 72 4d 65 6e 75 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 65 7c 7c 33 21 3d 3d 65 2e 77 68 69 63 68 26 26 28 22 6b 65 79 75 70 22 21 3d 3d 65 2e 74 79 70 Data Ascii: ar n=t(this).data(i);if(n||(n=new a(this,"object"==typeof e?e:null),t(this).data(i,n)),"string"==typeof e){if("undefined"==typeof n[e])throw new TypeError('No method named "'+e+'"');n[e]()}})},a._clearMenus=function(e){if(!e||3!==e.which&&("keyup"!==e.typ
2022-06-30 16:43:13 UTC	790	IN	Data Raw: 30 21 3d 3d 73 2e 6c 65 6e 67 74 68 29 7b 76 61 72 20 72 3d 73 2e 69 6e 64 65 78 4f 66 28 65 2e 74 61 72 67 65 74 29 3b 33 38 3d 3d 3d 65 2e 77 68 69 63 68 26 26 72 3e 30 26 26 72 2d 2d 2c 34 30 3d 3d 3d 65 2e 77 68 69 63 68 26 26 72 3c 73 2e 6c 65 6e 67 74 68 2d 31 26 26 72 2b 2b 2c 72 3c 30 26 26 28 72 3d 30 29 2c 73 5b 72 5d 2e 66 6f 63 75 73 28 29 7d 7d 65 6c 73 65 7b 69 66 28 32 37 3d 3d 3d 65 2e 77 68 69 63 68 29 7b 76 61 72 20 6f 3d 74 28 6e 29 2e 66 69 6e 64 28 45 29 5b 30 5d 3b 74 28 6f 29 2e 74 72 69 67 67 65 72 28 22 66 6f 63 75 73 22 29 7d 74 28 74 68 69 73 29 2e 74 72 69 67 67 65 72 28 22 63 6c 69 63 6b 22 29 7d 7d 7d 2c 73 28 61 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 Data Ascii: 0!==s.length){var r=s.indexOf(e.target);38===e.which&&r>0&&r--,40===e.which&&r<s.length-1&&r++,r<0&&(r=0),s[r].focus()}}else{if(27===e.which){var o=t(n).find(E)[0];t(o).trigger("focus")}t(this).trigger("click")}}},s(a,null,[{key:"VERSION",get:function(){r
2022-06-30 16:43:13 UTC	791	IN	Data Raw: 64 3d 22 66 61 64 65 22 2c 5f 3d 22 73 68 6f 77 22 2c 67 3d 7b 44 49 41 4c 4f 47 3a 22 2e 6d 6f 64 61 6c 2d 64 69 61 6c 6f 67 22 2c 44 41 54 41 5f 54 4f 47 47 4c 45 3a 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 6d 6f 64 61 6c 22 5d 27 2c 44 41 54 41 5f 44 49 53 4d 49 53 53 3a 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 46 49 58 45 44 5f 43 4f 4e 54 45 4e 54 3a 22 2e 66 69 78 65 64 2d 74 6f 70 2c 20 2e 66 69 78 65 64 2d 62 6f 74 74 6f 6d 2c 20 2e 69 73 2d 66 69 78 65 64 2c 20 2e 73 74 69 63 6b 79 2d 74 6f 70 22 2c 53 54 49 43 4b 59 5f 43 4f 4e 54 45 4e 54 3a 22 2e 73 74 69 63 6b 79 2d 74 6f 70 22 2c 4e 41 56 42 41 52 5f 54 4f 47 47 4c 45 52 3a 22 2e 6e 61 76 62 61 72 2d 74 6f 67 67 6c 65 72 22 7d 2c 70 3d 66 75 6e 63 74 69 Data Ascii: d="fade",_="show",g={DIALOG:".modal-dialog",DATA_TOGGLE:'[data-toggle="modal"]',DATA_DISMISS:'[data-dismiss="modal"]',FIXED_CONTENT:".fixed-top, .fixed-bottom, .is-fixed, .sticky-top",STICKY_CONTENT:".sticky-top",NAVBAR_TOGGLER:".navbar-toggler"},p=functi
2022-06-30 16:43:13 UTC	792	IN	Data Raw: 6c 74 28 29 2c 21 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 26 26 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 29 7b 76 61 72 20 69 3d 74 2e 45 76 65 6e 74 28 68 2e 48 49 44 45 29 3b 69 66 28 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 69 29 2c 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 26 26 21 69 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 3d 21 31 3b 76 61 72 20 73 3d 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 64 29 3b 73 26 26 28 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 21 30 29 2c 74 68 69 73 2e 5f 73 65 74 Data Ascii: lt(),!this._isTransitioning&&this._isShown){var i=t.Event(h.HIDE);if(t(this._element).trigger(i),this._isShown&&!i.isDefaultPrevented()){this._isShown=!1;var s=P.supportsTransitionEnd()&&t(this._element).hasClass(d);s&&(this._isTransitioning=!0),this._set
2022-06-30 16:43:13 UTC	794	IN	Data Raw: 6e 66 6f 72 63 65 46 6f 63 75 73 28 29 3b 76 61 72 20 73 3d 74 2e 45 76 65 6e 74 28 68 2e 53 48 4f 57 4e 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 65 7d 29 2c 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 2e 5f 63 6f 6e 66 69 67 2e 66 6f 63 75 73 26 26 6e 2e 5f 65 6c 65 6d 65 6e 74 2e 66 6f 63 75 73 28 29 2c 6e 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 21 31 2c 74 28 6e 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 73 29 7d 3b 69 3f 74 28 74 68 69 73 2e 5f 64 69 61 6c 6f 67 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 72 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 33 30 30 29 3a 72 28 29 7d 2c 70 2e 5f 65 6e 66 6f 72 63 65 46 6f 63 75 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 Data Ascii: nforceFocus();var s=t.Event(h.SHOWN,{relatedTarget:e}),r=function(){n._config.focus&&n._element.focus(),n._isTransitioning=!1,t(n._element).trigger(s)};i?t(this._dialog).one(P.TRANSITION_END,r).emulateTransitionEnd(300):r()},p._enforceFocus=function(){var
2022-06-30 16:43:13 UTC	795	IN	Data Raw: 62 61 63 6b 64 72 6f 70 2e 63 6c 61 73 73 4e 61 6d 65 3d 75 2c 69 26 26 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 61 64 64 43 6c 61 73 73 28 69 29 2c 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 61 70 70 65 6e 64 54 6f 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 68 2e 43 4c 49 43 4b 5f 44 49 53 4d 49 53 53 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 6e 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3f 6e 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3d 21 31 3a 74 2e 74 61 72 67 65 74 3d 3d 3d 74 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 3d 6e 2e 5f 63 6f 6e 66 69 67 2e 62 61 63 6b 64 72 6f 70 3f 6e 2e 5f Data Ascii: backdrop.className=u,i&&t(this._backdrop).addClass(i),t(this._backdrop).appendTo(document.body),t(this._element).on(h.CLICK_DISMISS,function(t){n._ignoreBackdropClick?n._ignoreBackdropClick=!1:t.target===t.currentTarget&&("static"===n._config.backdrop?n._

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	796	IN	Data Raw: 74 28 69 29 5b 30 5d 2e 73 74 79 6c 65 2e 70 61 64 64 69 6e 67 52 69 67 68 74 2c 72 3d 74 28 69 29 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 29 3b 74 28 69 29 2e 64 61 74 61 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 73 29 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 70 61 72 73 65 46 6c 6f 61 74 28 72 29 2b 65 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 2b 22 70 78 22 29 7d 29 2c 74 28 67 2e 53 54 49 43 4b 59 5f 43 4f 4e 54 45 4e 54 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 69 29 7b 76 61 72 20 73 3d 74 28 69 29 5b 30 5d 2e 73 74 79 6c 65 2e 6d 61 72 67 69 6e 52 69 67 68 74 2c 72 3d 74 28 69 29 2e 63 73 73 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 29 3b 74 28 69 29 2e 64 61 74 61 28 22 6d 61 Data Ascii: t(i)[0].style.paddingRight,r=t(i).css("padding-right");t(i).data("padding-right",s).css("padding-right",parseFloat(r)+e._scrollbarWidth+"px")}),t(g.STICKY_CONTENT).each(function(n,i){var s=t(i)[0].style.marginRight,r=t(i).css("margin-right");t(i).data("ma
2022-06-30 16:43:13 UTC	798	IN	Data Raw: 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 69 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 73 3d 74 28 74 68 69 73 29 2e 64 61 74 61 28 6e 29 2c 61 3d 72 28 7b 7d 2c 6f 2e 44 65 66 61 75 6c 74 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 29 3b 69 66 28 73 7c 7c 28 73 3d 6e 65 77 20 6f 28 74 68 69 73 2c 61 29 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 6e 2c 73 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 73 5b 65 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 Data Ascii: yInterface=function(e,i){return this.each(function(){var s=t(this).data(n),a=r({},o.Default,t(this).data(),"object"==typeof e&&e);if(s||(s=new o(this,a),t(this).data(n,s)),"string"==typeof e){if("undefined"==typeof s[e])throw new TypeError('No method name
2022-06-30 16:43:13 UTC	799	IN	Data Raw: 41 55 54 4f 3a 22 61 75 74 6f 22 2c 54 4f 50 3a 22 74 6f 70 22 2c 52 49 47 48 54 3a 22 72 69 67 68 74 22 2c 42 4f 54 54 4f 4d 3a 22 62 6f 74 74 6f 6d 22 2c 4c 45 46 54 3a 22 6c 65 66 74 22 7d 2c 75 3d 7b 61 6e 69 6d 61 74 69 6f 6e 3a 21 30 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 61 72 72 6f 77 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 2d 69 6e 6e 65 72 22 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 27 2c 74 72 69 67 67 65 72 3a 22 68 6f 76 65 72 20 66 6f 63 75 73 22 2c 74 69 74 6c 65 3a 22 22 2c 64 65 6c 61 79 3a 30 2c 68 74 6d 6c 3a 21 31 2c 73 65 6c 65 63 74 6f 72 3a 21 31 2c 70 6c 61 Data Ascii: AUTO:"auto",TOP:"top",RIGHT:"right",BOTTOM:"bottom",LEFT:"left"},u={animation:!0,template:' ',trigger:"hover focus",title:"",delay:0,html:!1,selector:!1,pla
2022-06-30 16:43:13 UTC	800	IN	Data Raw: 34 33 37 31 0d 0a 75 63 74 6f 72 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 2c 74 68 69 73 2e 5f 67 65 74 44 65 6c 65 67 61 74 65 43 6f 6e 66 69 67 28 29 29 2c 74 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 6e 2c 69 29 29 2c 69 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 2e 63 6c 69 63 6b 3d 21 69 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 2e 63 6c 69 63 6b 2c 69 2e 5f 69 73 57 69 74 68 41 63 74 69 76 65 54 72 69 67 67 65 72 28 29 3f 69 2e 5f 65 6e 74 65 72 28 6e 75 6c 6c 2c 69 29 3a 69 2e 5f 6c 65 61 76 65 28 6e 75 6c 6c 2c 69 29 7d 65 6c 73 65 7b 69 66 28 74 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 2e 68 61 73 43 6c 61 73 73 28 70 29 29 72 65 74 75 72 6e 20 76 6f 69 64 20 74 68 69 73 2e 5f 6c 65 Data Ascii: 4371uctor(e.currentTarget,this._getDelegateConfig()),t(e.currentTarget).data(n,i)),i._activeTrigger.click=!i._activeTrigger.click,i._isWithActiveTrigger()?i._enter(null,i):i._leave(null,i)}else{if(t(this.getTipElement()).hasClass(p))return void this._le
2022-06-30 16:43:13 UTC	802	IN	Data Raw: 2e 63 6f 6e 66 69 67 2e 70 6c 61 63 65 6d 65 6e 74 2c 68 3d 74 68 69 73 2e 5f 67 65 74 41 74 74 61 63 68 6d 65 6e 74 28 6c 29 3b 74 68 69 73 2e 61 64 64 41 74 74 61 63 68 6d 65 6e 74 43 6c 61 73 73 28 68 29 3b 76 61 72 20 63 3d 21 31 3d 3d 3d 74 68 69 73 2e 63 6f 6e 66 69 67 2e 63 6f 6e 74 61 69 6e 65 72 3f 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 3a 74 28 74 68 69 73 2e 63 6f 6e 66 69 67 2e 63 6f 6e 74 61 69 6e 65 72 29 3b 74 28 72 29 2e 64 61 74 61 28 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 41 54 41 5f 4b 45 59 2c 74 68 69 73 29 2c 74 2e 63 6f 6e 74 61 69 6e 73 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 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 74 68 69 73 2e 74 69 70 29 7c 7c 74 28 72 29 2e 61 Data Ascii: .config.placement,h=this._getAttachment(l);this.addAttachmentClass(h);var c=!1===this.config.container?document.body:t(this.config.container);t(r).data(this.constructor.DATA_KEY,this),t.contains(this.element.ownerDocument.documentElement,this.tip)||t(r).a
2022-06-30 16:43:13 UTC	803	IN	Data Raw: 76 65 6e 74 2e 48 49 44 44 45 4e 29 2c 6e 75 6c 6c 21 3d 3d 6e 2e 5f 70 6f 70 70 65 72 26 26 6e 2e 5f 70 6f 70 70 65 72 2e 64 65 73 74 72 6f 79 28 29 2c 65 26 26 65 28 29 7d 3b 74 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 73 29 2c 73 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 28 68 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 70 29 2c 22 6f 6e 74 6f 75 63 68 73 74 61 72 74 22 69 6e 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 26 26 74 28 22 62 6f 64 79 22 29 2e 63 68 69 6c 64 72 65 6e 28 29 2e 6f 66 66 28 22 6d 6f 75 73 65 6f 76 65 72 22 2c 6e 75 6c 6c 2c 74 2e 6e 6f 6f 70 29 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 79 5d 3d 21 31 2c 74 68 69 73 2e Data Ascii: vent.HIDDEN),null!==n._popper&&n._popper.destroy(),e&&e()};t(this.element).trigger(s),s.isDefaultPrevented()||(t(i).removeClass(p),"ontouchstart"in document.documentElement&&t("body").children().off("mouseover",null,t.noop),this._activeTrigger[y]=!1,this.
2022-06-30 16:43:13 UTC	804	IN	Data Raw: 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 69 66 28 22 63 6c 69 63 6b 22 3d 3d 3d 6e 29 74 28 65 2e 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 43 4c 49 43 4b 2c 65 2e 63 6f 6e 66 69 67 2e 73 65 6c 65 63 74 6f 72 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 2e 74 6f 67 67 6c 65 28 74 29 7d 29 3b 65 6c 73 65 20 69 66 28 6e 21 3d 43 29 7b 76 61 72 20 69 3d 6e 3d 3d 45 3f 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 4d 4f 55 53 45 45 4e 54 45 52 3a 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 46 4f 43 55 53 49 4e 2c 73 3d 6e 3d 3d 45 3f 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 4d 4f 55 53 45 4c 45 41 56 45 3a 65 2e 63 6f 6e 73 Data Ascii: ach(function(n){if("click"===n)t(e.element).on(e.constructor.Event.CLICK,e.config.selector,function(t){return e.toggle(t)});else if(n!==C){var i=n===E?e.constructor.Event.MOUSEENTER:e.constructor.Event.FOCUSIN,s=n===E?e.constructor.Event.MOUSELEAVE:e.cons
2022-06-30 16:43:13 UTC	806	IN	Data Raw: 6f 72 2e 44 41 54 41 5f 4b 45 59 3b 28 6e 3d 6e 7c 7c 74 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 69 29 29 7c 7c 28 6e 3d 6e 65 77 20 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 2c 74 68 69 73 2e 5f 67 65 74 44 65 6c 65 67 61 74 65 43 6f 6e 66 69 67 28 29 29 2c 74 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 69 2c 6e 29 29 2c 65 26 26 28 6e 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 22 66 6f 63 75 73 6f 75 74 22 3d 3d 3d 65 2e 74 79 70 65 3f 54 3a 45 5d 3d 21 31 29 2c 6e 2e 5f 69 73 57 69 74 68 41 63 74 69 76 65 54 72 69 67 67 65 72 28 29 7c 7c 28 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 6e 2e 5f 74 69 6d 65 6f 75 74 29 2c 6e 2e 5f 68 6f 76 65 72 53 Data Ascii: or.DATA_KEY;(n=n||t(e.currentTarget).data(i))||(n=new this.constructor(e.currentTarget,this._getDelegateConfig()),t(e.currentTarget).data(i,n)),e&&(n._activeTrigger["focusout"===e.type?T:E]=!1),n._isWithActiveTrigger()||(clearTimeout(n._timeout),n._hoverS

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	807	IN	Data Raw: 6d 6f 76 65 43 6c 61 73 73 28 67 29 2c 74 68 69 73 2e 63 6f 6e 66 69 67 2e 61 6e 69 6d 61 74 69 6f 6e 3d 21 31 2c 74 68 69 73 2e 68 69 64 65 28 29 2c 74 68 69 73 2e 73 68 6f 77 28 29 2c 74 68 69 73 2e 63 6f 6e 66 69 67 2e 61 6e 69 6d 61 74 69 6f 6e 3d 6e 29 7d 2c 61 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 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 6e 3d 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 29 2c 73 3d 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 3b 69 66 28 28 6e 7c 7c 21 2f 64 69 73 70 6f 73 65 7c 68 69 64 65 2f 2e 74 65 73 74 28 65 29 29 26 26 28 6e 7c 7c 28 6e 3d 6e 65 77 20 61 28 74 68 69 73 2c 73 29 2c 74 28 74 68 69 73 29 2e Data Ascii: moveClass(g),this.config.animation=!1,this.hide(),this.show(),this.config.animation=n)},a._jQueryInterface=function(e){return this.each(function(){var n=t(this).data(i),s="object"==typeof e&&e;if((n||!/dispose|hide/.test(e))&&(n||(n=new a(this,s),t(this).
2022-06-30 16:43:13 UTC	808	IN	Data Raw: 53 4f 55 54 3a 22 66 6f 63 75 73 6f 75 74 22 2b 69 2c 4d 4f 55 53 45 45 4e 54 45 52 3a 22 6d 6f 75 73 65 6e 74 65 72 22 2b 69 2c 4d 4f 55 53 45 4c 45 41 56 45 3a 22 6d 6f 75 73 65 6c 65 61 76 65 22 2b 69 7d 2c 67 3d 66 75 6e 63 74 69 6f 6e 28 72 29 7b 76 61 72 20 6f 2c 67 3b 66 75 6e 63 74 69 6f 6e 20 70 28 29 7b 72 65 74 75 72 6e 20 72 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7c 7c 74 68 69 73 7d 67 3d 72 2c 28 6f 3d 70 29 2e 70 72 6f 74 6f 74 79 70 65 3d 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 28 67 2e 70 72 6f 74 6f 74 79 70 65 29 2c 6f 2e 70 72 6f 74 6f 74 79 70 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3d 6f 2c 6f 2e 5f 5f 70 72 6f 74 6f 5f 5f 3d 67 3b 76 61 72 20 6d 3d 70 2e 70 72 6f 74 6f 74 79 70 65 3b 72 65 74 75 72 6e 20 Data Ascii: SOUT:"focusout"+i,MOUSEENTER:"mouseenter"+i,MOUSELEAVE:"mouseleave"+i},g=function(r){var o,g;function p(){return r.apply(this,arguments)||this}g=r,(o=p).prototype=Object.create(g.prototype),o.prototype.constructor=o,o.__proto__=g;var m=p.prototype;return
2022-06-30 16:43:13 UTC	810	IN	Data Raw: 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 65 7d 7d 2c 7b 6b 65 79 3a 22 44 41 54 41 5f 4b 45 59 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 7d 7d 2c 7b 6b 65 79 3a 22 45 76 65 6e 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 5f 7d 7d 2c 7b 6b 65 79 3a 22 45 56 45 4e 54 5f 4b 45 59 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 69 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 54 79 70 65 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 68 7d 7d 5d 29 2c 70 7d 28 55 29 3b 72 65 74 75 72 6e 20 74 2e 66 6e 5b 65 5d 3d 67 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 5b 65 5d 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 67 2c 74 Data Ascii: unction(){return e}},{key:"DATA_KEY",get:function(){return n}},{key:"Event",get:function(){return _}},{key:"EVENT_KEY",get:function(){return i}},{key:"DefaultType",get:function(){return h}}]),p}(U);return t.fn[e]=g._jQueryInterface,t.fn[e].Constructor=g,t
2022-06-30 16:43:13 UTC	811	IN	Data Raw: 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 2c 6e 3d 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 3d 3d 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 77 69 6e 64 6f 77 3f 64 3a 5f 2c 69 3d 22 61 75 74 6f 22 3d 3d 3d 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 67 65 74 28 6f 64 3f 6e 3a 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6d 65 74 68 6f 64 2c 73 3d 69 3d 3d 3d 5f 3f 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 54 6f 70 28 29 3a 30 3b 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 5f 74 61 72 67 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 48 65 69 67 68 74 3d 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 74 68 69 73 2e 5f 73 65 6c Data Ascii: on(){var e=this,n=this._scrollElement===this._scrollElement.window?d:_,i="auto"===this._config.method?n:this._config.method,s=i===_?this._getScrollTop():0;this._offsets=[],this._targets=[],this._scrollHeight=this._getScrollHeight(),t.makeArray(t(this._sel
2022-06-30 16:43:13 UTC	812	IN	Data Raw: 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 67 65 74 42 6f 75 6e 64 69 6e 67 43 6c 69 65 6e 74 52 65 63 74 28 29 2e 68 65 69 67 68 74 7d 2c 67 2e 5f 70 72 6f 63 65 73 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 54 6f 70 28 29 2b 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6f 66 66 73 65 74 2c 65 3d 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 6e 3d 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6f 66 66 73 65 74 2b 65 2d 74 68 69 73 2e 5f 67 65 74 4f 66 66 73 65 74 48 65 69 67 68 74 28 29 3b 69 66 28 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 48 65 69 67 68 74 21 3d 3d 65 26 26 74 68 69 73 2e 72 65 66 72 65 73 68 28 29 2c 74 3e 3d 6e 29 7b 76 61 72 20 69 3d 74 68 69 73 2e 5f 74 61 72 67 65 74 73 5b Data Ascii: rollElement.getBoundingClientRect().height},g._process=function(){var t=this._getScrollTop()+this._config.offset,e=this._getScrollHeight(),n=this._config.offset+e-this._getOffsetHeight();if(this._scrollHeight!==e&&this.refresh(),t>=n){var i=this._targets[
2022-06-30 16:43:13 UTC	814	IN	Data Raw: 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 69 5b 65 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 64 20 22 27 2b 65 2b 27 22 27 29 3b 69 5b 65 5d 28 29 7d 7d 29 7d 2c 73 28 6f 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 30 2e 30 22 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 7d 7d 5d 29 2c 6f 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 68 2e 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 66 6f 72 28 76 61 72 20 65 Data Ascii: ypeof e){if("undefined"==typeof i[e])throw new TypeError('No method named "'+e+'"');i[e]()}})},s(o,null,[{key:"VERSION",get:function(){return"4.0.0"}},{key:"Default",get:function(){return a}}]),o}();return t(window).on(h.LOAD_DATA_API,function(){for(var e
2022-06-30 16:43:13 UTC	815	IN	Data Raw: 69 26 26 74 28 69 29 2e 74 72 69 67 67 65 72 28 63 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 75 2e 45 76 65 6e 74 50 72 65 76 65 6e 74 65 64 28 29 26 26 21 63 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 6f 26 26 28 6e 3d 74 28 6f 29 5b 30 5d 29 2c 74 68 69 73 2e 5f 61 63 74 69 76 61 74 65 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 63 29 3b 76 61 72 20 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6e 3d 74 2e 45 76 65 6e 74 28 72 2e 48 49 44 44 45 4e 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 65 2e 5f 65 6c 65 6d 65 6e 74 7d 29 2c 73 3d 74 2e 45 76 65 6e 74 28 72 2e 53 48 4f 57 4e 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 69 7d 29 3b 74 28 69 29 2e 74 Data Ascii: i&&t(i).trigger(c),t(this._element).trigger(u),!u.isDefaultPrevented()&&!c.isDefaultPrevented()){o&&(n=t(o)[0]),this._activate(this._element,s);var g=function(){var n=t.Event(r.HIDDEN,{relatedTarget:e._element}),s=t.Event(r.SHOWN,{relatedTarget:i});t(i).t
2022-06-30 16:43:13 UTC	816	IN	Data Raw: 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 30 2e 30 22 7d 7d 5d 29 2c 6e 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 72 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 67 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 76 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 74 28 74 68 69 73 29 2c 22 73 68 6f 77 22 29 7d 29 2c 74 2e 66 6e 2e 74 61 62 3d 76 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 2e 74 61 62 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 76 2c 74 2e 66 6e 2e 74 61 62 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 74 2e 66 6e 2e 74 61 62 3d 69 2c 76 2e 5f 6a 51 75 65 72 79 Data Ascii: nction(){return"4.0.0"}}]),n}();return t(document).on(r.CLICK_DATA_API,g,function(e){e.preventDefault(),v._jQueryInterface.call(t(this),"show")}),t.fn.tab=v._jQueryInterface,t.fn.tab.Constructor=v,t.fn.tab.noConflict=function(){return t.fn.tab=i,v._jQuery
2022-06-30 16:43:13 UTC	817	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49951	104.17.25.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	748	OUT	GET /ajax/libs/popper.js/1.12.9/umd/popper.min.js HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: https://verbena-woolly-clutch.glitch.me User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:12 UTC	749	IN	HTTP/1.1 200 OK Date: Thu, 30 Jun 2022 16:43:12 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/"5eb03fa9-4af4" 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: 1189654 Expires: Tue, 20 Jun 2023 16:43:12 GMT Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=g2lQasYawQzWliqy2O%2BH29lN4poYRT9Q9B1LNBe6GRi3cq4fo3SUcbv8x0oas6S7RxSdDnSisPA1xZn9ltAFVx82v9I3X6KtYFXMbozpQCta9ZbtGkh9VnIRdYNTR%2F9nDOQkgEGY"}],"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: 72385c0e1fe29152-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-06-30 16:43:12 UTC	750	IN	Data Raw: 39 36 37 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 37 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: 967/* Copyright (C) Federico Zivolo 2017 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 16:43:12 UTC	750	IN	Data Raw: 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 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 6e 63 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}func
2022-06-30 16:43:12 UTC	751	IN	Data Raw: 3d 3d 69 29 7b 76 61 72 20 6e 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 6e 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 66 75 6e 63 74 69 6f 6e 20 6c 28 65 2c 74 29 7b 76 61 72 20 6f 3d 32 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 32 5d 2c 69 3d 61 28 74 2c 27 74 6f 70 27 29 2c 6e 3d 61 28 74 2c 27 6c 65 66 74 27 29 2c 72 3d 6f 3f 2d 31 3a 31 3b 72 65 74 75 72 6e 20 65 2e 74 6f 70 2b 3d 69 2a 72 2c 65 2e 62 6f 74 74 6f 6d 2b 3d 69 2a 72 2c 65 2e 6c 65 Data Ascii: ==i){var n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||n;return r[o]}return e[o]}function l(e,t){var o=2<arguments.length&&void 0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,'left'),r=o?-1:1;return e.top+=i*r,e.bottom+=i*r,e.le

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	752	IN	Data Raw: 34 31 38 64 0d 0a 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 73 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 68 74 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 67 28 65 29 7b 76 61 72 20 6f 3d 7b 7d 3b 69 66 28 69 65 28 29 29 74 72 79 7b 6f 3d 65 2e 67 65 74 42 6f 75 6e 64 69 6e 67 43 6c 69 65 6e 74 52 65 63 74 28 29 3b 76 61 72 20 69 3d 61 28 65 2c 27 74 6f 70 27 29 2c 6e 3d 61 28 65 2c 27 6c 65 66 74 27 29 3b 6f 2e 74 6f 70 2b 3d 69 2c 6f 2e 6c 65 66 74 2b 3d 6e 2c 6f 2e 62 6f 74 74 6f 6d 2b 3d 69 2c 6f 2e 72 69 67 68 74 2b 3d 6e 7d 63 61 74 63 68 28 65 29 7b 7d 65 6c 73 Data Ascii: 418d,width:m('Width',e,t,o)}}function c(e){return se({},e,{right:e.left+e.width,bottom:e.top+e.height})}function g(e){var o={};if(ie())try{o=e.getBoundingClientRect();var i=a(e,'top'),n=a(e,'left');o.top+=i,o.left+=n,o.bottom+=i,o.right+=n}catch(e){}els
2022-06-30 16:43:12 UTC	753	IN	Data Raw: 78 65 64 27 3d 3d 3d 74 28 65 2c 27 70 6f 73 69 74 69 6f 6e 27 29 7c 7c 77 28 6f 28 65 29 29 7d 66 75 6e 63 74 69 6f 6e 20 79 28 65 2c 74 2c 69 2c 72 29 7b 76 61 72 20 70 3d 7b 74 6f 70 3a 30 2c 6c 65 66 74 3a 30 7d 2c 73 3d 64 28 65 2c 74 29 3b 69 66 28 27 76 69 65 77 70 6f 72 74 27 3d 3d 3d 72 29 70 3d 62 28 73 29 3b 65 6c 73 65 7b 76 61 72 20 61 3b 27 73 63 72 6f 6c 6c 50 61 72 65 6e 74 27 3d 3d 3d 72 3f 28 61 3d 6e 28 6f 28 74 29 29 2c 27 42 4f 44 59 27 3d 3d 3d 61 2e 6e 6f 64 65 4e 61 6d 65 26 26 28 61 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 29 3a 27 77 69 6e 64 6f 77 27 3d 3d 3d 72 3f 61 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 3a 61 3d Data Ascii: xed'===t(e,'position')||w(o(e))}function y(e,t,i,r){var p={top:0,left:0},s=d(e,t);if('viewport'===r)p=b(s);else{var a;'scrollParent'===r?(a=n(o(t)),'BODY'===a.nodeName&&(a=e.ownerDocument.documentElement)):'window'===r?a=e.ownerDocument.documentElement:a=
2022-06-30 16:43:12 UTC	755	IN	Data Raw: 74 75 72 6e 20 6e 7d 66 75 6e 63 74 69 6f 6e 20 78 28 65 29 7b 76 61 72 20 74 3d 7b 6c 65 66 74 3a 27 72 69 67 68 74 27 2c 72 69 67 68 74 3a 27 6c 65 66 74 27 2c 62 6f 74 74 6f 6d 3a 27 74 6f 70 27 2c 74 6f 70 3a 27 62 6f 74 74 6f 6d 27 7d 3b 72 65 74 75 72 6e 20 65 2e 72 65 70 6c 61 63 65 28 2f 6c 65 66 74 7c 72 69 67 68 74 7c 62 6f 74 74 6f 6d 7c 74 6f 70 2f 67 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 5b 65 5d 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 53 28 65 2c 74 2c 6f 29 7b 6f 3d 6f 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 3b 76 61 72 20 69 3d 4c 28 65 29 2c 6e 3d 7b 77 69 64 74 68 3a 69 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 69 2e 68 65 69 67 68 74 7d 2c 72 3d 2d 31 21 3d 3d 5b 27 72 69 67 68 74 27 2c 27 6c 65 66 74 27 5d 2e 69 Data Ascii: turn n}function x(e){var t={left:'right',right:'left',bottom:'top',top:'bottom'};return e.replace(/left|right|bottom|top/g,function(e){return t[e]})}function S(e,t,o){o=o.split('-')[0];var i=L(e),n={width:i.width,height:i.height},r=-1!==['right','left'].i
2022-06-30 16:43:12 UTC	756	IN	Data Raw: 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2e 70 6f 73 69 74 69 6f 6e 3d 27 61 62 73 6f 6c 75 74 65 27 2c 65 3d 43 28 74 68 69 73 2e 6d 6f 64 69 66 69 65 72 73 2c 65 29 2c 74 68 69 73 2e 73 74 61 74 65 2e 69 73 43 72 65 61 74 65 64 3f 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 6e 55 70 64 61 74 65 28 65 29 3a 28 74 68 69 73 2e 73 74 61 74 65 2e 69 73 43 72 65 61 74 65 64 3d 21 30 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 6e 43 72 65 61 74 65 28 65 29 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 6b 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 65 2e 73 6f 6d 65 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 65 2e 6e 61 6d 65 2c 69 3d 65 2e 65 6e 61 62 6c 65 64 3b 72 65 74 75 72 6e 20 69 26 26 Data Ascii: ference,e.placement),e.offsets.popper.position='absolute',e=C(this.modifiers,e),this.state.isCreated?this.options.onUpdate(e):(this.state.isCreated=!0,this.options.onCreate(e))}}function k(e,t){return e.some(function(e){var o=e.name,i=e.enabled;return i&&
2022-06-30 16:43:12 UTC	757	IN	Data Raw: 65 74 75 72 6e 20 42 28 65 29 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 72 65 73 69 7a 65 27 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 29 2c 74 2e 73 63 72 6f 6c 50 61 72 65 6e 74 73 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 73 63 72 6f 6c 6c 27 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 29 7d 29 2c 74 2e 75 70 64 61 74 65 42 6f 75 6e 64 3d 6e 75 6c 6c 2c 74 2e 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 3d 5b 5d 2c 74 2e 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 21 31 2c 74 7d 66 75 6e 63 74 69 6f 6e 20 52 28 29 7b 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 Data Ascii: eturn B(e).removeEventListener('resize',t.updateBound),t.scrollParents.forEach(function(e){e.removeEventListener('scroll',t.updateBound)}),t.updateBound=null,t.scrollParents=[],t.scrollElement=null,t.eventsEnabled=!1,t}function R(){this.state.eventsEnable
2022-06-30 16:43:12 UTC	759	IN	Data Raw: 7d 76 61 72 20 64 3d 63 28 73 29 3b 72 65 74 75 72 6e 20 64 5b 74 5d 2f 31 30 30 2a 72 7d 69 66 28 27 76 68 27 3d 3d 3d 70 7c 7c 27 76 77 27 3d 3d 3d 70 29 7b 76 61 72 20 61 3b 72 65 74 75 72 6e 20 61 3d 27 76 68 27 3d 3d 3d 70 3f 4a 28 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 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 3a 4a 28 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 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 61 2f 31 30 30 2a 72 7d 72 65 74 75 72 6e 20 72 7d 66 75 6e 63 74 69 6f 6e 20 7a 28 65 2c 74 2c 6f 29 7b 76 61 72 20 6e 3d 5b 30 2c 30 5d 2c 72 3d 2d 31 21 Data Ascii: }var d=c(s);return d[t]/100*r}if('vh'===p||'vw'===p){var a;return a='vh'===p?J(document.documentElement.clientHeight,window.innerHeight||0):J(document.documentElement.clientWidth,window.innerWidth||0),a/100*r}return r}function z(e,t,o,i){var n=[0,0],r=-1!
2022-06-30 16:43:12 UTC	760	IN	Data Raw: 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 64 6f 63 75 6d 65 6e 74 2c 5a 3d 5b 27 45 64 67 65 27 2c 27 54 72 69 64 65 6e 74 27 2c 27 46 69 72 65 66 6f 78 27 5d 2c 24 3d 30 2c 65 65 3d 30 3b 65 65 3c 5a 2e 6c 65 6e 67 74 68 3b 65 65 2b 3d 31 29 69 66 28 51 26 26 30 3c 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 5a 5b 65 65 5d 29 29 7b 24 3d 31 3b 62 72 65 61 6b 7d 76 61 72 20 69 2c 74 65 3d 51 26 26 77 69 6e 64 6f 77 2e 50 72 6f 6d 69 73 65 2c 6f 65 3d 74 65 3f 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 21 31 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 74 7c 7c 28 74 3d 21 30 2c 77 69 6e 64 6f 77 2e 50 72 6f 6d 69 73 65 2e 72 65 73 6f 6c 76 65 28 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e Data Ascii: ined'!=typeof document,Z=['Edge','Trident','Firefox'],$=0,ee=0;ee<Z.length;ee+=1)if(Q&&0<=navigator.userAgent.indexOf(Z[ee])){$=1;break}var i,te=Q&&window.Promise,oe=te?function(e){var t=!1;return function(){t||(t=!0,window.Promise.resolve().then(function
2022-06-30 16:43:12 UTC	761	IN	Data Raw: 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 3f 61 72 67 75 6d 65 6e 74 73 5b 32 5d 3a 7b 7d 3b 6e 65 28 74 68 69 73 2c 74 29 2c 74 68 69 73 2e 73 63 68 65 64 75 6c 65 55 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 72 65 71 75 65 73 74 41 6e 69 6d 61 74 69 6f 6e 46 72 61 6d 65 28 6e 2e 75 70 64 61 74 65 29 7d 2c 74 68 69 73 2e 75 70 64 61 74 65 3d 6f 65 28 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 73 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 50 61 72 Data Ascii: ments.length&&void 0!==arguments[2]?arguments[2]:{};ne(this,t),this.scheduleUpdate=function(){return requestAnimationFrame(n.update)},this.update=oe(this.update.bind(this)),this.options=se({},t.Defaults,r),this.state={isDestroyed:!1,isCreated:!1,scrollPar

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:12 UTC	763	IN	Data Raw: 3a 7b 6f 72 64 65 72 3a 31 30 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 29 7b 76 61 72 20 74 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2c 6f 3d 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 2c 69 3d 74 2e 73 70 6c 69 74 28 27 2d 27 29 5b 31 5d 3b 69 66 28 69 29 7b 76 61 72 20 6e 3d 65 2e 6f 66 66 73 65 74 73 2c 72 3d 6e 2e 72 65 66 65 72 65 6e 63 65 2c 70 3d 6e 2e 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 70 65 28 7b 7d 2c 64 2c 72 5b 64 5d 29 2c 65 6e 64 3a 70 65 28 7b 7d 2c 64 2c 72 5b 64 5d 2b 72 5b 61 Data Ascii: :{order:100,enabled:!0,fn:function(e){var t=e.placement,o=t.split('-')[0],i=t.split('-')[1];if(i){var n=e.offsets,r=n.reference,p=n.popper,s=-1!==['bottom','top'].indexOf(o),d=s?'left':'top',a=s?'width':'height',l={start:pe({},d,r[d]),end:pe({},d,r[d]+r[a
2022-06-30 16:43:12 UTC	764	IN	Data Raw: 26 28 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 64 5d 3d 72 28 69 5b 73 5d 29 29 2c 65 7d 7d 2c 61 72 72 6f 77 3a 7b 6f 72 64 65 72 3a 35 30 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 6f 29 7b 76 61 72 20 69 3b 69 66 28 21 46 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 69 65 72 73 2c 27 61 72 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 6e 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 6e 29 7b 69 66 28 6e 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 6e 29 2c 21 6e 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 Data Ascii: &(e.offsets.popper[d]=r(i[s])),e}},arrow:{order:500,enabled:!0,fn:function(e,o){var i;if(!F(e.instance.modifiers,'arrow','keepTogether'))return e;var n=o.element;if('string'==typeof n){if(n=e.instance.popper.querySelector(n),!n)return e;}else if(!e.instan
2022-06-30 16:43:12 UTC	765	IN	Data Raw: 53 45 3a 70 3d 71 28 69 2c 21 30 29 3b 62 72 65 61 6b 3b 64 65 66 61 75 6c 74 3a 70 3d 74 2e 62 65 68 61 76 69 6f 72 3b 7d 72 65 74 75 72 6e 20 70 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 73 2c 64 29 7b 69 66 28 69 21 3d 3d 73 7c 7c 70 2e 6c 65 6e 67 74 68 3d 3d 3d 64 2b 31 29 72 65 74 75 72 6e 20 65 3b 69 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 6e 3d 78 28 69 29 3b 76 61 72 20 61 3d 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 66 3d 58 2c 6d 3d 27 6c 65 66 74 27 3d 3d 3d 69 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 69 26 26 66 28 61 2e 6c 65 66 74 29 3c 66 28 6c 2e 72 69 Data Ascii: SE:p=q(i,!0);break;default:p=t.behavior;}return p.forEach(function(s,d){if(i!==s||p.length===d+1)return e;i=e.placement.split('-')[0],n=x(i);var a=e.offsets.popper,l=e.offsets.reference,f=X,m='left'===i&&f(a.right)>f(l.left)||'right'===i&&f(a.left)<f(l.ri
2022-06-30 16:43:12 UTC	767	IN	Data Raw: 2e 6e 61 6d 65 7d 29 2e 62 6f 75 6e 64 61 72 69 65 73 3b 69 66 28 74 2e 62 6f 74 74 6f 6d 3c 6f 2e 74 6f 70 7c 7c 74 2e 6c 65 66 74 3e 6f 2e 72 69 67 68 74 7c 7c 74 2e 74 6f 70 3e 6f 2e 62 6f 74 74 6f 6d 7c 7c 74 2e 72 69 67 68 74 3c 6f 2e 6c 65 66 74 29 7b 69 66 28 21 30 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 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 Data Ascii: .name}).boundaries;if(t.bottom<o.top||t.left>o.right||t.top>o.bottom||t.right<o.left){if(!0===e.hide)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}},compute
2022-06-30 16:43:12 UTC	768	IN	Data Raw: 69 62 75 74 65 73 29 2c 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 26 26 4f 62 6a 65 63 74 2e 6b 65 79 73 28 65 2e 61 72 72 6f 77 53 74 79 6c 65 73 29 2e 6c 65 6e 67 74 68 26 26 59 28 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 2c 65 2e 61 72 72 6f 77 53 74 79 6c 65 73 29 2c 65 7d 2c 6f 6e 4c 6f 61 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 2c 69 2c 6e 29 7b 76 61 72 20 72 3d 4f 28 6e 2c 74 2c 65 29 2c 70 3d 76 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 Data Ascii: ibutes),e.arrowElement&&Object.keys(e.arrowStyles).length&&Y(e.arrowElement,e.arrowStyles),e},onLoad:function(e,t,o,i,n){var r=O(n,t,e),p=v(o.placement,r,t,e,o.modifiers.flip.boundariesElement,o.modifiers.flip.padding);return t.setAttribute('x-placement',
2022-06-30 16:43:12 UTC	768	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49953	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	817	OUT	GET /css/hover.css HTTP/1.1 Host: verbena-woolly-clutch.glitch.me Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:13 UTC	818	IN	HTTP/1.1 404 Not Found Date: Thu, 30 Jun 2022 16:43:13 GMT Content-Length: 3672 Connection: close Cache-Control: max-age=0

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:13 UTC	818	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 6c 6c 2c 20 79 6f 75 20 66 6f 75 6e 64 20 61 20 67 6c 69 74 63 68 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6c 6f 75 64 2e 77 65 62 74 79 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Well, you found a glitch.</title> <meta name="viewport" content="initial-scale=1, width=device-width"> <link rel="stylesheet" type="text/css" href ="https://cloud.webty

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49973	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	821	OUT	POST /o/RemoteUls.ashx?usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&officeserverversion=16.0.15417.41022 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 1321 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	825	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 04a638d2-058b-4b14-b824-0aa7c34f3ada X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006956 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onedrive.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-bULS-SuppressedTags: 378069,1671813,2209344,3290144,4298965,4298968,4298969,4751696,5306497,5904476,6375195,6572226,6948167,7463498,17085210,17085216,17162522,17358857,19743902,21627712,21631370,22401293,22410500,22558617,22598977,22680210,22680213,22680214,22836558,22946650,23909858,24401375,24462656,24515087,25514973,33592839,34388130,35682372,36472266,36546380,36546381,36546382,36569418,36708451,36773964,36791688,36811158,36811159,36963655,37288035,37876293,37876294,37889309,38293640,38535900,38543496,38580697,38637954,38922202,39076766,39076767,39105358,39408129,39613840,39966341,40437001,40935455,40957978,40957979,41003225,41207258,41502555,41711299,41952657,41964821,41964885,42272991,42496725,42513088,42815875,42857251,50406866,50431969,50619726,50622685,50622687,51451613,51504083,51667010,306230939,524883107,524883136,524883138,537159499,538542792,538543587,539874723,540378699,540378700,542700237,542994947,545783884,557077970,557322386,557389507,557670930,558735363,559423838,559424262,559486496,559760215,559760216,570507662,571549507,571786073,571786074,574468116,575157663,575157664,575157665,575157666,575157667,575157696,575157697,575157698,575157699,575157700,575157701,575157702,577295376,577626581,577831138,578164000,587862985,591684683,591729363,592259104,592556551,592843145,593780815,593838232,593862981,594134597,594396706,594830612,595137156,595714715,595895774,596115913,596444186,596464289,845836083,845836084,845836085,846166132,876178018,963472182,1630679666,1630679667,1633958006,1647605351,1664576567,1698260075,1718235956,1765045358,1802139698,1986689397,1986689633,1986689647,1986748791,1986748793,1986749030,1986749288,1986749546,2004443760,2004444278,2004448354 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006956 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 1E3D3BDC74BC4BD194E0A0AFCC914522 Ref B: AM3EDGE0715 Ref C: 2022-06-30 T16:43:14Z Date: Thu, 30 Jun 2022 16:43:13 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49966	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	824	OUT	GET /toy.htm HTTP/1.1 Host: verbena-woolly-clutch.glitch.me Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 If-None-Match: "49e28388e15f2554c9b456faf7eb2f27" If-Modified-Since: Tue, 28 Jun 2022 11:12:48 GMT
2022-06-30 16:43:14 UTC	831	IN	HTTP/1.1 304 Not Modified Date: Thu, 30 Jun 2022 16:43:14 GMT Connection: close x-amz-id-2: +A9UEO1bijGnAUjs8EqiFZSTpqnfolQ2lDEdz1JRvyfrhkRn0/560epxvJCcqLthafZKuYhucus= x-amz-request-id: GD0VM3DTSNZRFSHQ last-modified: Tue, 28 Jun 2022 11:12:48 GMT etag: "49e28388e15f2554c9b456faf7eb2f27" cache-control: no-cache x-amz-version-id: TZHib0m1dTZVgsFhvlyHpkF7J4OLqBMI server: AmazonS3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49967	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	824	OUT	GET /favicon.ico HTTP/1.1 Host: verbena-woolly-clutch.glitch.me 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://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:14 UTC	832	IN	HTTP/1.1 404 Not Found Date: Thu, 30 Jun 2022 16:43:14 GMT Content-Length: 3672 Connection: close Cache-Control: max-age=0
2022-06-30 16:43:14 UTC	832	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 6c 6c 2c 20 79 6f 75 20 66 6f 75 6e 64 20 61 20 67 6c 69 74 63 68 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6c 6f 75 64 2e 77 65 62 74 79 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Well, you found a glitch.</title> <meta name="viewport" content="initial-scale=1, width=device-width"> <link rel="stylesheet" type="text/css" href ="https://cloud.webty

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49974	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	828	OUT	GET /o/AppSettingsHandler.ashx?app=OneNote&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&build=16.0.15417.41022 HTTP/1.1 Host: onenote.officeapps.live.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: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:14 UTC	828	IN	HTTP/1.1 200 OK Cache-Control: private Content-Length: 2149 Content-Type: application/json; charset=utf-8 P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 578f6064-c034-4b47-b5fd-ca048d82f1db X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onedrive.live.com X-Content-Type-Options: nosniff X-OFFICEFD: AM4PEPF00006B54 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 8E660420D7CB44EEB15FF2064A1118C5 Ref B: AM3EDGE0213 Ref C: 2022-06-30T16:43:14Z Date: Thu, 30 Jun 2022 16:43:14 GMT Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:14 UTC	829	IN	Data Raw: 7b 22 74 69 6d 65 73 74 61 6d 70 22 3a 31 36 35 36 36 30 37 33 39 34 33 36 38 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 55 6c 73 48 65 61 72 74 42 65 61 74 49 73 45 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 53 65 74 74 69 6e 67 73 46 65 74 63 68 50 65 72 69 6f 64 22 3a 36 30 30 30 30 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 55 6c 73 48 65 61 72 74 62 65 61 74 49 6e 74 65 72 76 61 6c 4d 73 22 3a 35 30 30 30 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 4d 61 78 55 6c 73 48 65 61 72 74 62 65 61 74 54 69 6d 65 22 3a 33 30 30 30 30 30 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 4e 6f 43 6f 6d 70 6c 65 74 65 57 61 72 6e 69 6e 67 31 54 69 6d 65 22 3a 31 32 30 30 30 30 2c 22 42 6f 6f 74 73 74 72 61 70 70 65 72 4e 6f 43 6f 6d 70 Data Ascii: {"timestamp":1656607394368,"BootstrapperUlsHeartBeatIsEnabled":false,"BootstrapperSettingsFetchPeriod":60000,"BootstrapperUlsHeartbeatIntervalMs":5000,"BootstrapperMaxUlsHeartbeatTime":300000,"BootstrapperNoCompleteWarning1Time":120000,"BootstrapperNoComp
2022-06-30 16:43:14 UTC	830	IN	Data Raw: 34 30 36 38 36 36 2c 35 30 34 33 31 39 36 39 2c 35 30 36 31 39 37 32 36 2c 35 30 36 32 32 36 38 35 2c 35 30 36 32 32 36 38 37 2c 35 31 34 35 31 36 31 33 2c 35 31 35 30 34 30 38 33 2c 35 31 36 36 37 30 31 30 2c 33 30 36 32 33 30 39 33 39 2c 35 32 34 38 38 33 31 30 37 2c 35 32 34 38 38 33 31 33 36 2c 35 32 34 38 38 33 31 33 38 2c 35 33 37 31 35 39 34 39 39 2c 35 33 38 35 34 32 37 39 32 2c 35 33 38 35 34 33 35 38 37 2c 35 33 39 38 37 34 37 32 33 2c 35 34 30 33 37 38 36 39 39 2c 35 34 30 33 37 38 37 30 30 2c 35 34 32 37 30 30 32 33 37 2c 35 34 32 39 39 34 39 34 37 2c 35 34 35 37 38 33 38 38 34 2c 35 35 37 30 37 37 39 37 30 2c 35 35 37 33 32 32 33 38 36 2c 35 35 37 33 38 39 35 30 37 2c 35 35 37 36 37 30 39 33 30 2c 35 35 38 37 33 35 33 36 33 2c 35 35 39 34 32 Data Ascii: 406866,50431969,50619726,50622685,50622687,51451613,51504083,51667010,306230939,52488310 7,524883136,524883138,537159499,538542792,538543587,539874723,540378699,540378700,542700237,54299494 7,545783884,557077970,557322386,557389507,557670930,558735363,55942

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49976	52.22.91.148	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:15 UTC	835	OUT	GET /css/hover.css HTTP/1.1 Host: verbena-woolly-clutch.glitch.me Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://verbena-woolly-clutch.glitch.me/toy.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-30 16:43:15 UTC	836	IN	HTTP/1.1 404 Not Found Date: Thu, 30 Jun 2022 16:43:15 GMT Content-Length: 3672 Connection: close Cache-Control: max-age=0
2022-06-30 16:43:15 UTC	836	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 57 65 6c 6c 2c 20 79 6f 75 20 66 6f 75 6e 64 20 61 20 67 6c 69 74 63 68 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6c 6f 75 64 2e 77 65 62 74 79 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Well, you found a glitch.</title> <meta name="viewport" content="initial-scale=1, width=device-width"> <link rel="stylesheet" type="text/css" href ="https://cloud.webty

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	50016	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:28 UTC	839	OUT	POST /o/RemoteTelemetry.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 3486 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	8	OUT	POST /o/RemoteTelemetry.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 118 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8lJu1vdQXlP/bseSGMwIgEJuQSe1c=:F
2022-06-30 16:42:43 UTC	9	OUT	Data Raw: 7b 22 74 79 70 65 22 3a 22 4a 53 41 50 49 5f 53 54 41 54 45 22 2c 22 70 61 79 6c 6f 61 64 4a 73 6f 6e 22 3a 22 7b 5c 22 61 70 70 6c 69 63 61 74 69 6f 6e 5c 22 3a 5c 22 4f 6e 65 4e 6f 74 65 5c 22 2c 5c 22 62 75 69 6c 64 5c 22 3a 5c 22 31 36 2e 30 2e 31 35 34 31 37 2e 34 31 30 32 32 5c 22 2c 5c 22 73 74 61 74 65 5c 22 3a 5c 22 69 6e 69 74 5c 22 7d 22 7d Data Ascii: {"type":"JSAPI_STATE","payloadJson":"{\"application\":\"OneNote\",\"build\":\"16.0.15417.41022\",\"state\":\"init\"}"}
2022-06-30 16:42:43 UTC	11	IN	HTTP/1.1 200 OK Cache-Control: private P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: c898ac27-8ed6-4aa4-a01f-a27834250d47 X-UserSessionId: c898ac27-8ed6-4aa4-a01f-a27834250d47 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006958 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onedrive.live.com X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006958 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_visioslice,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: C13E233C05764EBAB8C940FD179F512C Ref B: AM3EDGE0108 Ref C: 2022-06-30T16:42:43Z Date: Thu, 30 Jun 2022 16:42:42 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	50027	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:36 UTC	845	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 23731 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1 033&data=1033; BIGipCookie=00000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000; ShCLSessionID=1656639775607_0.6 675230212797223; BP=l=SDX.Skydrive&FR=&ST=; MUID=210011B4A40D624F14CA0067A00D667C; xidseq=4; E=P:tcNhmbda2og=:PJLCcxjKwQVUWFIETez3k69O9vOeDWpicKYwq8SBqKA=:F; wlidperf=latency=238
2022-06-30 16:43:36 UTC	847	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 37 38 35 36 32 32 2c 22 4c 22 3a 5b 7b 22 47 22 3a 33 38 34 30 35 34 34 36 2c 22 54 22 3a 32 37 38 30 2c 22 4d 22 3a 22 55 73 65 72 41 63 74 69 76 69 74 79 48 6f 73 74 4e 6f 74 69 66 69 63 61 74 69 6f 6e 4d 61 6e 61 67 65 72 3a 20 73 65 6e 64 69 6e 67 20 70 6f 73 74 20 6d 65 73 73 61 67 65 20 74 6f 20 7 4 68 65 20 68 6f 73 74 2e 22 2c 22 43 22 3a 32 30 39 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 35 30 31 38 32 37 35 2c 22 54 22 3a 32 37 38 36 2c 22 4d 22 3a 22 53 65 6e 64 20 73 75 63 63 65 65 64 65 64 2e 20 7b 5c 22 69 64 5c 22 3a 5c 22 55 73 65 72 5f 41 63 74 69 76 69 74 79 5c 22 2c 5c 22 6f 72 69 67 69 6e 5c 22 3a 5c 22 68 74 74 70 73 3a 2f 2f 6f 6e 65 64 72 69 76 65 2e 6c 69 76 65 2e 63 6f 6d 2f 5c 22 7d 22 2c 22 43 Data Ascii: {"T":1656639785622,"L":[{"G":38405446,"T":2780,"M":"UserActivityHostNotificationManager: sending post message to the host.","C":209,"D":50},{"G":5018275,"T":2786,"M":"Send succeeded. {\"id\":\"User_Activity\",\"origin\ ":\"https://onedrive.live.com/\"}","C
2022-06-30 16:43:36 UTC	863	OUT	Data Raw: 2c 5c 22 44 6f 6d 61 69 6e 4c 6f 6f 6b 75 70 45 6e 64 5c 22 3a 5c 22 31 36 31 31 36 2e 30 38 5c 22 2c 5c 22 43 6f 6e 6e 65 63 74 53 74 61 72 74 5c 22 3a 5c 22 31 36 31 31 36 2e 30 38 5c 22 2c 5c 22 43 6f 6e 6e 65 63 74 45 6e 64 5c 22 3a 5c 22 31 36 31 38 34 2e 30 39 5c 22 2c 5c 22 53 65 63 75 72 65 43 6f 6e 6e 65 63 74 69 6f 6e 53 74 61 72 74 5c 22 3a 5c 22 31 36 31 31 36 2e 38 30 35 5c 22 2c 5c 22 52 65 71 75 65 73 74 53 74 61 72 74 5c 22 3a 5c 22 31 36 31 38 34 2e 33 38 5c 22 2c 5c 22 52 65 73 70 6f 6e 73 65 53 74 61 72 74 5c 22 3a 5c 22 31 36 32 31 36 2e 34 38 5c 22 2c 5 c 22 52 65 73 70 6f 6e 73 65 45 6e 64 5c 22 3a 5c 22 31 36 33 30 30 2e 39 33 5c 22 2c 5c 22 44 65 63 6f 64 65 64 42 6f 6 4 79 53 69 7a 65 5c 22 3a 5c 22 37 36 31 36 31 5c 22 2c 5c 22 45 Data Ascii: ,\"DomainLookupEnd\":\"16116.08\",\"ConnectStart\":\"16116.08\",\"ConnectEnd\":\"16184.09\",\"Secu reConnectionStart\":\"16116.805\",\"RequestStart\":\"16184.38\",\"ResponseStart\":\"16216.48\",\"ResponseEnd\" :\"16300.93\",\"DecodedBodySize\":\"76161\",\"E

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:36 UTC	870	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 52244361-7729-4fc6-8900-489c39e69d67 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF0000695B X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF0000695B X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: A8279A8BAC424961B27B5D15AAA3EA33 Ref B: AM3EDGE0222 Ref C: 2022-06-30T16:43:36Z Date: Thu, 30 Jun 2022 16:43:35 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	50036	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:47 UTC	872	OUT	POST /o/OneNote.ashx?perfTag=GetChanges_2 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 2430 X-ServerSideRendering: RenderingFull X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/json; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:43:47 UTC	874	OUT	Data Raw: 7b 22 4d 6f 64 65 22 3a 31 2c 22 73 72 73 22 3a 5b 5b 32 2c 7b 22 4f 70 65 72 61 74 69 6f 6e 49 64 22 3a 31 2c 22 44 65 70 65 6e 64 65 6e 74 4f 6e 22 3a 30 2c 22 4c 6f 63 61 6c 43 6f 62 61 6c 74 53 65 73 73 69 6f 6e 49 64 22 3a 6e 75 6c 6c 2c 22 4c 6f 63 61 6c 43 6f 62 61 6c 74 4d 61 63 68 69 6e 65 49 64 22 3a 6e 75 6c 6c 2c 22 4c 6f 63 61 6c 43 6f 62 61 6c 43 6f 62 61 6c 74 53 65 73 73 69 6f 6e 48 61 73 42 61 63 6b 75 70 22 3a 66 61 6c 73 65 2c 22 57 61 63 69 69 45 6e 61 62 6c 65 64 52 65 71 75 65 73 74 73 22 3a 30 2c 22 53 65 74 74 69 6e 67 73 52 6f 75 74 65 64 54 6f 53 65 72 76 65 72 22 3a 30 2c 22 4c 69 6e 65 61 67 65 49 64 22 3a 6e 75 6c 6c 2c 22 46 69 6c 65 49 64 22 3a 22 57 4f 50 Data Ascii: {"Mode":1,"srs":[[2,{"OperationId":1,"DependentOn":0,"LocalCobaltSessionId":null,"LocalCobaltMachineId":null,"LocalCobaltClusterId":null,"LocalCobaltSessionHasBackup":false,"WaciiEnabledRequests":0,"SettingsRoutedToServer":0,"LineageId":null,"FileId":"WOP
2022-06-30 16:43:48 UTC	876	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Length: 1066 Content-Type: application/json; charset=utf-8 Expires: -1 P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-ROUTED-TO-TARGET-SERVER-PATH: WAC_WFE_AFFINITY_TARGET_URL X-CorrelationId: 1d852c8d-9498-4c7d-a10a-45bfc58077e3 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-CorrelationId: 1d852c8d-9498-4c7d-a10a-45bfc58077e3 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006957 X-WacFrontEnd: AM4PEPF00006B54 X-Powered-By: ARR/3.0 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 9116D1E9919F4733842E812006B6D642 Ref B: AM3EDGE0522 Ref C: 2022-06-30T16:43:47Z Date: Thu, 30 Jun 2022 16:43:47 GMT Connection: close
2022-06-30 16:43:48 UTC	877	IN	Data Raw: ef bb bf 7b 22 52 65 73 70 6f 6e 73 65 73 22 3a 5b 5b 32 2c 7b 22 4f 70 65 72 61 74 69 6f 6e 49 64 22 3a 31 2c 22 53 74 61 74 75 73 43 6f 64 65 22 3a 30 2c 22 52 61 77 43 65 6c 6c 53 74 6f 72 61 67 65 45 72 72 6f 72 43 6f 64 65 22 3a 22 22 2c 22 53 65 72 76 65 72 50 61 67 65 53 74 61 74 73 54 72 61 63 65 22 3a 22 22 2c 22 50 61 72 74 4d 65 72 67 65 49 6e 66 6f 22 3a 30 2c 22 52 6f 6f 74 43 65 6c 6c 49 64 22 3a 22 6e 75 6c 6c 22 2c 22 41 76 61 69 6c 61 62 6c 65 46 69 6c 65 41 63 63 65 73 73 22 3a 32 2c 22 52 65 76 69 73 69 6f 6e 4c 69 73 74 22 3a 5b 5d 2c 22 50 69 6e 52 65 76 69 73 69 6f 6e 46 6f 72 41 75 67 4c 6f 6f 70 52 65 73 70 6f 6e 73 65 22 3a 30 2c 22 43 6c 69 65 6e 74 4b 6e 6f 77 6c 65 64 67 65 22 3a 22 68 41 41 6d 41 69 41 41 39 6a 56 36 4d 6d 45 Data Ascii: {"Responses":[[2,{"OperationId":1,"StatusCode":0,"RawCellStorageErrorCode":"","ServerPageStatsTrace":"","PartMergeInfo":0,"RootCellId":"null","AvailableFileAccess":2,"RevisionList":[],"PinRevisionForAugLoopResponse":0,"ClientKnowledge":"hAAmAiAA9jV6MmE
2022-06-30 16:43:48 UTC	878	IN	Data Raw: 61 45 50 37 57 52 50 34 4b 4f 43 70 6b 34 78 36 72 45 64 45 6c 4d 51 41 4a 55 41 56 30 41 6e 42 52 61 63 78 52 4b 56 41 41 55 41 41 41 74 52 4d 42 51 51 3d 3d 22 7d 5d 2c 5b 32 2c 7b 22 4f 70 65 72 61 74 69 6f 6e 49 64 22 3a 32 2c 22 53 74 61 74 75 73 43 6f 64 65 22 3a 30 2c 22 52 61 77 43 65 6c 6c 53 74 6f 72 61 67 65 45 72 72 6f 72 43 6f 64 65 22 3a 22 22 2c 22 53 65 72 76 65 72 50 61 67 65 53 74 61 74 73 54 72 61 63 65 22 3a 22 22 2c 22 50 61 72 74 4d 65 72 67 65 49 6e 66 6f 22 3a 30 2c 22 52 6f 6f 74 43 65 6c 6c 49 64 22 3a 22 6e 75 6c 6c 22 2c 22 41 76 61 69 6c 61 62 6c 65 46 69 6c 65 41 63 63 65 73 73 22 3a 32 2c 22 52 65 76 69 73 69 6f 6e 4c 69 73 74 22 3a 5b 5d 2c 22 50 69 6e 52 65 76 69 73 69 6f 6e 46 6f 72 41 75 67 4c 6f 6f 70 52 65 73 70 6f 6e Data Ascii: aEP7WRP4KOCpk4x6rEdElMQAJUAV0AnBRacxRKVAAUAAAtRMBQQ==}],[2,{"OperationId":2,"StatusCode":0,"RawCellStorageErrorCode":"","ServerPageStatsTrace":"","PartMergeInfo":0,"RootCellId":"null","AvailableFileAccess":2,"RevisionList":[],"PinRevisionForAugLoopRespon

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	50042	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:44:06 UTC	878	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 1182 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1033&data=1033; BIGipCookie=00000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:44:37 UTC	883	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 1842 X-WacFrontEnd: AM4PEPF00006B54 X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-AccessTokenTtl: 1658421761813 X-Requested-With: XMLHttpRequest X-xhr: 1 haep: 1 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-UserType: WOPI X-IsCoauthSession: true X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; DcLcid=ui=1 033&data=1033; BIGipCookie=0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000; ShCLSessionID=1656639775607_0.6 675230212797223; BP=l=SDX.Skydrive&FR=&ST=; MUID=210011B4A40D624F14CA0067A00D667C; xidseq=4; E=P:tcNhmbda2og=:PJLCcxjKwQVUWFIETez3k69O9vOeDWpicKYwq8SBqKA=:F; wlidperf=latency=238
2022-06-30 16:44:37 UTC	885	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 38 34 37 30 38 35 2c 22 4c 22 3a 5b 7b 22 47 22 3a 35 39 30 39 30 31 39 37 36 2c 22 54 22 3a 33 34 33 39 2c 22 4d 22 3a 22 7b 5c 22 46 72 6f 6d 53 74 61 74 65 5c 22 3a 5c 22 70 61 73 73 69 76 65 5c 22 2c 5c 22 54 6f 53 74 61 74 65 5c 22 3a 5c 22 68 69 64 64 65 6e 5c 22 2c 5c 22 4f 72 69 67 69 6e 61 74 6 9 6e 67 45 76 65 6e 74 5c 22 3a 5c 22 54 61 73 6b 49 74 65 6d 5c 22 2c 5c 22 54 69 6d 65 49 6e 53 74 61 74 65 5c 22 3a 5c 22 35 38 32 35 30 5c 22 7d 22 2c 22 43 22 3a 33 32 34 2c 22 44 22 3a 35 30 7d 2c 7b 22 47 22 3a 34 33 31 30 38 30 34 2c 22 54 22 3a 31 35 39 37 36 2c 22 4d 22 3a 22 7b 5c 22 55 72 6c 5c 22 3a 5c 22 68 74 74 70 73 3a 2f 2f 62 72 6f 77 73 65 72 2e 65 76 65 6e 74 73 2e 64 61 74 61 2e 6d 69 63 72 6f 73 6f Data Ascii: {"T":1656639847085,"L":[{"G":590901976,"T":3439,"M":"{\"FromState\":\"passive\",\"ToState\":\"hidden\",\"Ori ginatingEvent\":\"TaskItem\",\"TimeInState\":\"58250\"}","C":324,"D":50},{"G":4310804,"T":15976,"M":"{\"Url\":\"https:// browser.events.data.microso
2022-06-30 16:44:37 UTC	887	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: aa9d5f0d-e53f-4f30-a0d4-0fafa5c9830a X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006B53 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onenote.officeapps.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X- bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006B53 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: CC18491CF4B743B39904CA57E6D50234 Ref B: AM3EDGE0410 Ref C: 2022-06-30T16:44:37Z Date: Thu, 30 Jun 2022 16:44:37 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49769	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	9	OUT	POST /o/RemoteUls.ashx?usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&officeserverversion=16.0.15417.41022 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 1880 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 Content-Type: text/plain;charset=UTF-8 Accept: */* Origin: https://onedrive.live.com Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://onedrive.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F
2022-06-30 16:42:43 UTC	9	OUT	Data Raw: 7b 22 54 22 3a 31 36 35 36 36 33 39 37 36 33 30 36 33 2c 22 4c 22 3a 5b 7b 22 47 22 3a 35 39 36 34 34 34 32 33 38 2c 22 54 22 3a 31 39 2c 22 4d 22 3a 22 48 6f 73 74 49 6e 69 74 44 69 61 67 6e 6f 73 74 69 63 73 3a 20 7b 5c 22 65 6e 74 72 79 50 6f 69 6e 74 5c 22 3a 5c 22 55 6e 6b 6e 6f 77 6e 5c 22 2c 5c 22 75 73 65 72 43 6c 69 63 6b 54 69 6d 65 5c 22 3a 31 36 35 36 36 33 39 37 36 30 35 30 32 2c 5c 22 68 6f 73 74 50 61 67 65 4e 61 76 69 67 61 74 69 6f 6e 53 74 61 72 74 54 69 6d 65 5c 22 3a 31 36 35 36 36 33 39 37 36 30 35 30 32 2c 5c 22 68 6f 73 74 50 61 67 65 46 65 74 63 68 53 74 61 72 74 54 69 6d 65 5c 22 3a 31 36 35 36 36 33 39 37 36 30 35 30 34 2c 5c 22 68 6f 73 74 50 61 67 65 52 65 73 70 6f 6e 73 65 53 74 61 72 74 54 69 6d 65 5c 22 3a 31 36 35 36 36 30 Data Ascii: {"T":1656639763063,"L":[{"G":596444238,"T":19,"M":"HostInitDiagnostics: {\"entryPoint\":\"Unknown\",\"userClickTime\":1656639760502,\"hostPageNavigationStartTime\":1656639760502,\"hostPageFetchStartTime\":1656639760504,\"hostPageResponseStartTime\":165660
2022-06-30 16:42:43 UTC	12	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/plain P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: 917c1bf1-34ce-41b5-b2f5-8c3a208320e1 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF0000695D X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 Access-Control-Allow-Origin: https://onedrive.live.com Access-Control-Expose-Headers: X-EndSession, X-CorrelationId, X-OfficeFE, X-NewKey, X-bULS-SuppressionETag, X-bULS-SuppressedTags Cross-Origin-Resource-Policy: cross-origin X-bULS-SuppressionETag: CA78EF8008219FD41B3BEECBDC5469C32D39C9D9 X-bULS-SuppressedTags: 378069,1671813,2209344,3290144,4298965,4298968,4298969,4751696,5306497,5904476,6375195,6572226,6948167,7463498,17085210,17085216,17162522,17358857,19743902,21627712,21631370,22401293,22410500,22558617,22598977,22680210,22680213,22680214,22836558,22946650,23909858,24401375,24462656,24515087,25514973,33592839,34388130,35682372,36472266,36546380,36546381,36546382,36569418,36708451,36773964,36791688,36811158,36811159,36963655,37288035,37876293,37876294,37889309,38293640,38535900,38543496,38580697,38637954,38922202,39076766,39076767,39105358,39408129,39613840,39966341,40437001,40935455,40957978,40957979,41003225,41207258,41502555,41711299,41952657,41964821,41964885,42272991,42496725,42513088,42815875,42857251,50406866,50431969,50619726,50622685,50622687,51451613,51504083,51667010,306230939,524883107,524883136,524883138,537159499,538542792,538543587,539874723,540378699,540378700,542700237,542994947,545783884,557077970,557322386,557389507,557670930,558735363,559423838,559424262,559486496,559760215,559760216,570507662,571549507,571786073,571786074,574468116,575157663,575157664,575157665,575157666,575157667,575157696,575157697,575157698,575157699,575157700,575157701,575157702,577295376,577626581,577831138,578164000,587862985,591684683,591729363,592259104,592556551,592843145,593780815,593838232,593862981,594134597,594396706,594830612,595137156,595714715,595895774,596115913,596444186,596464289,845836083,845836084,845836085,846166132,876178018,963472182,1630679666,1630679667,1633958006,1647605351,1664576567,1698260075,1718235956,1765045358,1802139698,1986689397,1986689633,1986689647,1986748791,1986748793,1986749030,1986749288,1986749546,2004443760,2004444278,2004448354 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF0000695D X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wordslice_control,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 21FB2C3445BB4BD8AF24173FD617CD73 Ref B: AM3EDGE0414 Ref C: 2022-06-30T16:42:43Z Date: Thu, 30 Jun 2022 16:42:43 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49770	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	190	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":0,"MsSinceStart":0,"Value":"SessionStarted","Type":"SessionBoundary"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	192	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":1,"MsSinceStart":153,"Value":"https://c1-onenote-15.cdn.office.net:443/o/s/h816A0F42A2BF4732_resources/1033/EditSurface.css","Type":"ResourceDownloadSuccess"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	195	OUT	POST /o/OneNote.ashx HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 2605 X-AccessToken: 4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwgYjE8pGOzrhQHssjdDTNK8Jn21CpZ1 u3SbKIQsF-ynTSOSveEi0XEaPSoAexqp7-12GLVzZG1WjgR-aZoeDjLwtY20zVT5-XDPGmWP14AVg X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 X-ServerSideRendering: RenderingNoImages X-OfficeVersion: 16.0.15417.41022 X-Key: 0XpfQFtLDrRv4UQM6v/1i8MVOATyWv5at1Jp1IgB+lw=,637922041630980967 X-WacUserAgent: MSWACONSync Content-Type: application/json; charset=UTF-8 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 X-Requested-With: XMLHttpRequest X-UserType: WOPI X-SessionStartDimensions: {"Application":"OneNote","Browser":"Chrome","BrowserMajorVersion":"85","BrowserVersi on":"85.0.4183","Host":"OneDriveWOPI","IsSynthetic":"False","Os":"Windows","Ring":"5","RoutedVia":"AzureFrontD oor","SessionOrigin":"UNKNOWN","UiHost":"OneDrive","UserSessionApplicationMode":"View","WACDatacenter":"PNL1"} X-xhr: 1 X-WacCluster: PNL1 Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyz LCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150 FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostcli cktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&us id=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E =P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCooki e=00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000
2022-06-30 16:42:43 UTC	197	OUT	Data Raw: 7b 22 4d 6f 64 65 22 3a 31 2c 22 73 72 73 22 3a 5b 5b 31 2c 7b 22 46 69 6c 65 49 64 22 3a 22 57 4f 50 49 73 72 63 3d 68 74 74 70 73 25 33 41 25 32 46 25 32 46 77 6f 70 69 25 32 45 6f 6e 65 64 72 69 76 65 25 32 45 63 6f 6d 25 32 46 77 6f 70 69 25 32 46 66 6f 6c 64 65 72 73 25 32 46 31 46 36 46 43 38 38 31 35 30 46 45 33 39 37 45 25 32 31 33 35 31 39 37 26 61 63 63 65 73 73 5f 74 6f 6b 65 6e 3d 34 77 6f 53 6a 31 7a 44 6d 44 36 6a 57 6d 6a 48 42 4e 31 78 53 4 3 30 6c 55 4e 75 67 68 63 66 31 54 57 30 46 69 43 61 77 62 70 4c 4e 77 67 59 6a 45 38 70 47 4f 7a 72 68 51 48 73 73 6a 64 44 54 4e 4b 38 4a 6e 32 31 43 70 5a 31 75 33 53 62 4b 49 51 73 46 25 32 44 79 6e 54 53 4f 53 76 65 45 69 30 58 45 61 50 53 6f 41 65 78 71 70 37 25 32 44 31 32 47 4c 56 7a 5a 47 31 57 Data Ascii: {"Mode":1,"srs":[[1,{"FileId":"WOPIsrc=https%3A%2F%2Fwopi%2Eonedrive%2Ecom%2Fwopi%2Ffold ers%2F1F6FC88150FE397E%2135197&access_token=4woSj1zDmD6jWmjHBN1xSC0lUNughcf1TW0FiCawbpLNwg YjE8pGOzrhQHssjdDTNK8Jn21CpZ1u3SbKIQsF%2DynTSOSveEi0XEaPSoAexqp7%2D12GLVzZG1W
2022-06-30 16:42:43 UTC	202	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Length: 76618 Content-Type: application/json; charset=utf-8 Expires: -1 P3P: CP="CAO DSP COR ADMa DEV CONi TELi CUR PSA PSD TAI IVDi OUR SAMi BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR" Set-Cookie: X-CorrelationId: e6b7c6ba-c8a7-4a10-8541-33ad0329c174 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 Strict-Transport-Security: max-age=31536000 Timing-Allow-Origin: * X-OfficeFE: AM4PEPF00006961 X-OfficeVersion: 16.0.15417.41022 X-OfficeCluster: PNL1 X-Content-Type-Options: nosniff X-Download-Options: noopen Content-Disposition: attachment X-OFFICEFD: AM4PEPF00006961 X-WacFrontEnd: AM4PEPF00006961 X-Cache: CONFIG_NOCACHE X-MSEdge-Flight: 2i49=afd_wacinfra4,2i4a=afd_wacinfra5 X-MSEdge-Features: typeheadertest,afd_waccluster,afd_wacinfra4,afd_wacinfra5 X-MSEdge-Ref: Ref A: 8231F539BFEE47A486A5ADD782A8AB34 Ref B: AMS04EDGE3018 Ref C: 2022-06-30T16:42:4 3Z Date: Thu, 30 Jun 2022 16:42:43 GMT Connection: close
2022-06-30 16:42:43 UTC	203	IN	Data Raw: ef bb bf 7b 22 52 65 73 70 6f 6e 73 65 73 22 3a 5b 5b 31 2c 7b 22 4f 70 65 72 61 74 69 6f 6e 49 64 22 3a 31 2c 22 53 74 61 74 75 73 43 6f 64 65 22 3a 30 2c 22 52 61 77 43 65 6c 6c 53 74 6f 72 61 67 65 45 72 72 6f 72 43 6f 64 65 22 3a 22 22 2c 22 53 65 72 76 65 72 50 61 67 65 53 74 61 74 73 54 72 61 63 65 22 3a 22 22 2c 22 46 69 6c 65 49 64 22 3a 22 57 4f 50 49 73 72 63 3d 68 74 74 70 73 5c 75 30 30 32 35 33 41 5c 75 30 30 32 35 32 46 5c 75 30 30 32 35 32 46 77 6f 70 69 5c 75 30 30 32 35 32 45 6f 6e 65 64 72 69 76 65 5c 75 30 30 32 35 32 45 63 6f 6d 5c 75 30 30 32 35 32 46 77 6f 70 69 5c 75 30 30 32 35 32 46 66 6f 6c 64 65 72 73 5c 75 30 30 32 35 32 46 31 46 36 46 43 38 38 31 35 30 46 45 33 3 9 37 45 5c 75 30 30 32 35 32 31 33 35 31 39 37 5c 75 30 30 32 36 Data Ascii: {"Responses":[[1,{"OperationId":1,"StatusCode":0,"RawCellStorageErrorCode":"","ServerPageStatsTrac e":"","FileId":"WOPIsrc=https\u00253A\u00252F\u00252Fwopi\u00252Eonedrive\u00252Ecom\u00252Fwopi\u00 252Ffolders\u00252F1F6FC88150FE397E\u00252135197\u0026

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	206	IN	Data Raw: 61 2d 39 33 64 30 2d 63 66 32 65 64 35 36 61 30 62 37 64 7c 31 22 2c 22 52 65 6c 61 74 69 76 65 50 61 74 68 22 3a 6e 75 6c 6c 2c 22 49 73 46 6f 6c 64 65 72 43 65 6c 6c 22 3a 74 72 75 65 2c 22 4f 70 73 22 3a 5b 5d 7d 5d 2c 22 50 69 6e 52 65 76 69 73 69 6f 6e 46 6f 72 41 75 67 4c 6f 6f 70 52 65 73 70 6f 6e 73 65 22 3a 30 2c 22 4c 61 74 65 73 74 52 65 76 69 73 69 6f 6e 49 64 22 3a 22 63 32 64 64 37 65 39 37 2d 65 31 34 34 2d 34 30 30 61 2d 39 33 64 30 2d 63 66 32 65 64 35 36 61 30 62 37 64 7c 31 22 2c 22 43 6c 69 65 6e 74 4b 6e 6f 77 6c 65 64 67 65 22 3a 22 65 77 42 68 41 47 4d 41 4f 41 42 6c 41 44 63 41 5a 51 41 30 41 44 51 41 4c 51 42 6d 41 44 55 41 59 67 42 68 41 43 30 41 4e 41 41 33 41 44 63 41 4d 51 41 74 41 44 67 41 5a 41 42 69 41 47 51 41 4c 51 42 6a Data Ascii: a-93d0-cf2ed56a0b7d|1","RelativePath":null,"IsFolderCell":true,"Ops":[]}],"PinRevisionForAugLoopResponse":0,"LatestRevisionId":"c2dd7e97-e144-400a-93d0-cf2ed56a0b7d|1","ClientKnowledge":"ewBhAGMAOABlADcAZQA0ADQALQBmADUAYgBhAC0ANAA3ADcAMQAtADgAZABiAGQALQBj
2022-06-30 16:42:43 UTC	214	IN	Data Raw: 33 35 35 35 31 35 35 30 2c 22 35 38 39 38 33 36 22 2c 33 33 35 35 35 31 36 32 30 2c 22 30 22 2c 36 30 33 39 38 36 39 37 36 2c 22 7b 61 31 37 33 30 35 38 66 2d 38 33 30 62 2d 34 36 39 62 2d 38 37 32 33 2d 65 63 37 66 62 36 36 61 34 31 35 62 7d 7b 39 7d 2c 7b 61 31 37 33 30 35 38 66 2d 38 33 30 62 2d 34 36 39 62 2d 38 37 32 33 2d 65 63 37 66 62 36 36 61 34 31 35 62 7d 7b 32 36 7d 22 2c 33 33 35 35 35 31 38 36 36 2c 22 31 36 35 36 35 39 39 38 32 32 30 30 30 22 5d 7d 2c 7b 22 43 6c 61 73 73 49 64 22 3a 33 39 33 32 32 38 2c 22 4f 62 6a 65 63 74 49 64 22 3a 22 61 31 37 33 30 35 38 66 2d 38 33 30 62 2d 34 36 39 62 2d 38 37 32 33 2d 65 63 37 66 62 36 36 61 34 31 35 62 7c 39 22 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 32 30 31 33 33 33 37 36 33 2c 22 31 22 2c Data Ascii: 35551550,"589836",335551620,"0",603986976,"{a173058f-830b-469b-8723-ec7fb66a415b}{9},{a173058f-830b-469b-8723-ec7fb66a415b}{26}",335551866,"1656599822000"]},{"ClassId":393228,"ObjectId":"a173058f-830b-469b-8723-ec7fb66a415b|9","Properties":[201333763,"1",
2022-06-30 16:42:43 UTC	218	IN	Data Raw: 32 32 2c 22 32 22 2c 32 36 38 34 34 32 36 33 35 2c 22 32 32 22 2c 33 33 35 35 35 31 35 30 30 2c 22 31 31 38 39 32 30 31 34 22 2c 34 36 39 37 37 35 34 39 38 2c 22 70 22 2c 33 33 35 35 35 37 36 37 39 2c 22 30 22 2c 33 33 35 35 35 37 36 37 38 2c 22 30 22 2c 34 36 39 37 36 39 32 32 36 2c 22 43 61 6c 69 62 72 69 22 5d 7d 2c 7b 22 43 6c 61 73 73 49 64 22 3a 31 31 37 39 37 32 35 2c 22 4f 62 6a 65 63 74 49 64 22 3a 22 61 31 37 33 30 35 38 66 2d 38 33 30 62 2d 34 36 39 62 2d 38 37 32 33 2d 65 63 37 66 62 36 36 61 34 31 35 62 7c 31 38 22 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 34 36 39 37 37 35 34 35 30 2c 22 68 36 22 2c 32 30 31 33 34 30 31 32 32 2c 22 32 22 2c 32 36 38 34 34 32 36 33 35 2c 22 32 32 22 2c 33 33 35 35 35 31 35 30 30 2c 22 31 31 38 39 32 30 31 Data Ascii: 22,"2",268442635,"22",335551500,"11892014",469775498,"p",335557679,"0",335557678,"0",469769226,"Calibri"]},{"ClassId":1179725,"ObjectId":"a173058f-830b-469b-8723-ec7fb66a415b|18","Properties":[469775450,"h6",201340122,"2",268442635,"22",335551500,"1189201
2022-06-30 16:42:43 UTC	226	IN	Data Raw: 56 48 6c 51 35 5a 36 62 6a 6a 51 5c 75 30 30 32 36 61 63 63 65 73 73 5f 74 6f 6b 65 6e 5f 74 74 6c 3d 31 36 35 38 34 31 35 38 39 39 36 30 30 22 2c 22 49 64 22 3a 22 62 62 33 61 30 33 30 34 2d 37 37 36 34 2d 34 37 30 62 2d 62 65 32 30 2d 61 30 30 30 62 65 32 66 63 39 66 30 7c 32 39 22 2c 22 52 65 6c 61 74 69 76 65 50 61 74 68 22 3a 6e 75 6c 6c 2c 22 49 73 46 6f 6c 64 65 72 43 65 6c 6c 22 3a 66 61 6c 73 65 2c 22 4f 70 73 22 3a 5b 5d 7d 2c 7b 22 42 61 73 65 49 64 22 3a 22 62 62 33 61 30 33 30 34 2d 37 37 36 34 2d 34 37 30 62 2d 62 65 32 30 2d 61 30 30 30 62 65 32 66 63 39 66 30 7c 32 39 22 2c 22 4f 62 6a 65 63 74 47 72 6f 75 70 73 22 3a 5b 7b 22 49 64 22 3a 22 61 32 32 37 36 32 66 36 2d 62 38 62 30 2d 34 33 33 33 2d 61 32 33 30 2d 38 64 65 30 38 64 39 62 61 Data Ascii: VHlQ5Z6bjjQ\u0026access_token_ttl=1658415899600","Id":"bb3a0304-7764-470b-be20-a000be2fc9f0|29","RelativePath":null,"IsFolderCell":false,"Ops":[]},{"BaseId":"bb3a0304-7764-470b-be20-a000be2fc9f0|29","ObjectGroups":[{"Id":"a22762f6-b8b0-4333-a230-8de08d9ba
2022-06-30 16:42:43 UTC	234	IN	Data Raw: 35 32 46 66 69 6c 65 73 5c 75 30 30 32 35 32 46 31 46 36 46 43 38 38 31 35 30 46 45 33 39 37 45 5c 75 30 30 32 35 32 31 33 35 31 39 39 5c 75 30 30 32 36 61 63 63 65 73 73 5f 74 6f 6b 65 6e 3d 34 77 35 74 4b 4e 42 6b 63 62 6f 36 6b 32 78 45 64 6d 6a 55 30 50 56 69 6c 6c 62 46 5c 75 30 30 32 35 35 46 67 71 30 69 67 6e 48 70 71 6d 42 6d 33 41 61 61 55 79 68 55 55 50 78 44 41 6f 47 5c 75 30 30 32 35 32 44 71 30 47 53 65 4a 49 32 63 4c 66 6c 4a 72 44 44 71 6f 74 43 4f 70 58 4c 44 61 49 53 6e 36 6b 53 77 4d 33 61 56 31 70 33 52 35 64 77 4e 50 4d 4e 79 42 54 46 5c 75 30 30 32 35 32 44 78 45 5a 5c 75 30 30 32 35 32 44 70 6f 55 45 38 58 47 51 42 64 57 78 34 59 61 52 53 59 38 39 65 63 37 72 42 5c 75 30 30 32 35 32 44 42 56 48 6c 51 35 5a 36 62 6a 6a 51 5c 75 30 30 Data Ascii: 52Ffiles\u00252F1F6FC88150FE397E\u00252135199\u0026access_token=4w5tKNBkcbo6k2xEdmjU0PViIlbF\u00255Fgq0ignHpqmBm3AaaUyhUUPxDAoG\u00252Dq0GSeJI2cLflJrDDqotCOpXLDaISn6kSwM3aV1p3R5dwNPMNyBTF\u00252DxEZ\u00252DpoUE8XGQBdWx4YaRSY89ec7rB\u00252DBVHlQ5Z6bjjQ\u00
2022-06-30 16:42:43 UTC	242	IN	Data Raw: 34 7d 22 5d 7d 2c 7b 22 43 6c 61 73 73 49 64 22 3a 31 31 37 39 37 32 35 2c 22 4f 62 6a 65 63 74 49 64 22 3a 22 62 62 33 61 30 33 30 34 2d 37 37 36 34 2d 34 37 30 62 2d 62 65 32 30 2d 61 30 30 30 62 65 32 66 63 39 66 30 7c 37 32 22 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 31 33 34 32 32 35 34 32 38 2c 22 74 72 75 65 22 2c 31 33 34 32 32 35 34 33 30 2c 22 74 72 75 65 22 2c 31 33 34 32 32 35 34 33 33 2c 22 74 72 75 65 22 5d 7d 2c 7b 22 43 6c 61 73 73 49 64 22 3a 31 31 37 39 37 32 35 2c 22 4f 62 6a 65 63 74 49 64 22 3a 22 62 62 33 61 30 33 30 34 2d 37 37 36 34 2d 34 37 30 62 2d 62 65 32 30 2d 61 30 30 30 62 65 32 66 63 39 66 30 7c 37 34 22 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 31 33 34 32 32 34 39 30 30 2c 22 74 72 75 65 22 2c 31 33 34 32 32 35 34 Data Ascii: 4}"]},{"ClassId":1179725,"ObjectId":"bb3a0304-7764-470b-be20-a000be2fc9f0|72","Properties":[134225428,"true",134225430,"true",134225433,"true"]},{"ClassId":1179725,"ObjectId":"bb3a0304-7764-470b-be20-a000be2fc9f0|74","Properties":[134224900,"true",1342254
2022-06-30 16:42:43 UTC	250	IN	Data Raw: 3b 5c 75 30 30 32 32 5c 75 30 30 33 45 5c 75 30 30 33 43 64 69 76 20 63 6c 61 73 73 3d 5c 75 30 30 32 32 50 61 72 61 57 72 61 70 70 69 6e 67 44 69 76 5c 75 30 30 32 32 5c 75 30 30 33 45 5c 75 30 30 33 43 70 20 63 6c 61 73 73 3d 5c 75 30 30 32 32 50 61 72 61 67 72 61 70 68 5c 75 30 30 32 32 20 73 74 79 6c 65 3d 5c 75 30 30 32 32 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 43 61 6c 69 62 72 69 2c 53 61 6e 73 2d 53 65 72 69 66 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 63 6f 6c 6f 72 3a 23 38 30 38 30 38 30 3b 74 65 78 74 2d 61 6c 69 67 6e Data Ascii: ;\u0022\u003E\u003Cdiv class=\u0022ParaWrappingDiv\u0022\u003E\u003Cp class=\u0022Paragraph\u0022 style=\u0022font-weight:normal;font-style:normal;vertical-align:baseline;font-family:Calibri,Sans-Serif;background-color:transparent;color:#808080;text-align
2022-06-30 16:42:43 UTC	258	IN	Data Raw: 42 69 5c 75 30 30 32 46 43 50 5c 75 30 30 32 42 48 6a 66 5c 75 30 30 32 42 33 50 5c 75 30 30 32 46 41 47 34 53 69 69 69 76 6d 6a 5c 75 30 30 32 42 67 41 6f 6f 6f 6f 41 61 39 66 71 52 5c 75 30 30 32 42 77 39 5c 75 30 30 32 46 79 62 66 34 59 5c 75 30 30 32 46 77 43 75 6c 31 5c 75 30 30 32 46 36 55 50 58 35 64 50 58 36 69 5c 75 30 30 32 46 73 50 66 38 6d 33 5c 75 30 30 32 42 47 50 5c 75 30 30 32 42 75 6c 31 5c 75 30 30 32 46 36 55 50 58 76 5a 50 5c 75 30 30 32 46 41 4c 31 5c 75 30 30 32 46 32 37 5c 75 30 30 32 42 71 50 79 44 78 53 5c 75 30 30 32 46 35 45 63 50 38 41 72 36 76 5c 75 30 30 32 46 41 45 6d 52 38 34 66 74 78 7a 57 4e 6a 5c 75 30 30 32 42 30 31 34 4f 6d 31 51 52 79 61 55 6d 6d 57 62 33 55 63 6b 58 6d 4b 36 72 64 7a 4d 32 35 66 34 6c 32 37 76 6c 72 Data Ascii: Bi\u002FCP\u002BHjf\u002B3P\u002FAG4Siiivmj\u002BgAooooAa9fqR\u002Bw9\u002Fybf4Y\u002FwCul1\u002F6UPX5dPX6i\u002FsPf8m3\u002BGP\u002Bul1\u002F6UPXvZP\u002FAL1\u002F27\u002BqPyDxS\u002F5EcP8Ar6v\u002FAEmR84ftxzWNj\u002B014Om1QRyaUmmWb3UckXmK6rdzM25f4l27vlr

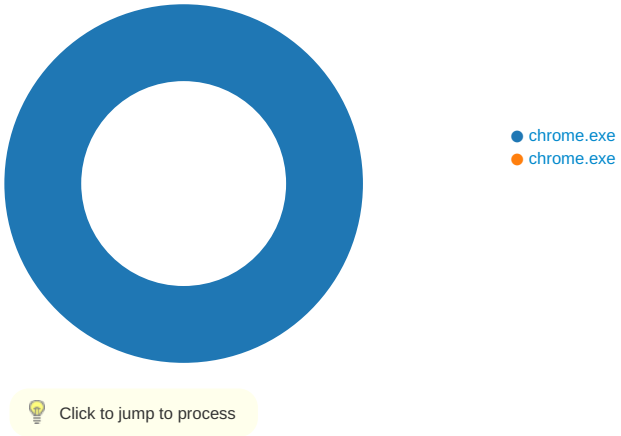
Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	266	IN	Data Raw: 51 42 52 31 54 5c 75 30 30 32 46 6b 47 33 33 5c 75 30 30 32 46 41 46 7a 66 5c 75 30 30 32 46 77 42 42 72 38 4f 58 5c 75 30 30 32 46 77 44 5a 5c 75 30 30 32 46 77 44 32 61 76 33 47 31 54 5c 75 30 30 32 46 6b 47 33 33 5c 75 30 30 32 46 41 46 7a 66 5c 75 30 30 32 46 77 42 42 72 38 4f 58 5c 75 30 30 32 46 77 41 5c 75 30 30 32 46 39 39 56 38 6a 6e 33 78 55 76 6e 5c 75 30 30 32 42 68 5c 75 30 30 32 46 52 66 68 48 38 4f 4e 5c 75 30 30 32 46 37 63 5c 75 30 30 32 46 77 44 62 68 76 4e 48 4e 48 4e 48 4e 66 4a 48 39 44 36 68 7a 52 7a 52 7a 52 7a 51 47 6f 63 30 63 30 63 30 63 30 77 44 6d 6a 6d 6a 6d 6a 6d 6b 50 55 4f 61 4f 61 4f 61 4f 61 41 31 44 6d 6a 6d 6a 6d 6a 6d 67 4e 51 35 6f 35 6f 35 6f 35 6f 44 55 4f 61 66 54 4f 61 4f 61 42 61 68 7a 52 7a 52 7a 52 7a 51 47 6f Data Ascii: QBR1T\u002FkG33\u002FAFzf\u002FwBBr8OX\u002FwDZ\u002FwD2av3G1T\u002FkG33\u002FAFzf\u002FwBBr8OX\u002FwA\u002F99V8jn3xUvn\u002Bh\u002FRfhH8ON\u002F7c\u002FwDbhvNHNHNHNfJH9D6hzRzRzRzQGoc0c0c0c0wDmjmjmjmkPUOaOaOaOaA1DmjmjmjmgNQ5o5o5o5oDUOafTOaOaBahzRzRzRzQGo
2022-06-30 16:42:43 UTC	274	IN	Data Raw: 78 74 2d 61 6c 69 67 6e 3a 6c 65 66 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 70 74 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 70 78 3b 5c 75 30 30 32 32 5c 75 30 30 33 45 5c 75 30 30 33 43 73 70 61 6e 20 64 61 74 61 2d 63 6f 6e 74 72 61 73 74 3d 5c 75 30 30 32 32 61 75 74 6f 5c 75 30 30 32 32 20 63 6c 61 73 73 3d 5c 75 30 30 32 32 54 65 78 74 52 75 6e 20 45 6d 70 74 79 54 65 78 74 52 75 6e 5c 75 30 30 32 32 20 73 74 79 6c 65 3d 5c 75 30 30 32 32 63 6f 6c 6f 72 3a 57 69 6e 64 6f 77 54 65 78 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 74 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 43 61 6c 69 62 72 69 2c 43 61 6c 69 62 72 69 5f 4d 53 46 6f 6e 74 53 65 72 76 69 63 65 2c 53 61 6e 73 2d 53 65 72 69 66 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 32 70 78 3b 5c 75 30 30 32 Data Ascii: xt-align:left;font-size:6pt;margin-top:0px;\u0022\u003E\u003Cspan data-contrast=\u0022auto\u0022 class=\u0022TextRun EmptyTextRun\u0022 style=\u0022color:WindowText;font-size:14pt;font-family:Calibri,Calibri_MSFontService,Sans-Serif;line-height:22px;\u002

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49788	13.107.6.171	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 16:42:43 UTC	200	OUT	POST /o/RemoteUls.ashx?build=16.0.15417.41022&waccluster=PNL1 HTTP/1.1 Host: onenote.officeapps.live.com Connection: keep-alive Content-Length: 0 X-UserSessionId: 98985cba-b3dc-48e7-ae9f-7bbc12744030 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 X-BrowserUlsBeacon: [{"Index":2,"MsSinceStart":343,"Value":"Making GetCells Request","Type":"BootLogs"}] Accept: */* Origin: https://onenote.officeapps.live.com Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://onenote.officeapps.live.com/o/onenoteframe.aspx?edit=0&ui=en-US&rs=en-US&hid=mnfhyzLCdkOTWRS%2FhUuNkA.0&wopisrc=https%3A%2F%2Fwopi.onedrive.com%2Fwopi%2Ffolders%2F1F6FC88150FE397E!35197&wdo=2&sc=host%3D%26qt%3DDefault&wdp=7&uih=OneDrive&wdorigin=Unknown&wdhostclicktime=1656639760502&jsapi=1&jsapiver=v1&newsession=1&corrid=98985cba-b3dc-48e7-ae9f-7bbc12744030&usid=98985cba-b3dc-48e7-ae9f-7bbc12744030&sftc=1&readonly=1&wdredirectionreason=Force_SingleStepBoot Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: xid=a94776a0-ee2a-458a-9854-05b95ebe50e6&&RDE42AAC93A332&222; wla42=; mkt=en-US; xidseq=3; E=P:3UE7jbda2og=:JYdRP+n4EC7rku8IJu1vdQXlP/bseSGMwIgEJuQSe1c=:F; DcLcid=ui=1033&data=1033; BIGipCookie=0000000000

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2912**, Parent PID: **988**

General

Target ID:	0
Start time:	18:42:33
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://1drv.ms:443/o/s!BH45_lCByG8fgpJ9gXzw1ulhl-qQkQ?e=yvEgUVzG9ES2PfoKuGIEfw&at=9
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: **5892**, Parent PID: **2912**

General

Target ID:	1
Start time:	18:42:34
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=1516,92260789639596916592122446891408978629,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1944 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly