

ID: 655318
Sample Name:
Imax_SUMMARY.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 22:50:57
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report Imax_SUMMARY.html 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
Initial Sample 5
HTML 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
Phishing 6
System Summary 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
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:\Users\user\AppData\Local\Google\Chrome\User Data\01c81b04-9141-421f-9dd3-1994454f1765.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\444f40e6-3bf3-4b03-8ffd-fe8bfdb2ec8c.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\57649811-d16d-42a9-bc25-7c3fadb977d7.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\5f8dd45d-1be8-48bf-8973-3af3cce629a1.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\811e1469-eb9a-483f-a63f-9175339cdb65.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\9c4703d8-bcf9-4e86-8490-9ff2041ef375.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\0e916028-8d62-440b-8b55-f9e09442417e.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4f8e2bb1-21b0-456d-9a3a-b0cb47824645.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ff4364e-8ac8-4095-affc-0468bcdadb74.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63cb9805-53a0-4684-8390-32af18076ad7.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6a9c2d3c-264a-49bb-b9a7-7a3fa532f899.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b6215de-6ada-4de3-a86f-3df2d2ced129.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\ae697778-df44-480e-b75f-483bdfc28f24.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State

(copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\c9e47505-c5b8-4802-bc4b-048db0d61dd5.tmp 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a3e1c25a-5140-43c2-ba19-6082e2ad8fe4.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a570ed14-ca22-4195-b0cf-1db289849cf2.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\a93cdb9f-80bd-4dff-ba07-ce5a03739492.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\b91e34f9-dcea-46fd-8adc-75ac0f6fcba2.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\d48f1bca-e69f-4f72-9441-20811847ea3a.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\dab0a513-874a-459f-908a-62552a45653e.tmp 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\f047babb-a42e-4e6d-96cb-903a6ef61db5.tmp 26
C:\Users\user\AppData\Local\Temp\0e9571a0-6afd-4b9f-92bd-81a3f563411a.tmp 26
C:\Users\user\AppData\Local\Temp\184c7535-18f6-4c0c-9683-3478f06d836f.tmp 27
C:\Users\user\AppData\Local\Temp\5056_1892588763_metadata\verified_contents.json 27
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_pnacl_json 27
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 28
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 28
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 28
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 29
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 29
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 29
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 30
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 30
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 30
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 31
C:\Users\user\AppData\Local\Temp\5056_1892588763\manifest.fingerprint 31
C:\Users\user\AppData\Local\Temp\5056_1892588763\manifest.json 31
C:\Users\user\AppData\Local\Temp\5056_58494094\Recovery.crx3 31
C:\Users\user\AppData\Local\Temp\5056_58494094_metadata\verified_contents.json 32
C:\Users\user\AppData\Local\Temp\5056_58494094\manifest.fingerprint 32
C:\Users\user\AppData\Local\Temp\5056_58494094\manifest.json 32
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\0e9571a0-6afd-4b9f-92bd-81a3f563411a.tmp 33
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\bg\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\ca\messages.json 33
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\cs\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\da\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\de\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\el\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\en\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\en_GB\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\es\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\es_419\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\et\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\fi\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\fil\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\fr\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\hi\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\hr\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\hu\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\id\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\it\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\ja\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\ko\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\lt\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\lv\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\nb\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\nl\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\pl\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\pt_BR\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\pt_PT\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\ro\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\ru\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\sk\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\sl\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\sr\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\sv\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\th\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\tr\messages.json 44
C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\uk\messages.json 44
Static File Info 44
General 44
Network Behavior 44
Network Port Distribution 45
TCP Packets 45

UDP Packets 47
DNS Queries 47
DNS Answers 48
HTTP Request Dependency Graph 49
HTTPS Proxied Packets 49
Statistics 81
Behavior 81
System Behavior 82
Analysis Process: chrome.exePID: 5056, Parent PID: 3600 82
General 82
File Activities 82
Registry Activities 82
Key Value Modified 82
Analysis Process: chrome.exePID: 3964, Parent PID: 5056 83
General 83
File Activities 83
Disassembly 83

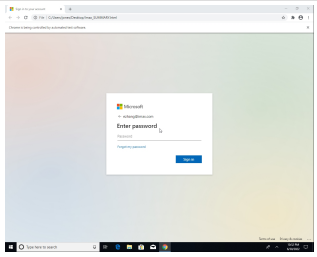
Windows Analysis Report

Imax_SUMMARY.html

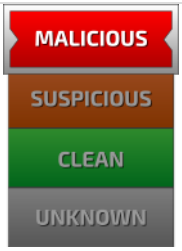
Overview

General Information

Sample Name:	Imax_SUMMARY.html
Analysis ID:	655318
MD5:	7396540ffe6dab2.
SHA1:	35801e9b7704dc..
SHA256:	a80beddc4d9de5..
Infos:	



Detection



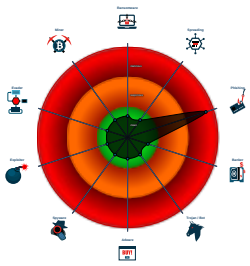
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish44
- HTML document with suspicious title
- Phishing site detected (based on im…
- Yara signature match
- Found iframes
- None HTTPS page querying sensitiv…
- No HTML title found
- JA3 SSL client fingerprint seen in co…
- HTML body contains low number of …
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5056 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\Imax_SUMMARY.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3964 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1588,1129215176533456628,2741544286314243644,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Imax_SUMMARY.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

HTML

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
86636.1.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0xca42a:$c5: return!![] • 0x79723:$c8: while(!![]) • 0x79742:$d1: parseInt(_0x55dd9d(0xe3))/0x1*(-parseInt(_0x55dd9d(0xef))/0x2)+-parseInt(_0x55dd9d(0xe1))/0x3*(-parseInt(_0x55dd9d(0xf5))/0x4)+-parseInt(_0x55dd9d(0xe7))/0x5+parseInt(_0x55dd9d(0xf0))/0x6+- • 0x79762:$d1: parseInt(_0x55dd9d(0xef))/0x2)+-parseInt(_0x55dd9d(0xe1))/0x3*(-parseInt(_0x55dd9d(0xf5))/0x4)+-parseInt(_0x55dd9d(0xe7))/0x5+parseInt(_0x55dd9d(0xf0))/0x6+-parseInt(_0x55dd9d(0x100))/0x7+- • 0x79782:$d1: parseInt(_0x55dd9d(0xe1))/0x3*(-parseInt(_0x55dd9d(0xf5))/0x4)+-parseInt(_0x55dd9d(0xe7))/0x5+parseInt(_0x55dd9d(0xf0))/0x6+-parseInt(_0x55dd9d(0x100))/0x7+-parseInt(_0x55dd9d(0xe8))/0x8+
86636.1.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected HtmlPhish44

Phishing site detected (based on image similarity)

System Summary



HTML document with suspicious title

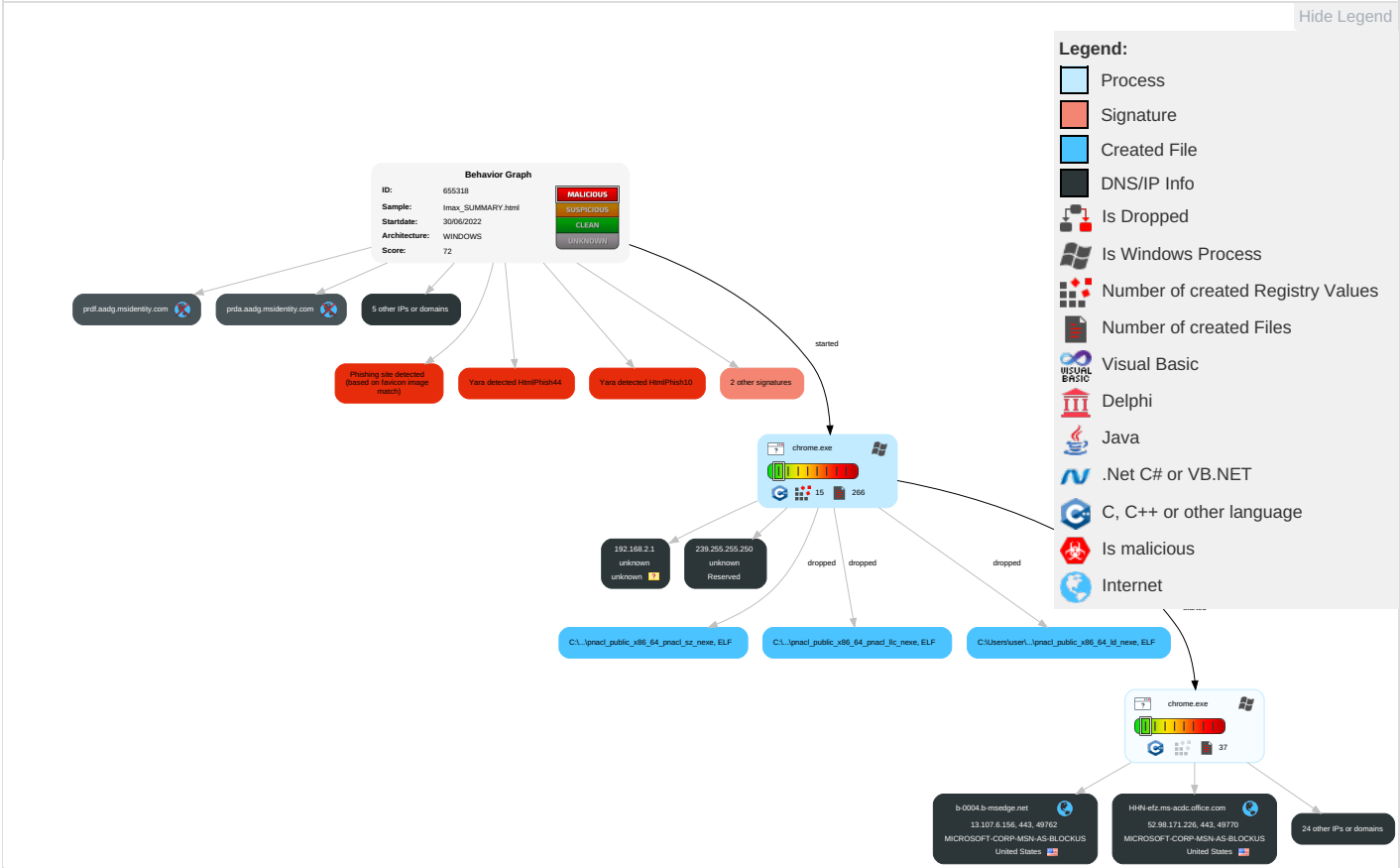
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	1 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	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 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	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

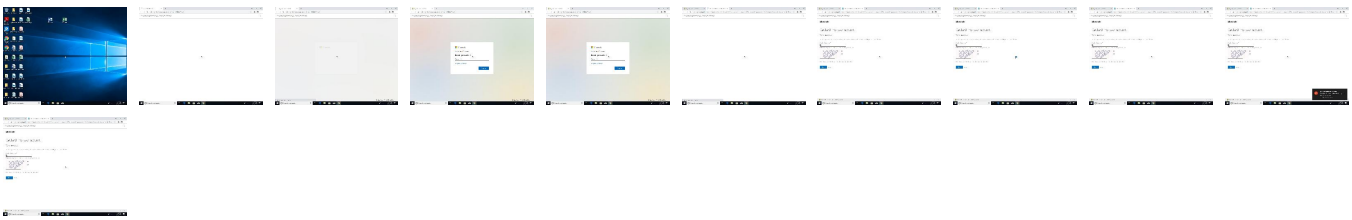
Behavior Graph

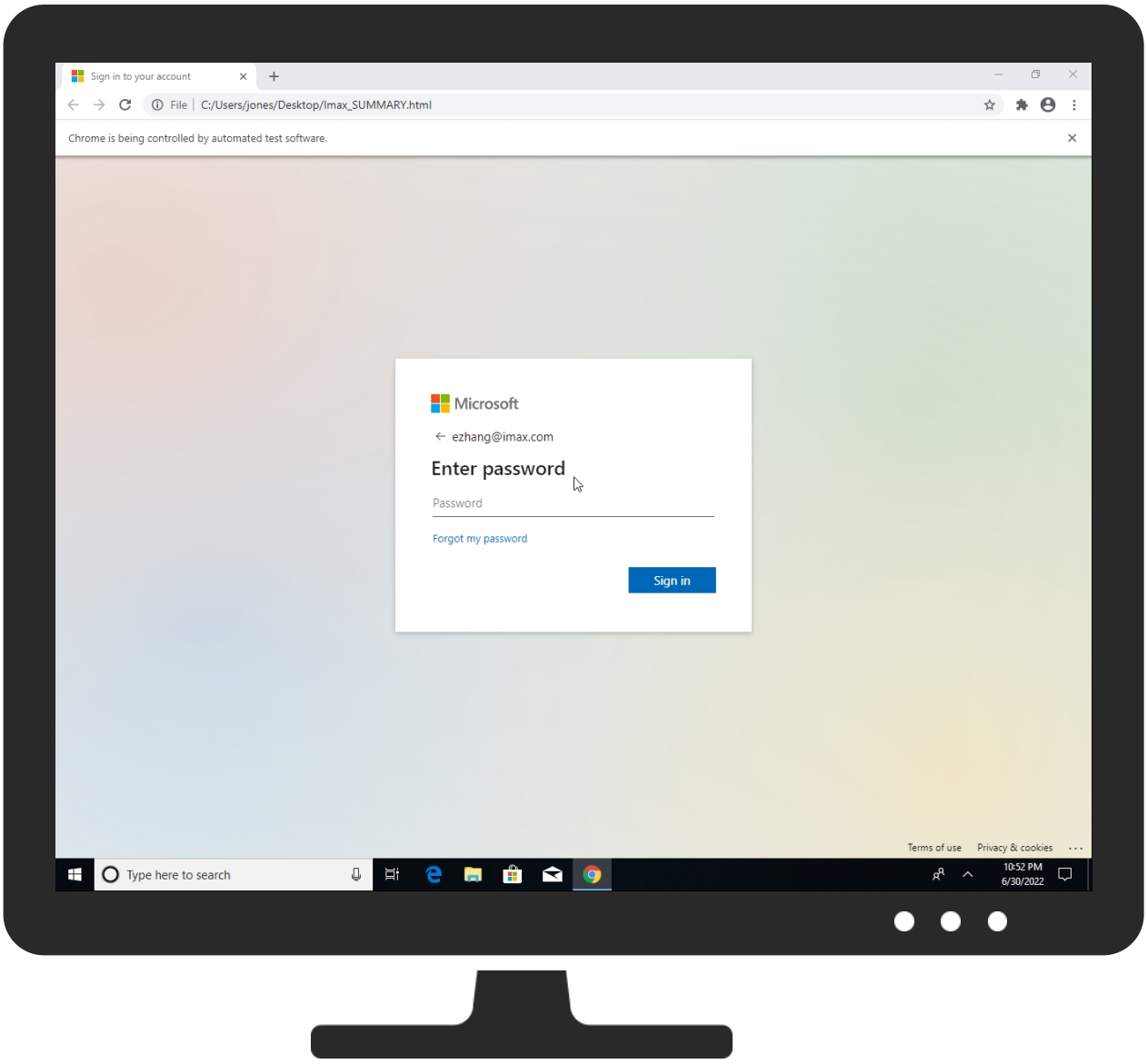


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Copyright Joe Security LLC 2022

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
part-0017.t-0009.fbs1-t-msedge.net	0%	Virustotal		Browse
b-0004.b-msedge.net	0%	Virustotal		Browse
sni1gl.wpc.sigmacdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_ppassword_2fbf6b08b73b1ba49bfa.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min__vnug8v1o1-mkptmkuydsg2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnfq3xbrj5zvj5ionvww2.css	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_Mo4A0Fxm-KbAvsKDen15VQ2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_ptiles_fdcf9ba11efc979408f4.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.251.36.205	true	false		high
part-0017.t-0009.fbs1-t-msedge.net	13.107.219.45	true	false	• 0%, Virustotal, Browse	unknown
b-0004.b-msedge.net	13.107.6.156	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.251.36.238	true	false		high
HHN-efz.ms-acdc.office.com	52.98.171.226	true	false		high
sni1gl.wpc.sigmacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
passwordreset.microsoftonline.com	unknown	unknown	false		high
www.office.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
r4.res.office365.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_ppassword_2fbf6b08b73b1ba49bfa.js	false	• Avira URL Cloud: safe	unknown
http://https://www.office.com/prefetch/prefetch	false		high
file:///C:/Users/user/Desktop/Imax_SUMMARY.html	true		low
http://https://outlook.office365.com/owa/prefetch.aspx	false		high

Copyright Joe Security LLC 2022

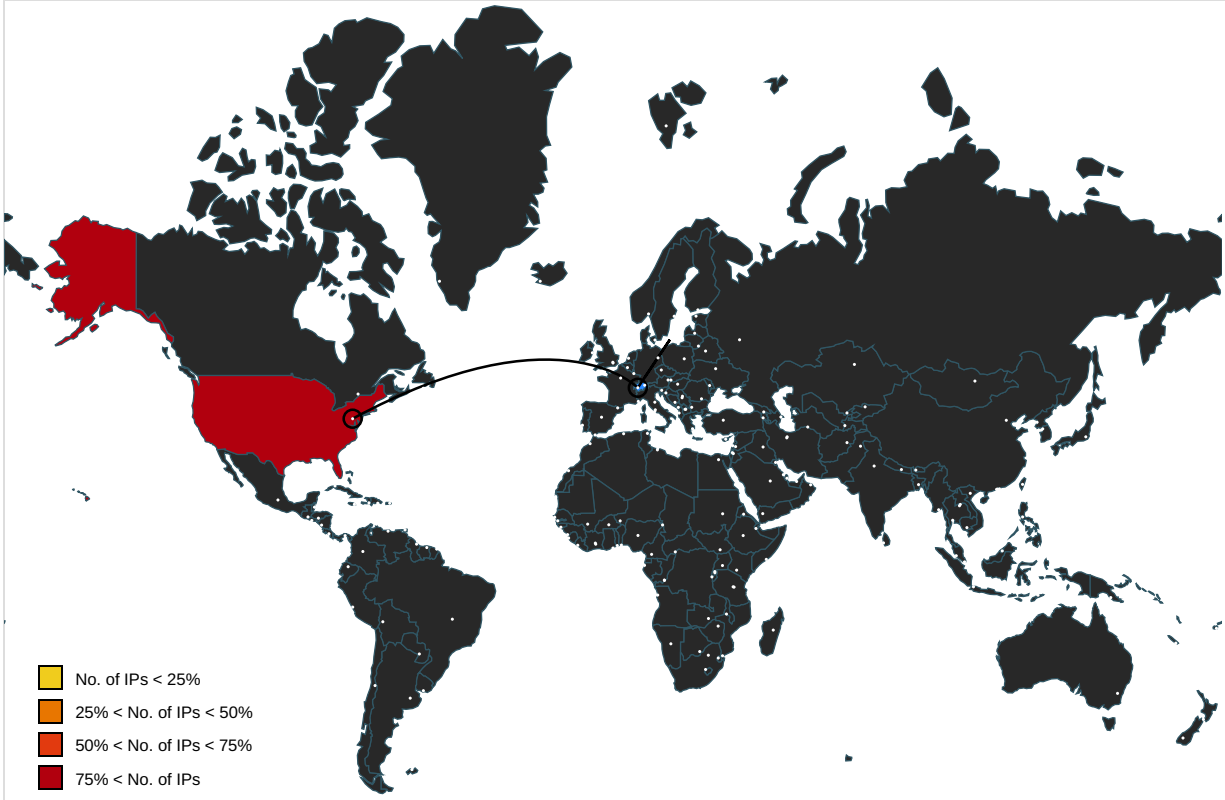
Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	false	• URL Reputation: safe	unknown
http://https://www.office.com/prefetch/prefetch	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min__vnug8v1o1-mkptmkuydsg2.js	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&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://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnfq3xbrj5zvj5ionvww2.css	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/owa/prefetch.aspx	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/js/ConvergedLogin_PCore_Mo4A0Fxm-KbAvsKDen15VQ2.js	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	false	• URL Reputation: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_ptiles_fdcf9ba11efc979408f4.js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	c9e47505-c5b8-4802-bc4b-048db0d61dd5.tmp.1.dr, a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, ae697778-df44-480e-b75f-483bdfc28f24.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.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	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.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://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, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://www.google.com	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://accounts.google.com	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apis.google.com	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high
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	a1bfc642-a373-4219-9ba3-fa3afcdf35e8.tmp.1.dr, cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.6.156	b-0004.b-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
52.98.171.226	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	sni1gl.wpc.sigmacdn.net	United States		15133	EDGECASTUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655318
Start date and time: 30/06/202222:50:57	2022-06-30 22:50:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Imax_SUMMARY.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.winHTML@31/117@10/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI • Browse: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSvYvTYADGm_au9wHqKSJOeqCDKGnffLxpWhBMP6-9Jv3l28s1S0ibtEnTJrkkbZrgLLrddMOBDuIgNwqCiqjzTTf7F4iTOIijvb_A5YEHHn7L89veYDJsBmTAwxSRIQr3aYqGam6Qx_MqQ-F0ngC4SpMMTkGKoUhAaBBQ3o3tHeKl8fluIuTfPz2592L59dkZdscIAtcvZLNhGGac0cgc6pmhM8tOVVsz7fEHDLvAsB8Ydppc1228J54lfYbKraCQASSgICRJks4IyDCFcmXJo3rAxw2zLwLAS8KkicYEH_MBj7QpH_cgP6tDIV7tZg1LQPWwJfWC_oQjhRIAAtmjmsiKBGStGB2yhYZQKHdgP-aI78lrLW4eGORlOJ4Z67-TWyPHmymu4wenqZMkqwSGW50sXEJCZNHrLyDdcq3BiIg63TgeOVy51MQPGkYoH3aHcMFOD_clxRbGsVVfOCocsULbG0CqPWk2w26xOWa5kGs3arJp1fQZyyOzRjsaPq_FymS8J9OqG7LyVBaVgVxXJwNR8KN9plqZlfwJZcxxziu6tRZtwapW7eSgNRQZ8XCQnxJ-MXDz0UEb2SKN25Vi1zJgLkZDmXOhJuL8wgf7YLaMlkpOZnr62Pe8nhZJKol0i7OWHTgktTJY7JXq-6V2I9R8qEoLQzK1hR4duq0elcdDJlBMuDePRvH4XSq9OnPm2Oepq46r26a263rOyJzqF2vYz7Vbm-mdzduJ3cSDmyBV2Nzc3klctr9r2Ov1lS2PnrxFf159qb6B7sej3-3E-Xr2KLuMapLUGpqsEPENzXdylUBsy4MBYrtxsxTmqH55aTeoPfYxKBDHaew4nT5PX6-XFaGCRMQJZa5bJhXwK40930h82vqPf9-uJP4B0&mkt=en-US&hosted=0&device_platform=Windows+10

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.159.68, 20.190.159.2, 20.190.159.23, 20.190.159.71, 20.190.159.64, 20.190.159.73, 20.190.159.0, 20.190.159.75, 34.104.35.123, 142.251.36.195, 184.30.21.171, 40.126.32.129, 40.126.32.6, 40.126.32.131, 40.126.32.66, 23.35.236.59, 152.199.19.160, 20.190.159.16, 172.217.16.170, 40.126.32.75, 20.190.160.13, 40.126.32.73, 20.190.160.12, 20.190.160.23, 40.126.32.69, 20.190.160.15, 40.126.32.132, 142.251.36.227
- Excluded domains from analysis (whitelisted): res-2.cdn.office.net, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, cdn-office.azureedge.net, www.ppetm.aadg.akadns.net, www.microsoft.com-c-3.edgekey.net, mscomajax.vo.msecnd.net, login.live.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, client.ppe.repmap.microsoft.com, global-entry-afdthirdparty-fallback.trafficmanager.net, www.bing.com, fs.microsoft.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, e1875.dscg.akamaiedge.net, cs22.wpc.v0cdn.net, www.tm.f.prd.aadg.akadns.net, aadcdn.msauth.net, www.tm.a.prd.aadg.akadns.net, cdn-office.ec.azureedge.net, firstparty-azurefd-prod.trafficmanager.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, res-prod.trafficmanage
- 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 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:\Users\user\AppData\Local\Google\Chrome\User Data\01c81b04-9141-421f-9dd3-1994454f1765.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):	206220
Entropy (8bit):	6.0433651764019345
Encrypted:	false
SSDEEP:	6144:dfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:P5M3tFqokPvqwNhHoZ
MD5:	15655B0EBCBD2267BED4C4911D891827
SHA1:	E61A5DACCAC62D588F7BB05A4DCCADB2F1F2386E
SHA-256:	C93F557C4C5202FD193EF1EC164E97158451013CEB7F983A3AD568ADE5CCBA42
SHA-512:	5F5B253043143E93DC8D87D2AAF0EB6A24AE1B983A224FB02618762F0F09634E93B7D20224739277BB83BD9C95DD0EE13C9A3D9B5935EC7EF1D247EC7283BE90
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\444f40e6-3bf3-4b03-8ffd-fe8bfdb2ec8c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.75177895304452

Encrypted:	false
SSDEEP:	384:l7UbDhes5ytRVqgnuNHrEvz538LlcHVYGInrStrTxElBJwranmiluZnjfsON9LNd:Ri69tS5EMMebvBt8PmO+9TK/ZjJ9
MD5:	AD02E0CDF556068D297E324B6B60D0BD
SHA1:	959DCD98FBE1F374BC9D9D261DE3A18CF523FABD
SHA-256:	4B4160384AA9B84085299B125B49F38B0EBA42233B6736C5AF417B2E41C6C729
SHA-512:	DB7899C3407D275CA0F2AC2F91CFDF13B831ADE2F79FE8C6E2A1BC4739738B08B9001814498A07C82537FBE737F14C7C69B4CDCD794765DC46B8CBBB4F461F 0
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\57649811-d16d-42a9-bc25-7c3fadb977d7.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7510008345884898
Encrypted:	false
SSDEEP:	384:z7UbDhesVtynuNHrEvz538LlcHVYGInrStrTxElBJwranmiluZnjfsON9LNS1fmK:869tS5EMMebvBt8PmO+9TK/ZjJSV
MD5:	833E0566EC747006EA1D4BA74A50A940
SHA1:	64C831F1E786E69BF879384F0D6C165B73B45C22
SHA-256:	D0F28B4D87536314970FB4E0DEB13B87F2A665593006A54BA9C1B1E90E175E4E
SHA-512:	AD930E6CBF40CBEDDD410663736C08D3DE434478E3D851ADED48A42536B0C3C93921ED2ABE275612E3E2830F400D814EB1527A30D4597CE3B8804FE8D4DABI BA
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\5f8dd45d-1be8-48bf-8973-3af3cce629a1.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):	206220
Entropy (8bit):	6.0433651764019345
Encrypted:	false
SSDEEP:	6144:dfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:P5M3tFqokPvqwNhHoZ
MD5:	15655B0EBCBD2267BED4C4911D891827
SHA1:	E61A5DACCAC62D588F7BB05A4DCCADB2F1F2386E
SHA-256:	C93F557C4C5202FD193EF1EC164E97158451013CEB7F983A3AD568ADE5CCBA42
SHA-512:	5F5B253043143E93DC8D87D2AAF0EB6A24AE1B983A224FB02618762F0F09634E93B7D20224739277BB83BD9C95DD0EE13C9A3D9B5935EC7EF1D247EC7283BE9 0
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encry pted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPq IYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqp s4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\811e1469-eb9a-483f-a63f-9175339cdb65.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified

Size (bytes):	206314
Entropy (8bit):	6.043606637338366
Encrypted:	false
SSDEEP:	6144:ZfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:j5M3tFqokPvqwNhHoZ
MD5:	1134AEB31B9A77DDB2D19A82AF487BA3
SHA1:	C302CE598EF28FED6DF8569A86B06AAD6C65C288
SHA-256:	C2498C5A962104D7C5EB413CE0F63A33B38EF120EB9D0DB800CC280A62ABBF9F
SHA-512:	F04E06F381D6E0E0DDEB8B582B3851FB1B6ED638E41FB1654C5FF4AAA89037BFBA33DE89FD1646117113386B5CF1EC40A905CBD123431FADB93D4985200F0BD6
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c4703d8-bcf9-4e86-8490-9ff2041ef375.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):	214570
Entropy (8bit):	6.070675169497312
Encrypted:	false
SSDEEP:	6144:q6fR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:qm5M3tFqokPvqwNhHoZ
MD5:	B78EEC8841F1B90080AFEC41A4162A33
SHA1:	05456E382EF37C60EE3C4953EF415ED3876463F1
SHA-256:	CD1A8B71CB04B752FADCC620F19CA14E02D38E34456995D626BE879241AB5DCF
SHA-512:	44901F85FA7CA4E6B947174FB4D1C7C7EE598917A70CCCD66F1A45F4D3B5008A346F11E0BD7000827A2E14F60E302C9133418519E65BDDE55717065C9832B3B7
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Reputation:	high, very likely benign file
Preview:	sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0e916028-8d62-440b-8b55-f9e09442417e.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):	4962

Entropy (8bit):	4.9348805655222545
Encrypted:	false
SSDEEP:	48:YcwUkKSChkliEqAbRiqTlYGlQKHoTw0Y+rN4MqM8C1Nfct/9BhUJo3KhmeSnpNGC:nwsLPAR1pIKIX5k0JCKL8bbOTlVuHn
MD5:	31D27DC620D8A41FE9C2D8867B398AD0
SHA1:	51015CCFF031805FE8D5AFBBE81CF208792BA1DB
SHA-256:	AC45865541ED054EDCB0A27AE6FB5B16119C980AB7D2ED1B9DC79575ED9E5ACC
SHA-512:	04E6BBE46217370B7AC6EF16A5143026F213ECDF5B2A7C68FC47EBCDE67EA9E6F83F99EE09FF9C07FFCADDA3322FAEB22BA671091AA919023820A001CC9A4 DF7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301095921372083","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_res et_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"wor k_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"," 0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4f8e2bb1-21b0-456d-9a3a-b0cb47824645.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):	4989
Entropy (8bit):	4.939725251065497
Encrypted:	false
SSDEEP:	48:YcwUkKSChklinb4qAbRiqTlYGlQKHoTw0Y+rN4MqM8C1Nfct/9BhUJo3KhmeSnp3:nwsLjAR1pIKIX5k0JCKL8hbOTlVuHn
MD5:	0E490143953BA9B71EDF25CE3AC6FFF2
SHA1:	9A9A7DC70F87B8D6044A1AC968C905B92E3AA360
SHA-256:	106F6FDDDD16B31F379AABEACE898805DC56647D9FE0F5021FE6E2F1F992196C
SHA-512:	F0DD4C4FEA3A3540ED8FF92D3BC380D0AA70A0E945E8E0F1694D1C1B73804C50966BB62C29C0A86C48AA3A31E2D8EBF9FFB2335BD5D6854FFD6073391852C9 F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301095921372083","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_res et_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"wor k_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"," 0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ff4364e-8ac8-4095-affc-0468bcdadb74.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):	19796
Entropy (8bit):	5.56376189858181
Encrypted:	false
SSDEEP:	384:tuCVtELlCfXj1kXqKf/pUZNCgVLH2HfDerUNHGEO3sI4h:J0LlAj1kXqKf/pUZNCgVLH2HfyrUxGEJ
MD5:	EC5CDC1BBA9DB4D0B0C776FAF1ED1AA3
SHA1:	E504AEAB8B911422DA64ACCF49E9028FFABC5AD9
SHA-256:	1C40E1240BC17F62DE1B7DC93D1D1FC0020EAC0F5C680F2BFEE1B7501161AF2F
SHA-512:	2A48F6CA6EEFDB11EAB5781236D60476642312FAB8EC580CFCD6DFF12FEFD153A644168CCBC52F46C4E24609FB21DDB306644331722DFEE9FDDB360AB3FC8 37
Malicious:	false
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":"13301095920610205","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\63cb9805-53a0-4684-8390-32af18076ad7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703

Entropy (8bit):	5.576361768710827
Encrypted:	false
SSDEEP:	384:tuCVtELlCfXj1kXqKf/pUZNCgVLH2HfDerUOO3vI4E:J0LlAj1kXqKf/pUZNCgVLH2HfyrUOAIL
MD5:	4646AF75186601D3AD2C2333FF798CFA
SHA1:	E2270C4F7168C74AB65F93CCFD54F40704FB0D7E
SHA-256:	FE9B0C5D29DFD5E75F12F5469FE72F87000B47A04D38A91CBBE8A45B847515B1
SHA-512:	AA59975C442A289AEB558AD6FA46B9E1C1E155AB4AFD5B552669D8571F0E3F4B14F5CDE60E27CB9CFDD641B208054578201A7899178ED43197C0CAEE83DB5DDD
Malicious:	false
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":"13301095920610205","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\6a9c2d3c-264a-49bb-b9a7-7a3fa532f899.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):	4914
Entropy (8bit):	4.934186256712151
Encrypted:	false
SSDEEP:	48:YcwUkKSChkliO7qAbRiqTlYGlQKHoTw0Y+rf4MqM8C1Nfct/9BhUJo3KhmeSnpNv:nwsLDAR1pIKI55k0JCKL8bbOTlVuHn
MD5:	138DCAEECB3F6F3AB1FA44F3A85124D3
SHA1:	CCFE7D288E2EAF404EE61785965FE7867EB88B13
SHA-256:	92786295726B972E626FD0613549EEB3E2D47C46349F4819C126CFA01FB29B62
SHA-512:	636564B67EAB117012C874132B6AEBA63B03D28D40F20DE8ACFEFEB7A5DADBD9291A1E462EC0724C7C10A22F0E6FF6E838961DBE5C7CBBEC43A9148C831A7241
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301095921372083","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b6215de-6ada-4de3-a86f-3df2d2ced129.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):	17702
Entropy (8bit):	5.576501820210807
Encrypted:	false
SSDEEP:	384:tuCVt9LlCfXj1kXqKf/pUZNCgVLH2HfDerUOw3vI4z:JNLlAj1kXqKf/pUZNCgVLH2HfyrUOaIM
MD5:	B9F654CE303040B7DD370563F051B625
SHA1:	820512A6DE788487DE181F3C359706A528807D9A
SHA-256:	7912EAEB9C9C0A3CC61A8F9C26ECFE715D19896AC38E4D15B3A91C11A8B0FCED
SHA-512:	F73797CEE4FBA97689324F283652B1A376E8A03BD4D69F63C4330580A5ADB3DC16FB35D4E62EB18F05E5B7FE6AA49DD325A7F1F29BCCC85623568D209BEAB11D
Malicious:	false
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":"13301095920610205","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
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
Malicious:	false
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):	369
Entropy (8bit):	5.245352336052642
Encrypted:	false
SSDEEP:	6:xi+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVKZmwYVmVkwOwkn23iKKdK25+Xqx8chn:xi+vYf5KkTXfchI3FUtJ/PV5Jf5KkTXc
MD5:	A4E396F161DA78A625B6DDF6F539B640
SHA1:	BBF7DAFE02E55A83FE5AA38EEDA54D63F433EFAB
SHA-256:	3E1BCEC53E660EA655DF51C85A309AF3FA3C083C0843F4C8F55F8682B3B7A05D
SHA-512:	74A2DCFB06BD7A224C6D863F51A97EB81CC0B90E50475009CA56E780E15900A0A9A5BDD59200EDBBD01E9760C371CB46BC5A094CF513B8E78706153BC113A1AA
Malicious:	false
Preview:	2022/06/30-22:52:07.891 8bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-22:52:07.892 8bc Recovering log #3.2022/06/30-22:52:07.892 8bc 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):	369
Entropy (8bit):	5.245352336052642
Encrypted:	false
SSDEEP:	6:xi+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVKZmwYVmVkwOwkn23iKKdK25+Xqx8chn:xi+vYf5KkTXfchI3FUtJ/PV5Jf5KkTXc
MD5:	A4E396F161DA78A625B6DDF6F539B640
SHA1:	BBF7DAFE02E55A83FE5AA38EEDA54D63F433EFAB
SHA-256:	3E1BCEC53E660EA655DF51C85A309AF3FA3C083C0843F4C8F55F8682B3B7A05D

SHA-512:	74A2DCFB06BD7A224C6D863F51A97EB81CC0B90E50475009CA56E780E15900A0A9A5BDD59200EDBBD01E9760C371CB46BC5A094CF513B8E78706153BC113A1AA
Malicious:	false
Preview:	2022/06/30-22:52:07.891 8bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/06/30-22:52:07.892 8bc Recovering log #3.2022/06/30-22:52:07.892 8bc 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):	723
Entropy (8bit):	5.246205699501957
Encrypted:	false
SSDEEP:	12:IseI3OIuh6VeZfHxnv7gYAx7AWo82n/AGaxz4oaCfn1rFBk778B/xgskZBa9sNi1:IseKOnh6gRFjgthAWo825yHBfn1rDY7w
MD5:	934201C05A156777913C8F2803D9A424
SHA1:	4329DBF3A05827B79D1A07242AD59E245D481C51
SHA-256:	519C638A1BAF6AF182B65AFEC715603541221F6DBC9BE2A92C2026BC9E0CC523
SHA-512:	5DCA31EE8A536D9EBA1C5D343F628080C68470AA8EF4EBBADC9C53A386817C4523988FAB8629188B0759DD022228B6DBFDE75F9106A9A6852C4D48A34AABF752
Malicious:	false
Preview:	.....T....account..c..desktop..file..html..imax..in..user..sign..summary..to..users..your*.....account.....c.....desktop.....file.....html.....imax.....in.....user.....sign.....summary.....to.....users.....your..2.....a.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....x.....y....:w.....Bo...k..... .....*0file:///C:/Users/user/Desktop/Imax_SUMMARY.html 2.Sign in to your account:.....J.....$,.....

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):	1705
Entropy (8bit):	4.838581220950164
Encrypted:	false
SSDEEP:	48:Y2nzM3qyvK6qDHGXCtwWscRLs075sLMHCYhbw:JnzMa+KxDHGXCO6z7EGnhM
MD5:	0D2CF997D1E2F6962507382EB8A162D1
SHA1:	0DB712E4A6FE76D0E75556B296C31ACEA8D53C1B
SHA-256:	BF9C649C31E8C8E1BBCDB2FB2AD91BFB94996612EAF1863A8973F18EE25021CF
SHA-512:	672819CFBA1545DA0304DA916395983CC6F476DF2F5457A5B9ECADF3F9AE1FEC55D4A388019C11F902D6746CEB6208E4AFFA9205B1338A302957B17C80C1A79B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

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):	4989
Entropy (8bit):	4.939725251065497
Encrypted:	false
SSDEEP:	48:YcwUkKSChklinb4qAbRiqTlYGlQKHoTw0Y+rN4MqM8C1Nfct/9BhUJo3KhmeSnp3:nwsLjAR1pIKIX5k0JCKL8hbOTlVuHn
MD5:	0E490143953BA9B71EDF25CE3AC6FFF2
SHA1:	9A9A7DC70F87B8D6044A1AC968C905B92E3AA360
SHA-256:	106F6FDDDD16B31F379AABEACE898805DC56647D9FE0F5021FE6E2F1F992196C
SHA-512:	F0DD4C4FEA3A3540ED8FF92D3BC380D0AA70A0E945E8E0F1694D1C1B73804C50966BB62C29C0A86C48AA3A31E2D8EBF9FFB2335BD5D6854FFD6073391852C9F8
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301095921372083","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19796
Entropy (8bit):	5.56376189858181
Encrypted:	false
SSDEEP:	384:tuCVtELlCfXj1kXqKf/pUZNCgVLH2HfDerUNHGEO3sI4h:J0LlAj1kXqKf/pUZNCgVLH2HfyrUxGEJ
MD5:	EC5CDC1BBA9DB4D0B0C776FAF1ED1AA3
SHA1:	E504AEAB8B911422DA64ACCF49E9028FFABC5AD9
SHA-256:	1C40E1240BC17F62DE1B7DC93D1D1FC0020EAC0F5C680F2BFEE1B7501161AF2F
SHA-512:	2A48F6CA6EEFDB11EAB5781236D60476642312FAB8EC580CFCD6DFF12FEFD153A644168CCBC52F46C4E24609FB21DDB306644331722DFEE9FDDB360AB3FC8 37
Malicious:	false
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":"13301095920610205","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\ae697778-df44-480e-b75f-483bdfc28f24.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\c9e47505-c5b8-4802-bc4b-048db0d61dd5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

Category:	modified
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\a1bfc642-a373-4219-9ba3-fa3afcdf35e8.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):	1705
Entropy (8bit):	4.838581220950164
Encrypted:	false
SSDEEP:	48:Y2nzM3qyvK6qDHGXCtwWscRLs075sLMHCYhbw:JnzMa+KxDHGXCO6z7EGnhM
MD5:	0D2CF997D1E2F6962507382EB8A162D1
SHA1:	0DB712E4A6FE76D0E75556B296C31ACEA8D53C1B
SHA-256:	BF9C649C31E8C8E1BBCDB2FB2AD91BFB94996612EAF1863A8973F18EE25021CF
SHA-512:	672819CFBA1545DA0304DA916395983CC6F476DF2F5457A5B9ECADF3F9AE1FEC55D4A388019C11F902D6746CEB6208E4AFFA9205B1338A302957B17C80C1A79B
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a3e1c25a-5140-43c2-ba19-6082e2ad8fe4.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):	19795
Entropy (8bit):	5.563924512998909
Encrypted:	false
SSDEEP:	384:tuCVtELlCfXj1kXqKf/pUZNCgVLH2HfDerUNHGHO3FNI4L:J0LlAj1kXqKf/pUZNCgVLH2HfyrUxGHE
MD5:	FCBD8D78197F4E3A170250C7E1163A5B
SHA1:	0336CF4CA9715F04A7C3706B0FD03DC568FB2F32
SHA-256:	20406521DFB2FCF02DB23EED84D63A2E12FAB5757500B8A8CFA1E7EE2485FAB4
SHA-512:	2D6CDA4134A9FC34143D6743C72FB7D13139ADE114668590D7A0B84026BBEC4E1568AFA51B21308CE7D4A4AE7E188543DDBC8A76267868F271B2068B195385B
Malicious:	false
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":"13301095920610205","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\a570ed14-ca22-4195-b0cf-1db289849cf2.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb4d5f91-917d-4085-b811-2a2e8954f37e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhlGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1 C
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service": [{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstat ic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"networ k_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

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
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
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):	206314
Entropy (8bit):	6.043606637338366
Encrypted:	false
SSDEEP:	6144:ZfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:j5M3tFqokPvqwNhHoZ
MD5:	1134AEB31B9A77DDB2D19A82AF487BA3
SHA1:	C302CE598EF28FED6DF8569A86B06AAD6C65C288
SHA-256:	C2498C5A962104D7C5EB413CE0F63A33B38EF120EB9D0DB800CC280A62ABBF9F
SHA-512:	F04E06F381D6E0E0DDEB8B582B3851FB1B6ED638E41FB1654C5FF4AAA89037BFBA33DE89FD1646117113386B5CF1EC40A905CBD123431FADB93D4985200F0BD6
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

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):	3.751081121861475
Encrypted:	false

SSDEEP:	384:V7UbDhes5ytRVqgnuNHrEvz538LlcHVYGInrStrTxElBJwranmiGYuZnjfsON9LW:hi69tS5sMMebvBt8PmO+9TK/ZjJg
MD5:	672F290D48CDDFEAE330F5639C33B0C7
SHA1:	4624984042F8BD3020CA2C0DFD4AB537CE9F029D
SHA-256:	B0A1060E2203F215E76F88643C941A4CE1A46C0E0DCA5ED1875C1D2EBD30BF0C
SHA-512:	8695DC704D89A2D10C537BC62D6B16765A7B86080C9927AF094AE87F88A0730DA285A52F86288A8662B2D0D17E8FC35E9143966B1AA33D52C52B1FA74DBF166
Malicious:	false
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\a93cdb9f-80bd-4dff-ba07-ce5a03739492.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):	206128
Entropy (8bit):	6.043120629996927
Encrypted:	false
SSDEEP:	6144:GfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:q5M3tFqokPvqwNhHoZ
MD5:	31622CD027C9726E08CD96CC2A9ADE54
SHA1:	AAA3AAA8EAF8FAD0CBDE28502C32993914F22EAA
SHA-256:	F1E412D4AAAE344FA5CD0E6826CAD7ABB56E305B97957F23A5DC1C1AE0A9A81F
SHA-512:	7208271ECAB6C2949391349770D476289A1062EBA986C6D16539462CC1774AB323C5DF0FD426CB55993E620ABDE1B62882FF9FEA86B00145DB701FE2DC26455
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\b91e34f9-dcea-46fd-8adc-75ac0f6fcba2.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):	206314
Entropy (8bit):	6.043606637338366
Encrypted:	false
SSDEEP:	6144:ZfR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:j5M3tFqokPvqwNhHoZ
MD5:	1134AEB31B9A77DDB2D19A82AF487BA3
SHA1:	C302CE598EF28FED6DF8569A86B06AAD6C65C288
SHA-256:	C2498C5A962104D7C5EB413CE0F63A33B38EF120EB9D0DB800CC280A62ABBF9F
SHA-512:	F04E06F381D6E0E0DDEB8B582B3851FB1B6ED638E41FB1654C5FF4AAA89037BFBA33DE89FD1646117113386B5CF1EC40A905CBD123431FADB93D4985200F0BD6
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\d48f1bca-e69f-4f72-9441-20811847ea3a.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):	214570
Entropy (8bit):	6.070675294740772
Encrypted:	false
SSDEEP:	6144:r2fR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:ra5M3tFqokPvqwNhHoZ

MD5:	32ED21765F300DFE005BBAA96FF6A27C
SHA1:	667F0389B4788AE9717A5149AB772D966E7DC702
SHA-256:	6701879E437073105158FBE5B388909DAF3DB476053F2310C1AF539AA65F889B
SHA-512:	38FDFED6FD508B1EBF75A7AD297A06AB00536640BD5A7B191AAEE098DC8A444549F4B4D2FFFD69DB3FB3B01EACB48A1FB36E681221E07F84F7428F6617D270D7
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129595273"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\dab0a513-874a-459f-908a-62552a45653e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751081121861475
Encrypted:	false
SSDEEP:	384:V7UbDhes5ytRVqgnuNHrEvz538LlcHVYGInrStrTxElBJwranmiGYuZnjfsON9LW:hi69tS5sMMebvBt8PmO+9TK/ZjJg
MD5:	672F290D48CDDFEAE330F5639C33B0C7
SHA1:	4624984042F8BD3020CA2C0DFD4AB537CE9F029D
SHA-256:	B0A1060E2203F215E76F88643C941A4CE1A46C0E0DCA5ED1875C1D2EBD30BF0C
SHA-512:	8695DC704D89A2D10C537BC62D6B16765A7B86080C9927AF094AE87F88A0730DA285A52F86288A8662B2D0D17E8FC35E9143966B1AA33D52C52B1FA74DBF166
Malicious:	false
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\f047babb-a42e-4e6d-96cb-903a6ef61db5.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):	214570
Entropy (8bit):	6.070674575980348
Encrypted:	false
SSDEEP:	6144:n2fR5M3tFquiMkPvqXANlzYaqfIlUOoSiuRK:na5M3tFqokPvqwNhHoZ
MD5:	6F6AB392960F8AC76925D6472071D404
SHA1:	0348C711F044BECB9E9915D7135FAD2307885786
SHA-256:	67CDD564A1084C84903F25F729E12F9B689D81F9AB49B6661FB79B5F520E7CE3
SHA-512:	91225F5ACDA1B42B9E771F3B76DDA7B6A0F53EA849173E74DA59646F7ACE4FE14842024194C784E413403ED9F3C00170D9BA08A01DD89834DD5DAF3F2B2DE2F
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}}, "network_time":{"network_time_mapping":{"local":1.656622323014413e+12,"network":1.656622325e+12,"ticks":112027751.0,"uncertainty":4339977.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"}, "password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Temp\0e9571a0-6afd-4b9f-92bd-81a3f563411a.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
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\184c7535-18f6-4c0c-9683-3478f06d836f.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
Preview:	.

C:\Users\user\AppData\Local\Temp\5056_1892588763_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F502
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\5056_1892588763_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
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\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
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\5056_1892588763_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
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\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_crtend_o

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

C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonlwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.... .....@.....!.....@.8...@.....{.....W.....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w.....?.....Y@.....@.....1@.....B@.....P@.....@X@....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@....`..@.....@.....A.....A.....p.....@.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp.memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\5056_1892588763_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:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333EA
Malicious:	false
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.__divmoddi4.__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\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E38B
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 94 `..... _pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@....@.....NaCl....x86-64.....A.L...A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\5056_1892588763_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/+I
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
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\5056_1892588763_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....!.....!.....'.....G.....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i.....0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!..-DT.!.?.....?.....?.....?."..."..."..."..."......@.....`..... ...@...`..... ...@...`..... ...@...`..... ...@...`..... ...@...`.....`... ...@...`.....`...`.....@...@..... ....1..`3.. 4..`-..`-..:...:....F..@H..`H...H...F...F...G...H.. H...F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\5056_1892588763_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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\5056_1892588763\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5056_1892588763\manifest.json

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

C:\Users\user\AppData\Local\Temp\5056_58494094\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:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FF CAF
Malicious:	false
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\5056_58494094_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:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F0 FE
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbml mZXN0Lmpzb24iLCJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCI sImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxI iwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZg QvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8ql Ry7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZ dkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\user\AppData\Local\Temp\5056_58494094\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
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\5056_58494094\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
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\scoped_dir5056_1736904211\0e9571a0-6afd-4b9f-92bd-81a3f563411a.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
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..$.J....+M!.Hz.n`U.l)N.\|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir5056_1736904211\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
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_dir5056_1736904211\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false

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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE01 28
Malicious:	false
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_dir5056_1736904211\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:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA 53
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\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
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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 . un r.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_dir5056_1736904211\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
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_dir5056_1736904211\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:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
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 completed.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\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
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlakozzon 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_dir5056_1736904211\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
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_dir5056_1736904211\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
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.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 transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\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
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_dir5056_1736904211\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:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7
Malicious:	false
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_dir5056_1736904211\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+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
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_dir5056_1736904211\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
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_dir5056_1736904211\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:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_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_dir5056_1736904211\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+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
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_dir5056_1736904211\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
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_dir5056_1736904211\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:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D
Malicious:	false
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 com pleted.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\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:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC(9D
Malicious:	false
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_unavailabl e": {.. "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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
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_dir5056_1736904211\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
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "craw_app_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavailable": {.. "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.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5056_1736904211\CRX_INSTALL_locales\uk\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):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	12:1HEJ7wILkSlXZGG7wILkSlXZ+WYpU34zb1Oy2P+dgSV1EjiTO8ZpU347qtfP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF
Malicious:	false
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.".. }..}..

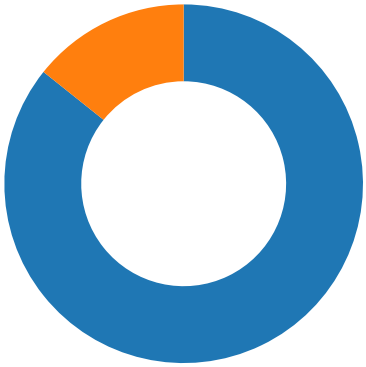
Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.197518824382674
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	Imax_SUMMARY.html
File size:	497139
MD5:	7396540ffe6dab2cd0334f920ecef28b
SHA1:	35801e9b7704dc77990a3f03318d082fdc3a21f7
SHA256:	a80beddc4d9de50aa917e5b433cfb9f054142bf836d8dab3964487b4f304c842
SHA512:	0ffe982384bd9518d893efd8c227fc3301814a3332803a5bc6996ac77e54a6ea9a9968ff2ea51c3ff1d041d973da5b11a3655b0dd26099c5eaf7d03a3ee62966
SSDEEP:	384:+k8e6D7Q4v82nhD793IkbmDg1McjeQV+QgoJcjcrKcUst7FxjSYg+T05JzF3t7o7:+xr
TLSH:	28B4CC324223CE6B6D13957D51AB7307ADE8F08D361232E8DAA57E6137863530FD89B1
File Content Preview:	<script language=javascript>document.write(unescape('%3Cscript%20language%3Djavascript%3Evar%20_0x541002%3D_0x30dc%3B%28function%28_0x4a2fbe%2C_0x21b5b1%29%7Bvar%20_0x55dd9d%3D_0x30dc%2C_0x53e532%3D_0x4a2fbe%28%29%3Bwhile%28%21%21%5B%5D%29%7Btry%7Bvar%20_

Network Behavior

Network Port Distribution



Total Packets: 70

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:52:03.311600924 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.311686039 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.311788082 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.311961889 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312004089 CEST	443	49752	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.312064886 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312480927 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312520027 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.312674999 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312737942 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312783003 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.312921047 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312964916 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.312994003 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.313128948 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.313344002 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.313357115 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.313522100 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.313853025 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.313878059 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.314016104 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.314588070 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.314630985 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.314805031 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.314834118 CEST	443	49752	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.315016031 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.315047026 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.315296888 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.315324068 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.315668106 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.315696001 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.315891981 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.315906048 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.316214085 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.316231012 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.367250919 CEST	443	49752	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.367759943 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.367798090 CEST	443	49752	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.368576050 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.368871927 CEST	443	49752	152.199.23.37	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:52:03.368944883 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.368959904 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.368998051 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.371053934 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.371200085 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.374825001 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.375468016 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.375897884 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.376374960 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.376415968 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.376585960 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.376599073 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.376791954 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.376791954 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.376832008 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.376897097 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.377582073 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.377676964 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.377938986 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.377942085 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.378025055 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.378768921 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.378818035 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.379105091 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.379136086 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.381052017 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.381149054 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.385019064 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.385360003 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.385390997 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.386550903 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.386636972 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.495448112 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.630162954 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.630409002 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.630414009 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.630458117 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.630582094 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.630641937 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.630713940 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.630739927 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.630899906 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.630940914 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.631763935 CEST	49757	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:03.632076979 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.635153055 CEST	49752	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.635446072 CEST	443	49752	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.636166096 CEST	49754	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.636209965 CEST	443	49754	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.636270046 CEST	49753	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.636302948 CEST	443	49753	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.636400938 CEST	49751	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.636426926 CEST	443	49751	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.636502981 CEST	49755	443	192.168.2.4	152.199.23.37
Jun 30, 2022 22:52:03.636523008 CEST	443	49755	152.199.23.37	192.168.2.4
Jun 30, 2022 22:52:03.636756897 CEST	49756	443	192.168.2.4	142.251.36.205
Jun 30, 2022 22:52:03.636771917 CEST	443	49756	142.251.36.205	192.168.2.4
Jun 30, 2022 22:52:03.636982918 CEST	49757	443	192.168.2.4	142.251.36.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:52:03.637021065 CEST	443	49757	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:03.637175083 CEST	49752	443	192.168.2.4	152.199.23.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 22:52:03.268387079 CEST	64454	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:03.276319027 CEST	64277	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:03.277235031 CEST	56076	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:03.295452118 CEST	53	64454	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:03.297833920 CEST	53	56076	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:03.304126978 CEST	53	64277	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:03.865145922 CEST	56509	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:03.883752108 CEST	53	56509	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:04.342112064 CEST	58171	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:04.358764887 CEST	53	58171	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:04.683643103 CEST	50445	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:06.292052984 CEST	51679	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:07.335844040 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.367975950 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.368498087 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.400312901 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.400340080 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.400361061 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.400382042 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.400763035 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.402084112 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.435651064 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.436054945 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.479464054 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.481327057 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.481548071 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.481832027 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.498353958 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.498461962 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.498503923 CEST	443	51681	142.251.36.238	192.168.2.4
Jun 30, 2022 22:52:07.498954058 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:07.524449110 CEST	51681	443	192.168.2.4	142.251.36.238
Jun 30, 2022 22:52:08.964041948 CEST	60612	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:08.981101990 CEST	53	60612	8.8.8.8	192.168.2.4
Jun 30, 2022 22:52:21.542916059 CEST	53989	53	192.168.2.4	8.8.8.8
Jun 30, 2022 22:52:23.255964994 CEST	50800	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 22:52:03.268387079 CEST	192.168.2.4	8.8.8.8	0x3479	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.276319027 CEST	192.168.2.4	8.8.8.8	0x2c1f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.277235031 CEST	192.168.2.4	8.8.8.8	0x8a81	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.865145922 CEST	192.168.2.4	8.8.8.8	0x6fa8	Standard query (0)	www.office.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.342112064 CEST	192.168.2.4	8.8.8.8	0x4b6d	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.683643103 CEST	192.168.2.4	8.8.8.8	0xad20	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:06.292052984 CEST	192.168.2.4	8.8.8.8	0x68e7	Standard query (0)	r4.res.office365.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:08.964041948 CEST	192.168.2.4	8.8.8.8	0xf2ed	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 22:52:21.542916059 CEST	192.168.2.4	8.8.8.8	0x8ca2	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:23.255964994 CEST	192.168.2.4	8.8.8.8	0x25c7	Standard query (0)	passwordreset.microsoftonline.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 22:52:03.295452118 CEST	8.8.8.8	192.168.2.4	0x3479	No error (0)	accounts.google.com		142.251.36.205	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.297043085 CEST	8.8.8.8	192.168.2.4	0xd05a	No error (0)	dual.part-0017.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.297043085 CEST	8.8.8.8	192.168.2.4	0xd05a	No error (0)	dual.part-0017.t-0009.fbs1-t-msedge.net	part-0017.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.297043085 CEST	8.8.8.8	192.168.2.4	0xd05a	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.219.45	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.297043085 CEST	8.8.8.8	192.168.2.4	0xd05a	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.227.45	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.297833920 CEST	8.8.8.8	192.168.2.4	0x8a81	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.297833920 CEST	8.8.8.8	192.168.2.4	0x8a81	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.304126978 CEST	8.8.8.8	192.168.2.4	0x2c1f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.304126978 CEST	8.8.8.8	192.168.2.4	0x2c1f	No error (0)	clients.l.google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:03.323829889 CEST	8.8.8.8	192.168.2.4	0x730e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.883752108 CEST	8.8.8.8	192.168.2.4	0x6fa8	No error (0)	www.office.com	home-portal.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.883752108 CEST	8.8.8.8	192.168.2.4	0x6fa8	No error (0)	home-portal.office.com	home-office365-com.b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.883752108 CEST	8.8.8.8	192.168.2.4	0x6fa8	No error (0)	home-office365-com.b-0004.b-msedge.net	b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:03.883752108 CEST	8.8.8.8	192.168.2.4	0x6fa8	No error (0)	b-0004.b-msedge.net		13.107.6.156	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.312959909 CEST	8.8.8.8	192.168.2.4	0xc5e1	No error (0)	scdn1cc4b.wpc.9aea3.sigmacdn.net	sni1gl.wpc.sigmacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:04.312959909 CEST	8.8.8.8	192.168.2.4	0xc5e1	No error (0)	sni1gl.wpc.sigmacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	HHN-efz.ms-acdc.office.com		40.99.150.114	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	HHN-efz.ms-acdc.office.com		52.98.175.2	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.358764887 CEST	8.8.8.8	192.168.2.4	0x4b6d	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.194	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:04.704585075 CEST	8.8.8.8	192.168.2.4	0xad20	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 22:52:04.704585075 CEST	8.8.8.8	192.168.2.4	0xad20	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:04.704585075 CEST	8.8.8.8	192.168.2.4	0xad20	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:06.312648058 CEST	8.8.8.8	192.168.2.4	0x68e7	No error (0)	r4.res.office365.com	r4.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:08.981101990 CEST	8.8.8.8	192.168.2.4	0xf2ed	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:08.981101990 CEST	8.8.8.8	192.168.2.4	0xf2ed	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 30, 2022 22:52:21.561866999 CEST	8.8.8.8	192.168.2.4	0x8ca2	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:21.965137005 CEST	8.8.8.8	192.168.2.4	0x329e	No error (0)	ppe.aadg.privatelink.msidentity.com	www.ppetm.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:23.289118052 CEST	8.8.8.8	192.168.2.4	0x25c7	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:23.289118052 CEST	8.8.8.8	192.168.2.4	0x25c7	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:23.289118052 CEST	8.8.8.8	192.168.2.4	0x25c7	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:23.455981970 CEST	8.8.8.8	192.168.2.4	0xe9f	No error (0)	ppe.aadg.privatelink.msidentity.com	www.ppetm.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 22:52:39.097022057 CEST	8.8.8.8	192.168.2.4	0x9b28	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- aadcdn.msftauth.net
- accounts.google.com
- clients2.google.com
- www.office.com
- https:
  - res.cdn.office.net
  - outlook.office365.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49754	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	0	OUT	GET /shared/1.0/content/js/asyncchunk/convergedlogin_ptiles_fdcf9ba11efc979408f4.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	88	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 10929283 Cache-Control: public, max-age=31536000 Content-MD5: BLPwS4L9l6RsHwFrFxd9Dw== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D9313DA6D9F360 Last-Modified: Thu, 17 Jun 2021 03:11:51 GMT Server: ECAcc (muc/330B) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 12372de7-201e-0019-685c-29b88f000000 x-ms-version: 2009-09-19 Content-Length: 24875 Connection: close
2022-06-30 20:52:03 UTC	89	IN	Data Raw: 2f 2a 21 0a 20 2a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 53 54 41 52 54 20 4f 46 20 54 48 49 52 44 20 50 41 52 54 59 20 4e 4f 54 49 43 45 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0a 20 2a 20 0a 20 2a 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 62 61 73 65 64 20 6f 6e 20 6f 72 20 69 6e 63 6f 72 70 6f 72 61 74 65 73 20 6d 61 74 65 72 69 61 6c 20 66 72 6f 6d 20 74 68 65 20 70 72 6f 6a 65 63 74 73 20 6c 69 73 74 65 64 20 62 65 6c 6f 77 20 28 54 68 69 72 64 20 50 61 72 74 79 20 49 50 29 2e 20 54 68 65 20 6f 72 69 67 69 6e 61 6c 20 63 6f 70 79 72 69 67 68 74 20 6e 6f 74 69 63 65 20 61 Data Ascii: /*! * --- START OF THIRD PARTY NOTICE --- * * This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice a
2022-06-30 20:52:03 UTC	106	IN	Data Raw: 65 6e 74 4c 69 73 74 65 6e 65 72 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2c 22 63 6c 69 63 6b 22 2c 41 29 2c 70 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2c 22 6b 65 79 64 6f 77 6e 22 2c 4c 29 7d 66 75 6e 63 74 69 6f 6e 20 50 28 29 7b 69 2e 66 6f 72 67 65 74 46 6f 63 75 73 28 21 64 2e 69 73 53 69 67 6e 65 64 49 6e 29 2c 69 2e 73 69 67 6e 6f 75 74 46 6f 63 75 73 28 64 2e 69 73 53 69 67 6e 65 64 49 6e 26 26 21 64 2e 69 73 4d 65 43 6f 6e 74 72 6f 6c 53 65 73 73 69 6f 6e 29 2c 69 2e 73 69 67 6e 6f 75 74 41 6e 64 46 6f 72 67 65 74 46 6f 63 75 73 28 64 2e 69 73 53 69 67 6e 65 64 49 6e 26 26 64 2e 69 73 4d 65 43 6f 6e 74 72 6f 6c 53 65 7 3 73 69 6f 6e 29 7d 66 75 6e 63 74 69 6f 6e 20 71 28 65 29 7b 77 Data Ascii: entListener(document.body,"click",A),p.removeEventListener(document.body,"keydown",L)}function P(){i.forgetFocus(!d.isSignedIn),i.signoutFocus(d.isSignedIn&&!d.isMeControlSession),i.signoutAndForgetFocus(d.isSignedIn&&d.isMeControlSession)}function q(e){w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49753	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	0	OUT	GET /ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnfq3xbrj5zvj5ionvww2.css HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive Origin: null 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 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	3	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 2084673 Cache-Control: public, max-age=31536000 Content-MD5: mU+G3bfjPvbbh+JW3ypW1g== Content-Type: text/css Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D927B31E2905FD Last-Modified: Fri, 04 Jun 2021 23:47:30 GMT Server: ECAcc (muc/3372) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: b70b69e6-001e-0048-37cd-790508000000 x-ms-version: 2009-09-19 Content-Length: 109838 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	4	IN	Data Raw: 2f 2a 21 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 20 2a 2f 2f 2a 21 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 53 54 41 52 54 20 4f 46 20 54 48 49 52 44 20 50 41 52 54 59 20 4e 4f 54 49 43 45 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0a 0a 54 68 69 73 20 66 69 6c 65 20 69 73 20 62 61 73 65 64 20 6f 6e 20 6f 72 20 69 6e 63 6f 72 70 6f 72 61 74 65 73 20 6d 61 74 65 72 69 61 6c 20 66 72 6f 6d 20 74 68 65 20 70 72 6f 6a 65 63 74 73 20 6c 69 73 74 65 64 20 Data Ascii: /*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!--- START OF THIRD PARTY NOTICE ---This file is based on or incorporates material from the projects listed
2022-06-30 20:52:03 UTC	20	IN	Data Raw: 73 Data Ascii: s
2022-06-30 20:52:03 UTC	20	IN	Data Raw: 2d 31 2c 2e 63 6f 6c 2d 78 73 2d 32 2c 2e 63 6f 6c 2d 78 73 2d 33 2c 2e 63 6f 6c 2d 78 73 2d 34 2c 2e 63 6f 6c 2d 78 73 2d 35 2c 2e 63 6f 6c 2d 78 73 2d 36 2c 2e 63 6f 6c 2d 78 73 2d 37 2c 2e 63 6f 6c 2d 78 73 2d 38 2c 2e 63 6f 6c 2d 78 73 2d 39 2c 2e 63 6f 6c 2d 78 73 2d 31 30 2c 2e 63 6f 6c 2d 78 73 2d 31 31 2c 2e 63 6f 6c 2d 78 73 2d 31 32 2c 2e 63 6f 6c 2d 78 73 2d 31 33 2c 2e 63 6f 6c 2d 78 73 2d 31 34 2c 2e 63 6f 6c 2d 78 73 2d 31 35 2c 2e 63 6f 6c 2d 78 73 2d 31 36 2c 2e 63 6f 6c 2d 78 73 2d 31 37 2c 2e 63 6f 6c 2d 78 73 2d 31 38 2c 2e 63 6f 6c 2d 78 73 2d 31 39 2c 2e 63 6f 6c 2d 78 73 2d 32 30 2c 2e 63 6f 6c 2d 78 73 2d 32 31 2c 2e 63 6f 6c 2d 78 73 2d 32 32 2c 2e 63 6f 6c 2d 78 73 2d 32 33 2c 2e 63 6f 6c 2d 78 73 2d 32 34 7b 66 6c 6f 61 74 3a 6c Data Ascii: -1,.col-xs-2,.col-xs-3,.col-xs-4,.col-xs-5,.col-xs-6,.col-xs-7,.col-xs-8,.col-xs-9,.col-xs-10,.col-xs-11,.col-xs-12,.col-xs-13,.col-xs-14,.col-xs-15,.col-xs-16,.col-xs-17,.col-xs-18,.col-xs-19,.col-xs-20,.col-xs-21,.col-xs-22,.col-xs-23,.col-xs-24{float:l
2022-06-30 20:52:03 UTC	146	IN	Data Raw: 67 69 6e 2d 6c 65 66 74 3a 39 35 2e 38 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 6c 2d 6f 66 66 73 65 74 2d 32 34 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 30 25 7d 7d 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 62 6f 72 64 65 72 3a 30 3b 6d 69 6e 2d 77 69 64 74 68 3a 30 7d 6c 65 67 65 6e 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 31 30 30 25 3b 70 61 64 64 69 6e 67 3a 30 3b 62 6f 72 64 65 72 3a 30 7d 6c 61 62 65 6c 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 65 61 72 63 68 22 5d 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 6f Data Ascii: gin-left:95.83333%}.col-xl-offset-24{margin-left:100%}}fieldset{padding:0;margin:0;border:0;min-width:0}legend{display:block;width:100%;padding:0;border:0}label{display:inline-block;max-width:100%}input[type="search"]{-webkit-box-sizing:border-box;-moz-bo
2022-06-30 20:52:03 UTC	162	IN	Data Raw: 6c 6f Data Ascii: lo
2022-06-30 20:52:03 UTC	162	IN	Data Raw: 77 2d 78 3a 61 75 74 6f 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 2e 30 31 25 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 33 39 70 78 29 7b 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 35 70 78 3b 6f 76 65 72 66 6c 6f 77 2d 79 3a 68 69 64 64 65 6e 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 2d 6d 73 2d 61 75 74 6f 68 69 64 69 6e 67 2d 73 63 72 6f 6c 6c 62 61 72 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 3e 74 68 65 61 64 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 Data Ascii: w-x:auto;min-height:.01%}@media screen and (max-width:539px){.table-responsive{width:100%;margin-bottom:15px;overflow-y:hidden;-ms-overflow-style:-ms-autohiding-scrollbar}.table-responsive>.table{margin-bottom:0}.table-responsive>.table>thead>tr>th,.table
2022-06-30 20:52:03 UTC	178	IN	Data Raw: 2c 22 54 75 6e 67 61 22 2c 22 4c 61 6f 20 55 49 22 2c 22 52 61 61 76 69 22 2c 22 49 73 6b 6f 6f 6c 61 20 50 6f 74 61 22 2c 22 4c 61 74 68 61 22 2c 22 4c 65 65 6c 61 77 61 64 65 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 20 55 49 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4a 68 65 6e 67 48 65 69 20 55 49 22 2c 22 4d 61 6c 67 75 6e 20 47 6f 74 68 69 63 22 2c 22 45 73 74 72 61 6e 67 65 6c 6f 20 45 64 65 73 73 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 48 69 6d 61 6c 61 79 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4e 65 77 20 54 61 69 20 4c 75 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 50 68 61 67 73 50 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 54 61 69 20 4c 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 69 20 42 61 69 74 69 22 2c 22 4d 6f 6e 67 6f 6c Data Ascii: ,"Tunga","Lao UI","Raavi","Iskoola Pota","Latha","Leelawadee","Microsoft YaHei UI","Microsoft JhengHei UI","Malgun Gothic","Estrangelo Edessa","Microsoft Himalaya","Microsoft New Tai Lue","Microsoft PhagsPa","Microsoft Tai Le","Microsoft Yi Baiti","Mongol
2022-06-30 20:52:03 UTC	194	IN	Data Raw: 69 6e Data Ascii: in
2022-06-30 20:52:03 UTC	194	IN	Data Raw: 70 75 74 5b 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 75 62 6d 69 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 72 65 73 65 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 2d 6d 73 2d 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 3b 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 7d 2e 62 75 74 74 6f 6e 2e 73 65 63 6f 6e 64 61 72 79 7b 64 69 73 70 6c 61 79 3a 69 6e 6c Data Ascii: put[type="button"].btn-primary:active,input[type="submit"].btn-primary:active,input[type="reset"].btn-primary:active{outline:none;text-decoration:none;-ms-transform:scale(.98);-webkit-transform:scale(.98);transform:scale(.98)}.button.secondary{display:inl
2022-06-30 20:52:03 UTC	286	IN	Data Raw: 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 6d 65 6d 62 65 72 6e 61 6d 65 50 72 65 66 69 6c 6c 53 65 6c 65 63 74 2e 68 61 73 2d 65 72 72 6f 72 2c 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 6d 65 6d 62 65 72 6e 61 6d 65 50 72 65 66 69 6c 6c 53 65 6c 65 63 74 2e 68 61 73 2d 65 72 72 6f 72 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 65 38 31 31 32 33 7d 2e 6f 75 74 6c 6f 6f 6b 45 6d 61 69 6c 4c 61 62 65 6c 7b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 2e 73 75 62 74 69 74 6c 65 7b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 31 32 35 Data Ascii: ropdown-toggle.membernamePrefillSelect.has-error,.dropdown-toggle.membernamePrefillSelect.has-error:hover{border-width:1px;border-color:#e81123}.outlookEmailLabel{border-left:none;border-right:none;border-top:none;padding-right:0}.subtitle{font-size:.8125

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49762	13.107.6.156	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	667	OUT	GET /prefetch/prefetch HTTP/1.1 Host: www.office.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	668	IN	HTTP/1.1 200 OK Cache-Control: no-store,no-cache Pragma: no-cache Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Set-Cookie: OH.SID=bcf0b4f6-6488-4ae7-8eb2-72facc5d68f2; path=/; secure; samesite=none; httponly Set-Cookie: OH.DCAffinity=OH-weu; expires=Fri, 01 Jul 2022 04:52:04 GMT; path=/; secure; samesite=none; httponly Set-Cookie: OH.FLID=615708bd-08f8-4d0e-9060-74dca536722e; expires=Fri, 30 Jun 2023 20:52:04 GMT; path=/; secure; samesite=none; httponly Request-Context: appId= Strict-Transport-Security: max-age=31536000; includeSubDomains Referrer-Policy: strict-origin-when-cross-origin X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-UA-Compatible: IE=edge,chrome=1 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: C5EAE878307640879C9D8002D394A03B Ref B: AM3EDGE0221 Ref C: 2022-06-30T20:52:04Z Set-Cookie: MUID=0E3470C8A19365C9046C611BA0E86456; path=/; secure; expires=Tue, 25-Jul-2023 20:52:04 GMT; domain=office.com Date: Thu, 30 Jun 2022 20:52:03 GMT Connection: close
2022-06-30 20:52:04 UTC	669	IN	Data Raw: 33 63 64 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 20 70 72 65 66 65 74 63 68 20 70 61 67 65 20 66 6f 72 20 4f 66 66 69 63 65 48 6f 6d 65 20 61 70 70 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 77 69 64 74 68 3a 30 3b 68 65 69 67 68 74 3a 30 3b 22 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 72 65 73 2e 63 64 6e 2e 6f 66 66 69 63 65 2e 6e 65 74 2f 6f 66 66 69 63 65 68 75 62 2f 62 75 6e 64 6c 65 73 2f 70 6f 6c 79 66 69 6c 6c 73 2d 62 75 6e 64 6c 65 2d 32 32 32 63 31 36 63 37 30 65 38 31 65 33 66 33 31 37 64 37 2e 6a 73 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 Data Ascii: 3cd<html><head> <title>A prefetch page for OfficeHome app</title></head><body style="width:0;height:0;"> <link rel="prefetch" href="https://res.cdn.office.net/officehub/bundles/polyfills-bundle-222c16c70e81e3f317d7.js" />
2022-06-30 20:52:04 UTC	670	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49767	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	670	OUT	GET /officehub/bundles/polyfills-bundle-222c16c70e81e3f317d7.js HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	673	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 488354 Content-Type: application/javascript Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Thu, 16 Jun 2022 20:30:34 GMT Server: ECAcc (muc/3378) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon X-Content-Type-Options: nosniff x-ms-request-id: 7b625b0f-f01e-003a-3152-88d0b9000000 Content-Length: 100488 Connection: close
2022-06-30 20:52:04 UTC	673	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 72 3d 7b 7d 3b 66 75 6e 63 74 69 6f 6e 20 6e 28 65 29 7b 69 66 28 72 5b 65 5d 29 72 65 74 75 72 6e 20 72 5b 65 5d 2e 65 78 70 6f 72 74 73 3b 76 61 72 20 6f 3d 72 5b 65 5d 3d 7b 69 3a 65 2c 6c 3a 21 31 2c 65 78 70 6f 72 74 73 3a 7b 7d 7d 3b 72 65 74 75 72 6e 20 74 5b 65 5d 2e 63 61 6c 6c 28 6f 2e 65 78 70 6f 72 74 73 2c 6f 2c 6f 2e 65 78 70 6f 72 74 73 2c 6e 29 2c 6f 2e 6c 3d 21 30 2c 6f 2e 65 78 70 6f 72 74 73 7d 6e 2e 6d 3d 74 2c 6e 2e 63 3d 72 2c 6e 2e 64 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 65 29 7b 6e 2e 6f 28 74 2c 72 29 7c 7c 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 72 2c 7b 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 67 65 74 3a 65 7d 29 7d 2c 6e 2e 72 3d 66 75 6e Data Ascii: !function(t){var r={};function n(e){if(r[e])return r[e].exports;var o=r[e]={i:e,l:!1,exports:{}};return t[e].call(o.exports,o,o.exports,n),o.l=!0,o.exports}n.m=t,n.c=r,n.d=function(t,r,e){n.o(t,r)||Object.defineProperty(t,r,{enumerable:!0,get:e})},n.r=fun
2022-06-30 20:52:04 UTC	689	IN	Data Raw: 28 22 4a 52 4d 30 22 29 2c 6f 3d 6e 28 22 50 43 71 54 22 29 2c 69 3d 6e 28 22 55 56 64 56 22 29 2c 61 3d 6e 28 22 67 44 59 4d 22 29 2c 75 3d 6e 28 22 6a 6d 55 71 22 29 2c 63 3d 6e 28 22 61 37 32 51 22 29 2c 66 3d 6e 28 22 36 6b 61 35 22 29 2c 73 3d 6e 28 22 76 2b 4b 54 22 29 2c 6c 3d 6e 28 22 6d 61 59 6a 22 29 3b 65 28 7b 74 61 72 67 65 74 3a 22 53 65 74 22 2c 70 72 6f 74 6f 3a 21 30 2c 72 65 61 6c 3a 21 30 2c 66 6f 72 63 65 64 3a 6f 7d 2c 7b 6d 61 70 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 72 3d 61 28 74 68 69 73 29 2c 6e 3d 73 28 72 29 2c 65 3d 63 28 74 2c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 3e 31 3f 61 72 67 75 6d 65 6e 74 73 5b 31 5d 3a 76 6f 69 64 20 30 2c 33 29 2c 6f 3d 6e 65 77 28 66 28 72 2c 69 28 22 53 65 74 22 29 29 29 2c Data Ascii: ("JRM0"),o=n("PCqT"),i=n("UVdV"),a=n("gDYM"),u=n("jmUq"),c=n("a72Q"),f=n("6ka5"),s=n("v+KT"),l=n("maYj");e({target:"Set",proto:!0,real:!0,forced:o},{map:function(t){var r=a(this),n=s(r),e=c(t,arguments.length>1?arguments[1]:void 0,3),o=new(f(r,i("Set"))),
2022-06-30 20:52:04 UTC	705	IN	Data Raw: 69 22 Data Ascii: i"
2022-06-30 20:52:04 UTC	827	IN	Data Raw: 29 2c 69 3d 6e 28 22 64 35 65 39 22 29 3b 65 28 7b 74 61 72 67 65 74 3a 22 41 72 72 61 79 22 2c 70 72 6f 74 6f 3a 21 30 7d 2c 7b 63 6f 70 79 57 69 74 68 69 6e 3a 6f 7d 29 2c 69 28 22 63 6f 70 79 57 69 74 68 69 6e 22 29 7d 2c 4b 78 7a 36 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 65 3d 6e 28 22 4a 52 4d 30 22 29 2c 6f 3d 6e 28 22 6a 69 64 2f 22 29 3b 65 28 7b 74 61 72 67 65 74 3a 22 53 74 72 69 6e 67 22 2c 70 72 6f 74 6f 3a 21 30 2c 66 6f 72 63 65 64 3a 6e 28 22 55 6f 35 30 22 29 28 22 73 74 72 69 6b 65 22 29 7d 2c 7b 73 74 72 69 6b 65 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6f 28 74 68 69 73 2c 22 73 74 72 69 6b 65 22 2c 22 22 2c 22 22 29 7d 7d 29 7d 2c 22 4c 2f 59 62 22 3a 66 75 Data Ascii:),i=n("d5e9");e({target:"Array",proto:!0},{copyWithin:o}),i("copyWithin")},Kxz6:function(t,r,n){"use strict";var e=n("JRM0"),o=n("jid/");e({target:"String",proto:!0,forced:n("Uo50")("strike")},{strike:function(){return o(this,"strike","","")}})},"L/Yb":fu
2022-06-30 20:52:04 UTC	843	IN	Data Raw: 2c 69 6e 64 65 78 3a 30 7d 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 72 3d 63 28 74 68 69 73 29 2c 6e 3d 72 2e 73 74 72 69 6e 67 2c 6f 3d 72 2e 69 6e 64 65 78 3b 72 65 74 75 72 6e 20 6f 3e 3d 6e 2e 6c 65 6e 67 74 68 3f 7b 76 61 6c 75 65 3a 76 6f 69 64 20 30 2c 64 6f 6e 65 3a 21 30 7d 3a 28 74 3d 65 28 6e 2c 6f 29 2c 72 2e 69 6e 64 65 78 2b 3d 74 2e 6c 65 6e 67 74 68 2c 7b 76 61 6c 75 65 3a 74 2c 64 6f 6e 65 3a 21 31 7d 29 7d 29 29 7d 2c 58 32 31 65 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 76 61 72 20 65 3d 6e 28 22 6e 48 49 6b 22 29 2c 6f 3d 6e 28 22 51 53 6b 36 22 29 2c 69 3d 6e 28 22 47 48 66 32 22 29 28 22 74 6f 50 72 69 6d 69 74 69 76 65 22 29 2c 61 3d 44 61 74 65 2e 70 72 6f 74 6f 74 79 70 65 3b 69 20 69 6e 20 61 7c Data Ascii: ,index:0})}),(function(){var t,r=c(this),n=r.string,o=r.index;return o>=n.length?{value:void 0,done:!0}:(t=e(n,o),r.index+=t.length,{value:t,done:!1})})},X21e:function(t,r,n){var e=n("nHlk"),o=n("QSk6"),i=n("GHf2")("toPrimitive"),a=Date.prototype;i in a|
2022-06-30 20:52:04 UTC	859	IN	Data Raw: 75 72 6e 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 74 3f 6e 75 6c 6c 21 3d 3d 74 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 74 7d 7d 2c 66 70 37 59 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 65 3d 6e 28 22 48 76 70 6b 22 29 2c 6f 3d 6e 28 22 6e 45 61 50 22 29 2c 69 3d 6e 28 22 39 6e 58 32 22 29 2c 61 3d 6e 28 22 30 4b 32 70 22 29 2c 75 3d 6e 28 22 74 46 30 37 22 29 2c 63 3d 6e 28 22 66 53 49 7a 22 29 2c 66 3d 6e 28 22 35 43 46 62 22 29 2c 73 3d 6e 28 22 57 39 66 68 22 29 2c 6c 3d 6e 28 22 2b 69 4c 37 22 29 2c 70 3d 6e 28 22 77 2f 4a 69 22 29 2c 76 3d 6e 28 22 4f 56 68 61 22 29 2e 66 2c 67 3d 6e 28 22 46 75 70 37 22 29 2e 66 2c 68 3d 6e 28 22 6e 52 63 36 22 29 2e 66 2c 64 Data Ascii: urn"object"==typeof t?null!==t:"function"==typeof t}},fp7Y:function(t,r,n){"use strict";var e=n("Hvpk"),o=n("nEaP"),i=n("9nX2"),a=n("0K2p"),u=n("tF07"),c=n("fSIz"),f=n("5CFb"),s=n("W9fh"),l=n("+iL7"),p=n("w/Ji"),v=n("OVha").f,g=n("Fup7").f,h=n("nRc6").f,d
2022-06-30 20:52:04 UTC	975	IN	Data Raw: 3d 74 79 70 65 6f 66 20 67 6c 6f 62 61 6c 54 68 69 73 26 26 67 6c 6f 62 61 6c 54 68 69 73 29 7c 7c 6e 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 26 26 77 69 6e 64 6f 77 29 7c 7c 6e 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 73 65 6c 66 26 26 73 65 6c 66 29 7c 7c 6e 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 72 26 26 72 29 7c 7c 46 75 6e 63 74 69 6f 6e 28 22 72 65 74 75 72 6e 20 74 68 69 73 22 29 28 29 7d 29 2e 63 61 6c 6c 28 74 68 69 73 2c 6e 28 22 70 43 76 41 22 29 29 7d 29 2c 6e 48 49 6b 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 76 61 72 20 65 3d 6e 28 22 48 76 70 6b 22 29 2c 6f 3d 6e 28 22 52 63 36 22 29 2c 69 3d 6e 28 22 56 53 57 38 22 29 3b 74 2e 65 78 70 6f 72 74 73 3d 65 3f 66 75 6e 63 74 Data Ascii: =typeof globalThis&&globalThis)||n("object"==typeof window&&window)||n("object"==typeof self&&self)||n("object"==typeof r&&r)||Function("return this")()}).call(this,n("pCvA"))},nHlk:function(t,r,n){var e=n("Hvpk"),o=n("nRc6"),i=n("VSW8");t.exports=e?funct

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	991	IN	Data Raw: 74 72 69 6e 67 22 2c 70 72 6f 74 6f 3a 21 30 2c 66 6f 72 63 65 64 3a 6e 28 22 55 6f 35 30 22 29 28 22 6c 69 6e 6b 22 29 7d 2c 7b 6c 69 6e 6b 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 6f 28 74 68 69 73 2c 22 61 22 2c 22 68 72 65 66 22 2c 74 29 7d 7d 29 7d 2c 22 79 45 41 2f 22 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 6e 28 22 4a 52 4d 30 22 29 28 7b 74 61 72 67 65 74 3a 22 4f 62 6a 65 63 74 22 2c 73 74 61 74 3a 21 30 7d 2c 7b 69 73 3a 6e 28 22 6d 76 4f 6d 22 29 7d 29 7d 2c 79 50 4c 52 3a 66 75 6e 63 74 69 6f 6e 28 74 2c 72 2c 6e 29 7b 76 61 72 20 65 3d 6e 28 22 4a 52 4d 30 22 29 2c 6f 3d 6e 28 22 53 6c 76 4d 22 29 3b 65 28 7b 67 6c 6f 62 61 6c 3a 21 30 2c 66 6f 72 63 65 64 3a 70 61 72 73 65 49 6e 74 21 3d 6f 7d 2c 7b 70 61 72 73 Data Ascii: tring",proto:!0,forced:n("Uo50")("link")},{link:function(t){return o(this,"a","href",t)}}}},"yEA/":function(t,r,n){n("JRM0")({target:"Object",stat:!0},{is:n("mvOm")}}},yPLR:function(t,r,n){var e=n("JRM0"),o=n("SlvM");e({global:!0,forced:parseInt!=o},{pars

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49766	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	670	OUT	GET /officehub/bundles/sharedscripts-c77f7edec8.js HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	705	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 166401 Content-Type: application/javascript Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Mon, 09 May 2022 22:16:27 GMT Server: ECAcc (muc/3380) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon X-Content-Type-Options: nosniff x-ms-request-id: 3ae12f9e-101e-0050-483f-8b0891000000 Content-Length: 53098 Connection: close
2022-06-30 20:52:04 UTC	706	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 69 66 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 29 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3b 65 6c 73 65 20 69 66 28 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 29 64 65 66 69 6e 65 28 5b 5d 2c 74 29 3b 65 6c 73 65 7b 76 61 72 20 69 3d 74 28 29 3b 66 6f 72 28 76 61 72 20 6e 20 69 6e 20 69 29 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 3f 65 78 70 6f 72 74 73 3a 65 29 5b 6e 5d 3d 69 5b 6e 5d 7d 7d 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 Data Ascii: !function(e,t){if("object"==typeof exports&&"object"==typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);else{var i=t();for(var n in i)("object"==typeof exports?exports:e)[n]=i[n]}}(this, function(){return function(
2022-06-30 20:52:04 UTC	722	IN	Data Raw: 69 Data Ascii: i
2022-06-30 20:52:04 UTC	722	IN	Data Raw: 73 2e 4a 26 26 28 6e 2e 64 65 66 61 75 6c 74 2e 63 68 65 63 6b 41 6e 64 53 61 76 65 44 65 76 69 63 65 49 64 28 65 29 2c 74 68 69 73 2e 24 28 22 44 65 76 69 63 65 49 6e 66 6f 2e 49 64 22 2c 65 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 73 65 74 44 65 76 69 63 65 4f 73 4e 61 6d 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 68 69 73 2e 4a 26 26 74 68 69 73 2e 24 28 22 44 65 76 69 63 65 49 6e 66 6f 2e 4f 73 4e 61 6d 65 22 2c 65 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 73 65 74 44 65 76 69 63 65 4f 73 56 65 72 73 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 68 69 73 2e 4a 26 26 74 68 69 73 2e 24 28 22 44 65 76 69 63 65 49 6e 66 6f 2e 4f 73 56 65 72 73 69 6f 6e 22 2c 65 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 73 65 74 44 65 76 69 63 65 42 72 Data Ascii: s.J&&(n.default.checkAndSaveDeviceId(e),this.$("DeviceInfo.Id",e))},e.prototype.setDeviceOsName=function(e){this.J&&this.$("DeviceInfo.OsName",e)},e.prototype.setDeviceOsVersion=function(e){this.J&&this.$("DeviceInfo.OsVersion",e)},e.prototype.setDeviceBr

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	875	IN	Data Raw: 67 74 68 25 33 2c 72 3d 30 2c 6f 3d 65 2e 6c 65 6e 67 74 68 2d 6e 3b 72 3c 6f 3b 72 2b 3d 33 29 7b 76 61 72 20 73 3d 28 65 5b 72 5d 3c 3c 31 36 29 2b 28 65 5b 72 2b 31 5d 3c 3c 38 29 2b 65 5b 72 2b 32 5d 3b 69 2e 70 75 73 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 5b 74 2e 63 68 61 72 41 74 28 65 3e 3e 31 38 26 36 33 29 2c 74 2e 63 68 61 72 41 74 28 65 3e 3e 31 32 26 36 33 29 2c 74 2e 63 68 61 72 41 74 28 65 3e 3e 36 26 36 33 29 2c 74 2e 63 68 61 72 41 74 28 36 33 26 65 29 5d 2e 6a 6f 69 6e 28 22 22 29 7d 28 73 29 29 7d 73 77 69 74 63 68 28 6e 29 7b 63 61 73 65 20 31 3a 76 61 72 20 73 3d 65 5b 65 2e 6c 65 6e 67 74 68 2d 31 5d 3b 69 2e 70 75 73 68 28 74 2e 63 68 61 72 41 74 28 73 3e 3e 32 29 29 2c 69 2e 70 75 73 68 28 74 2e 63 68 61 72 41 Data Ascii: gth%3,r=0,o=e.length-n;r<o;r+=3){var s=(e[r]<<16)+(e[r+1]<<8)+e[r+2];i.push(function(e){return[t.charAt(e>>18&63),t.charAt(e>>12&63),t.charAt(e>>6&63),t.charAt(63&e)].join("")}(s))}switch(n){case 1:var s=e[e.length-1];i.push(t.charAt(s>>2)),i.push(t.charA
2022-06-30 20:52:04 UTC	891	IN	Data Raw: 64 29 2c 65 2e 4c 6f 67 67 65 72 2e 53 74 61 72 74 53 65 73 73 69 6f 6e 28 29 2c 65 2e 4c 6f 67 67 65 72 2e 45 6e 64 53 65 73 73 69 6f 6e 4f 6e 55 6e 6c 6f 61 64 28 69 29 2c 65 2e 4c 6f 67 67 65 72 2e 46 6c 75 73 68 51 75 65 75 65 64 45 76 65 6e 74 73 28 29 7d 7d 7d 2c 74 2e 45 6e 64 53 65 73 73 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 69 29 7b 69 66 28 65 2e 4c 6f 67 67 65 72 2e 61 72 69 61 4c 6f 67 67 65 72 26 26 65 2e 4c 6f 67 67 65 72 2e 73 65 73 73 69 6f 6e 41 63 74 69 76 65 29 7b 69 66 28 65 2e 4c 6f 67 67 65 72 2e 73 65 73 73 69 6f 6e 41 63 74 69 76 65 3d 21 31 2c 21 77 69 6e 64 6f 77 2e 64 69 73 61 62 6c 65 4c 6f 67 73 29 7b 76 61 72 20 6e 3d 65 2e 4c 6f 67 67 65 72 2e 47 65 74 53 65 73 73 69 6f 6e 50 72 6f 70 65 72 74 69 65 73 28 29 3b 65 2e Data Ascii: d),e.Logger.StartSession(),e.Logger.EndSessionOnUnload(i),e.Logger.FlushQueuedEvents()}}},t.EndSession=function(t,i){if(e.Logger.ariaLogger&&e.Logger.sessionActive){if(e.Logger.sessionActive=!1,!window.disableLogs){var n=e.Logger.GetSessionProperties();e.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49765	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	671	OUT	GET /officehub/bundles/staticscripts-db293b874e.js HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	738	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 534090 Content-Type: application/javascript Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Thu, 02 Jun 2022 20:00:52 GMT Server: ECAcc (muc/3336) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon X-Content-Type-Options: nosniff x-ms-request-id: 16ba8e66-901e-0003-38e7-872ba5000000 Content-Length: 16187 Connection: close
2022-06-30 20:52:04 UTC	739	IN	Data Raw: 76 61 72 20 46 6c 75 73 68 55 74 69 6c 69 74 69 65 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 29 7b 7d 76 61 72 20 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 72 65 74 75 72 6e 20 6e 26 26 6e 2e 6d 65 73 73 61 67 65 3f 65 2b 22 3a 20 22 2b 6e 2e 6d 65 73 73 61 67 65 3a 65 7d 2c 74 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 76 61 72 20 74 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 74 69 74 6c 65 22 29 3b 74 2e 69 6e 6e 65 72 48 54 4d 4c 3d 6e 2c 65 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 74 29 7d 2c 69 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 69 66 28 65 26 26 68 69 73 74 6f 72 79 26 26 68 69 73 74 6f 72 79 2e 72 65 70 6c 61 63 65 53 74 61 74 65 29 7b 76 61 72 20 74 3d 68 69 73 74 6f 72 Data Ascii: var FlushUtilities=function(){function e(){}var n=function(e,n){return n&&n.message?e+": "+n.message:e},t=function(e,n){var t=document.createElement("title");t.innerHTML=n,e.appendChild(t)},i=function(e,n){if(e&&history&&history.replaceState){var t=histor

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49768	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	671	OUT	GET /officehub/bundles/app-bundle-f2fd0b05c66150f9b6e9.js HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	754	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 187686 Content-Type: application/javascript Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Mon, 27 Jun 2022 20:37:08 GMT Server: ECAcc (muc/3315) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon X-Content-Type-Options: nosniff x-ms-request-id: da667c21-801e-000f-4d0e-8bbcad000000 Content-Length: 1257937 Connection: close
2022-06-30 20:52:04 UTC	755	IN	Data Raw: 2f 2a 21 20 46 6f 72 20 6c 69 63 65 6e 73 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 73 65 65 20 61 70 70 2d 62 75 6e 64 6c 65 2d 66 32 66 64 30 62 30 35 63 36 36 31 35 30 66 39 62 36 65 39 2e 6a 73 2e 4c 49 43 45 4e 53 45 2e 74 78 74 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 74 28 74 29 7b 66 6f 72 28 76 61 72 20 69 2c 72 2c 63 3d 74 5b 30 5d 2c 6c 3d 74 5b 31 5d 2c 75 3d 74 5b 32 5d 2c 64 3d 74 5b 33 5d 7c 7c 5b 5d 2c 70 3d 30 2c 68 3d 5b 5d 3b 70 3c 63 2e 6c 65 6e 67 74 68 3b 70 2b 2b 29 72 3d 63 5b 70 5d 2c 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 2e 63 61 6c 6c 28 6f 2c 72 29 26 26 6f 5b 72 5d 26 26 68 2e 70 75 73 68 28 6f 5b 72 5d 5b 30 5d 29 Data Ascii: /*! For license information please see app-bundle-f2fd0b05c66150f9b6e9.js.LICENSE.txt */!function(e){function t(t){for(var i,r,c=t[0],l=t[1],u=t[2],d=t[3]||[],p=0,h=[];p<c.length;p++)r=c[p],Object.prototype.hasOwnProperty.call(o,r)&&o[r]&&h.push(o[r][0])
2022-06-30 20:52:04 UTC	771	IN	Data Raw: 2c Data Ascii: ,
2022-06-30 20:52:04 UTC	771	IN	Data Raw: 35 33 33 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 33 22 2c 35 33 34 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 34 22 2c 35 33 35 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 35 22 2c 35 33 36 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 36 22 2c 35 33 37 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 37 22 2c 35 33 38 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 36 38 22 2c 35 33 39 3a 22 69 6e 66 6f 72 6d 61 74 69 6f 6e 70 72 6f 74 65 63 74 69 6f 6e 73 74 72 69 6e 67 73 Data Ascii: 533:"informationprotectionstrings63",534:"informationprotectionstrings64",535:"informationprotectionstrings65",536:"informationprotectionstrings66",537:"informationprotectionstrings67",538:"informationprotectionstrings68",539:"informationprotectionstrings
2022-06-30 20:52:04 UTC	895	IN	Data Raw: 30 63 63 35 31 66 30 32 63 31 36 36 38 36 64 32 63 22 2c 34 39 37 3a 22 36 63 39 33 38 64 36 31 65 38 62 31 61 34 37 64 65 66 31 34 22 2c 34 39 38 3a 22 64 30 39 30 31 61 38 65 36 37 31 31 63 31 31 36 64 64 36 39 22 2c 34 39 39 3a 22 36 63 37 36 36 33 37 35 33 37 64 62 32 37 32 38 66 65 62 39 22 2c 35 30 30 3a 22 63 34 65 32 63 61 64 37 34 34 66 65 34 31 63 66 64 30 66 35 22 2c 35 30 31 3a 22 30 35 30 33 37 34 35 65 63 62 63 34 64 30 63 62 30 37 34 33 22 2c 35 30 32 3a 22 61 32 62 33 36 66 31 31 65 36 30 62 61 30 36 34 65 34 66 37 22 2c 35 30 33 3a 22 31 66 32 30 66 63 66 37 66 36 36 33 35 63 66 39 62 35 65 61 22 2c 35 30 34 3a 22 36 66 64 39 33 36 32 63 63 32 34 35 66 36 32 33 33 33 66 38 22 2c 35 30 35 3a 22 32 39 64 65 66 62 33 37 38 64 62 31 63 64 63 Data Ascii: 0cc51f02c16686d2c",497:"6c938d61e8b1a47def14",498:"d0901a8e6711c116dd69",499:"6c76637537db2728feb9",500:"c4e2cad744fe41cfd0f5",501:"0503745ecbc4d0cb0743",502:"a2b36f11e60ba064e4f7",503:"1f20fcf7f6635cf9b5ea",504:"6fd9362cc245f62333f8",505:"29defb378db1cdc
2022-06-30 20:52:04 UTC	911	IN	Data Raw: 72 2d 64 69 61 6c 6f 67 22 2c 31 39 38 3a 22 65 72 72 6f 72 2d 64 69 61 6c 6f 67 2d 72 63 22 2c 31 39 39 3a 22 65 77 2d 72 63 22 2c 32 30 30 3a 22 66 62 2d 74 68 65 6d 65 22 2c 32 30 31 3a 22 66 65 61 74 75 72 65 2d 63 61 6c 6c 6f 75 74 22 2c 32 30 32 3a 22 66 65 61 74 75 72 65 2d 74 6f 6c 74 69 70 2d 63 6f 6e 74 61 69 6e 65 72 22 2c 32 30 33 3a 22 66 65 65 64 22 2c 32 30 34 3a 22 66 65 65 64 62 61 63 6b 22 2c 32 30 35 3a 22 66 69 72 73 74 2d 72 75 6e 22 2c 32 30 36 3a 22 66 6c 2d 63 6e 74 22 2c 32 30 37 3a 22 66 6c 2d 75 6e 73 75 70 70 6f 72 74 65 64 2d 70 61 67 65 22 2c 32 30 38 3a 22 66 6c 63 6f 6e 74 61 69 6e 65 72 73 74 72 69 6e 67 73 30 22 2c 32 30 39 3a 22 66 6c 63 6f 6e 74 61 69 6e 65 72 73 74 72 69 6e 67 73 31 22 2c 32 31 30 3a 22 66 6c 63 6f Data Ascii: r-dialog",198:"error-dialog-rc",199:"ew-rc",200:"fb-theme",201:"feature-callout",202:"feature-tooltip-container",203:"feed",204:"feedback",205:"first-run",206:"fl-cnt",207:"fl-unsupported-page",208:"flcontainerstrings0",209:"flcontainerstrings1",210:"flco
2022-06-30 20:52:04 UTC	927	IN	Data Raw: 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 35 38 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 35 39 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 30 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 31 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 32 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 33 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 34 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 35 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 31 36 36 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 Data Ascii: 1d6cfe0d16ae931b73c",158:"31d6cfe0d16ae931b73c",159:"31d6cfe0d16ae931b73c",160:"31d6cfe0d16ae931b73c",161:"31d6cfe0d16ae931b73c",162:"31d6cfe0d16ae931b73c",163:"31d6cfe0d16ae931b73c",164:"31d6cfe0d16ae931b73c",165:"31d6cfe0d16ae931b73c",166:"31d6cfe0d16ae

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	993	IN	Data Raw: 37 36 36 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 36 37 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 36 38 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 36 39 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 30 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 31 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 32 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 33 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 34 3a 22 33 31 64 36 63 66 65 30 64 31 36 61 65 39 33 31 62 37 33 63 22 2c 37 37 35 3a 22 33 31 64 36 63 66 65 Data Ascii: 766:"31d6cfe0d16ae931b73c",767:"31d6cfe0d16ae931b73c",768:"31d6cfe0d16ae931b73c",769:"31d6cfe0d16ae931b73c",770:"31d6cfe0d16ae931b73c",771:"31d6cfe0d16ae931b73c",772:"31d6cfe0d16ae931b73c",773:"31d6cfe0d16ae931b73c",774:"31d6cfe0d16ae931b73c",775:"31d6cfe
2022-06-30 20:52:04 UTC	1009	IN	Data Raw: 75 6c 6c 3d 3d 6e 2e 70 65 72 73 6f 6e 3f 6e 75 6c 6c 3a 6e 2e 70 65 72 73 6f 6e 2e 66 75 6c 6c 4e 61 6d 65 2c 22 22 29 29 2c 65 28 74 2c 32 2c 30 2c 6e 75 6c 6c 3d 3d 6e 2e 70 65 72 73 6f 6e 3f 6e 75 6c 6c 3a 6e 2e 70 65 72 73 6f 6e 2e 66 75 6c 6c 4e 61 6d 65 2e 73 6c 69 63 65 28 30 2c 31 29 29 7d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 62 28 65 29 7b 72 65 74 75 72 6e 20 69 2e 62 63 28 30 2c 5b 28 65 28 29 28 29 2c 69 2e 7a 62 28 30 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 34 2c 22 64 69 76 22 2c 5b 5b 22 61 72 69 61 2d 68 69 64 64 65 6e 22 2c 22 74 72 75 65 22 5d 2c 5b 22 63 6c 61 73 73 22 2c 22 70 65 72 73 6f 6e 2d 70 69 63 74 75 72 65 5f 5f 69 6d 61 67 65 20 70 65 72 73 6f 6e 2d 70 69 63 74 75 72 65 5f 5f 69 6d 61 67 65 2d 2d 69 63 6f 6e 22 5d 2c 5b 22 73 Data Ascii: ull==n.person?null:n.person.fullName,"")),e(t,2,0,null==n.person?null:n.person.fullName.slice(0,1))}}}function b(e){return i.bc(0,[(e()(),i.zb(0,0,null,null,4,"div",[["aria-hidden","true"],["class","person-picture__image person-picture__image--icon"],["s
2022-06-30 20:52:04 UTC	1025	IN	Data Raw: 65 76 65 6e 74 73 2e 77 69 74 68 53 63 6f 70 65 28 30 29 2e 70 69 70 65 28 4f 62 6a 65 63 74 28 66 2e 61 29 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 22 6d 72 75 49 74 65 6d 53 74 61 74 65 43 68 61 6e 67 65 22 3d 3d 3d 65 2e 6e 61 6d 65 7d 29 29 29 2e 73 75 62 73 63 72 69 62 65 28 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 2e 61 72 67 73 5b 31 5d 2e 64 6f 63 49 64 3d 3d 3d 65 2e 69 74 65 6d 2e 64 6f 63 49 64 26 26 28 30 21 3d 3d 74 2e 61 72 67 73 5b 30 5d 26 26 31 21 3d 3d 74 2e 61 72 67 73 5b 30 5d 7c 7c 28 65 2e 6d 72 75 49 74 65 6d 53 74 61 74 65 3d 74 2e 61 72 67 73 5b 30 5d 29 29 7d 29 29 2c 74 68 69 73 2e 6d 79 41 6e 61 6c 79 74 69 63 73 53 74 61 74 65 3d 32 2c 74 68 69 73 2e 75 69 43 61 72 64 54 79 70 65 3d 74 68 69 73 2e 69 73 4d Data Ascii: events.withScope(0).pipe(Object(f.a)((function(e){return"mruItemStateChange"===e.name}))).subscribe((function(t){t.args[1].docId===e.item.docId&&(0!==t.args[0]&&1!==t.args[0]||(e.mruItemState=t.args[0]))})),this.myAnalyticsState=2,this.uiCardType=this.isM
2022-06-30 20:52:04 UTC	1041	IN	Data Raw: 65 28 32 29 5d 29 2e 74 68 65 6e 28 6e 2e 62 69 6e 64 28 6e 75 6c 6c 2c 22 44 5a 51 39 22 29 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 6c 61 75 6e 63 68 55 72 6c 28 65 7c 7c 61 2e 75 72 6c 2c 7b 61 63 74 69 6f 6e 3a 74 2e 74 6f 53 74 72 69 6e 67 28 29 7d 29 7d 29 3a 61 2e 75 72 6c 4c 61 75 6e 63 68 65 72 53 65 72 76 69 63 65 2e 6f 70 65 6e 55 72 6c 28 65 7c 7c 61 2e 75 72 6c 2c 74 29 2c 61 2e 69 6e 73 74 72 75 6d 65 6e 74 41 63 74 69 6f 6e 28 69 2c 72 29 7d 3b 6f 3f 28 74 68 69 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 53 65 72 76 69 63 65 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 63 6f 6e 74 65 6e 74 4c 61 75 6e 63 68 65 72 45 6e 61 62 6c 65 64 3f 50 72 6f 6d 69 73 65 2e 61 6c 6c 28 5b 6e 2e 65 28 30 29 2c 6e 2e 65 28 31 29 2c Data Ascii: e(2)]).then(n.bind(null,"DZQ9")).then((function(n){n.launchUrl(e||a.url,{action:t.toString()})})):a.urlLauncherService.openUrl(e||a.url,t),a.instrumentAction(i,r)};o?(this.capabilitiesService.capabilities.contentLauncherEnabled?Promise.all([n.e(0),n.e(1),
2022-06-30 20:52:04 UTC	1057	IN	Data Raw: 70 6c 6f 61 64 41 63 74 69 6f 6e 49 74 65 6d 28 29 29 2c 74 68 69 73 2e 73 68 61 72 65 43 6f 6e 74 72 6f 6c 45 6e 61 62 6c 65 64 26 26 28 74 68 69 73 2e 73 68 6f 77 44 65 73 6b 74 6f 70 53 68 61 72 65 43 6f 6e 74 72 6f 6c 3d 21 31 2c 74 68 69 73 2e 67 65 74 53 68 61 72 65 43 6f 6e 74 72 6f 6c 45 6c 65 6d 65 6e 74 73 28 72 29 29 3b 76 61 72 20 75 2c 64 3d 74 68 69 73 2e 69 74 65 6d 2e 66 69 6c 65 54 79 70 65 21 3d 3d 79 2e 62 2e 50 6f 77 65 72 42 49 26 26 74 68 69 73 2e 69 74 65 6d 2e 66 69 6c 65 54 79 70 65 21 3d 3d 79 2e 62 2e 53 77 61 79 26 26 74 68 69 73 2e 69 74 65 6d 2e 66 69 6c 65 54 79 70 65 21 3d 3d 79 2e 62 2e 4f 6e 65 4e 6f 74 65 26 26 74 68 69 73 2e 69 74 65 6d 2e 66 69 6c 65 54 79 70 65 21 3d 3d 79 2e 62 2e 46 6f 72 6d 73 26 26 74 68 69 73 2e Data Ascii: ploadActionItem()),this.shareControlEnabled&&(this.showDesktopShareControl=!1,this.getShareControlElements(r));var u,d=this.item.fileType!==y.b.PowerBI&&this.item.fileType!==y.b.Sway&&this.item.fileType!==y.b.OneNote&&this.item.fileType!==y.b.Forms&&this.
2022-06-30 20:52:04 UTC	1073	IN	Data Raw: 2e 67 65 74 41 63 74 69 76 69 74 79 43 6f 6c 6c 61 62 28 29 2c 6e 2e 70 61 72 61 6d 73 2e 41 63 74 69 76 69 74 79 44 69 73 70 6c 61 79 65 64 3d 77 2e 61 5b 74 68 69 73 2e 61 63 74 69 76 69 74 79 44 65 73 63 72 69 70 74 69 6f 6e 53 65 72 76 69 63 65 2e 64 69 73 70 6c 61 79 65 64 41 63 74 69 76 69 74 79 54 79 70 65 28 6f 2c 74 68 69 73 2e 69 74 65 6d 2e 6c 61 73 74 56 69 65 77 65 64 54 69 6d 65 2c 21 31 29 5d 7d 72 65 74 75 72 6e 20 6e 2e 70 61 72 61 6d 73 2e 43 6c 69 63 6b 44 65 73 74 69 6e 61 74 69 6f 6e 3d 22 45 78 74 65 72 6e 61 6c 50 61 67 65 22 2c 6e 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 41 74 74 72 69 62 75 74 69 6f 6e 43 6c 69 63 6b 44 61 74 61 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 2e 69 74 65 6d 2e 67 65 74 Data Ascii: .getActivityCollab(),n.params.ActivityDisplayed=w.a[this.activityDescriptionService.displayedActivityType(o,this.item.lastViewedTime,!1)]}return n.params.ClickDestination="ExternalPage",n},e.prototype.getAttributionClickData=function(){var e=this.item.get
2022-06-30 20:52:04 UTC	1089	IN	Data Raw: 65 3d 66 75 6e 63 74 69 6f 6e Data Ascii: e=function
2022-06-30 20:52:04 UTC	1089	IN	Data Raw: 28 65 29 7b 72 65 74 75 72 6e 20 65 2e 6d 61 70 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 2e 75 73 65 72 5f 72 65 6c 61 74 69 6f 6e 73 68 69 70 2c 6e 3d 65 2e 61 63 74 69 76 69 74 69 65 73 3f 65 2e 61 63 74 69 76 69 74 69 65 73 2e 6d 61 70 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 4a 53 4f 4e 2e 70 61 72 73 65 28 65 5b 31 5d 7d 63 61 74 63 68 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 45 72 72 6f 72 20 70 61 72 73 69 6e 67 20 61 63 74 69 76 69 74 79 3a 20 22 2b 65 2e 61 29 7d 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 73 73 69 67 6e 29 28 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 73 73 69 67 6e 29 28 7b 7d 2c 65 29 2c 7b 74 3a 6e 65 77 20 44 61 74 65 28 65 2e 74 29 2c 64 61 3a 4f 62 Data Ascii: (e){return e.map((function(e){var t=e.user_relationship,n=e.activities?e.activities.map((function(e){var t;try{t=JSON.parse(e.a)}catch(t){console.log("Error parsing activity: "+e.a)}return Object(i.__assign)(Object(i.__assign)({},e),{t:new Date(e.t),da:Ob
2022-06-30 20:52:04 UTC	1105	IN	Data Raw: 61 70 61 62 69 6c 69 74 69 65 73 2e 63 6c 69 65 6e 74 50 77 61 73 45 6e 61 62 6c 65 64 26 26 65 7d 29 29 29 2c 74 68 69 73 2e 6f 70 65 6e 57 69 74 68 55 49 48 6f 73 74 2e 73 75 62 73 63 72 69 62 65 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 6c 2e 73 68 6f 75 6c 64 4f 70 65 6e 57 69 74 68 55 49 48 6f 73 74 3d 65 7d 29 29 2c 76 6f 69 64 20 30 3d 3d 3d 74 68 69 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 74 65 6d 70 6c 61 74 65 73 45 6e 61 62 6c 65 64 29 7b 76 61 72 20 75 3d 73 2e 6e 61 74 69 76 65 57 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 6f 73 74 6e 61 6d 65 3b 74 68 69 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 74 65 6d 70 6c 61 74 65 73 45 6e 61 62 6c 65 64 3d 75 26 26 75 2e 6c 61 73 74 49 6e 64 65 78 4f 66 28 22 2e 63 6f Data Ascii: apabilities.clientPwasEnabled&&e})),this.openWithUIHost.subscribe((function(e){return l.shouldOpenWithUIHost=e})),void 0===this.capabilities.templatesEnabled){var u=s.nativeWindow.location.hostname;this.capabilities.templatesEnabled=u&&u.lastIndexOf(".co

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1149	IN	Data Raw: 69 6f 6e 28 65 2c 74 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 6e 2e 64 28 74 2c 22 61 22 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 75 7d 29 29 3b 76 61 72 20 69 3d 6e 28 22 51 6a 58 55 22 29 2c 72 3d 6e 28 22 41 2f 75 6d 22 29 2c 6f 3d 6e 28 22 42 61 41 67 22 29 2c 61 3d 6e 28 22 34 61 63 68 22 29 2c 73 3d 6e 28 22 4a 54 31 71 22 29 2c 63 3d 6e 28 22 66 4b 52 37 22 29 2c 6c 3d 28 6e 28 22 45 59 63 62 22 29 2c 6e 28 22 37 47 77 6b 22 29 2c 6e 28 22 54 44 7a 72 22 29 2c 6e 28 22 35 35 41 39 22 29 2c 6e 28 22 63 67 6e 64 22 29 2c 6e 28 22 2f 49 30 32 22 29 2c 6e 28 22 50 42 4a 48 22 29 2c 6e 28 22 49 42 52 75 22 29 29 2c 75 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 65 2c 74 2c 6e 2c 69 2c 72 2c 6f 2c 61 Data Ascii: ion(e,t,n){"use strict";n.d(t,"a",(function(){return u}));var i=n("QjXU"),r=n("A/um"),o=n("BaAg"),a=n("4ach"),s=n("JT1q"),c=n("fKR7"),l=(n("EYcb"),n("7Gwk"),n("TDzr"),n("55A9"),n("cgnd"),n("/l02"),n("PBJH"),n("IBRu")),u=function(){function e(e,t,n,i,r,o,a
2022-06-30 20:52:04 UTC	1165	IN	Data Raw: 63 74 69 76 69 74 79 5f 69 6e 66 6f 3f 65 2e 61 63 74 69 76 69 74 79 5f 69 6e 66 6f 2e 62 61 64 67 65 3a 76 6f 69 64 20 30 2c 73 3d 61 26 26 61 2e 74 69 6d 65 73 74 61 6d 70 3f 6e 65 77 20 44 61 74 65 28 61 2e 74 69 6d 65 73 74 61 6d 70 29 3a 6e 75 6c 6c 2c 63 3d 22 50 6c 61 79 4c 69 73 74 22 3d 3d 3d 65 2e 61 70 70 2c 6c 3d 22 45 6d 61 69 6c 41 74 74 61 63 68 6d 65 6e 74 22 3d 3d 3d 65 2e 73 65 72 76 69 63 65 5f 69 6e 66 6f 2e 73 65 72 76 69 63 65 5f 69 64 7c 7c 22 46 50 5f 45 58 43 48 41 4e 47 45 5f 4f 52 47 49 44 22 3d 3d 3d 65 2e 73 65 72 76 69 63 65 5f 69 6e 66 6f 2e 73 65 72 76 69 63 65 5f 69 64 2c 75 3d 6e 75 6c 6c 3b 6c 26 26 28 75 3d 7b 41 74 74 61 63 68 6d 65 6e 74 54 79 70 65 3a 31 2c 43 6f 6e 76 65 72 73 61 74 69 6f 6e 49 64 3a 22 22 2c 53 75 Data Ascii: ctivity_info?e.activity_info.badge:void 0,s=a&&a.timestamp?new Date(a.timestamp):null,c="PlayList"===e.app,l="EmailAttachment"===e.service_info.service_id||"FP_EXCHANGE_ORGID"===e.service_info.service_id,u=null;l&&(u={AttachmentType:1,ConversationId:"",Su
2022-06-30 20:52:04 UTC	1181	IN	Data Raw: 61 64 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 63 6f 6e 66 69 67 2e 65 64 69 74 61 62 6c 65 46 69 6c 65 54 79 70 65 73 2e 68 61 73 28 6f 29 29 7b 76 61 72 20 61 3d 22 61 63 74 69 6f 6e 3d 65 64 69 74 22 3b 2d 31 3d 3d 3d 28 72 3d 72 2e 72 65 70 6c 61 63 65 28 6e 65 77 20 52 65 67 45 78 70 28 22 28 5b 3f 26 5d 29 61 63 74 69 6f 6e 5b 5e 26 5d 2a 22 29 2c 22 24 31 61 63 74 69 6f 6e 3d 65 64 69 74 22 29 29 2e 6c 61 73 74 49 6e 64 65 78 4f 66 28 61 29 26 26 28 72 3d 67 2e 61 2e 61 70 70 65 6e 64 51 75 65 72 79 28 72 2c 61 29 29 7d 72 65 74 75 72 6e 20 69 2e 77 65 62 55 72 6c 3d 72 2c 69 7d 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 75 70 6c 6f 61 64 53 6d 61 6c 6c 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 6f 6e 65 44 72 Data Ascii: adConfigService.config.editableFileTypes.has(o)){var a="action=edit";-1===(r=r.replace(new RegExp("([?&])action[^&]*"),"$1action=edit")).lastIndexOf(a)&&(r=g.a.appendQuery(r,a))}return i.webUrl=r,i})},e.prototype.uploadSmall=function(e){return this.oneDr
2022-06-30 20:52:04 UTC	1197	IN	Data Raw: 74 43 6f 6e 74 Data Ascii: tCont
2022-06-30 20:52:04 UTC	1197	IN	Data Raw: 65 78 74 2c 74 68 69 73 2e 66 6c 75 69 64 49 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 53 65 72 76 69 63 65 2c 74 68 69 73 2e 69 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 53 65 72 76 69 63 65 2c 74 68 69 73 2e 6f 66 66 69 63 65 48 6f 6d 65 41 70 69 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2c 74 68 69 73 2e 6f 66 66 69 63 65 52 6f 75 74 65 53 65 72 76 69 63 65 2c 74 68 69 73 2e 63 6c 69 65 6e 74 53 74 61 72 74 75 70 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2c 74 68 69 73 2e 70 65 72 66 6f 72 6d 61 6e 63 65 53 65 72 76 69 63 65 2c 74 68 69 73 2e 61 72 69 61 45 76 65 6e 74 46 61 63 74 6f 72 79 53 65 72 76 69 63 65 2c 74 68 69 73 2e 73 65 72 76 69 63 65 57 6f 72 6b 65 72 53 74 61 74 65 53 65 72 76 69 63 65 2c 74 68 69 73 2e 73 63 68 65 64 75 6c 65 72 2c 74 68 69 Data Ascii: ext,this.fluidInstrumentationService,this.instrumentationService,this.officeHomeApiConfigService,this.officeRouteService,this.clientStartupConfigService,this.performanceService,this.ariaEventFactoryService,this.serviceWorkerStateService,this.scheduler,thi
2022-06-30 20:52:04 UTC	1213	IN	Data Raw: 69 29 2c 22 65 72 72 6f 72 22 3d 3d 3d 74 26 26 28 69 3d 21 31 21 3d 3d 72 2e 6f 6e 54 68 75 6d 62 6e 61 69 6c 45 72 72 6f 72 28 29 26 26 69 29 2c 69 7d 29 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 29 2c 69 2e 79 62 28 31 2c 32 37 38 35 32 38 2c 6e 75 6c 6c 2c 30 2c 79 2e 69 2c 5b 69 2e 73 2c 69 2e 74 2c 69 2e 6c 2c 69 2e 44 5d 2c 7b 6b 6c 61 73 73 3a 5b 30 2c 22 6b 6c 61 73 73 22 5d 2c 6e 67 43 6c 61 73 73 3a 5b 31 2c 22 6e 67 43 6c 61 73 73 22 5d 7d 2c 6e 75 6c 6c 29 2c 69 2e 52 62 28 32 2c 7b 22 64 6f 63 75 6d 65 6e 74 2d 63 61 72 64 5f 5f 74 68 75 6d 62 6e 61 69 6c 2d 6f 66 66 69 63 65 6f 66 65 64 2d 6e 65 77 73 22 3a 30 7d 29 5d 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 65 28 74 2c 32 2c 30 2c 74 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 69 73 Data Ascii: i),"error"===t&&(i=!1!==r.onThumbnailError()&&i),i}),null,null)),i.yb(1,278528,null,0,y.i,[i.s,i.t,i.l,i.D],{klass:[0,"klass"],ngClass:[1,"ngClass"]},null),i.Rb(2,{"document-card__thumbnail-officefeed-news":0})],(function(e,t){var n=e(t,2,0,t.component.is
2022-06-30 20:52:04 UTC	1229	IN	Data Raw: 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 31 36 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 6e 75 6c 6c 2c 49 74 29 29 2c 69 2e 79 62 28 32 2c 31 36 33 38 34 2c 6e 75 6c 6c 2c 30 2c 79 2e 6b 2c 5b 69 2e 4f 2c 69 2e 4c 5d 2c 7b 6e 67 49 66 3a 5b 30 2c 22 6e 67 49 66 22 5d 7d 2c 6e 75 6c 6c 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 31 36 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 6e 75 6c 6c 2c 54 74 29 29 2c 69 2e 79 62 28 34 2c 31 36 33 38 34 2c 6e 75 6c 6c 2c 30 2c 79 2e 6b 2c 5b 69 2e 4f 2c 69 2e 4c 5d 2c 7b 6e 67 49 66 3a 5b 30 2c 22 6e 67 49 66 22 5d 7d 2c 6e 75 6c 6c 29 5d 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 74 2e 63 6f 6d 70 6f 6e 65 6e 74 3b 65 28 Data Ascii: null,null,null)),(e()(),i.ib(16777216,null,null,1,null,It)),i.yb(2,16384,null,0,y.k,[i.O,i.L],{ngIf:[0,"ngIf"]},null),(e()(),i.ib(16777216,null,null,1,null,Tt)),i.yb(4,16384,null,0,y.k,[i.O,i.L],{ngIf:[0,"ngIf"]},null)],(function(e,t){var n=t.component;e(
2022-06-30 20:52:04 UTC	1245	IN	Data Raw: 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 31 36 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 6e 75 6c 6c 2c 48 74 29 29 2c 69 2e 79 62 28 32 2c 31 36 33 38 34 2c 6e 75 6c 6c 2c 30 2c 79 2e 6b 2c 5b 69 2e 4f 2c 69 2e 4c 5d 2c 7b 6e 67 49 66 3a 5b 30 2c 22 6e 67 49 66 22 5d 7d 2c 6e 75 6c 6c 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 31 36 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 6e 75 6c 6c 2c 71 74 29 29 2c 69 2e 79 62 28 34 2c 31 36 33 38 34 2c 6e 75 6c 6c 2c 30 2c 79 2e 6b 2c 5b 69 2e 4f 2c 69 2e 4c 5d 2c 7b 6e 67 49 66 3a 5b 30 2c 22 6e 67 49 66 22 5d 7d 2c 6e 75 6c 6c 29 2c 28 65 28 29 28 29 2c 69 2e 7a 62 28 35 2c 30 2c 6e 75 6c 6c 2c 6e Data Ascii: ull,null,null,null,null,null)),(e()(),i.ib(16777216,null,null,1,null,Ht)),i.yb(2,16384,null,0,y.k,[i.O,i.L],{ngIf:[0,"ngIf"]},null),(e()(),i.ib(16777216,null,null,1,null,qt)),i.yb(4,16384,null,0,y.k,[i.O,i.L],{ngIf:[0,"ngIf"]},null),(e()(),i.zb(5,0,null,n
2022-06-30 20:52:04 UTC	1261	IN	Data Raw: 6d 73 2d 66 63 6c 2d 74 70 22 2c 22 47 6c 69 6d 6d 65 72 22 2c 22 31 32 22 2c 74 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 69 73 4e 65 77 54 69 74 6c 65 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 65 28 74 2c 30 2c 30 2c 74 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 69 73 4e 65 77 54 69 74 6c 65 29 7d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 6d 6e 28 65 29 7b 72 65 74 75 72 6e 20 69 2e 62 63 28 30 2c 5b 28 65 28 29 28 29 2c 69 2e 7a 62 28 30 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 22 6f 68 70 2d 69 63 6f 6e 2d 66 6f 6e 74 22 2c 5b 5b 22 63 73 73 43 6c 61 73 73 22 2c 22 64 6f 63 75 6d 65 6e 74 2d 74 69 6c 65 5f 5f 73 68 61 72 69 6e 67 20 64 6f 63 75 6d 65 6e 74 2d 74 69 6c 65 5f 64 65 73 63 72 69 70 74 69 6f 6e 5f 69 63 6f 6e 20 6d 73 2d 66 63 6c 2d 6e 70 Data Ascii: ms-fcl-tp","Glimmer","12",t.component.isNewTitle)}),(function(e,t){e(t,0,0,t.component.isNewTitle)}))}function mn(e){return i.bc(0,[(e()(),i.zb(0,0,null,null,1,"ohp-icon-font",[["cssClass","document-tile__sharing document-tile__description__icon ms-fcl-np
2022-06-30 20:52:04 UTC	1277	IN	Data Raw: 6d 72 75 50 69 Data Ascii: mruPi

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1277	IN	Data Raw: 6e 45 6e 61 62 6c 65 64 29 2c 65 28 74 2c 31 32 2c 30 2c 6e 2e 63 6f 6e 74 65 78 74 4d 65 6e 75 2c 6e 2e 69 6e 64 65 78 2c 6e 2e 66 6c 75 65 6e 74 52 65 66 72 65 73 68 3f 22 22 3a 22 63 6f 6d 6d 61 6e 64 69 6e 67 2d 69 74 65 6d 5f 5f 69 63 6f 6e 20 6d 73 2d 66 63 6c 2d 6e 64 22 2c 6e 2e 64 61 74 61 53 65 63 75 72 69 74 79 54 68 72 65 73 68 6f 6c 64 2c 6e 2e 69 74 65 6d 2e 66 69 6c 65 4e 61 6d 65 2c 6e 2e 61 63 74 69 6f 6e 43 6f 6e 74 65 78 74 4d 65 6e 75 45 6e 61 62 6c 65 64 2c 6e 2e 61 63 74 69 6f 6e 43 6f 6e 74 65 78 74 4d 65 6e 75 29 7d 29 2c 6e 75 6c 6c 29 7d 66 75 6e 63 74 69 6f 6e 20 78 28 65 29 7b 72 65 74 75 72 6e 20 69 2e 62 63 28 30 2c 5b 28 65 28 29 28 29 2c 69 2e 7a 62 28 30 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 30 2c 22 64 69 76 22 2c 5b Data Ascii: nEnabled),e(t,12,0,n.contextMenu,n.index,n.fluentRefresh?"":"commanding-item__icon ms-fcl-nd",n.da taSecurityThreshold,n.item.fileName,n.actionContextMenuEnabled,n.actionContextMenu)}),null)}function xn(e){return i.bc(0,[(e()(),i.zb(0,0,null,null,0,"div",[
2022-06-30 20:52:04 UTC	1293	IN	Data Raw: 31 2c 22 6e 67 43 6c 61 73 73 22 5d 7d 2c 6e 75 6c 6c 29 2c 69 2e 52 62 28 32 2c 7b 22 64 6f 63 75 6d 65 6e 74 2d 63 61 72 64 5f 5f 74 68 75 6d 62 6e 61 69 6c 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 73 75 67 67 65 73 74 65 64 2d 61 63 74 69 6f 6e 73 20 64 6f 63 75 6d 65 6e 74 2d 63 61 72 64 5f 5f 74 68 75 6d 62 6e 61 69 6c 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 79 41 6e 61 6c 79 74 69 63 73 22 3a 30 7d 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 31 36 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 6e 75 6c 6c 2c 24 6e 29 29 2c 69 2e 79 62 28 34 2c 31 36 33 38 34 2c 6e 75 6c 6c 2c 30 2c 79 2e 6b 2c 5b 69 2e 4f 2c 69 2e 4c 5d 2c 7b 6e 67 49 66 3a 5b 30 2c 22 6e 67 49 66 22 5d 7d 2c 6e 75 6c 6c 29 2c 28 65 28 29 28 29 2c 69 2e 69 62 28 31 36 37 37 37 32 Data Ascii: 1,"ngClass"]},null),i.Rb(2,{"document-card__thumbnail-container--suggested-actions document-card__ thumbnail-container--myAnalytics":0}),(e()(),i.ib(16777216,null,null,1,null,$n)),i.yb(4,16384,null,0,y.k,[i.O,i.L],{ngIf:[0,"ngIf"]},null),(e()(),i.ib(167772
2022-06-30 20:52:04 UTC	1314	IN	Data Raw: 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 28 6e 75 6c 6c 29 7d 29 29 2e 63 61 74 63 68 28 72 29 7d 29 2c 34 29 7d 29 7d 29 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 29 7b 65 2e 77 69 6e 64 6f 77 53 65 72 76 69 63 65 2e 65 6e 73 75 72 65 5a 6f 6e 65 4a 73 28 29 2c 65 2e 6c 70 63 3d 65 2e 77 69 6e 64 6f 77 53 65 72 76 69 63 65 2e 6e 61 74 69 76 65 57 69 6e 64 6f 77 2e 4c 50 43 3b 76 61 72 20 74 3d 76 2e 61 2e 6e 6f 77 28 29 2d 65 2e 73 74 61 72 74 54 69 6d 65 3b 65 2e 69 6e 73 74 72 75 6d 65 6e 74 49 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 28 22 53 74 61 72 74 22 2c 74 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 65 2e 77 69 6e 64 6f 77 53 65 72 76 69 63 65 2e 65 6e 73 75 72 65 5a 6f 6e 65 4a 73 28 29 3b 76 61 72 20 6e 3d 76 2e 61 2e 6e 6f Data Ascii: ion(){return n(null)})).catch(r)}),4)})))).then((function(){e.windowService.ensureZoneJs(),e.lpc=e.windowSe rvice.nativeWindow.LPC;var t=v.a.now()-e.startTime;e.instrumentInitialization("Start",t)}),(function(t){e.windowService. ensureZoneJs();var n=v.a.no
2022-06-30 20:52:04 UTC	1330	IN	Data Raw: 64 66 5d 5d 3d 5b 22 70 64 66 22 5d 2c 65 2e 66 69 6c 65 54 79 70 65 53 74 72 69 6e 67 54 6f 45 78 74 65 6e 73 69 6f 6e 73 5b 69 5b 69 2e 41 75 64 69 6f 5d 5d 3d 5b 22 6d 70 33 22 5d 2c 65 2e 66 69 6c 65 54 79 70 65 53 74 72 69 6e 67 54 6f 45 78 74 65 6e 73 69 6f 6e 73 5b 69 5b 69 2e 54 65 78 74 5d 5d 3d 5b 22 74 78 74 22 5d 2c 65 2e 66 69 6c 65 54 79 70 65 53 74 72 69 6e 67 54 6f 45 78 74 65 6e 73 69 6f 6e 73 5b 69 5b 69 2e 46 6c 75 69 64 5d 5d 3d 5b 22 6 6 6c 75 69 64 22 2c 22 6c 6f 6f 70 22 5d 2c 65 2e 66 69 6c 65 54 79 70 65 53 74 72 69 6e 67 54 6f 45 78 74 65 6e 73 69 6f 6e 73 5b 69 5b 69 2e 53 74 72 65 61 6d 5d 5d 3d 65 2e 53 74 72 65 61 6d 45 78 74 65 6e 73 69 6f 6e 73 2c 65 2e 66 69 6c 65 54 79 70 65 53 74 72 69 6e 67 54 6f 45 78 74 65 6e 73 69 6f Data Ascii: df]]=["pdf"],e.fileTypeStringToExtensions[i[i.Audio]]=["mp3"],e.fileTypeStringToExtensions[i[i.Text]]=["txt"],e.fileTypeStringToExtensions[i[i.Fluid]]=["fluid","loop"],e.fileTypeStringToExtensions[i[i.Stream]]=e.StreamExtensions ,e.fileTypeStringToExtensio
2022-06-30 20:52:04 UTC	1346	IN	Data Raw: 65 6e 74 28 65 29 2b 22 2f 69 74 65 6d 73 2f 22 2b 65 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 74 29 2b 22 2f 63 72 65 61 74 65 4c 69 6e 6b 22 2c 72 3d 7b 74 79 70 65 3a 22 61 64 64 72 65 73 73 42 61 72 22 7d 2c 6f 3d 74 68 69 73 2e 67 65 74 52 65 71 75 65 73 74 43 6f 6e 66 69 67 28 29 3b 72 65 74 75 72 6e 20 6f 2e 68 65 61 64 65 72 73 2e 73 65 74 28 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 2c 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 22 29 2c 6e 65 77 20 50 72 6f 6d 69 73 65 28 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 6e 2e 70 6f 73 74 28 22 56 72 6f 6f 6d 5f 43 72 65 61 74 65 5f 4c 69 6e 6b 5f 52 65 71 75 65 73 74 22 2c 22 56 72 6f 6f 6d 5f 43 72 65 61 74 65 5f 4c 69 6e 6b 22 2c 69 2c 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 Data Ascii: ent(e)+"/items/"+encodeURIComponent(t)+"/createLink",r={type:"addressBar"},o=this.getRequestConfig ();return o.headers.set("Content-Type","application/json"),new Promise((function(e,t){n.post("Vroom_Create_Lin k_Request","Vroom_Create_Link",i,JSON.stringify
2022-06-30 20:52:04 UTC	1362	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 26 26 28 74 68 69 73 2e 68 6f 73 74 53 63 65 6e 61 72 69 6f 53 74 61 72 74 54 69 6d 65 3d 76 6f 69 64 20 30 2c 74 68 69 73 2e 68 6f 73 74 53 63 65 6e 61 72 69 6f 4e 61 6d 65 3d 76 6f 69 64 20 30 29 2c 74 68 69 73 2e 62 6f 6f 74 49 64 2b 2b 7d 2c 65 2e c9 b5 70 72 6f 76 3d 73 2e 63 63 28 7b 66 61 63 74 6f 72 79 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 65 28 73 2e 64 63 28 72 2e 62 29 2c 73 2e 64 63 28 6f 2e 61 29 2c 73 2e 64 63 28 69 2e 61 29 2c 73 2e 64 63 28 61 2e 61 29 29 7d 2c 74 6f 6b 65 6e 3a 65 2c 70 72 6f 76 69 64 65 64 49 6e 3a 22 72 6f 6f 74 22 7d 29 2c 65 7d 28 29 7d 2c 44 54 4e 46 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 2e 64 Data Ascii: function(e){e&&(this.hostScenarioStartTime=void 0,this.hostScenarioName=void 0),this.bootId++},e.p rov=s.cc({factory:function(){return new e(s.dc(r.b),s.dc(o.a),s.dc(i.a),s.dc(a.a))},token:e,providedIn:"root"}),e}()},DT NF:function(e,t,n){"use strict";n.d
2022-06-30 20:52:04 UTC	1378	IN	Data Raw: 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 69 3d 21 30 3b 72 65 74 75 72 6e 22 6d 6f 75 73 65 6e 74 65 72 22 3d 3d 3d 74 26 26 28 69 3d 21 31 21 3d 3d 65 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 6f 6e 48 6f 76 65 72 28 29 26 26 69 29 2c 6e 7d 29 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 2c 69 2e 79 62 28 34 2c 32 37 38 35 32 38 2c 6e 75 6c 6c 2c 30 2c 75 2e 69 2c 5b 69 2e 73 2c 69 2e 74 2c 69 2e 6c 2c 69 2e 44 5d 2c 7b 6e 67 43 6c 61 73 73 3a 5b 30 2c 22 6e 67 43 6c 61 73 73 22 5d 7d 2c 6e 75 6c 6c 29 2c 69 2e 52 62 28 35 2c 7b 22 61 63 74 69 76 69 74 79 2d 64 65 65 70 2d 6c 69 6e 6b 20 6d 73 2d 66 63 6c 2d 74 70 22 3a 30 2c 22 6c 69 73 74 2d 69 74 65 6d 5f 5f 74 65 78 74 2d 2d 6c 61 72 67 65 20 61 63 74 69 76 69 74 79 2d 64 65 73 63 72 69 70 74 69 6f Data Ascii: unction(e,t,n){var i=!0;return"mouseenter"===t&&(i=!1!==e.component.onHover()&&i),i}),null,null)),i.yb(4,278 528,null,0,u.i,[i.s,i.t,i.l,i.D],{ngClass:[0,"ngClass"]},null),i.Rb(5,{"activity-deep-link ms-fcl-tp":0,"list-item__text--large activity-descriptio
2022-06-30 20:52:04 UTC	1394	IN	Data Raw: 65 6e 67 74 68 3e 30 Data Ascii: ength>0
2022-06-30 20:52:04 UTC	1394	IN	Data Raw: 26 26 74 68 69 73 2e 6c 6f 67 52 65 63 6f 6d 6d 65 6e 64 65 64 49 6d 70 72 65 73 73 69 6f 6e 28 74 68 69 73 2e 63 61 72 64 73 5b 74 68 69 73 2e 63 75 72 72 65 6e 74 43 61 72 6f 75 73 65 6c 50 61 67 65 5d 2e 66 72 6f 6d 43 61 63 68 65 29 2c 74 68 69 73 2e 73 74 61 74 75 73 41 6e 6e 6f 75 6e 63 65 6d 65 6e 74 3d 22 22 2c 74 68 69 73 2e 63 68 61 6e 67 65 44 65 74 65 63 74 6f 72 2e 64 65 74 65 63 74 43 68 61 6e 67 65 73 28 29 2c 74 68 69 73 2e 73 74 61 74 75 73 41 6e 6e 6f 75 6e 63 65 6d 65 6e 74 3d 74 68 69 73 2e 6c 6f 63 53 65 72 76 69 63 65 2e 52 65 6d 6f 76 65 44 6f 63 75 6d 65 6e 74 41 72 69 61 54 69 74 6c 65 7d 2c 74 2e 70 72 6f 74 6f 74 79 70 65 2e 6c 6f 67 4e 61 76 43 6c 69 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 7b 7d 3b 74 2e Data Ascii: &&this.logRecommendedImpression(this.cards[this.currentCarouselPage].fromCache),this.statusAnnounc ement="",this.changeDetector.detectChanges(),this.statusAnnouncement=this.locService.RemoveDocumentAriaTitle}, t.prototype.logNavClick=function(e){var t={};t.

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1410	IN	Data Raw: 69 6c 69 74 69 65 73 53 65 72 76 69 63 65 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 69 73 50 77 61 49 6e 55 77 70 29 74 68 69 73 2e 63 6f 6e 66 69 67 50 72 6f 6d 69 73 65 3d 50 72 6f 6d 69 73 65 2e 72 65 73 6f 6c 76 65 28 74 68 69 73 2e 63 6f 6e 66 69 67 50 61 72 73 65 72 53 65 72 76 69 63 65 2e 70 61 72 73 65 28 22 77 6f 72 6b 6c 6f 61 64 50 75 62 6c 69 63 44 61 74 61 22 29 29 3b 65 6c 73 65 7b 76 61 72 20 74 3d 74 68 69 73 2e 65 76 65 6e 74 53 65 72 76 69 63 65 2e 65 76 65 6e 74 73 2e 77 69 74 68 53 63 6f 70 65 28 30 29 2e 70 69 70 65 28 4f 62 6a 65 63 74 28 69 2e 61 29 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 22 70 72 69 6d 61 72 79 54 6f 6b 65 6e 73 4c 6f 61 64 65 64 22 3d 3d 3d 65 2e 6e 61 6d 65 7d 29 29 2c 4f 62 6a 65 63 74 28 72 Data Ascii: ilitiesService.capabilities.isPwaInUwp)this.configPromise=Promise.resolve(this.configParserService.parse("workloadPublicData"));else{var t=this.eventService.events.withScope(0).pipe(Object(i.a)((function(e){return"primaryTokensLoaded"===e.name})),Object(r
2022-06-30 20:52:04 UTC	1426	IN	Data Raw: 4c 69 6e 6b 7c 7c 74 68 69 73 2e 74 65 61 6d 73 44 65 65 70 4c 69 6e 6b 29 7b 65 26 26 65 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 3b 76 61 72 20 69 3d 74 68 69 73 2e 61 63 74 69 76 69 74 79 44 65 65 70 4c 69 6e 6b 7c 7c 74 68 69 73 2e 74 65 61 6d 73 44 65 65 70 4c 69 6e 6b 3b 21 74 68 69 73 2e 74 65 61 6d 73 44 65 65 70 4c 69 6e 6b 26 26 74 68 69 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 77 61 63 48 6f 73 74 45 6e 61 62 6c 65 64 26 26 74 68 69 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 63 61 70 61 62 69 6c 69 74 69 65 73 53 65 72 76 69 63 65 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 77 61 63 48 6f 73 74 41 70 70 73 2e 68 61 73 28 74 68 69 73 2e 66 69 6c 65 54 79 70 65 29 3f 28 74 68 69 73 2e 6c 6f 67 43 6c 69 63 6b 28 Data Ascii: Link||this.teamsDeepLink){e&&e.preventDefault();var i=this.activityDeepLink||this.teamsDeepLink;!this.teamsDeepLink&&this.capabilitiesService.capabilities.wacHostEnabled&&this.capabilitiesService.capabilities.wacHostApps.has(this.fileType)?(this.logClick(
2022-06-30 20:52:04 UTC	1442	IN	Data Raw: 76 61 62 6c 65 28 29 7d 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 63 6f 6e 66 69 67 75 72 61 62 6c 65 3a 21 30 7d 29 2c 65 2e c9 b5 70 72 6f 76 3d 72 2e 63 63 28 7b 66 61 63 74 6f 72 79 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 65 7d 2c 74 6f 6b 65 6e 3a 65 2c 70 72 6f 76 69 64 65 64 49 6e 3a 22 72 6f 6f 74 22 7d 29 2c 65 7d 28 29 7d 2c 4f 4f 74 49 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 6e 2e 64 28 74 2c 22 61 22 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 73 7d 29 29 3b 76 61 72 20 69 3d 6e 28 22 51 6a 58 55 22 29 2c 72 3d 6e 28 22 6b 65 56 65 22 29 2c 6f 3d 28 6e 28 22 6d 4e 61 56 22 29 2c 6e 28 22 64 4f 67 44 22 29 2c 6e 28 22 52 4a 69 79 22 29 2c 6e 28 22 Data Ascii: vable(){},enumerable:!0,configurable:!0}),e.prov=r.cc({factory:function(){return new e},token:e,providedIn:"root"}),e}()},OOtI:function(e,t,n){"use strict";n.d(t,"a",(function(){return s}));var i=n("QjXU"),r=n("keVe"),o=(n("mNaV"),n("dOgD"),n("RJiy"),n("
2022-06-30 20:52:04 UTC	1458	IN	Data Raw: 75 69 64 53 75 70 70 6f 72 74 45 6e 61 62 6c 65 64 2c 63 61 6e 4f 70 65 6e 42 6c 61 6e 6b 44 6f 63 49 6e 4e 61 74 69 76 65 41 70 70 3a 21 31 2c 63 61 6e 46 61 6c 6c 62 61 63 6b 54 6f 4c 61 6e 64 69 6e 67 50 61 67 65 3a 21 30 2c 63 72 65 61 74 65 44 6f 63 41 73 70 78 45 6e 61 62 6c 65 64 3a 21 31 7d 29 2c 46 2e 73 74 61 72 74 50 61 67 65 41 70 70 73 2e 68 61 73 28 63 2e 62 2e 46 6f 72 6d 73 29 26 26 28 74 68 69 73 2e 63 72 65 61 74 65 4c 69 6e 6b 43 61 6e 64 69 64 61 74 65 73 2e 73 65 74 28 63 2e 62 2e 46 6f 72 6d 73 2c 7b 61 70 70 4e 61 6d 65 3a 6d 2e 46 6f 72 6d 73 4e 61 6d 65 2c 74 69 74 6c 65 3a 6d 2e 43 72 65 61 74 65 4d 65 6e 75 4c 69 6e 6b 46 6f 72 6d 73 54 69 74 6c 65 2c 66 69 6c 65 54 79 70 65 4e 61 6d 65 3a 6d 2e 43 72 65 61 74 65 4d 6f 64 61 6c Data Ascii: uidSupportEnabled,canOpenBlankDocInNativeApp:!1,canFallbackToLandingPage:!0,createDocAspxEnabled:!1}),F.startPageApps.has(c.b.Forms)&&(this.createLinkCandidates.set(c.b.Forms,{appName:m.FormsName,title:m.CreateMenuLinkFormsTitle,fileTypeName:m.CreateModal
2022-06-30 20:52:04 UTC	1474	IN	Data Raw: 72 6d 3a 22 57 65 62 22 7d 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 28 22 4f 70 65 6e 46 61 69 6c 65 64 22 29 7d 29 29 3a 76 6f 69 64 20 30 21 3d 3d 61 2e 6f 70 65 6e 3f 28 75 26 26 75 28 7b 74 79 70 65 3a 69 2c 6c 61 74 65 6e 63 79 3a 53 28 29 2c 70 6c 61 74 66 6f 72 6d 3a 22 57 65 62 22 7d 29 2c 76 2e 63 61 70 61 62 69 6c 69 74 69 65 73 53 65 72 76 69 63 65 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 63 6f 6e 74 65 6e 74 4c 61 75 6e 63 68 65 72 45 6e 61 62 6c 65 64 3f 50 72 6f 6d 69 73 2e 61 6c 6c 28 5b 6e 2e 65 28 30 29 2c 6e 2e 65 28 31 29 2c 6e 2e 65 28 32 29 5d 29 2e 74 68 65 6e 28 6e 2e 62 69 6e 64 28 6e 75 6c 6c 2c 22 44 5a 51 39 22 29 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 6c 61 75 6e 63 68 55 72 6c 28 74 2c Data Ascii: rm:"Web"})}),(function(){o("OpenFailed")})):void 0!==a.open?(u&&u({type:i,latency:S(),platform:"Web"}),v.capabilitiesService.capabilities.contentLauncherEnabled?Promise.all([n.e(0),n.e(1),n.e(2)]).then(n.bind(null,"DZQ9")).then((function(e){e.launchUrl(t,
2022-06-30 20:52:04 UTC	1490	IN	Data Raw: 69 63 22 2c 77 65 65 6b 64 61 79 3a 22 6c 6f 6e 67 22 7d 29 2c 74 68 69 73 2e 64 61 74 65 46 6f 72 6d 61 74 4f 70 74 69 6f 6e 73 4d 61 70 2e 73 65 74 28 33 2c 7b 64 61 79 3a 22 6e 75 6d 65 72 69 63 22 2c 77 65 65 6b 64 61 79 3a 22 73 68 6f 72 74 22 7d 29 2c 74 68 69 73 2e 64 61 74 65 46 6f 72 6d 61 74 4f 70 74 69 6f 6e 73 4d 61 70 2e 73 65 74 28 34 2c 7b 64 61 79 3a 22 6e 75 6d 65 72 69 63 22 2c 77 65 65 6b 64 61 79 3a 22 6c 6f 6e 67 22 7d 29 2c 74 68 69 73 2e 64 61 74 65 46 6f 72 6d 61 74 4f 70 74 69 6f 6e 73 4d 61 70 2e 73 65 74 28 35 2c 7b 6d 6f 6e 74 68 3a 22 73 68 6f 72 74 22 2c 64 61 79 3a 22 6e 75 6d 65 72 69 63 22 7d 29 2c 74 68 69 73 2e 64 61 74 65 46 6f 72 6d 61 74 4f 70 74 69 6f 6e 73 4d 61 70 2e 73 65 74 28 36 2c 7b 77 65 65 6b 64 61 79 3a 22 Data Ascii: ic",weekday:"long"}),this.dateFormatOptionsMap.set(3,{day:"numeric",weekday:"short"}),this.dateFormatOptionsMap.set(4,{day:"numeric",weekday:"long"}),this.dateFormatOptionsMap.set(5,{month:"short",day:"numeric"}),this.dateFormatOptionsMap.set(6,{weekday:"
2022-06-30 20:52:04 UTC	1506	IN	Data Raw: 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 50 72 6f 6d 69 73 65 28 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 69 29 7b 6f 2e 70 75 73 68 28 5b 65 2c 74 2c 6e 2c 69 5d 29 3e 31 7c 7c 73 28 65 2c 74 29 7d 29 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 73 28 65 2c 74 29 7b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 76 61 6c 75 65 20 69 6e 73 74 61 6e 63 65 6f 66 20 76 3f 50 72 6f 6d 69 73 65 2e 72 65 73 6f 6c 76 65 28 65 2e 76 61 6c 75 65 2e 76 29 2e 74 68 65 6e 28 63 2c 6c 29 3a 75 28 6f 5b 30 5d 5b 32 5d 2c 65 29 7d 28 72 5b 65 5d 28 74 29 29 7d 63 61 74 63 68 28 65 29 7b 75 28 6f 5b 30 5d 5b 33 5d 2c 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 63 28 65 29 7b 73 28 22 6e 65 78 74 22 2c 65 29 7d 66 75 6e 63 74 69 6f 6e 20 6c 28 65 29 7b 73 28 22 Data Ascii: tion(t){return new Promise((function(n,i){o.push([e,t,n,i])>1||s(e,t)})})}function s(e,t){try{!function(e){e.value instanceof v?Promise.resolve(e.value.v).then(c,l):u(o[0][2],e)}(r[e](t))}catch(e){u(o[0][3],e)}}function c(e){s("next",e)}function l(e){s("
2022-06-30 20:52:04 UTC	1522	IN	Data Raw: 2e 63 61 6e 53 77 69 70 65 52 65 63 6f 6d 6d 65 6e 64 65 64 29 2c 65 28 74 2c 33 31 2c 30 2c 21 6e 2e 63 61 6e 53 77 69 70 65 52 65 63 6f 6d 6d 65 6e 64 65 64 26 26 21 6e 2e 72 65 63 6f 6d 6d 65 6e 64 65 64 4d 6f 74 69 6f 6e 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 74 2e 63 6f 6d 70 6f 6e 65 6e 74 3b 65 28 74 2c 37 2c 30 2c 21 6e 2e 63 61 72 64 73 7c 7c 21 6e 2e 63 61 72 64 73 2e 6c 65 6e 67 74 68 2c 76 6f 69 64 20 30 2c 6e 2e 64 69 73 61 62 6c 65 41 6e 69 6d 61 74 69 6f 6e 2c 6e 2e 72 65 63 6f 6d 6d 65 6e 64 65 64 54 69 74 6c 65 29 3b 76 61 72 20 69 3d 65 28 74 2c 32 35 2c 30 2c 6e 2e 6d 6f 74 69 6f 6e 53 74 61 74 65 2c 65 28 74 2c 32 34 2c 30 2c 6e 2e 74 72 61 6e 73 6c 61 74 65 58 29 29 3b 65 28 74 2c 32 30 2c 30 2c 69 Data Ascii: .canSwipeRecommended),e(t,31,0,!n.canSwipeRecommended&&!n.recommendedMotion)}),(function(e,t){var n=t.component;e(t,7,0,!n.cards||!n.cards.length,void 0,n.disableAnimation,n.recommendedTitle);var i=e(t,25,0,n.motionState,e(t,24,0,n.translateX));e(t,20,0,i

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1538	IN	Data Raw: 2c 6e 2c 69 2c 72 2c 6f 2c 61 2c 73 2c 63 2c 6c 2c 75 2c 64 2c 70 2c 66 2c 68 2c 6d 2c 62 2c 67 29 7b 76 61 72 20 76 3d 65 2e 63 61 6c 6c 28 74 68 69 73 2c 74 2c 6e 2c 69 2c 72 2c 6f 2c 73 2c 63 2c 6c 2c 75 2c 22 76 32 2f 72 65 63 65 6e 74 22 2c 73 2e 63 6f 6e 66 69 67 2e 73 75 70 70 6f 72 74 65 64 46 69 6c 65 54 79 70 65 73 2c 66 29 7c 7c 74 68 69 73 3b 72 65 74 75 72 6e 20 76 2e 75 73 65 72 43 6f 6e 74 65 78 74 53 65 72 76 69 63 65 3d 61 2c 76 2e 6d 72 75 43 6f 6e 66 69 67 53 65 72 76 69 63 65 3d 73 2c 76 2e 70 65 72 66 6f 72 6d 61 6e 63 65 53 65 72 76 69 63 65 3d 64 2c 76 2e 75 70 64 61 74 65 43 6f 6e 74 65 6e 74 53 65 72 76 69 63 65 3d 70 2c 76 2e 77 69 6e 64 6f 77 53 65 72 76 69 63 65 3d 68 2c 76 2e 63 61 70 61 62 69 6c 69 74 69 65 73 53 65 72 76 69 Data Ascii: ,n,i,r,o,a,s,c,l,u,d,p,f,h,m,b,g){var v=e.call(this,t,n,i,r,o,s,c,l,u,"v2/recent",s.config.supportedFileTypes,f)||this ;return v.userContextService=a,v.mruConfigService=s,v.performanceService=d,v.updateContentService=p,v.windowSe rvice=h,v.capabilitiesServi
2022-06-30 20:52:04 UTC	1554	IN	Data Raw: 65 6e 75 49 74 65 6d 73 3a 31 7d 29 5d 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 65 28 74 2c 31 2c 30 29 7d 29 2c 6e 75 6c 6c 29 7d 29 2c 7b 6d 65 6e 75 4d 6f 64 65 6c 3a 22 6d 65 6e 75 4d 6f 64 65 6c 22 2c 61 6e 69 6d 61 74 65 43 6c 6f 73 65 3a 22 61 6e 69 6d 61 74 65 43 6c 6f 73 65 22 2c 6d 6f 62 69 6c 65 4d 65 6e 75 3a 22 6d 6f 62 69 6c 65 4d 65 6e 75 22 2c 6c 65 66 74 41 6c 69 67 6e 65 64 43 61 72 64 3a 22 6c 65 66 74 41 6c 69 67 6e 65 64 43 61 72 64 22 2c 6d 75 6c 74 69 53 65 6c 65 63 74 3a 22 6d 75 6c 74 69 53 65 6c 65 63 74 22 2c 63 6f 6e 74 65 78 74 41 72 69 61 4c 61 62 65 6c 3a 22 63 6f 6e 74 65 78 74 41 72 69 61 4c 61 62 65 6c 22 2c 61 72 69 61 52 6f 6c 65 3a 22 61 72 69 61 52 6f 6c 65 22 2c 73 65 6c 65 63 74 65 64 49 6e 64 65 78 3a 22 73 Data Ascii: enuItems:1})],(function(e,t){e(t,1,0)}),null)}),{menuModel:"menuModel",animateClose:"animateClose" ,mobileMenu:"mobileMenu",leftAlignedCard:"leftAlignedCard",multiSelect:"multiSelect",contextAriaLabel:"context AriaLabel",ariaRole:"ariaRole",selectedIndex:"s
2022-06-30 20:52:04 UTC	1570	IN	Data Raw: 74 54 6f 6f 6c 74 69 70 2c 61 72 69 61 4c 61 62 65 6c 3a 74 68 69 73 2e 6c 6f 63 53 65 72 76 69 63 65 2e 41 6c 6c 4d 79 46 6f 72 6d 73 52 65 64 69 72 65 63 74 54 6f 6f 6c 74 69 70 2c 72 65 66 65 72 72 61 6c 3a 63 2e 61 2e 46 6f 72 6d 73 2c 7a 65 72 6f 54 69 74 6c 65 3a 74 68 69 73 2e 6c 6f 63 53 65 72 76 69 63 65 2e 41 6c 6c 4d 79 46 6f 72 6d 73 52 65 64 69 72 65 63 74 4c 61 62 65 6c 7d 3b 72 65 74 75 72 6e 20 74 68 69 73 2e 66 6f 72 6d 73 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 63 6f 6e 66 69 67 2e 6e 65 6f 50 6f 72 74 61 6c 50 61 67 65 45 6e 61 62 6c 65 64 3f 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 73 69 67 6e 29 28 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 73 69 67 6e 29 28 7b 7d 2c 74 29 2c 7b 75 72 6c 3a 74 68 69 73 2e 75 72 6c 41 75 74 68 65 6e 74 69 Data Ascii: tTooltip,ariaLabel:this.locService.AllMyFormsRedirectTooltip,referral:c.a.Forms,zeroTitle:this.locService.Al lMyFormsRedirectLabel};return this.formsConfigService.config.neoPortalPageEnabled?Object(i.__assign)(Object(i. __assign)({},t),{url:this.urlAuthenti
2022-06-30 20:52:04 UTC	1586	IN	Data Raw: 66 65 65 64 62 61 63 6b 53 65 72 76 69 63 65 2e 4f 43 56 41 64 6d 69 6e 50 6f 6c 69 63 79 26 26 73 2e 66 65 65 64 62 61 63 6b 53 65 72 76 69 63 65 2e 4f 43 56 41 64 6d 69 6e 50 6f 6c 69 63 79 2e 45 6d 61 69 6c 43 6f 6c 6c 65 63 74 69 6f 6e 2e 53 74 61 74 65 29 2c 4f 66 66 69 63 65 42 72 6f 77 73 65 72 46 65 65 64 62 61 63 6b 2e 66 65 65 64 62 61 63 6b 2e 69 6e 69 74 4f 70 74 69 6f 6e 73 2e 6f 6e 53 75 72 76 65 79 41 63 74 69 76 61 74 65 64 43 61 6c 6c 62 61 63 6b 3d 7b 6f 6e 53 75 72 76 65 79 41 63 74 69 76 61 74 65 64 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 73 2e 61 63 74 69 76 61 74 65 53 75 72 76 65 79 28 65 29 7d 7d 29 2c 4f 66 66 69 63 65 42 72 6f 77 73 65 72 46 65 65 64 62 61 63 6b 2e 66 6c 6f 6f 64 67 61 74 65 2e 69 6e 69 74 Data Ascii: feedbackService.OCVAdminPolicy&&s.feedbackService.OCVAdminPolicy.EmailCollection.State),OfficeBrow serFeedback.floodgate.initOptions.onSurveyActivatedCallback={onSurveyActivated:function(e){return s.activateSu rvey(e)}}),OfficeBrowserFeedback.floodgate.init
2022-06-30 20:52:04 UTC	1602	IN	Data Raw: 29 7b 73 77 69 74 63 68 28 69 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 72 6e 5b 34 2c 74 68 69 73 2e 67 65 74 28 29 5d 3b 63 61 73 65 20 31 3a 66 6f 72 28 6e 20 69 6e 20 69 2e 73 65 6e 74 28 29 2e 6d 65 74 72 69 63 73 29 69 66 28 74 3f 6e 3d 3d 3d 65 3a 6e 2e 69 6e 63 6c 75 64 65 73 28 65 29 29 72 65 74 75 72 6e 5b 32 2c 21 30 5d 3b 72 65 74 75 72 6e 5b 32 2c 21 31 5d 7d 7d 29 29 7d 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 66 75 6c 6c 44 61 79 73 53 69 6e 63 65 46 69 72 73 74 56 69 73 69 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 74 68 69 73 2e 66 69 72 73 74 54 69 6d 65 55 73 65 72 29 72 65 74 75 72 6e 20 30 3b 69 66 28 76 6f 69 64 20 30 3d 3d 3d 74 68 69 73 2e 66 69 72 73 74 56 69 73 69 74 54 69 6d 65 73 74 61 6d 70 7c 7c 74 Data Ascii:){switch(i.label){case 0:return[4,this.get()];case 1:for(n in i.sent().metrics)if(t?n===e:n.includes(e))return[2,!0];r eturn[2,!1]}}}}}}},e.prototype.fullDaysSinceFirstVisit=function(){if(this.firstTimeUser)return 0;if(void 0===this.firstVisitTimes tamp||t
2022-06-30 20:52:04 UTC	1618	IN	Data Raw: 61 3a 7b 7d 7d 29 3b 66 75 6e 63 74 69 6f 6e 20 73 28 65 29 7b 72 65 74 75 72 6e 20 69 2e 62 63 28 30 2c 5b 28 65 28 29 28 29 2c 69 2e 7a 62 28 30 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 31 2c 22 64 69 76 22 2c 5b 5b 22 61 72 69 61 2d 6c 69 76 65 22 2c 22 61 73 73 65 72 74 69 76 65 22 5d 2c 5b 22 63 6c 61 73 73 22 2c 22 74 69 74 6c 65 2d 61 6e 6e 6f 75 6e 63 65 6d 65 6e 74 22 5d 2c 5b 22 72 6f 6c 65 22 2c 22 61 6c 65 72 74 22 5d 2c 5b 22 74 61 62 69 6e 64 65 78 22 2c 22 2d 31 22 5d 5d 2c 5b 5b 31 2c 22 61 72 69 61 2d 6c 61 62 65 6c 22 2c 30 5d 5d 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 29 2c 28 65 28 29 28 29 2c 69 2e 59 62 28 31 2c 6e 75 6c 6c 2c 5b 22 20 22 2c 22 5c 6e 22 5d 29 29 5d 2c 6e 75 6c 6c 2c 28 66 75 6e 63 74 69 6f 6e 28 Data Ascii: a:{}});function s(e){return i.bc(0,[(e()(),i.zb(0,0,null,null,1,"div",[["aria-live","assertive"],["class","title-annou ncement"],["role","alert"],["tabindex","-1"]],[[1,"aria-label",0]],null,null,null,null)),(e()(),i.Yb(1,null,[" ","\n"]))],null,(function(
2022-06-30 20:52:04 UTC	1634	IN	Data Raw: 62 65 64 4d 6f 64 65 29 7b 76 61 72 20 72 3d 69 2e 73 68 69 66 74 28 29 2c 6f 3d 72 2e 73 70 6c 69 74 28 22 2f 22 29 2e 6a 6f 69 6e 28 22 22 29 3b 69 2e 75 6e 73 68 69 66 74 28 22 2f 45 6d 62 65 64 2f 22 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 2c 6f 29 7d 74 68 69 73 2e 72 6f 75 74 65 72 2e 6e 61 76 69 67 61 74 65 28 69 2c 7b 71 75 65 72 79 50 61 72 61 6d 73 48 61 6e 64 6c 69 6e 67 3a 22 70 72 65 73 65 72 76 65 22 2c 72 65 70 6c 61 63 65 55 72 6c 3a 21 30 7d 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 73 75 62 73 63 72 69 62 65 54 6f 52 6f 75 74 65 43 68 61 6e 67 65 53 74 61 72 74 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 72 6f 75 74 65 73 2e 70 69 70 65 28 4f 62 6a 65 63 74 28 63 2e 61 29 28 74 68 69 73 2e 69 73 52 6f Data Ascii: bedMode){var r=i.shift(),o=r.split("/").join("");i.unshift("/Embed/".toLowerCase(),o)}this.router.navigate(i, {queryParamsHandling:"preserve",replaceUrl:!0})},e.prototype.subscribeToRouteChangeStart=function(e){return t his.routes.pipe(Object(c.a)(this.isRo
2022-06-30 20:52:04 UTC	1650	IN	Data Raw: 43 6f 6e 74 65 6e 74 5f 41 63 74 69 6f 6e 73 5f Data Ascii: Content_Actions_
2022-06-30 20:52:04 UTC	1650	IN	Data Raw: 4d 65 6e 75 5f 49 74 65 6d 5f 43 6c 69 63 6b 22 2c 65 2e 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 4d 65 6e 75 49 74 65 6d 5f 43 6c 69 63 6b 4c 61 75 6e 63 68 44 6f 63 75 6d 65 6e 74 3d 22 43 6f 6e 74 65 6e 74 5f 41 63 74 69 6f 6e 73 5f 4d 65 6e 75 5f 49 74 65 6d 5f 43 6c 69 63 6b 5f 4c 61 75 6e 63 68 5f 44 6f 63 75 6d 65 6e 74 22 2c 65 2e 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 49 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 3d 22 43 6f 6e 74 65 6e 74 5f 41 63 74 69 6f 6e 5f 49 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 22 2c 65 2e 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 52 65 67 69 73 74 65 72 65 64 3d 22 43 6f 6e 74 65 6e 74 5f 41 63 74 69 6f 6e 5f 52 65 67 69 73 74 65 72 65 64 22 2c 65 2e 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 53 75 63 63 65 73 73 3d 22 43 6f 6e 74 Data Ascii: Menu_Item_Click",e.ContentActionsMenuItemClickLaunchDocument="Content_Actions_Menu_Item_ Click_Launch_Document",e.ContentActionInitialization="Content_Action_Initialization",e.ContentActionRegistered ="Content_Action_Registered",e.ContentActionSuccess="Cont

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1666	IN	Data Raw: 73 6f 63 6b 65 74 5f 52 65 71 75 65 73 74 22 2c 65 2e 53 68 61 72 65 50 6f 69 6e 74 53 69 74 65 73 52 65 71 75 65 73 74 3d 22 53 68 61 72 65 50 6f 69 6e 74 5f 53 69 74 65 73 5f 52 65 71 75 65 73 74 22 2c 65 2e 53 68 65 6c 6c 42 6f 6f 74 73 74 72 61 70 70 65 72 45 72 72 6f 72 3d 22 53 68 65 6c 6c 5f 42 6f 6f 74 73 74 72 61 70 70 65 72 5f 45 72 72 6f 72 22 2c 65 2e 53 68 6f 77 4d 6f 72 65 54 69 6c 65 73 49 6d 70 72 65 73 73 69 6f 6e 3d 22 53 68 6f 77 4d 6f 72 65 54 69 6c 65 73 5f 49 6d 70 72 65 73 73 69 6f 6e 22 2c 65 2e 53 69 6d 70 6c 65 50 65 72 73 69 73 74 65 6e 63 65 52 65 61 64 45 72 72 6f 72 3d 22 53 69 6d 70 6c 65 5f 50 65 72 73 69 73 74 65 6e 63 65 5f 52 65 61 64 5f 45 72 72 6f 72 22 2c 65 2e 53 69 6d 70 6c 65 50 65 72 73 69 73 74 65 Data Ascii: socket_Request",e.SharePointSitesRequest="SharePoint_Sites_Request",e.ShellBootstrapperError="Shel l_Bootstrapper_Load_Error",e.ShowMoreTilesImpression="ShowMoreTiles_Impression",e.SimplePersistenceReadError=" Simple_Persistence_Read_Error",e.SimplePersiste
2022-06-30 20:52:04 UTC	1682	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 5f 6b 65 79 50 72 6f 6d 69 73 65 7c 7c 28 74 68 69 73 2e 5f 6b 65 79 50 72 6f 6d 69 73 65 3d 74 68 69 73 2e 69 6d 70 6f 72 74 4b 65 79 28 29 29 2c 74 68 69 73 2e 5f 6b 65 79 50 72 6f 6d 69 73 65 7d 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 63 6f 6e 66 69 67 75 72 61 62 6c 65 3a 21 30 7d 29 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 69 6d 70 6f 72 74 4b 65 79 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 77 61 69 74 65 72 29 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 67 65 6e 65 72 61 74 6f 72 29 28 74 68 69 73 2c 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b Data Ascii: function(){return this._keyPromise||(this._keyPromise=this.importKey()),this._keyPromise},enumerable:!0,conf igurable:!0}),e.prototype.importKey=function(){return Object(i.__awaiter)(this,void 0,void 0,(function(){return Object(i .__generator)(this,(functio
2022-06-30 20:52:04 UTC	1698	IN	Data Raw: 65 72 29 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 67 65 6e 65 72 61 74 6f 72 29 28 74 68 69 73 2c 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 73 77 69 74 63 68 28 74 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 72 6e 20 74 68 69 73 2e 63 6c 69 65 6e 74 53 74 61 72 74 75 70 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 63 6f 6e 66 69 67 2e 61 75 74 68 54 79 70 65 21 3d 3d 54 2e 61 2e 4d 53 41 3f 5b 33 2c 32 5d 3a 5b 34 2c 74 68 69 73 2e 63 6f 6e 73 75 6d 65 72 49 6e 73 74 61 6c 6c 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 67 65 74 43 75 72 72 65 6e 74 53 6b 75 28 29 5d 3b 63 61 73 65 20 31 3a 72 65 74 75 72 6e 5b 32 2c 6e 75 6c Data Ascii: er)(this,void 0,void 0,(function(){var e;return Object(i.__generator)(this,(function(t){switch(t.label){case 0:return this.clientStartupConfigService.config.authType!==T.a.MSA?[3,2]:[4,this.consumerInstallConfigService.getCurren tSku()];case 1:return[2,nul
2022-06-30 20:52:04 UTC	1714	IN	Data Raw: 6e 74 65 78 74 2e 6f 66 66 69 63 65 48 6f 6d 65 41 70 69 52 6f 6f 74 2b 22 2f 53 74 72 65 61 6d 73 54 68 75 6d 62 6e 61 69 6c 22 29 3b 76 61 72 20 6e 3d 6e 65 77 20 46 69 6c 65 52 65 61 64 65 72 3b 72 65 74 75 72 6e 20 6e 65 77 20 50 72 6f 6d 69 73 65 28 28 66 75 6e 63 74 69 6f 6e 28 69 2c 72 29 7b 76 61 72 20 6f 3d 74 2e 63 72 65 61 74 65 52 65 71 75 65 73 74 43 6f 6e 66 69 67 28 74 2e 73 74 61 72 74 75 70 43 6f 6e 66 69 67 2e 73 68 61 72 65 64 43 6c 69 65 6e 74 53 74 61 72 74 75 70 43 6f 6e 74 65 78 74 2e 63 6f 72 72 65 6c 61 74 69 6f 6e 49 64 2c 22 53 74 72 65 61 6d 73 54 68 75 6d 62 6e 61 69 6c 22 2c 22 62 6c 6f 62 22 29 3b 74 2e 67 65 74 28 22 4f 66 66 69 63 65 46 65 65 64 5f 53 74 72 65 61 6d 5f 54 68 75 6d 62 6e 61 69 6c 5f 52 65 71 75 65 73 74 22 Data Ascii: ntext.officeHomeApiRoot+"/StreamsThumbnail");var n=new FileReader;return new Promise((function(i,r){var o=t.createRequestConfig(t.startupConfig.sharedClientStartupContext.correlationId,"StreamsThumbnail","blob");t.get("OfficeFeed_Stream_Thumbnail_Request"
2022-06-30 20:52:04 UTC	1730	IN	Data Raw: 28 21 65 7c 7c 30 3d 3d 3d 65 2e 6c 65 6e 67 74 68 29 72 65 74 75 72 6e 20 6f 2e 61 2e 4e 6f 6e 65 3b 6e 26 26 28 65 3d 74 68 69 73 2e 66 69 6c 74 65 72 41 63 74 69 76 69 74 69 65 73 28 65 2c 74 29 29 3b 66 6f 72 28 76 61 72 20 69 3d 30 2c 72 3d 30 2c 61 3d 30 2c 73 3d 30 3b 73 3c 65 2e 6c 65 6e 67 74 68 3b 73 2b 2b 29 7b 76 61 72 20 63 3d 65 5b 73 5d 2e 61 63 74 69 6f 6e 2e 74 79 70 65 3b 63 3d 3d 3d 6f 2e 61 2e 4d 65 6e 74 69 6f 6e 3f 69 2b 2b 3a 63 3d 3d 3d 6f 2e 61 2e 43 6f 6d 6d 65 6e 74 3f 72 2b 2b 3a 63 3d 3d 3d 6f 2e 61 2e 45 64 69 74 26 26 61 2b 2b 7d 72 65 74 75 72 6e 20 69 3e 30 3f 6f 2e 61 2e 4d 65 6e 74 69 6f 6e 3a 72 3e 30 3f 6f 2e 61 2e 43 6f 6d 6d 65 6e 74 3a 61 3e 30 3f 6f 2e 61 2e 45 64 69 74 3a 6f 2e 61 2e 4e 6f 6e 65 7d 2c 65 2e 70 72 Data Ascii: (!e||0===e.length)return o.a.None;n&&(e=this.filterActivities(e,t));for(var i=0,r=0,a=0,s=0;s<e.length;s++){var c=e[s].action.type;c===o.a.Mention?i++:c===o.a.Comment?r++:c===o.a.Edit&&a++}return i>0?o.a.Mention:r>0?o. a.Comment:a>0?o.a.Edit:o.a.None},e.pr
2022-06-30 20:52:04 UTC	1746	IN	Data Raw: 77 65 72 43 61 73 65 28 29 26 26 74 68 69 73 2e 73 75 62 54 79 70 65 43 61 74 65 67 6f 72 79 29 73 77 69 74 63 68 28 74 68 69 73 2e 73 75 62 54 79 70 65 43 61 74 65 67 6f 72 79 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 7b 63 61 73 65 22 70 6f 6c 6c 22 3a 63 61 73 65 22 74 65 61 6d 73 20 70 6f 6c 6c 22 3a 63 61 73 65 22 70 70 74 70 6f 6c 6c 22 3a 63 61 73 65 22 77 6f 72 64 70 6f 6c 6c 22 3a 72 65 74 75 72 6e 22 70 6f 6c 6c 22 3b 63 61 73 65 22 61 73 73 69 67 6e 6d 65 6e 74 73 22 3a 72 65 74 75 72 6e 22 61 73 73 69 67 6e 6d 65 6e 74 73 22 7d 65 6c 73 65 20 69 66 28 22 70 6f 6c 6c 22 3d 3d 3d 74 68 69 73 2e 73 75 62 54 79 70 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 72 65 74 75 72 6e 22 70 6f 6c 6c 22 3b 72 65 74 75 72 6e 22 66 6f 72 6d 22 7d 2c 74 Data Ascii: werCase()&&this.subTypeCategory)switch(this.subTypeCategory.toLowerCase()){case"poll":case"teams p oll":case"pptpoll":case"wordpoll":return"poll";case"assignments":return"assignments"}else if("poll"===this.subType.toLow erCase())return"poll";return"form"},t
2022-06-30 20:52:04 UTC	1762	IN	Data Raw: 5f 53 43 4f 50 45 22 29 2c 43 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 65 2c 74 2c 6e 2c 69 2c 72 2c 6f 2c 61 2c 73 2c 63 2c 6c 2c 75 2c 64 29 7b 74 68 69 73 2e 73 65 72 76 69 63 65 57 6f 72 6b 65 72 43 6f 6e 66 69 67 53 65 72 76 69 63 65 3d 65 2c 74 68 69 73 2e 73 65 72 76 69 63 65 57 6f 72 6b 65 72 45 6e 61 62 6c 65 64 3d 74 2c 74 68 69 73 2e 68 61 73 53 65 72 76 69 63 65 57 6f 72 6b 65 72 41 70 69 3d 6e 2c 74 68 69 73 2e 77 69 6e 64 6f 77 53 65 72 76 69 63 65 3d 69 2c 74 68 69 73 2e 73 74 61 72 74 75 70 43 6f 6e 66 69 67 53 65 72 76 69 63 65 3d 72 2c 74 68 69 73 2e 67 6c 6f 62 61 6c 45 72 72 6f 72 48 61 6e 64 6c 65 72 3d 6f 2c 74 68 69 73 2e 77 6f 72 6b 6c 6f 61 64 51 75 65 72 79 50 61 72 61 6d 65 74 65 72 56 61 6c 75 65 3d Data Ascii: _SCOPE"),C=function(){function e(e,t,n,i,r,o,a,s,c,l,u,d){this.serviceWorkerConfigService=e,this.serviceWork erEnabled=t,this.hasServiceWorkerApi=n,this.windowService=i,this.startupConfigService=r,this.globalErrorHandle r=o,this.workloadQueryParameterValue=
2022-06-30 20:52:04 UTC	1778	IN	Data Raw: 28 69 2e 5f 5f 67 65 6e 65 72 61 74 6f 72 29 28 74 68 69 73 2c 28 66 75 6e 63 74 69 6f 6e 28 69 29 7b 73 77 69 74 63 68 28 69 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 72 6e 20 69 2e 74 72 79 73 2e 70 75 73 68 28 5b 30 2c 32 2c 2c 33 5d 29 2c 75 65 28 72 3d 6e 65 77 20 55 52 4c 28 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 6f 72 69 67 69 6e 2b 22 2f 61 70 69 2f 73 68 65 6c 6c 61 6e 64 63 6f 6e 66 69 67 64 61 74 61 22 29 2c 22 6d 6f 63 6b 61 75 74 68 22 29 2c 75 65 28 72 2c 22 65 6e 76 54 79 70 65 22 29 2c 75 65 28 72 2c 22 66 6c 69 67 68 74 22 29 2c 72 2e 73 65 61 72 63 68 50 61 72 61 6d 73 2e 73 65 74 28 22 77 6f 72 6b 6c 6f 61 64 22 2c 22 6f 66 66 69 63 65 68 6f 6d 65 22 29 2c 5b 34 2c 66 65 74 63 68 28 72 2e 74 6f 53 74 72 69 6e 67 Data Ascii: (i.__generator)(this,(function(i){switch(i.label){case 0:return i.trys.push([0,2,,3]),ue(r=new URL(window.lo cation.origin+"/api/shellandconfigdata"),"mockauth"),ue(r,"envType"),ue(r,"flight"),r.searchParams.set("workload","offic ehome"),[4,fetch(r.toString

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1794	IN	Data Raw: 61 6c 6c 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 68 69 73 2e 65 76 65 6e 74 53 65 72 76 69 63 65 2e 62 72 6f 61 64 63 61 73 74 45 76 65 6e 74 28 7b 6e 61 6d 65 3a 22 62 65 66 6f 72 65 49 6e 73 74 61 6c 6c 50 72 6f 6d 70 74 22 2c 61 72 67 73 3a 5b 65 5d 7d 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 6f 6e 41 70 70 49 6e 73 74 61 6c 6c 65 64 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 2e 69 73 4d 6f 62 69 6c 65 3f 22 41 70 70 5f 41 64 64 65 64 5f 54 6f 5f 48 6f 6d 65 5f 53 63 72 65 65 6e 5f 4d 6f 62 69 6c 65 22 3a 22 41 70 70 5f 41 64 64 65 64 5f 54 6f 5f 48 6f 6d 65 5f 53 63 72 65 65 6e 5f 44 65 73 6b 74 6f 70 22 3b 74 68 69 73 2e 69 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 53 65 72 76 69 63 65 2e 6c 6f 67 47 65 6e 65 72 69 63 45 Data Ascii: all=function(e){this.eventService.broadcastEvent({name:"beforeInstallPrompt",args:[e]})},e.prototype.onAppInstalled=function(){var e=this.isMobile?"App_Added_To_Home_Screen_Mobile":"App_Added_To_Home_Screen_Desktop";this.instrumentationService.logGenericE
2022-06-30 20:52:04 UTC	1810	IN	Data Raw: 29 2c 65 28 74 2c 32 36 2c 30 2c 6e 2e 70 69 6e 6e 65 64 41 70 70 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 74 2e 63 6f 6d 70 6f 6e 65 6e 74 3b 65 28 74 2c 31 2c 30 2c 72 2e 47 62 28 31 2c 22 22 2c 6e 2e 65 6c 65 6d 65 6e 74 49 64 2c 22 22 29 2c 72 2e 47 62 28 31 2c 22 22 2c 6e 2e 77 6f 72 6b 6c 6f 61 64 2e 55 72 6c 2c 22 22 29 2c 6e 2e 61 72 69 61 4c 61 62 65 6c 2c 72 2e 4f 62 28 74 2c 36 29 2e 74 61 72 67 65 74 29 2c 65 28 74 2c 31 36 2c 30 2c 72 2e 47 62 28 31 2c 22 22 2c 6e 2e 65 6c 65 6d 65 6e 74 49 64 2c 22 5f 74 65 78 74 22 29 29 2c 65 28 74 2c 31 39 2c 30 2c 6e 2e 77 6f 72 6b 6c 6f 61 64 2e 54 65 78 74 29 2c 65 28 74 2c 32 32 2c 30 2c 6e 2e 77 6f 72 6b 6c 6f 61 64 2e 54 65 78 74 29 7d 29 29 7d 72 2e 76 62 28 22 6f Data Ascii:),e(t,26,0,n.pinnedApp)}),(function(e,t){var n=t.component;e(t,1,0,r.Gb(1,"",n.elementId,""),r.Gb(1,"",n.workload.Url,""),n.ariaLabel,r.Ob(t,6).target),e(t,16,0,r.Gb(1,"",n.elementId,"_text")),e(t,19,0,n.workload.Text),e(t,22,0,n.workload.Text))}))}r.vb("o
2022-06-30 20:52:04 UTC	1826	IN	Data Raw: 61 72 67 73 26 26 65 2e 61 72 67 73 2e 6c 65 6e 67 74 68 29 72 65 74 75 72 6e 20 50 72 6f 6d 69 73 65 2e 72 65 73 6f 6c 76 65 28 65 2e 61 72 67 73 5b 30 5d 29 7d 29 29 2c 74 68 69 73 2e 63 6f 6e 73 75 6d 65 72 53 75 62 73 63 72 69 70 74 69 6f 6e 53 74 61 74 75 73 50 72 6f 6d 69 73 65 3d 74 68 69 73 2e 63 6f 6e 73 75 6d 65 72 49 6e 73 74 61 6c 6c 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 67 65 74 43 6f 6e 66 69 67 28 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 65 2e 63 75 72 72 65 6e 74 53 6b 75 49 6e 66 6f 26 26 65 2e 63 75 72 72 65 6e 74 53 6b 75 49 6e 66 6f 2e 73 6b 75 54 79 70 65 7d 29 29 2c 74 68 69 73 2e 73 74 61 72 74 75 70 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 63 6f 6e 66 69 67 2e 61 75 74 68 54 79 Data Ascii: args&&e.args.length)return Promise.resolve(e.args[0])})),this.consumerSubscriptionStatusPromise=this.consumerInstallConfigService.getConfig().then((function(e){return e&&e.currentSkuInfo&&e.currentSkuInfo.skuType})),this.startupConfigService.config.authTy
2022-06-30 20:52:04 UTC	1842	IN	Data Raw: 59 6f 75 72 65 41 6c 6c 53 65 74 54 69 74 6c 65 2c 65 2e 6c 6f 63 53 65 72 76 69 63 65 2e 46 69 72 73 74 52 75 6e 59 6f 75 72 65 41 6c 6c 53 65 74 53 75 62 74 69 74 6c 65 52 65 74 75 72 6e 69 6e 67 55 73 65 72 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 21 31 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 65 2e 63 6f 6e 66 69 67 2e 61 6c 6c 53 65 74 53 76 67 2c 21 30 2c 21 31 2c 22 52 65 74 75 72 6e 69 6e 67 5f 55 73 65 72 5f 43 61 6c 6c 6f 75 74 73 5f 49 6d 70 72 65 73 73 69 6f 6e 22 29 29 29 3b 76 61 72 20 66 3d 7b 7d 3b 66 2e 46 69 72 73 74 52 75 6e 54 6f 74 61 6c 53 74 65 70 73 3d 6c 2e 6c 65 6e 67 74 68 2e 74 6f 53 74 72 69 6e 67 28 29 2c 66 2e 53 74 61 Data Ascii: YoureAllSetTitle,e.locService.FirstRunYoureAllSetSubtitleReturningUser,null,null,null,null,null,!1,null,null,null,null,null,null,e.config.allSetSvg,!0,!1,"Returning_User_Callouts_Impression"))));var f={};f.FirstRunTotalSteps=l.length.toString(),f.Sta
2022-06-30 20:52:04 UTC	1858	IN	Data Raw: 65 77 28 7b 62 65 68 61 76 69 6f 72 3a 22 73 6d 6f 6f 74 68 22 2c 62 6c 6f 63 6b 3a 22 6e 65 61 72 65 73 74 22 2c 69 6e 6c 69 6e 65 3a 22 65 6e 64 22 7d 29 7d 29 29 2c 6f 26 26 6f 5b 30 5d 26 26 28 6f 5b 30 5d 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 66 6f 63 75 73 22 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 5b 30 5d 2e 73 63 72 6f 6c 6c 49 6e 74 6f 56 69 65 77 28 7b 62 65 68 61 76 69 6f 72 3a 22 73 6d 6f 6f 74 68 22 2c 62 6c 6f 63 6b 3a 22 6e 65 61 72 65 73 74 22 2c 69 6e 6c 69 6e 65 3a 22 65 6e 64 22 7d 29 7d 29 29 2c 74 68 69 73 2e 61 6e 6e 6f 75 6e 63 65 6d 65 6e 74 4c 69 73 74 65 6e 65 72 41 64 64 65 64 3d 21 30 29 7d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 6e 67 4f 6e 44 65 73 74 72 6f 79 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 Data Ascii: ew({behavior:"smooth",block:"nearest",inline:"end"})})),o&&o[0]&&(o[0].addEventListener("focus",(function(){o[0].scrollIntoView({behavior:"smooth",block:"nearest",inline:"end"})}))),this.announcementListenerAdded=!0)}},e.prototype.ngOnDestroy=function(){th
2022-06-30 20:52:04 UTC	1874	IN	Data Raw: 49 66 22 5d 7d 2c 6e 75 6c 6c 29 2c 28 65 28 29 28 29 2c 72 2e 69 62 28 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 30 29 29 5d 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 65 28 74 2c 32 2c 30 2c 74 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 73 68 6f 77 43 72 65 61 74 65 4c 6f 63 61 74 69 6f 6e 29 7d 29 2c 6e 75 6c 6c 29 7d 66 75 6e 63 74 69 6f 6e 20 59 6e 28 65 29 7b 72 65 74 75 72 6e 20 72 2e 62 63 28 30 2c 5b 28 65 28 29 28 29 2c 72 2e 7a 62 28 30 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 34 2c 22 64 69 76 22 2c 5b 5d 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 6e 75 6c 6c 29 29 2c 28 65 28 29 28 29 2c 72 2e 7a 62 28 31 2c 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 33 2c 22 61 22 2c 5b 5b 22 63 6c 61 73 73 22 2c 22 67 65 6e 65 72 69 63 2d 62 75 74 74 6f 6e Data Ascii: If"]},null),(e()(),r.ib(0,null,null,0))],(function(e,t){e(t,2,0,t.component.showCreateLocation)}),null)}function Yn(e){return r.bc(0,[(e()(),r.zb(0,0,null,null,4,"div",[],null,null,null,null,null)),(e()(),r.zb(1,0,null,null,3,"a",[["class","generic-button
2022-06-30 20:52:04 UTC	1890	IN	Data Raw: 2e 79 62 28 31 2c 34 37 35 31 33 36 2c 6e 75 6c 6c 2c 30 2c 71 74 2e 61 2c 5b 47 74 2e 61 2c 72 2e 4f 2c 6c 2e 62 2c 66 2e 62 2c 46 65 2e 61 2c 51 74 2e 61 2c 50 74 2e 61 2c 72 2e 7a 2c 51 2e 61 5d 2c 7b 6e 67 4d 6f 64 75 6c 65 50 61 74 68 3a 5b 30 2c 22 6e 67 4d 6f 64 75 6c 65 50 61 74 68 22 5d 2c 69 6e 70 75 74 73 3a 5b 31 2c 22 69 6e 70 75 74 73 22 5d 7d 2c 6e 75 6c 6c 29 2c 72 2e 52 62 28 32 2c 7b 72 65 6e 64 65 72 46 6c 75 69 64 44 6f 63 75 6d 65 6e 74 3a 30 7d 29 2c 28 65 28 29 28 29 2c 72 2e 69 62 28 30 2c 6e 75 6c 6c 2c 6e 75 6c 6c 2c 30 29 29 5d 2c 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 6e 3d 65 28 74 2c 32 2c 30 2c 74 2e 63 6f 6d 70 6f 6e 65 6e 74 2e 6f 6e 46 6c 75 69 64 43 6f 6e 74 65 6e 74 50 61 67 65 29 3b 65 28 74 2c 31 2c Data Ascii: .yb(1,475136,null,0,qt.a,[Gt.a,r.O,l.b,f.b,Fe.a,Qt.a,Pt.a,r.z,Q.a],{ngModulePath:[0,"ngModulePath"],inputs:[1,"inputs"]},null),r.Rb(2,{renderFluidDocument:0}),(e()(),r.ib(0,null,null,0))],(function(e,t){var n=e(t,2,0,t.component.onFluidContentPage);e(t,1,
2022-06-30 20:52:04 UTC	1906	IN	Data Raw: 6e 64 43 6f 6e 66 69 67 50 72 6f 6d 69 73 65 28 Data Ascii: ndConfigPromise(
2022-06-30 20:52:04 UTC	1906	IN	Data Raw: 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 69 6e 69 74 69 61 6c 69 7a 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 69 6e 69 74 69 61 6c 69 7a 65 64 7c 7c 28 74 68 69 73 2e 69 6e 69 74 69 61 6c 69 7a 65 64 3d 21 30 2c 74 68 69 73 2e 73 65 74 53 68 65 6c 6c 41 6e 64 43 6f 6e 66 69 67 50 72 6f 6d 69 73 65 28 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 66 65 74 63 68 53 68 65 6c 6c 41 6e 64 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 77 61 69 74 65 72 29 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 67 65 6e 65 72 61 74 6f 72 29 28 74 68 69 73 2c 28 66 75 6e Data Ascii:)},e.prototype.initialize=function(){this.initialized||(this.initialized=!0,this.setShellAndConfigPromise())},e.prototype.fetchShellAndConfig=function(){return Object(i.__awaiter)(this,void 0,void 0,(function(){var e;return Object(i.__generator)(this,(fun

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1922	IN	Data Raw: 65 48 6f 6d 65 20 74 6f 6b 65 6e 22 29 29 3b 6d 28 74 7c 7c 21 21 64 2e 74 6f 6b 65 6e 2e 54 6f 6b 65 6e 56 61 6c 75 65 2c 21 31 29 7d 65 6c 73 65 20 6f 28 7b 73 75 63 63 65 73 73 3a 21 30 2c 74 6f 6b 65 6e 3a 64 2e 74 6f 6b 65 6e 2e 54 6f 6b 65 6e 56 61 6c 75 65 2c 65 78 70 69 72 79 4d 73 3a 64 2e 74 6f 6b 65 6e 2e 45 78 70 69 72 79 4d 73 2c 66 6f 72 6d 61 74 3a 22 4a 57 54 22 2c 73 6f 75 72 63 65 3a 22 4f 66 66 69 63 65 48 6f 6d 65 22 7d 29 7d 29 29 2e 63 61 74 63 68 28 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 63 2e 65 72 72 6f 72 48 61 6e 64 6c 65 72 2e 68 61 6e 64 6c 65 45 72 72 6f 72 28 74 2c 22 46 5a 57 50 69 22 29 2c 75 28 6e 65 77 20 6a 2e 61 28 22 54 6f 6b 65 6e 20 66 6f 72 20 3c 22 2b 65 2b 22 3e 20 64 6f 65 73 20 6e 6f 74 20 68 61 76 65 20 69 6e Data Ascii: eHome token"));m(t||!!d.token.TokenValue,!1)}else o({success:!0,token:d.token.TokenValue,expiryMs:d.token.ExpiryMs,format:"JWT",source:"OfficeHome"})})).catch((function(t){c.errorHandler.handleError(t,"FZWPi"),u(new j.a("Token for <"+e+"> does not have in
2022-06-30 20:52:04 UTC	1938	IN	Data Raw: 3d 21 31 2c 74 68 69 73 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 53 65 72 76 69 63 65 2e 73 65 74 47 6c 6f 62 61 6c 28 74 68 69 73 2e 75 73 65 72 49 64 53 74 6f 72 61 67 65 4b 65 79 2c 74 29 2c 74 68 69 73 2e 75 70 64 61 74 65 53 74 6f 72 61 67 65 45 6e 74 72 69 65 73 28 5b 5d 29 2c 5b 32 5d 29 3a 28 6e 3d 74 68 69 73 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 53 65 72 76 69 63 65 2e 67 65 74 47 6c 6f 62 61 6c 28 74 68 69 73 2e 75 72 6c 50 61 74 74 65 72 6e 53 74 6f 72 61 67 65 4b 65 79 29 29 3f 28 74 68 69 73 2e 75 70 64 61 74 65 53 74 6f 72 61 67 65 45 6e 74 72 69 65 73 28 6e 2e 6e 69 6c 74 65 72 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 21 21 72 2e 67 65 74 4d 61 72 6b 65 72 4e 61 6d 65 28 65 2e 75 72 6c 29 7d 29 29 29 2c 5b 32 5d 29 3a 5b Data Ascii: =!1,this.localStorageService.setGlobal(this.userIdStorageKey,t),this.updateStorageEntries([]),[2]):(n=this.localStorageService.getGlobal(this.urlPatternStorageKey))?(this.updateStorageEntries(n.filter((function(e){return!!r.getMarkerName(e.url)}))),[2]):[
2022-06-30 20:52:04 UTC	1954	IN	Data Raw: 62 2e 57 6f 72 64 5d 2c 5b 22 53 68 65 6c 6c 45 78 63 65 6c 4f 6e 6c 69 6e 65 22 2c 41 65 2e 62 2e 45 78 63 65 6c 5d 2c 5b 22 53 68 65 6c 6c 50 6f 77 65 72 50 6f 69 6e 74 4f 6e 6c 69 6e 65 22 2c 41 65 2e 62 2e 50 6f 77 65 72 50 6f 69 6e 74 5d 2c 5b 22 53 68 65 6c 6c 4f 6e 65 4e 6f 74 65 4f 6e 6c 69 6e 65 22 2c 41 65 2e 62 2e 4f 6e 65 4e 6f 74 65 5d 2c 5b 22 53 68 65 6c 6c 43 6c 61 73 73 4e 6f 74 65 62 6f 6f 6b 22 2c 41 65 2e 62 2e 4f 6e 65 4e 6f 74 65 43 6c 61 73 73 4e 6f 74 65 42 6f 6f 6b 5d 2c 5b 22 53 68 65 6c 6c 56 69 73 69 6f 4f 6e 6c 69 6e 65 22 2c 41 65 2e 62 2e 56 69 73 69 6f 5d 2c 5b 22 53 68 65 6c 6c 53 77 61 79 22 2c 41 65 2e 62 2e 53 77 61 79 5d 2c 5b 22 53 68 65 6c 6c 4f 66 66 69 63 65 46 6f 72 6d 73 22 2c 41 65 2e 62 2e 46 6f 72 6d 73 5d 2c Data Ascii: b.Word],["ShellExcelOnline",Ae.b.Excel],["ShellPowerPointOnline",Ae.b.PowerPoint],["ShellOneNoteOnline",Ae.b.OneNote],["ShellClassNotebook",Ae.b.OneNoteClassNoteBook],["ShellVisioOnline",Ae.b.Visio],["ShellSway",Ae.b.Sway],["ShellOfficeForms",Ae.b.Forms],
2022-06-30 20:52:04 UTC	1970	IN	Data Raw: 72 63 68 50 61 72 61 6d 73 2e 67 65 74 28 74 29 3b 69 26 26 28 65 2e 61 70 69 51 73 50 61 72 61 6d 73 3f 65 2e 61 70 69 51 73 50 61 72 61 6d 73 5b 74 5d 3d 69 3a 65 2e 61 70 69 51 73 50 61 72 61 6d 73 3d 28 28 6e 3d 7b 7d 29 5b 74 5d 3d 69 2c 6e 29 29 7d 2c 65 7d 28 29 29 2c 78 6f 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 74 68 69 73 2e 73 65 72 76 69 63 65 57 6f 72 6b 65 72 45 6e 61 62 6c 65 64 3d 65 7d 72 65 74 75 72 6e 20 65 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 6e 64 6c 65 52 65 67 69 73 74 72 61 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 28 69 2e 5f 5f 61 77 61 69 74 65 72 29 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 28 66 75 6e 63 74 69 6f 6e 28 29 Data Ascii: rchParams.get(t);i&&(e.apiQsParams?e.apiQsParams[t]=i:e.apiQsParams=((n={})[t]=i,n))},e}()),xo=function(){function e(e){this.serviceWorkerEnabled=e}return e.prototype.handleRegistration=function(e){return Object(i.__awaiter)(this,void 0,void 0,(function()
2022-06-30 20:52:04 UTC	1986	IN	Data Raw: 74 2e c9 b5 70 72 6f 76 3d 72 2e 63 63 28 7b 66 61 63 74 6f 72 79 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 74 28 72 2e 64 63 28 5a 2e 6e 29 2c 72 2e 64 63 28 58 2e 61 29 2c 72 2e 64 63 28 61 61 2e 61 29 2c 72 2e 64 63 28 6b 2e 61 29 29 7d 2c 74 6f 6b 65 6e 3a 74 2c 70 72 6f 76 69 64 65 64 49 6e 3a 22 72 6f 6f 74 22 7d 29 2c 74 7d 28 4b 6f 2e 61 29 2c 63 61 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 74 28 74 2c 6e 29 7b 76 61 72 20 69 3d 65 2e 63 61 6c 6c 28 74 68 69 73 2c 6e 2c 74 29 7c 7c 74 68 69 73 3b 72 65 74 75 72 6e 20 69 2e 6d 79 43 6f 6e 74 65 6e 74 50 61 67 65 45 6e 61 62 6c 65 64 3d 69 2e 63 61 70 61 62 69 6c 69 74 69 65 73 53 65 72 76 69 63 65 2e 63 61 70 61 62 69 6c 69 74 69 65 73 2e 6d 79 43 Data Ascii: t.prov=r.cc({factory:function(){return new t(r.dc(Z.n),r.dc(X.a),r.dc(aa.a),r.dc(k.a))},token:t,providedIn:"root"}),t}(Ko.a),ca=function(e){function t(t,n){var i=e.call(this,n,t)||this;return i.myContentPageEnabled=i.capabilitiesService.capabilities.myC
2022-06-30 20:52:04 UTC	2002	IN	Data Raw: 7b 74 68 69 73 2e 67 65 74 44 6f 63 75 6d 65 6e 74 28 29 2e 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 74 6f 75 63 68 6d 6f 76 65 22 2c 74 68 69 73 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 75 70 64 61 74 65 54 68 65 6d 65 43 6f 6c 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 74 68 69 73 2e 67 65 74 44 6f 63 75 6d 65 6e 74 28 29 3b 69 66 28 74 29 7b 76 61 72 20 6e 3d 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 27 6d 65 74 61 5b 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 5d 27 29 3b 69 66 28 6e 29 6e 2e 63 6f 6e 74 65 6e 74 21 3d 3d 65 26 26 28 6e 2e 63 6f 6e 74 65 6e 74 3d 65 29 3b 65 6c 73 65 7b 76 61 72 20 69 3d 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e Data Ascii: {this.getDocument().removeEventListener("touchmove",this.preventDefault)},e.prototype.updateThemeColor=function(e){var t=this.getDocument();if(t){var n=t.querySelector('meta[name="theme-color"]');if(n)n.content!==e&&(n.content=e);else{var i=t.createElemen
2022-06-30 20:52:04 UTC	2018	IN	Data Raw: 73 68 65 6c 66 2d 72 65 61 63 74 2e 6e 67 66 61 63 74 6f 72 79 22 3a 5b 22 41 49 62 57 22 2c 30 2c 35 2c 36 2c 37 2c 31 34 2c 31 39 2c 33 37 2c 35 30 2c 37 34 2c 36 32 32 2c 35 36 35 5d 2c 22 6c 65 66 74 2d 6e 61 76 2d 72 65 61 63 74 2e 6e 67 66 61 63 74 6f 72 79 22 3a 5b 22 34 36 54 6c 22 2c 34 2c 36 32 33 2c 35 36 36 5d 2c 22 6d 6f 62 69 6c 65 2d 61 70 70 2d 62 61 6e 6e 65 72 2e 6e 67 66 61 63 74 6f 72 79 22 3a 5b 22 31 6a 6d 65 22 2c 33 2c 35 37 32 5d 2c 22 6d 6f 76 65 2d 74 6f 2d 66 6f 6c 64 65 72 2d 63 6f 6e 74 72 6f 6c 2e 6e 67 66 61 63 74 6f 72 79 22 3a 5b 22 50 73 48 38 22 2c 35 37 33 5d 2c 22 6d 72 75 2e 6e 67 66 61 63 74 6f 72 79 22 3a 5b 22 47 48 58 52 22 2c 33 34 2c 35 37 34 5d 2c 22 6e 65 77 2d 63 6f 6e 73 75 6d 65 72 2d 65 78 70 65 72 69 65 Data Ascii: shelf-react.ngfactory":["AIbW",0,5,6,7,14,19,37,50,74,622,565],"left-nav-react.ngfactory":["46Tl",4,623,566],"mobile-app-banner.ngfactory":["1jme",3,572],"move-to-folder-control.ngfactory":["PsH8",573],"mru.ngfactory":["GHXR",34,574],"new-consumer-experie
2022-06-30 20:52:04 UTC	2034	IN	Data Raw: 6c 76 65 28 7b 73 75 63 63 65 73 73 3a 21 31 2c 74 6f 6b 65 6e 3a 22 22 2c 66 6f 72 6d 61 74 3a 74 68 69 73 2e 64 65 66 61 75 6c 74 54 6f 6b 65 6e 46 6f 72 6d 61 74 2c 73 6f 75 72 63 65 3a 74 68 69 73 2e 64 65 66 61 75 6c 74 54 6f 6b 65 6e 53 6f 75 72 63 65 2c 65 72 72 6f 72 3a 6e 65 77 20 45 72 72 6f 72 28 22 69 6e 76 61 6c 69 64 20 74 6f 6b 65 6e 43 6f 6e 73 75 6d 65 72 22 29 7d 29 5d 7d 29 29 7d 29 2c 7d 29 29 7d 29 2c 7d 29 2c 65 7d 28 29 2c 6e 28 22 51 6a 58 55 22 29 2c 72 3d 28 6e 28 22 45 55 56 73 22 29 2c 6e 28 22 34 2f 57 65 22 29 2c 66 75 6e 63 Data Ascii: lve({success:!1,token:"",format:this.defaultTokenFormat,source:this.defaultTokenSource,error:new Error("invalid tokenConsumer")})]}))}))},e}()},kq70:function(e,t,n){"use strict";n.d(t,"a",(function(){return r}));var i=n("QjXU"),r=(n("EUVs"),n("4/We"),func

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	2050	IN	Data Raw: 74 68 3b 6e 2b 2b 29 69 66 28 65 5b 6e 5d 26 26 65 5b 6e 5d 2e 69 64 3d 3d 3d 74 29 72 65 74 75 72 6e 20 65 5b 6e 5d 2e 61 6e 61 6c 79 74 69 63 73 7d 2c 74 2e 65 78 74 72 61 63 74 4c 6f 6f 6b 75 70 49 64 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 67 2e 61 2e 67 65 74 4c 6f 63 61 74 69 6f 6e 28 65 29 2e 70 61 74 68 2e 73 70 6c 69 74 28 22 2f 22 29 2e 66 69 6c 74 65 72 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 7d 29 29 5b 30 5d 7d 2c 74 2e 73 70 6c 69 74 54 6f 42 61 74 63 68 65 73 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 66 6f 72 28 76 61 72 20 6e 3d 5b 5d 2c 69 3d 65 2e 73 6c 69 63 65 28 29 3b 69 26 26 69 2e 6c 65 6e 67 74 68 26 26 74 3b 29 6e 2e 70 75 73 68 28 69 2e 73 70 6c 69 63 65 28 30 2c 74 29 29 3b 72 65 Data Ascii: th;n++)if(e[n]&&e[n].id===t)return e[n].analytics},t.extractLookupId=function(e){return g.a.getLocation(e).path.split("/").filter((function(e){return e}))[0]},t.splitToBatches=function(e,t){for(var n=[],i=e.slice();i&&i.length&&t;)n.push(i.splice(0,t));re
2022-06-30 20:52:04 UTC	2066	IN	Data Raw: 2c 6d 29 3b 76 61 72 20 76 3d 6e 75 6c 6c 3d 3d 28 6c 3d 74 2e 6d 65 65 74 69 6e 67 73 29 7c 7c 76 6f 69 64 20 30 3d 3d 3d 6c 3f 76 6f 69 64 20 30 3a 6c 2e 66 69 6c 74 65 72 28 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 6e 3b 72 65 74 75 72 6e 21 28 6e 75 6c 6c 3d 3d 3d 28 6e 3d 65 2e 6d 65 65 74 69 6e 67 73 29 7c 7c 76 6f 69 64 20 30 3d 3d 3d 6e 3f 76 6f 69 64 20 30 3a 6e 2e 69 6e 63 6c 75 64 65 73 28 74 29 29 7d 29 29 3b 76 26 26 76 2e 66 6f 72 45 61 63 68 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 75 2e 5f 61 6c 6c 46 69 6c 65 73 4d 61 70 2e 64 65 6c 65 74 65 28 65 29 7d 29 29 7d 2c 74 2e 70 72 6f 74 6f 74 79 70 65 3d 6d 2e 6d 72 75 5f 69 64 3d 6d 2e 6d 72 75 5f 69 64 7c 7c 65 2e 6d 72 75 5f 69 64 2c 6d 2e 6d 72 75 5f 74 79 70 65 3d 6d 2e 6d 72 75 5f 74 79 70 65 7c 7c Data Ascii: ,m);var v=null===(l=t.meetings)||void 0===l?void 0:l.filter((function(t){var n;return!(null===(n=e.meetings)||void 0===n?void 0:n.includes(t))}));v&&v.forEach((function(e){u._allFilesMap.delete(e)}))}b&&(m.mru_id=m.mru_id||e.mru_id,m.mru_type=m.mru_type||
2022-06-30 20:52:04 UTC	2082	IN	Data Raw: 62 6e 61 69 6c 41 6e 64 49 64 73 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 2c 69 2c 72 2c 6f 2c 61 29 7b 72 65 74 75 72 6e 20 76 6f 69 64 20 30 3d 3d 3d 6f 26 26 28 6f 3d 21 31 29 2c 76 6f 69 64 20 30 3d 3d 3d 61 26 26 28 61 3d 30 29 2c 74 68 69 73 2e 67 65 74 53 68 61 72 65 64 49 74 65 6d 57 69 74 68 50 61 72 61 6d 73 28 65 2c 74 2c 6e 2c 49 2e 61 2e 67 65 74 49 74 65 6d 50 61 72 61 6d 73 28 5b 22 73 68 61 72 65 70 6f 69 6e 74 49 64 73 22 5d 2c 72 2c 21 30 29 2c 69 2c 6f 2c 61 29 7d 2c 74 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 49 74 65 6d 57 69 74 68 57 61 63 44 61 74 61 41 6e 64 54 68 75 6d 62 6e 61 69 6c 73 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 2c 69 29 7b 76 6f 69 64 20 30 3d 3d 3d 6e 26 26 28 6e 3d 21 31 29 2c 76 6f 69 64 20 30 3d 3d 3d Data Ascii: bnailAndIds=function(e,t,n,i,r,o,a){return void 0===o&&(o=!1),void 0===a&&(a=0),this.getSharedItemWithParams(e,t,n,I.a.getItemParams(["sharepointIds"],r,!0),i,o,a)},t.prototype.getItemWithWacDataAndThumbnails=function(e,t,n,i){void 0===n&&(n=!1),void 0===
2022-06-30 20:52:04 UTC	2098	IN	Data Raw: 64 57 69 74 68 52 6f 75 74 65 3d 21 30 29 7d 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 72 65 67 69 73 74 65 72 45 76 65 6e 74 46 61 63 74 6f 72 69 65 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 74 68 69 73 2e 72 65 67 69 73 74 65 72 65 64 45 76 65 6e 74 46 61 63 74 6f 72 69 65 73 2e 6c 65 6e 67 74 68 3e 30 29 74 68 72 6f 77 20 6e 65 77 20 69 2e 61 28 22 44 69 73 70 61 74 63 68 65 72 49 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 53 65 72 76 69 63 65 2e 72 65 67 69 73 74 65 72 45 76 65 6e 74 46 61 63 74 6f 72 69 65 73 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 74 6f 20 62 65 20 63 61 6c 6c 65 64 20 6d 6f 72 65 20 74 68 61 6e 20 6f 6e 63 65 22 29 3b 69 66 28 21 65 7c 7c 30 3d 3d 3d 65 2e 6c 65 6e 67 74 68 29 74 68 72 6f 77 20 6e 65 77 20 69 Data Ascii: dWithRoute=!0)}))},e.prototype.registerEventFactories=function(e){if(this.registeredEventFactories.length>0)throw new i.a("DispatcherInstrumentationService.registerEventFactories is not allowed to be called more than once");if(!e||0===e.length)throw new i
2022-06-30 20:52:04 UTC	2114	IN	Data Raw: 68 69 73 2e 63 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 48 65 6c 70 65 72 26 26 74 68 69 73 2e 63 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 48 65 6c 70 65 72 2e 64 65 73 74 72 6f 79 28 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 67 65 74 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 47 72 6f 75 70 49 6e 66 6f 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 6d 61 79 62 65 47 65 74 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 48 65 6c 70 65 72 28 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 3d 3d 65 3f 76 6f 69 64 20 30 3a 65 2e 67 65 74 43 6f 6e 74 65 6e 74 41 63 74 69 6f 6e 73 47 72 6f 75 70 49 6e 66 6f 28 29 7d 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 6e 67 4f 6e 44 65 73 74 72 6f 79 3d Data Ascii: his.contentActionsHelper&&this.contentActionsHelper.destroy()},e.prototype.getContentActionsGroupInfo=function(){return this.maybeGetContentActionsHelper().then((function(e){return null==e?void 0:e.getContentActionsGroupInfo()}))},e.prototype.ngOnDestroy=
2022-06-30 20:52:04 UTC	2130	IN	Data Raw: 53 74 61 72 74 54 69 6d 65 3a 30 29 7d 29 29 7d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 73 74 61 72 74 53 65 73 73 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 21 74 68 69 73 2e 63 6f 6e 74 65 78 74 53 65 72 76 69 63 65 2e 73 68 61 72 65 64 43 6f 6e 74 65 78 74 2e 61 63 74 69 76 69 74 79 54 72 61 63 6b 69 6e 67 45 6e 61 62 6c 65 64 29 72 65 74 75 72 6e 20 6e 75 6c 6c 3b 69 66 28 74 68 69 73 2e 63 75 72 72 65 6e 74 53 65 73 73 69 6f 6e 49 64 3b 74 68 69 73 2e 63 75 72 72 65 6e 74 53 65 73 73 69 6f 6e 53 74 61 72 74 54 69 6d 65 3d 6f 2e 61 2e 6e 6f 77 28 29 2c 74 68 69 73 2e 63 75 72 72 65 6e 74 53 65 73 73 69 6f 6e 49 64 3d 63 2e 61 2e 63 72 65 61 74 65 47 75 Data Ascii: StartTime:0)}))}},e.prototype.startSession=function(){if(!this.contextService.sharedContext.activityTrackingEnabled)return null;if(this.currentSessionId)return this.currentSessionId;this.currentSessionStartTime=o.a.now(),this.currentSessionId=c.a.createGu
2022-06-30 20:52:04 UTC	2146	IN	Data Raw: 69 76 65 22 3a 22 47 72 61 70 68 22 2c 21 31 2c 6e 75 6c 6c 2c 6c 7c 6f 2e 75 70 6c 6f 61 64 43 6f 6e 66 69 67 53 65 72 76 69 63 65 2e 63 6f 6e 66 69 67 2e 63 61 70 50 6f 70 75 70 45 6e 61 62 6c 65 64 2c 7b 63 61 74 65 67 6f 72 79 3a 22 55 70 6c 6f 61 64 22 2c 66 69 6c 65 54 79 70 65 3a 73 7d 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 2e 75 70 6c 6f 61 64 46 69 6c 65 28 61 2c 6e 2c 74 2c 69 2c 72 29 7d 29 29 7d 29 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 6c 6f 67 43 6c 69 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 2c 69 2c 72 2c 6f 29 7b 76 61 72 20 61 3d 74 68 69 73 2e 67 65 74 43 6c 69 63 6b 44 61 74 61 46 6f 72 49 64 28 65 2c 74 2c 6e 29 3b 74 68 69 73 2e 69 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 53 65 72 76 69 63 65 Data Ascii: ive":"Graph",!1,null,l||o.uploadConfigService.config.capPopupEnabled,{category:"Upload",fileType:s}).then((function(){o.uploadFile(a,n,t,i,r)}))}))},e.prototype.logClick=function(e,t,n,i,r,o){var a=this.getClickDataForId(e,t,n);this.instrumentationService
2022-06-30 20:52:04 UTC	2162	IN	Data Raw: 74 68 69 73 2e 72 6f 75 74 65 53 65 72 76 69 63 Data Ascii: this.routeServic
2022-06-30 20:52:04 UTC	2162	IN	Data Raw: 65 2e 67 65 74 52 6f 75 74 65 43 68 61 6e 67 65 53 74 61 72 74 4f 62 73 65 72 76 61 62 6c 65 28 29 2e 70 69 70 65 28 4f 62 6a 65 63 74 28 6d 2e 61 29 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3b 72 65 74 75 72 6e 20 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 26 26 22 43 6f 6e 74 65 6e 74 22 21 3d 3d 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 2e 72 6f 75 74 65 7c 7c 22 43 6f 6e 74 65 6e 74 22 3d 3d 3d 28 6e 75 6c 6c 3d 3d 3d 28 74 3d 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 29 7c 7c 76 6f 69 64 20 30 3d 3d 3d 74 3f 76 6f 69 64 20 30 3a 74 2e 72 6f 75 74 65 29 26 26 28 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 2e 61 70 70 3d 3d 3d 67 2e 62 2e 46 6c 75 69 64 7c 7c 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 2e 61 70 70 3d 3d 3d 67 2e 62 2e 46 6c 75 69 64 7c 7c 65 2e 63 75 72 72 65 6e 74 52 6f 75 74 65 2e 61 70 70 3d 3d 3d 67 2e 62 2e 46 6c Data Ascii: e.getRouteChangeStartObservable().pipe(Object(m.a)((function(e){var t;return e.currentRoute&&"Content"!==e.currentRoute.route||"Content"===(null===(t=e.currentRoute)||void 0===t?void 0:t.route)&&(e.currentRoute.app===g.b.Fluid||e.currentRoute.app===g.b.Fl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49764	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	672	OUT	GET /officehub/bundles/app-bundle-e85ead0ff8c76e2e6300.css HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	787	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 10230 Content-Type: text/css Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Wed, 22 Jun 2022 22:22:51 GMT Server: ECAcc (muc/337F) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon X-Content-Type-Options: nosniff x-ms-request-id: 02b57bca-501e-0041-3fab-8c9225000000 Content-Length: 94036 Connection: close
2022-06-30 20:52:04 UTC	788	IN	Data Raw: 2e 6f 66 66 69 63 65 48 6f 6d 65 2d 63 61 6c 6c 6f 75 74 7b 7a 2d 69 6e 64 65 78 3a 31 30 30 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6d 61 72 67 69 6e 3a 31 36 70 78 20 61 75 74 6f 3b 77 69 64 74 68 3a 32 38 38 70 78 7d 2e 6f 66 66 69 63 65 48 6f 6d 65 2d 63 61 6c 6c 6f 75 74 2e 6f 66 66 69 63 65 48 6f 6d 65 2d 63 61 6c 6c 6f 75 74 2d 2d 61 72 72 6f 77 53 69 64 65 3a 61 66 74 65 72 2c 2e 6f 66 66 69 63 65 48 6f 6d 65 2d 63 61 6c 6c 6f 75 74 2e 6f 66 66 69 63 65 48 6f 6d 65 2d 63 61 6c 6c 6f 75 74 2d 2d 61 72 72 6f 77 53 69 64 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 22 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 72 6f 74 61 74 65 28 2d 34 35 64 65 67 29 3b 74 Data Ascii: .officeHome-callout{z-index:100;position:relative;margin:16px auto;width:288px}.officeHome-callout.officeHome-callout--arrowSide:after,.officeHome-callout.officeHome-callout--arrowSide:before{content:"";position:absolute;-webkit-transform:rotate(-45deg);t
2022-06-30 20:52:04 UTC	804	IN	Data Raw: 28 Data Ascii: (
2022-06-30 20:52:04 UTC	804	IN	Data Raw: 33 2c 6d 69 6e 6d 61 78 28 31 37 38 70 78 2c 31 66 72 29 29 7d 7d 2e 65 78 70 61 6e 64 61 62 6c 65 2d 6c 69 73 74 5f 5f 69 74 65 6d 2e 6e 67 2d 6c 65 61 76 65 7b 74 72 61 6e 73 69 74 69 6f 6e 3a 6f 70 61 63 69 74 79 20 2e 33 36 37 73 20 63 75 62 69 63 2d 62 65 7a 69 65 72 28 2e 31 2c 2e 32 35 2c 2e 37 35 2c 2e 39 29 3b 6f 70 61 63 69 74 79 3a 31 7d 2e 65 78 70 61 6e 64 61 62 6c 65 2d 6c 69 73 74 5f 5f 69 74 65 6d 2e 6e 67 2d 6c 65 61 76 65 2e 6e 67 2d 6c 65 61 76 65 2d 61 63 74 69 76 65 7b 6f 70 61 63 69 74 79 3a 30 7d 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 2d 77 72 61 70 70 65 72 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 7d 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 2d 77 72 61 70 70 65 72 2d 2d 72 65 6c 61 74 69 76 65 7b 70 6f 73 Data Ascii: 3,minmax(178px,1fr))}}.expandable-list__item.ng-leave{transition:opacity .367s cubic-bezier(.1,.25,.75,.9);opacity:1}.expandable-list__item.ng-leave.ng-leave-active{opacity:0}.dropdown-menu-wrapper{display:inline-block}.dropdown-menu-wrapper--relative{pos
2022-06-30 20:52:04 UTC	943	IN	Data Raw: 6e 2d 2d 66 6c 75 65 6e 74 2d 2d 73 65 63 6f 6e 64 61 72 79 2e 67 65 6e 65 72 69 63 2d 62 75 74 74 6f 6e 2d 2d 62 6f 72 64 65 72 65 64 3a 6e 6f 74 28 2e 67 65 6e 65 72 69 63 2d 62 75 74 74 6f 6e 2d 2d 64 69 73 61 62 6c 65 64 29 7b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 66 33 66 32 66 31 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 7d 2e 67 65 6e 65 72 69 63 2d 62 75 74 74 6f 6e 5f 5f 74 65 78 74 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 53 65 67 6f 65 55 49 2d 53 65 6d 69 42 6f 6c 64 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 7d 2e 67 65 6e 65 72 69 63 2d 62 75 74 74 6f 6e 2d 2d 66 6c 75 65 6e 74 Data Ascii: n--fluent--secondary.generic-button--bordered:not(.generic-button--disabled){border:1px solid #f3f2f1;border-radius:3px}.generic-button__text{font-family:SegoeUI-SemiBold,Helvetica,Arial,sans-serif;font-size:14px;white-space:nowrap}.generic-button--fluent
2022-06-30 20:52:04 UTC	959	IN	Data Raw: 61 62 73 6f 6c 75 74 65 3b 6d 61 78 2d 77 69 64 74 68 3a 32 30 30 70 78 3b 7a 2d 69 6e 64 65 78 3a 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 7d 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 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 66 6c 65 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 66 6c 65 78 7d 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 5f 5f 74 65 78 74 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 7d 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 5f 5f 69 63 6f 6e 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 32 70 78 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 34 70 78 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 6f 74 Data Ascii: absolute;max-width:200px;z-index:1;font-size:12px}.alert-message{display:-webkit-inline-flex;display:inline-flex}.alert-message__text{font-size:14px}.alert-message__icon{font-size:14px;margin-bottom:2px;line-height:12px;margin-right:4px;vertical-align:bot

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1121	IN	Data Raw: 69 64 74 68 3a 63 61 6c 63 28 33 32 2e 33 38 30 39 35 76 77 20 2d 20 31 32 70 78 29 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 37 70 78 29 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 34 37 39 70 78 29 7b 2e 63 61 72 6f 75 73 65 6c 2d 63 61 72 64 2d 63 6f 6e 74 61 69 6e 65 72 2e 63 61 72 6f 75 73 65 6c 2d 63 61 72 64 2d 2d 76 69 72 74 75 61 6c 2d 74 6f 75 63 68 7b 77 69 64 74 68 3a 63 61 6c 63 28 35 39 2e 32 35 39 32 36 76 77 20 2d 20 31 32 70 78 29 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 34 38 30 70 78 29 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 30 31 2e 37 37 31 37 33 39 31 33 70 78 29 7b 2e 63 61 72 6f 75 73 65 6c 2d 63 61 72 64 2d 63 6f 6e 74 61 69 6e 65 72 2e 63 61 72 6f 75 73 65 6c 2d 63 61 72 64 2d 63 6f 6e 74 61 69 6e 65 72 2e 63 61 72 6f 75 73 65 6c 2d 63 61 72 64 Data Ascii: idth:calc(32.38095vw - 12px)}}@media (min-width:17px) and (max-width:479px){.carousel-card-contain er.carousel-card--virtual-touch{width:calc(59.25926vw - 12px)}}@media (min-width:480px) and (max-width:501.771 73913px){.carousel-card-container.carousel-card
2022-06-30 20:52:04 UTC	1137	IN	Data Raw: 6e 74 46 61 6d 69 6c 79 42 61 73 65 2c 22 53 65 67 6f 65 20 55 49 22 2c 22 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 22 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 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 73 61 6e 73 2d 73 65 72 69 66 29 7d 2e 61 63 74 69 76 69 74 79 2d 64 65 65 70 2d 6c 69 6e 6b 20 2e 61 63 74 69 76 69 74 79 2d 64 65 65 70 2d 6c 69 6e 6b 5f 5f 75 6e 64 65 72 6c 69 6e 65 64 2c 2e 61 63 74 69 76 69 74 79 2d 64 65 73 63 72 69 70 74 69 6f 6e 5f 5f 64 61 74 65 20 2e 61 63 74 69 76 69 74 79 2d 64 65 65 70 2d 6c 69 6e 6b 5f 5f 75 6e 64 65 72 6c 69 6e 65 64 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 Data Ascii: ntFamilyBase,"Segoe UI","Segoe UI Web (West European)",-apple-system,BlinkMacSystemFont,Roboto,"He lvetica Neue",sans-serif)}.activity-deep-link .activity-deep-link__underlined,.activity-description__date .activity-deep-link__underlined{text-decoration:und

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49769	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	672	OUT	GET /officehub/images/content/images/fluent-background-sources/header-default-desktop-652cc04392.svg HTTP/1.1 Host: res.cdn.office.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	820	IN	HTTP/1.1 200 OK Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET,HEAD,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: date Age: 166278 Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:04 GMT Last-Modified: Wed, 21 Jul 2021 22:37:56 GMT Server: ECAcc (muc/336A) Strict-Transport-Security: max-age=31536000; includeSubDomains Timing-Allow-Origin: * Vary: Accept-Encoding X-Cache: HIT X-CDN-Provider: Verizon x-ms-request-id: 88b2d1f0-401e-005d-0e40-8bc045000000 Content-Length: 6805 Connection: close
2022-06-30 20:52:04 UTC	820	IN	Data Raw: 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 0d 0a 3c 73 76 67 20 77 69 64 74 68 3d 22 32 35 36 30 70 78 22 20 68 65 69 67 68 74 3d 22 33 34 30 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 35 36 30 20 33 34 30 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 31 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 3e 0d 0a 20 20 20 20 3c 21 2d 2d 20 47 65 6e 65 72 61 74 6f 72 3a 20 53 6b 65 74 63 68 20 35 31 2e 32 20 28 35 37 35 31 39 29 20 2d 20 68 74 74 70 3a 2f 2f 77 77 77 2e 62 6f 68 65 6d 69 61 6e 63 6f Data Ascii: <?xml version="1.0" encoding="UTF-8"?><svg width="2560px" height="340px" viewBox="0 0 2560 340" ve rsion="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"> ... Generator: Sketch 51.2 (57519) - http://www.bohemianco

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49770	52.98.171.226	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:04 UTC	1073	OUT	GET /owa/prefetch.aspx HTTP/1.1 Host: outlook.office365.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://www.office.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:04 UTC	1309	IN	HTTP/1.1 200 OK Cache-Control: private, no-store Content-Length: 2734 Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/10.0 request-id: fd58c36a-a184-de9b-633a-c039e48b8aa4 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Alt-Svc: h3=":443",h3-29=":443" X-CalculatedFETarget: BE1P281CU008.internal.outlook.com X-BackEndHttpStatus: 200 Set-Cookie: ClientId=263CA778711A442DB3D9D088E8911E67; expires=Fri, 30-Jun-2023 20:52:04 GMT; path=/;SameSite=None; secure Set-Cookie: ClientId=263CA778711A442DB3D9D088E8911E67; expires=Fri, 30-Jun-2023 20:52:04 GMT; path=/;SameSite=None; secure Set-Cookie: OIDC=1; expires=Fri, 30-Dec-2022 20:52:04 GMT; path=/;SameSite=None; secure; HttpOnly Set-Cookie: OWAPF=v:15.20.5417.6&l:mouse; path=/ X-CalculatedBETarget: BE0P281MB0275.DEUP281.PROD.OUTLOOK.COM X-BackEndHttpStatus: 200 X-RUM-Validated: 1 X-Content-Type-Options: nosniff X-BeSku: WCS6 X-OWA-Version: 15.20.5417.6 X-OWA-DiagnosticsInfo: 1;0;0 X-IIDs: 0 X-BackEnd-Begin: 2022-06-30T20:52:04.457 X-BackEnd-End: 2022-06-30T20:52:04.457 X-DiagInfo: BE0P281MB0275 X-BEServer: BE0P281MB0275 X-UA-Compatible: IE=EmulateIE7 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 200 X-FEProxyInfo: FR0P281CA0046.DEUP281.PROD.OUTLOOK.COM X-FEEFZInfo: HHN X-FEServer: BE1P281CA0070 Report-To: {"group":"NelOfficeUpload1","max_age":7200,"endpoints":[{"url":"https://exo.nel.measure.office.net/api/report?TenantId=&FrontEnd=Cafe&DestinationEndpoint=HHN"}],"include_subdomains":true} NEL: {"report_to":"NelOfficeUpload1","max_age":7200,"include_subdomains":true,"failure_fraction":1.0,"success_fraction":0.01} X-FirstHopCafeEFZ: HHN X-FEServer: FR0P281CA0046 Date: Thu, 30 Jun 2022 20:52:03 GMT Connection: close
2022-06-30 20:52:04 UTC	1311	IN	Data Raw: 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 50 72 65 66 65 74 63 68 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 22 3e 0d 0a 0d 0a 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 40 66 6f 6e 74 2d 66 61 63 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 6f 66 66 69 63 65 33 36 35 69 63 6f 6e 73 27 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 72 63 3a 20 75 72 6c 28 27 68 74 74 70 73 3a 2f Data Ascii: <!DOCTYPE html><html><head> <title>Prefetch</title> <meta http-equiv="x-ua-compatible" content="IE=Edge"> <style> @font-face { font-family: 'office365icons'; src: url('https:/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49778	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:06 UTC	2174	OUT	GET /shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:06 UTC	2175	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 4320118 Cache-Control: public, max-age=31536000 Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Content-Type: image/x-icon Date: Thu, 30 Jun 2022 20:52:06 GMT Etag: 0x8D8731240E548EB Last-Modified: Sun, 18 Oct 2020 03:02:30 GMT Server: ECAcc (muc/3374) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 89c38479-601e-001b-6d78-65b5e2000000 x-ms-version: 2009-09-19 Content-Length: 17174 Connection: close
2022-06-30 20:52:06 UTC	2175	IN	Data Raw: 00 00 01 00 06 00 80 80 10 00 00 00 00 00 68 28 00 00 66 00 00 00 48 48 10 00 00 00 00 00 e8 0d 00 00 ce 28 00 00 30 30 10 00 00 00 00 00 68 06 00 00 b6 36 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 1e 3d 00 00 18 18 10 00 00 00 00 00 e8 01 00 00 06 40 00 00 10 10 10 00 00 00 00 00 28 01 00 00 ee 41 00 00 28 00 00 00 80 00 00 00 00 01 00 00 01 00 04 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 20 00 00 03 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 Data Ascii: h(fHH(00h6 =@(A(("P"""""""""""""""""""""""""""""" 333333333333333
2022-06-30 20:52:06 UTC	2191	IN	Data Raw: 01 80 00 00 01 80 00 28 00 00 00 18 00 00 00 30 00 00 00 01 00 04 00 00 00 00 00 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 Data Ascii: (0"P""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49799	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2192	OUT	GET /shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net
2022-06-30 20:52:09 UTC	2193	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 4320121 Cache-Control: public, max-age=31536000 Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Content-Type: image/x-icon Date: Thu, 30 Jun 2022 20:52:09 GMT Etag: 0x8D8731240E548EB Last-Modified: Sun, 18 Oct 2020 03:02:30 GMT Server: ECAcc (muc/3374) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 89c38479-601e-001b-6d78-65b5e2000000 x-ms-version: 2009-09-19 Content-Length: 17174 Connection: close

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2193	IN	Data Raw: 00 00 01 00 06 00 80 80 10 00 00 00 00 00 68 28 00 00 66 00 00 00 48 48 10 00 00 00 00 00 e8 0d 00 00 ce 28 00 00 30 30 10 00 00 00 00 00 68 06 00 00 b6 36 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 1e 3d 00 00 18 18 10 00 00 00 00 00 e8 01 00 00 06 40 00 00 10 10 10 00 00 00 00 00 28 01 00 00 ee 41 00 00 28 00 00 00 80 00 00 00 00 01 00 00 01 00 04 00 00 00 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 0 0 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22 20 00 00 03 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 Data Ascii: h(fHH(00h6 =@(A(("P"""""""""""""""""""""""""""""" 333333333333333
2022-06-30 20:52:09 UTC	2209	IN	Data Raw: 01 80 00 00 01 80 00 28 00 00 00 18 00 00 00 30 00 00 00 01 00 04 00 00 00 00 00 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ef a4 00 00 00 b9 ff 00 00 ba 7f 00 22 50 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 22 22 22 22 22 20 33 33 33 33 33 30 Data Ascii: (0"P""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330""""" 333330

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49751	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	0	OUT	GET /shared/1.0/content/js/ConvergedLogin_PCore_Mo4A0Fxm-KbAvsKDen15VQ2.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	36	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 10929283 Cache-Control: public, max-age=31536000 Content-MD5: wP3Ut/VHugsJQxzFYXBV5g== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D9313DAC35CC62 Last-Modified: Thu, 17 Jun 2021 03:12:00 GMT Server: ECAcc (muc/3331) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 3df3b834-701e-009d-025c-29ab66000000 x-ms-version: 2009-09-19 Content-Length: 466060 Connection: close
2022-06-30 20:52:03 UTC	56	IN	Data Raw: 2f 2a 21 0a 20 2a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 53 54 41 52 54 20 4f 46 20 54 48 49 52 44 20 50 41 52 54 59 20 4e 4f 54 49 43 45 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0a 20 2a 20 0a 20 2a 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 62 61 73 65 64 20 6f 6e 20 6f 72 20 69 6e 63 6f 72 70 6f 72 61 74 65 73 20 6d 61 74 65 72 69 61 6c 20 66 72 6f 6d 20 74 68 65 20 70 72 6f 6a 65 63 74 73 20 6c 69 73 74 65 64 20 62 65 6c 6f 77 20 28 54 68 69 72 64 20 50 61 72 74 79 20 49 50 29 2e 20 54 68 65 20 6f 72 69 67 69 6e 61 6c 20 63 6f 70 79 72 69 67 68 74 20 6e 6f 74 69 63 65 20 61 Data Ascii: /*! * -- START OF THIRD PARTY NOTICE -- * * This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice a
2022-06-30 20:52:03 UTC	72	IN	Data Raw: 65 Data Ascii: e
2022-06-30 20:52:03 UTC	72	IN	Data Raw: 6e 64 43 61 6c 6c 3a 22 55 73 65 72 56 6f 69 63 65 41 75 74 68 46 61 69 6c 65 64 50 72 6f 76 69 64 65 72 43 6f 75 6c 64 6e 74 53 65 6e 64 43 61 6c 6c 22 2c 55 73 65 72 32 57 61 79 53 4d 53 41 75 74 68 46 61 69 6c 65 64 50 72 6f 76 69 64 65 72 43 6f 75 6c 64 6e 74 53 65 6e 64 53 4d 53 3a 22 55 73 65 72 32 57 61 79 53 4d 53 41 75 74 68 46 61 69 6c 65 64 50 72 6f 76 69 64 65 72 43 6f 75 6c 64 6e 74 53 65 6e 64 53 4d 53 22 2c 53 4d 53 41 75 74 68 46 61 69 6c 6 5 64 50 72 6f 76 69 64 65 72 43 6f 75 6c 64 6e 74 53 65 6e 64 53 4d 53 3a 22 53 4d 53 41 75 74 68 46 61 69 6c 65 64 50 72 6f 76 69 64 65 72 43 6f 75 6c 64 6e 74 53 65 6e 64 53 4d 53 22 2c 55 73 65 72 32 57 61 79 53 4d 53 41 75 74 68 46 61 69 6c 65 64 4e 6f 52 65 73 70 6f 6e 73 65 54 69 6d 65 6f 75 74 3a Data Ascii: ndCall:"UserVoiceAuthFailedProviderCouldntSendCall",User2WaySMSAuthFailedProviderCouldntSendSMS:"User2WaySMSAuthFailedProviderCouldntSendSMS",SMSAuthFailedProviderCouldntSendSMS:"SMSAuthFailedProviderCouldntSendSMS",User2WaySMSAuthFailedNoResponseTimeout:

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	210	IN	Data Raw: 7b 6e 6f 74 69 66 79 3a 22 61 6c 77 61 79 73 22 7d 29 2c 61 2e 74 72 61 63 69 6e 67 4f 70 74 69 6f 6e 73 3d 65 2c 61 2e 73 75 62 73 63 72 69 62 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 61 2e 65 76 65 6e 74 41 72 67 73 2e 73 75 62 73 63 72 69 62 65 28 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 6e 3d 65 28 74 29 7d 29 29 2c 74 26 26 28 6e 3d 65 28 61 2e 65 76 65 6e 74 41 72 67 73 2e 70 65 65 6b 28 29 29 29 7d 2c 61 7d 2c 6e 2e 69 73 43 6f 6d 70 6f 6e 65 6e 74 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 69 2e 69 73 4f 62 73 65 72 76 61 62 6c 65 28 65 2e 65 76 65 6e 74 41 72 67 73 29 7d 7d 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 2c 74 29 7b 76 61 72 20 69 3d 77 69 6e 64 6f 77 3b 65 2e 65 78 70 6f 72 74 73 3d 69 2e 50 72 6f Data Ascii: {notify:"always"}),a.tracingOptions=e,a.subscribe=function(e){a.eventArgs.subscribe((function(t){n=e(t)})),t&&(n=e(a.eventArgs.peek()))},a},n.isComponentEvent=function(e){return e&&i.isObservable(e.eventArgs)}},function(e,n,t){var i=window;e.exports=i.Pro
2022-06-30 20:52:03 UTC	226	IN	Data Raw: 75 74 Data Ascii: ut
2022-06-30 20:52:03 UTC	226	IN	Data Raw: 74 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 6e 2e 69 73 53 65 63 6f 6e 64 61 72 79 42 75 74 74 6f 6e 56 69 73 69 62 6c 65 28 65 29 7d 2c 6e 2e 73 65 74 45 6e 61 62 6c 65 64 50 72 69 6d 61 72 79 42 75 74 74 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 6e 2e 69 73 50 72 69 6d 61 72 79 42 75 74 74 6f 6e 45 6e 61 62 6c 65 64 28 65 29 7d 2c 6e 2e 73 65 74 45 6e 61 62 6c 65 64 53 65 63 6f 6e 64 61 72 79 42 75 74 74 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 6e 2e 69 73 53 65 63 6f 6e 64 61 72 79 42 75 74 74 6f 6e 45 6e 61 62 6c 65 64 28 65 29 7d 2c 6e 2e 70 72 69 6d 61 72 79 42 75 74 74 6f 6e 5f 6f 6e 43 6c 69 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 2e 6f 6e 50 72 69 6d 61 72 79 42 75 74 74 6f 6e 43 6c 69 63 6b 28 29 7d 2c 6e 2e 73 65 63 6f 6e 64 61 Data Ascii: ton=function(e){n.isSecondaryButtonVisible(e)},n.setEnabledPrimaryButton=function(e){n.isPrimaryButtonEnabled(e)},n.setEnabledSecondaryButton=function(e){n.isSecondaryButtonEnabled(e)},n.primaryButton_onClick=function(){n.onPrimaryButtonClick()},n.seconda
2022-06-30 20:52:03 UTC	242	IN	Data Raw: 6e 63 6f 64 65 55 52 49 43 6f 6d 70 6f 6e 65 6e 74 28 6e 29 2e 72 65 70 6c 61 63 65 28 6e 65 77 20 52 65 67 45 78 70 28 22 27 22 2c 22 67 22 29 2c 22 25 32 37 22 29 3b 65 3d 70 2e 61 70 70 65 6e 64 4f 72 52 65 70 6c 61 63 65 28 65 2c 22 75 73 65 72 6e 61 6d 65 22 2c 74 29 2c 6b 65 26 26 28 65 3d 70 2e 61 70 70 65 6e 64 4f 72 52 65 70 6c 61 63 65 28 65 2c 22 6c 6f 67 69 6e 5f 68 69 6e 74 22 2c 74 29 29 3b 76 61 72 20 69 3d 64 65 3f 66 2e 63 6c 6f 6e 65 28 64 65 29 3a 6e 75 6c 6c 3b 72 65 74 75 72 6e 20 69 26 26 28 69 2e 75 6e 73 61 66 65 5f 75 73 65 72 6e 61 6d 65 3d 6e 29 2c 57 65 28 65 2c 69 2c 21 30 2c 64 2e 45 76 65 6e 74 49 64 73 2e 52 65 64 69 72 65 63 74 5f 4f 74 68 65 72 49 64 70 52 65 64 69 72 65 63 74 69 6f 6e 29 7d 66 75 6e 63 74 69 6f 6e 20 4f Data Ascii: ncodeURIComponent(n).replace(new RegExp("'","g"),"%27");e=p.appendOrReplace(e,"username",t),ke&&(e=p.appendOrReplace(e,"login_hint",t));var i=de?f.clone(de):null;return i&&(i.unsafe_username=n),We(e,i,!0,d.EventIds.Redirect_OtherIdpRedirection)}function O
2022-06-30 20:52:03 UTC	258	IN	Data Raw: 29 29 Data Ascii:))
2022-06-30 20:52:03 UTC	258	IN	Data Raw: 29 7d 6e 2e 6f 6e 53 77 69 74 63 68 56 69 65 77 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 52 65 64 69 72 65 63 74 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 52 65 67 69 73 74 65 72 44 69 61 6c 6f 67 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 55 6e 72 65 67 69 73 74 65 72 44 69 61 6c 6f 67 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 53 68 6f 77 44 69 61 6c 6f 67 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 53 65 74 50 65 6e 64 69 6e 67 52 65 71 75 65 73 74 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 55 70 64 61 74 65 46 6c 6f 77 54 6f 6b 65 6e 3d 6f 2e 63 72 65 61 74 65 28 29 2c 6e 2e 63 72 65 64 65 6e 74 69 61 6c 43 6f 75 6e 74 3d 30 2c 6e 2e 73 65 6c 65 63 74 65 64 43 72 65 64 54 79 70 65 3d 6e 75 6c 6c 2c 6e 2e 73 65 6c 65 63 Data Ascii:)}n.onSwitchView=o.create(),n.onRedirect=o.create(),n.onRegisterDialog=o.create(),n.onUnregisterDialog=o.create(),n.onShowDialog=o.create(),n.onSetPendingRequest=o.create(),n.onUpdateFlowToken=o.create(),n.credentialCount=0,n.selectedCredType=null,n.selec
2022-06-30 20:52:03 UTC	297	IN	Data Raw: 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 2e 70 61 67 69 6e 61 74 69 6f 6e 43 6f 6e 74 72 6f 6c 4d 65 74 68 6f 64 73 28 29 26 26 21 61 2e 70 61 67 69 6e 61 74 69 6f 6e 43 6f 6e 74 72 6f 6c 4d 65 74 68 6f 64 73 28 29 2e 63 75 72 72 65 6e 74 56 69 65 77 48 61 73 4d 65 74 61 64 61 74 61 28 22 68 69 64 65 4c 77 61 44 69 73 63 6c 61 69 6d 65 72 22 29 7d 29 29 2c 61 2e 73 68 6f 77 50 61 67 65 4c 65 76 65 6c 54 69 74 6c 65 43 6f 6e 74 72 6f 6c 3d 69 2e 70 75 72 65 43 6f 6d 70 75 74 65 64 28 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 73 26 26 21 28 61 2e 70 61 67 69 6e 61 74 69 6f 6e 43 6f 6e 74 72 6f 6c 4d 65 74 68 6f 64 73 28 29 26 26 61 2e 70 61 67 69 6e 61 74 69 6f 6e 43 6f 6e 74 72 6f 6c 4d 65 74 68 6f 64 73 28 29 2e 63 75 72 72 65 6e 74 56 69 65 Data Ascii: on(){return a.paginationControlMethods()&&!a.paginationControlMethods().currentViewHasMetadata("hideLwaDisclaimer")})),a.showPageLevelTitleControl=i.pureComputed((function(){return s&&!(a.paginationControlMethods()&&a.paginationControlMethods().currentVie
2022-06-30 20:52:03 UTC	313	IN	Data Raw: 73 65 20 75 2e 47 65 6e 65 72 69 63 45 72 72 6f 72 4d 6f 62 69 6c 65 3a 63 61 73 65 20 75 2e 47 65 6e 65 72 69 63 45 72 72 6f 72 48 6f 73 74 3a 63 61 73 65 20 75 2e 53 77 69 74 63 68 55 73 65 72 3a 63 61 73 65 20 75 2e 53 77 69 74 63 68 55 73 65 72 4d 6f 62 69 6c 65 3a 63 61 73 65 20 75 2e 53 77 69 74 63 68 55 73 65 72 48 6f 73 74 3a 63 61 73 65 20 75 2e 49 6e 76 69 74 65 42 6c 6f 63 6b 65 64 3a 63 61 73 65 20 75 2e 53 65 72 76 69 63 65 42 6c 6f 63 6b 65 64 3a 63 61 73 65 20 75 2e 49 44 50 46 61 69 6c 65 64 3a 63 61 73 65 20 75 2e 48 49 50 5f 4c 6f 63 6b 6f 75 74 3a 63 61 73 65 20 75 2e 48 49 50 5f 4c 6f 63 6b 6f 75 74 4d 6f 62 69 6c 65 3a 63 61 73 65 20 75 2e 48 49 50 5f 4c 6f 63 6b 6f 75 74 48 6f 73 74 3a 63 61 73 65 20 75 2e 42 69 6e 64 46 61 69 6c 65 Data Ascii: se u.GenericErrorMobile:case u.GenericErrorHost:case u.SwitchUser:case u.SwitchUserMobile:case u.SwitchUserHost:case u.InviteBlocked:case u.ServiceBlocked:case u.IDPFailed:case u.HIP_Lockout:case u.HIP_LockoutMobile:case u.HIP_LockoutHost:case u.BindFaile
2022-06-30 20:52:03 UTC	329	IN	Data Raw: 69 73 2e 66 62 3d 6e 75 6c 6c 29 7d 2c 5f 2e 69 63 2e 70 72 6f 74 6f 74 79 70 65 2e 6c 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 68 69 73 2e 4a 62 3d 65 2c 5f 2e 61 2e 4b 2e 7a 61 28 65 2c 74 68 69 73 2e 66 62 3d 74 68 69 73 2e 73 2e 62 69 6e 64 28 74 68 69 73 29 29 7d 2c 5f 2e 54 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 5f 2e 61 2e 41 62 28 74 68 69 73 2c 77 29 2c 77 2e 71 62 28 74 68 69 73 29 7d 3b 76 61 72 20 77 3d 7b 71 62 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 55 3d 7b 63 68 61 6e 67 65 3a 5b 5d 7d 2c 65 2e 73 63 3d 31 7d 2c 73 75 62 73 63 72 69 62 65 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 2c 74 29 7b 76 61 72 20 69 3d 74 68 69 73 3b 74 3d 74 7c 7c 22 63 68 61 6e 67 65 22 3b 76 61 72 20 61 3d 6e 65 77 20 5f 2e 69 63 28 69 2c 6e 3f 65 2e 62 69 6e 64 Data Ascii: is.fb=null)},_.ic.prototype.l=function(e){this.Jb=e,_.a.K.za(e,this.fb=this.s.bind(this))},_.T=function(){_.a.Ab(this,w),w.qb(this)};var w={qb:function(e){e.U={change:[]},e.sc=1},subscribe:function(e,n,t){var i=this;t=t||"change";var a=new _.ic(i,n?e.bind

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	345	IN	Data Raw: 6e 2e 6e 65 78 74 53 69 62 6c 69 6e 67 2c 61 3d 30 2c 6f 3d 74 2e 6c 65 6e 67 74 68 3b 61 3c 6f 3b 61 2b 2b 29 69 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 74 5b 61 5d 2c 69 29 7d 65 6c 73 65 20 5f 2e 61 2e 76 61 28 6e 2c 74 29 7d 2c 56 63 3a 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 76 61 72 20 69 3b 65 28 6e 29 3f 28 69 3d 6e 2e 6e 65 78 74 53 69 62 6c 69 6e 67 2c 6e 3d 6e 2e 70 61 72 65 6e 74 4e 6f 64 65 29 3a 69 3d 6e 2e 66 69 72 73 74 43 68 69 6c 64 2c 69 3f 74 21 3d 3d 69 26 26 6e 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 74 2c 69 29 3a 6e 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 74 29 7d 2c 57 62 3a 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 2c 69 29 7b 69 3f 28 69 3d 69 2e 6e 65 78 74 53 69 62 6c 69 6e 67 2c 65 28 6e 29 26 Data Ascii: n.nextSibling,a=0,o=t.length;a<o;a++)i.parentNode.insertBefore(t[a],i)}else _.a.va(n,t)},Vc:function(n,t){var i;e(n)?(i=n.nextSibling,n=n.parentNode):i=n.firstChild,i?t!==i&&n.insertBefore(t,i):n.appendChild(t)},Wb:function(n,t,i){i?(i=i.nextSibling,e(n)&
2022-06-30 20:52:03 UTC	361	IN	Data Raw: 2e 68 2e 65 61 2e 66 6f 72 65 61 63 68 3d 21 30 2c 5f 2e 63 2e 68 61 73 66 6f 63 75 73 3d 7b 69 6e 69 74 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 69 28 69 29 7b 65 2e 5f 5f 6b 6f 5f 68 61 73 66 6f 63 75 73 55 70 64 61 74 69 6e 67 3d 21 30 3b 76 61 72 20 61 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 3b 69 66 28 22 61 63 74 69 76 65 45 6c 65 6d 65 6e 74 22 69 6e 20 61 29 7b 76 61 72 20 6f 3b 74 72 79 7b 6f 3d 61 2e 61 63 74 69 76 65 45 6c 65 6d 65 6e 74 7d 63 61 74 63 68 28 72 29 7b 6f 3d 61 2e 62 6f 64 79 7d 69 3d 6f 3d 3d 3d 65 7d 61 3d 6e 28 29 2c 5f 2e 6d 2e 65 62 28 61 2c 74 2c 22 68 61 73 66 6f 63 75 73 22 2c 69 2c 21 30 29 2c 65 2e 5f 5f 6b 6f 5f 68 61 73 66 6f 63 75 73 4c 61 73 74 56 61 6c 75 65 3d 69 2c 65 Data Ascii: .h.ea.foreach=!0,_.c.hasfocus={init:function(e,n,t){function i(i){e.__ko_hasfocusUpdating=!0;var a=e.ownerDocument;if("activeElement"in a){var o;try{o=a.activeElement}catch(r){o=a.body}i=o===e}a=n(),_.m.eb(a,t,"hasfocus",i,!0),e.__ko_hasfocusLastValue=i,e
2022-06-30 20:52:03 UTC	377	IN	Data Raw: 61 2e 65 63 3d 66 Data Ascii: a.ec=f
2022-06-30 20:52:03 UTC	377	IN	Data Raw: 75 6e 63 74 69 6f 6e 28 69 2c 61 2c 6f 2c 73 2c 63 2c 6c 29 7b 66 75 6e 63 74 69 6f 6e 20 64 28 65 29 7b 67 3d 7b 41 61 3a 65 2c 70 62 3a 5f 2e 74 61 28 77 2b 2b 29 7d 2c 53 2e 70 75 73 68 28 67 29 7d 66 75 6e 63 74 69 6f 6e 20 75 28 65 29 7b 67 3d 76 5b 65 5d 2c 77 21 3d 3d 67 2e 70 62 2e 76 28 29 26 26 49 2e 70 75 73 68 28 67 29 2c 67 2e 70 62 28 77 2b 2b 29 2c 5f 2e 61 2e 55 61 28 67 2e 59 2c 69 29 2c 53 2e 70 75 73 3 68 28 67 29 7d 66 75 6e 63 74 69 6f 6e 20 70 28 65 2c 6e 29 7b 69 66 28 65 29 66 6f 72 28 76 61 72 20 74 3d 30 2c 69 3d 6e 2e 6c 65 6e 67 74 68 3b 74 3c 69 3b 74 2b 2b 29 5f 2e 61 2e 44 28 6e 5b 74 5d 2e 59 2c 28 66 75 6e 63 74 69 6f 6e 28 69 29 7b 65 28 69 2c 74 2c 6e 5b 74 5d 2e 41 61 29 7d 29 29 7d Data Ascii: unction(i,a,o,s,c,l){function d(e){g={Aa:e,pb:_.ta(w++)},S.push(g),b||k.push(g)}function u(e){g=v[e],w!==g.pb.v()&&l.push(g),g.pb(w++),_.a.Ua(g.Y,i),S.push(g)}function p(e,n){if(e)for(var t=0,i=n.length;t<i;t++)_.a.D(n[t].Y,(function(i){e(i,t,n[t].Aa)}))}
2022-06-30 20:52:03 UTC	393	IN	Data Raw: 21 6e 2e 6e 65 77 53 65 73 73 69 6f 6e 28 29 26 26 73 2e 6c 65 6e 67 74 68 3e 30 26 26 6e 2e 6e 65 77 53 65 73 73 69 6f 6e 28 73 5b 30 5d 29 2c 73 3d 5b 5d 29 29 7d 66 75 6e 63 74 69 6f 6e 20 74 6e 28 65 2c 69 29 7b 65 3f 75 2e 72 65 73 6f 6c 76 65 28 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 32 37 29 2c 6e 2e 73 68 6f 77 44 65 62 75 67 44 65 74 61 69 6c 73 28 21 30 29 2c 69 26 26 6e 2e 64 65 62 75 67 44 65 74 61 69 6c 73 4d 65 74 68 6f 64 73 28 29 26 26 6e 2e 64 65 62 75 67 44 65 74 61 69 6c 73 4d 65 74 68 6f 64 73 28 29 2e 61 63 74 69 76 61 74 65 46 6f 63 75 73 28 29 7d 2e 62 69 6e 64 28 6e 75 6c 6c 2c 74 29 29 5b 22 63 61 74 63 68 22 5d 28 74 2e 6f 65 29 3a 6e 2e 73 68 6f 77 44 65 62 75 67 44 65 74 61 69 6c 73 28 21 31 29 2c 21 65 26 Data Ascii: !n.newSession()&&s.length>0&&n.newSession(s[0]),s=[]))}function tn(e,i){e?u.resolve().then(function(){t(27),n.showDebugDetails(!0),i&&n.debugDetailsMethods()&&n.debugDetailsMethods().activateFocus()}.bind(null,t))["catch"](t.oe):n.showDebugDetails(!1),!e&
2022-06-30 20:52:03 UTC	409	IN	Data Raw: 61 74 63 68 22 5d 28 74 2e 6f 65 29 3b 62 72 65 61 6b 3b 63 61 73 65 20 49 2e 46 65 74 63 68 53 65 73 73 69 6f 6e 73 50 72 6f 67 72 65 73 73 3a 74 2e 65 28 31 35 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 34 33 39 29 2c 6e 28 29 7d 2e 62 69 6e 64 28 6e 75 6c 6c 2c 74 29 29 5b 22 63 61 74 63 68 22 5d 28 74 2e 6f 65 29 3b 62 72 65 61 6b 3b 63 61 73 65 20 49 2e 54 69 6c 65 73 3a 74 2e 65 28 33 33 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 34 34 30 29 2c 6e 28 29 7d 2e 62 69 6e 64 28 6e 75 6c 6c 2c 74 29 29 5b 22 63 61 74 63 68 22 5d 28 74 2e 6f 65 29 3b 62 72 65 61 6b 3b 63 61 73 65 20 49 2e 4c 77 41 43 6f 6e 73 65 6e 74 3a 74 2e 65 28 31 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 74 28 34 34 31 29 2c 6e 28 29 7d Data Ascii: atch"](t.oe);break;case I.FetchSessionsProgress:t.e(15).then(function(){t(439),n()}.bind(null,t))["catch"](t.oe);break;case I.Tiles:t.e(33).then(function(){t(440),n()}.bind(null,t))["catch"](t.oe);break;case I.LwaConsent:t.e(1).then(function(){t(441),n()}
2022-06-30 20:52:03 UTC	427	IN	Data Raw: 74 2e 70 2b 22 63 6f 6e 74 65 6e 74 2f 69 6d 61 67 65 73 2f 61 70 70 62 61 63 6b 67 72 6f 75 6e 64 73 2f 33 38 5f 37 62 65 36 63 32 62 30 38 33 64 65 31 61 63 37 66 36 64 35 66 63 66 31 32 31 31 33 65 37 31 65 2e 6a 70 67 22 7d 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 2c 74 29 7b 65 2e 65 78 70 6f 72 74 73 3d 74 2e 70 2b 22 63 6f 6e 74 65 6e 74 2f 69 6d 61 67 65 73 2f 61 70 70 62 61 63 6b 67 72 6f 75 6e 64 73 2f 33 39 2d 73 6d 61 6c 6c 5f 37 62 33 30 39 31 63 32 66 35 64 64 63 35 33 34 63 33 31 62 32 31 31 34 36 65 37 31 30 38 62 36 2e 6a 70 67 22 7d 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 2c 74 29 7b 65 2e 65 78 70 6f 72 74 73 3d 74 2e 70 2b 22 63 6f 6e 74 65 6e 74 2f 69 6d 61 67 65 73 2f 61 70 70 62 61 63 6b 67 72 6f 75 6e 64 73 2f 33 39 5f 39 33 31 64 61 Data Ascii: t.p+"content/images/appbackgrounds/38_7be6c2b083de1ac7f6d5fcf12113e71e.jpg"},function(e,n,t){e.exports=t.p+"content/images/appbackgrounds/39-small_7b3091c2f5ddc534c31b21146e7108b6.jpg"},function(e,n,t){e.exports=t.p+"content/images/appbackgrounds/39_931da
2022-06-30 20:52:03 UTC	443	IN	Data Raw: 29 2c 73 2e Data Ascii:),s.
2022-06-30 20:52:03 UTC	443	IN	Data Raw: 6c 6f 67 4d 65 73 73 61 67 65 28 6e 2b 22 20 69 6e 69 74 69 61 74 65 64 20 73 75 63 63 65 73 73 66 75 6c 6c 79 20 28 74 6f 6f 6b 20 22 2b 65 2b 22 20 6d 73 29 22 29 7d 29 2c 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 22 74 69 6d 65 6f 75 74 22 3d 3d 65 29 73 2e 6c 6f 67 44 61 74 61 50 6f 69 6e 74 28 22 6d 73 4c 61 75 6e 63 68 55 72 69 2e 72 65 73 70 6f 6e 73 65 22 2c 64 3f 22 74 69 6d 65 6f 75 74 22 3a 22 74 69 6d 65 6f 75 74 2d 63 6f 6e 74 69 6e 75 65 22 29 2c 73 2e 6c 6f 67 4d 65 73 73 61 67 65 28 22 22 29 3b 65 6c 73 65 7b 76 61 72 20 69 3d 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 2d 74 3b 73 2e 6c 6f 67 44 61 74 61 50 6f 69 6e 74 28 22 6d 73 4c 61 75 6e 63 68 55 72 69 2e 66 61 69 6c 75 72 65 2e 6d 73 22 2c 69 29 2c 73 2e 6c Data Ascii: logMessage(n+" initiated successfully (took "+e+" ms)")}),(function(e){if("timeout"===e)s.logDataPoint("msLaunchUri.response",d?"timeout":"timeout-continue"),s.logMessage("");else{var i=(new Date).getTime()-t;s.logDataPoint("msLaunchUri.failure.ms",i),s.l
2022-06-30 20:52:03 UTC	459	IN	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	459	IN	Data Raw: 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 5c 6e 5c 6e 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 64 61 74 61 2d 76 69 65 77 69 64 3d 22 27 2b 74 28 30 29 2e 50 61 67 69 6e 61 74 65 64 53 74 61 74 65 2e 50 68 6f 6e 65 44 69 73 61 6d 62 69 67 75 61 74 69 6f 6e 2b 27 22 20 64 61 74 61 2d 62 69 6e 64 3d 22 70 61 67 65 56 69 65 77 43 6f 6d 70 6f 6e 65 6e 74 3a 20 7b 20 6e 61 6d 65 3a 20 5c 27 6c 6f 67 69 6e 2d 70 68 6f 6e 65 2d 64 69 73 61 6d 62 69 67 75 61 74 69 6f 6e 2d 76 69 65 77 5c 27 2c 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 72 61 6d 73 3a 20 7b 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 72 76 65 72 44 61 74 61 3a 20 73 76 72 2c 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: \n\n <div data-viewid="'+t(0).PaginatedState.PhoneDisambiguation+'" data-bind="pag eViewComponent: { name: \'login-phone-disambiguation-view\',\n params: {\n serverData: svr,\n
2022-06-30 20:52:03 UTC	475	IN	Data Raw: 74 61 2d 62 69 6e 64 3d 22 76 61 6c 75 65 3a 20 63 74 78 22 20 2f 3e 5c 6e 20 20 20 20 20 20 20 20 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 68 70 67 72 65 71 75 65 73 74 69 64 22 20 64 61 74 61 2d 62 69 6e 64 3d 22 76 61 6c 75 65 3a 20 73 76 72 2e 73 65 73 73 69 6f 6e 49 64 22 20 2f 3e 5c 6e 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 69 64 3d 22 69 30 33 32 37 22 20 64 61 74 61 2d 62 69 6e 64 3d 22 61 74 74 72 3a 20 7b 20 6e 61 6d 65 3a 20 73 76 72 2e 73 46 54 4e 61 6d 65 20 7d 2c 20 76 61 6c 75 65 3a 20 66 6c 6f 77 54 6f 6b 65 6e 22 20 2f 3e 5c 6e 20 20 20 20 20 20 20 20 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 50 50 53 58 22 20 64 Data Ascii: ta-bind="value: ctx" />\n <input type="hidden" name="hpgrequestid" data-bind="value: svr.sessionId" />\n <input type="hidden" id="i0327" data-bind="attr: { name: svr.sFTName }, value: flowToken" />\n <input type="hidden" name="PPSX" d
2022-06-30 20:52:03 UTC	491	IN	Data Raw: 6f 6e 28 65 29 7b 66 6f 72 28 76 61 72 20 6e 3d 30 2c 74 3d 65 3b 6e 3c 74 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 61 3d 74 5b 6e 5d 3b 74 68 69 73 2e 5f 69 73 41 70 70 49 6e 73 69 67 68 74 73 4d 61 6e 61 67 65 72 28 69 2e 54 65 6c 65 6d 65 74 72 79 2e 61 70 70 49 6e 73 69 67 68 74 73 29 3f 28 74 68 69 73 2e 5f 61 70 70 49 6e 73 69 67 68 74 73 7c 7c 28 74 68 69 73 2e 5f 61 70 70 49 6e 73 69 67 68 74 73 3d 69 2e 54 65 6c 65 6d 65 74 72 79 2e 61 70 70 49 6e 73 69 67 68 74 73 2e 6e 65 77 49 6e 73 74 28 74 68 69 73 2e 5f 61 72 67 73 2e 61 70 70 49 6e 73 69 67 68 74 73 43 6f 6e 66 69 67 2e 69 6e 73 74 72 75 6d 65 6e 74 61 74 69 6f 6e 4b 65 79 2c 5b 5d 2c 5b 5d 29 29 2c 74 68 69 73 2e 5f 61 70 70 49 6e 73 69 67 68 74 73 2e 74 72 61 63 6b 28 61 29 29 Data Ascii: on(e){for(var n=0,t=e;n<t.length;n++){var a=t[n];this._isAppInsightsManager(i.Telemetry.appInsights)?(this._ appInsights||(this._appInsights=i.Telemetry.appInsights.newInst(this._args.appInsightsConfig.instrumentationKey,[],[])), this._appInsights.track(a))
2022-06-30 20:52:03 UTC	507	IN	Data Raw: 63 74 69 Data Ascii: cti
2022-06-30 20:52:03 UTC	507	IN	Data Raw: 6f 6e 28 65 29 7b 76 61 72 20 74 2c 69 2c 61 3d 6e 75 6c 6c 3b 74 72 79 7b 69 3d 6e 65 77 20 44 61 74 65 2c 28 61 3d 65 3d 3d 3d 6e 2e 4c 6f 63 61 6c 53 74 6f 72 61 67 65 3f 77 69 6e 64 6f 77 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 3a 77 69 6e 64 6f 77 2e 73 65 73 73 69 6f 6e 53 74 6f 72 61 67 65 29 2e 73 65 74 49 74 65 6d 28 69 2c 69 29 2c 74 3d 61 2e 67 65 74 49 74 65 6d 28 69 29 21 3d 69 2c 61 2e 72 65 6d 6f 76 65 49 74 65 6d 28 69 29 2c 74 26 26 28 61 3d 6e 75 6c 6c 29 7d 63 61 74 63 68 28 6f 29 7b 61 3d 6e 75 6c 6c 7d 72 65 74 75 72 6e 20 61 7d 2c 74 2e 63 61 6e 55 73 65 4c 6f 63 61 6c 53 74 6f 72 61 67 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 2e 5f 63 61 6e 55 73 65 4c 6f 63 61 6c 53 74 6f 72 61 67 65 3d 3d 3d 75 6e 64 65 66 69 Data Ascii: on(e){var t,i,a=null;try{i=new Date,(a=e===n.LocalStorage?window.localStorage:window.sessionStorag e).setItem(i,i),t=a.getItem(i)!=i,a.removeItem(i),t&&(a=null)}catch(o){a=null}return a},t.canUseLocalStorage=function(){ return t._canUseLocalStorage===undefi
2022-06-30 20:52:03 UTC	523	IN	Data Raw: 63 6f 72 65 28 65 29 3c 74 68 69 73 2e 73 61 6d 70 6c 65 52 61 74 65 7d 2c 6e 7d 28 29 3b 6e 2e 53 61 6d 70 6c 65 3d 74 7d 28 65 2e 43 6f 6e 74 65 78 74 7c 7c 28 65 2e 43 6f 6e 74 65 78 74 3d 7b 7d 29 29 7d 28 65 2e 41 70 70 6c 69 63 61 74 69 6f 6e 49 6e 73 69 67 68 74 73 7c 7c 28 65 2e 41 70 70 6c 69 63 61 74 69 6f 6e 49 6e 73 69 67 68 74 73 3d 7b 7d 29 29 7d 28 6f 7c 7c 28 6f 3d 7b 7d 29 29 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 21 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 5b 65 2e 53 74 61 72 74 3d 30 5d 3d 22 53 74 61 72 74 22 2c 65 5b 65 2e 45 6e 64 3d 31 5d 3d 22 45 6e 64 22 7d 28 65 2e 53 65 73 73 69 6f 6e 53 74 61 74 65 7c 7c 28 65 2e 53 65 73 73 69 6f 6e 53 74 61 74 65 3d 7b 7d 29 29 7d 28 61 3d 7b 7d 29 29 2c 66 75 6e 63 74 69 6f 6e 28 Data Ascii: core(e)<this.sampleRate},n};n.Sample=t}(e.Context||(e.Context={}))}(e.ApplicationInsights||(e.ApplicationI nsights={}))}(o||(o={})),function(e){!function(e){e[e.Start=0]="Start",e[e.End=1]="End"}(e.SessionState||(e.SessionState= {}))}(a||(a={})),function(
2022-06-30 20:52:03 UTC	539	IN	Data Raw: 2e 63 61 6e 55 73 65 53 65 73 73 69 6f 6e 53 74 6f 72 61 67 65 28 29 26 26 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 65 6e 61 62 6c 65 53 65 73 73 69 6f 6e 53 74 6f 72 61 67 65 42 75 66 66 65 72 28 29 3f 6e 65 77 20 65 2e 53 65 73 73 69 6f 6e 53 74 6f 72 61 67 65 53 65 6e 64 42 75 66 66 65 72 28 6e 29 3a 6e 65 77 20 65 2e 41 72 72 61 79 53 65 6e 64 42 75 66 66 65 72 28 6e 29 2c 21 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 69 73 42 65 61 63 6f 6e 41 70 69 44 69 73 61 62 6c 65 64 28 29 26 26 65 2e 55 74 69 6c 2e 49 73 42 65 61 63 6f 6e 41 70 69 53 75 70 70 6f 72 74 65 64 28 29 29 3f 74 68 69 73 2e 5f 73 65 6e 64 65 72 3d 74 68 69 73 2e 5f 62 65 61 63 6f 6e 53 65 6e 64 65 72 3a 22 75 6e 64 65 66 69 6e 65 64 22 21 3d 74 79 70 65 6f 66 20 58 4d 4c 48 74 74 70 52 65 Data Ascii: .canUseSessionStorage()&&this._config.enableSessionStorageBuffer()?new e.SessionStorageSendBuffer(n):new e.ArraySendBuffer(n),!this._config.isBeaconApiDisabled()&&e.Util.IsBeaconApiSupported())?this._sender=t his._beaconSender:"undefined"!=typeof XMLHttpRe
2022-06-30 20:52:03 UTC	555	IN	Data Raw: 2e 73 61 6e 69 74 69 7a 65 55 72 6c 28 61 29 2c 63 2e 6e 61 6d 65 3d 6e 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 53 74 72 69 6e 67 28 69 29 7c 7c 65 2e 55 74 69 6c 2e 4e 6f 74 53 70 65 63 69 66 69 65 64 2c 69 73 4e 61 4e 28 6f 29 7c 7c 28 63 2e 64 75 72 61 74 69 6f 6e 3d 65 2e 55 74 69 6c 2e 6d 73 54 6f 54 69 6d 65 53 70 61 6e 28 6f 29 29 2c 63 2e 70 72 6f 70 65 72 74 69 65 73 3d 65 2e 54 65 6c 65 6d 65 74 72 79 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 50 72 6f 70 65 72 74 69 65 73 28 72 29 2c 63 2e 6d 65 61 73 75 72 65 6d 65 6e 74 73 3d 65 2e 54 65 6c 65 6d 65 74 72 79 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 Data Ascii: .sanitizeUrl(a),c.name=n.Common.DataSanitizer.sanitizeString(i)||e.Util.NotSpecified,isNaN(o)||(c.duration=e .Util.msToTimeSpan(o)),c.properties=e.Telemetry.Common.DataSanitizer.sanitizeProperties(r),c.measurements=e.Te lemetry.Common.DataSanitizer.sanitize
2022-06-30 20:52:03 UTC	571	IN	Data Raw: 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 53 74 72 69 6e 67 28 64 3f 64 2b 22 20 22 2b 6d 3a 6d 29 7d 65 6c 73 65 20 67 2e 6e 61 6d 65 3d 6e 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 53 74 72 69 6e 67 28 6f 29 7d 65 6c 73 65 20 67 2e 74 61 72 67 65 74 3d 72 2c 67 2e 6e 61 6d 65 3d 72 3b 72 65 74 75 72 6e 20 67 2e 70 72 6f 70 65 72 74 69 65 73 3d 65 2e 54 65 6c 65 6d 65 74 72 79 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 50 72 6f 70 65 72 74 69 65 73 28 75 29 2c 67 2e 6d 65 61 73 75 72 65 6d 65 6e 74 73 3d 65 2e 54 65 6c 65 6d 65 74 72 79 2e 43 6f 6d 6d 6f 6e 2e 44 61 74 61 53 61 6e 69 74 69 7a 65 72 2e 73 61 6e 69 74 69 7a 65 4d 65 61 73 Data Ascii: DataSanitizer.sanitizeString(d?d+" "+m:m)}else g.name=n.Common.DataSanitizer.sanitizeString(o)}else g.target=r,g.name=r;return g.properties=e.Telemetry.Common.DataSanitizer.sanitizeProperties(u),g.measurement s=e.Telemetry.Common.DataSanitizer.sanitizeMeas

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	587	IN	Data Raw: 50 65 72 63 65 Data Ascii: Perce
2022-06-30 20:52:03 UTC	587	IN	Data Raw: 6e 74 61 67 65 3d 31 30 30 29 2c 65 2e 64 69 73 61 62 6c 65 41 6a 61 78 54 72 61 63 6b 69 6e 67 3d 6e 2e 55 74 69 6c 2e 73 74 72 69 6e 67 54 6f 42 6f 6f 6c 4f 72 44 65 66 61 75 6c 74 28 65 2e 64 69 73 61 62 6c 65 41 6a 61 78 54 72 61 63 6b 69 6e 67 29 2c 65 2e 6d 61 78 41 6a 61 78 43 61 6c 6c 73 50 65 72 56 69 65 77 3d 69 73 4e 61 4e 28 65 2e 6d 61 78 41 6a 61 78 43 61 6c 6c 73 50 65 72 56 69 65 77 29 3f 35 30 30 3a 65 2e 6d 61 78 41 6a 61 78 43 61 6c 6c 73 50 65 72 56 69 65 77 2c 65 2e 69 73 42 65 61 63 6f 6e 41 70 69 44 69 73 61 62 6c 65 64 3d 6e 2e 55 74 69 6c 2e 73 74 72 69 6e 67 54 6f 42 6f 6f 6c 4f 72 44 65 66 61 75 6c 74 28 65 2e 69 73 42 65 61 63 6f 6e 41 70 69 44 69 73 61 62 6c 65 64 2c 21 30 29 2c 65 2e 64 69 73 61 62 6c 65 43 6f 72 72 65 6c 61 Data Ascii: ntage=100),e.disableAjaxTracking=n.Util.stringToBoolOrDefault(e.disableAjaxTracking),e.maxAjaxCall sPerView=isNaN(e.maxAjaxCallsPerView)?500:e.maxAjaxCallsPerView,e.isBeaconApiDisabled=n.Util.stringToBoolOrDef ault(e.isBeaconApiDisabled,!0),e.disableCorrela
2022-06-30 20:52:03 UTC	603	IN	Data Raw: 22 63 6f 6d 70 6f 6e 65 6e 74 3a 20 7b 20 6e 61 6d 65 3a 20 5c 27 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 2d 63 6f 6e 74 72 6f 6c 5c 27 2c 5c 6e 20 20 20 20 70 75 62 6c 69 63 4d 65 74 68 6f 64 73 3a 20 24 70 61 67 65 2e 62 61 63 6b 67 72 6f 75 6e 64 43 6f 6e 74 72 6f 6c 4d 65 74 68 6f 64 73 2c 5c 6e 20 20 20 20 65 76 65 6e 74 3a 20 7b 20 6c 6f 61 64 3a 20 24 70 61 67 65 2e 62 61 63 6b 67 72 6f 75 6e 64 49 6d 61 67 65 43 6f 6e 74 72 6f 6c 5f 6f 6e 4c 6f 61 64 20 7d 20 7d 22 3e 5c 6e 3c 2f 64 69 76 3e 5c 6e 5c 6e 5c 78 33 63 21 2d 2d 20 6b 6f 20 69 66 3a 20 73 76 72 2e 69 42 61 6e 6e 65 72 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2d 2d 5c 78 33 65 5c 6e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 6e 76 2d 62 61 6e 6e 65 72 22 20 64 61 74 61 2d 62 69 6e 64 3d Data Ascii: "component: { name: \'background-image-control\',\n publicMethods: $page.backgroundControlMethods,\n event: { load: $page.backgroundImageControl_onLoad } }">\n \n\n\x3c!-- ko if: svr.iBannerEnvironment --\x3e\n<div class="env-banner" data-bind=
2022-06-30 20:52:03 UTC	619	IN	Data Raw: 65 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 78 33 63 21 2d 2d 20 6b 6f 20 69 66 3a 20 73 76 72 2e 73 65 73 73 69 6f 6e 49 64 20 2d 2d 5c 78 33 65 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 3e 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 62 6f 6c 64 22 3e 52 65 71 75 65 73 74 20 49 64 3a 20 3c 2f 73 70 61 6e 3e 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 70 61 6e 20 64 61 74 61 2d 62 69 6e 64 3d 22 74 65 78 74 3a 20 73 76 72 2e 73 65 73 73 69 6f 6e 49 64 22 3e 3c 2f 73 70 61 6e 3e 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 78 33 63 21 2d 2d 20 2f Data Ascii: e\n \x3c!-- ko if: svr.sessionId --\x3e\n \n Request Id: \n \n \n \x3c!-- /
2022-06-30 20:52:03 UTC	635	IN	Data Raw: 45 78 63 65 70 74 69 6f 6e 4f 6e 52 65 6a 65 63 74 69 6f 6e 28 53 2e 69 73 50 6c 61 74 66 6f 72 6d 41 75 74 68 65 6e 74 69 63 61 74 6f 72 41 76 61 69 6c 61 62 6c 65 28 29 2e 74 68 65 6e 28 6e 75 6c 6c 2c 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 21 31 7d 29 29 2e 74 68 65 6e 28 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 26 26 28 6e 2e 66 69 64 6f 4c 69 6e 6b 54 65 78 74 28 55 2e 43 54 5f 50 57 44 5f 53 54 52 5f 53 77 69 74 63 68 54 6f 46 69 64 6f 5f 4c 69 6e 6b 29 2c 6e 2e 69 73 50 6c 61 74 66 6f 72 6d 41 75 74 68 65 6e 74 69 63 61 74 6f 72 41 76 61 69 6c 61 62 6c 65 28 21 30 29 29 7d 29 29 29 7d 6e 2e 6f 6e 53 77 69 74 63 68 56 69 65 77 3d 75 2e 63 72 65 61 74 65 28 29 2c 6e 2e 6f 6e 52 65 64 69 72 65 63 74 3d 75 2e 63 72 65 61 74 65 28 29 Data Ascii: ExceptionOnRejection(S.isPlatformAuthenticatorAvailable().then(null,(function(){return!1})).then((function(e) {e&&(n.fidoLinkText(U.CT_PWD_STR_SwitchToFido_Link),n.isPlatformAuthenticatorAvailable(!0))}))}n.onSwitchVi ew=u.create(),n.onRedirect=u.create()
2022-06-30 20:52:03 UTC	651	IN	Data Raw: 42 6f 69 6c 65 72 50 6c 61 74 65 54 65 78 74 22 20 63 6c 61 73 73 3d 22 77 72 61 70 2d 63 6f 6e 74 65 6e 74 22 20 64 61 74 61 2d 62 69 6e 64 3d 22 5c 6e 20 20 20 20 68 74 6d 6c 57 69 74 68 4d 6f 64 73 3a 20 74 65 6e 61 6e 74 42 72 61 6e 64 69 6e 67 2e 42 6f 69 6c 65 72 50 6c 61 74 65 54 65 78 74 2c 5c 6e 20 20 20 20 68 74 6d 6c 4d 6f 64 73 3a 20 7b 20 66 69 6c 74 65 72 4c 69 6e 6b 73 3a 20 73 76 72 2e 66 49 73 48 6f 73 74 65 64 20 7d 2c 5c 6e 20 20 20 20 63 73 73 3a 20 7b 20 5c 27 74 72 61 6e 73 70 61 72 65 6e 74 2d 6c 69 67 68 74 62 6f 78 5c 27 3a 20 74 65 6e 61 6e 74 42 72 61 6e 64 69 6e 67 2e 55 73 65 54 72 61 6e 73 70 61 72 65 6e 74 4c 69 67 68 74 42 6f 78 20 7d 2c 5c 6e 20 20 20 20 65 78 74 65 72 6e 61 6c 43 73 73 3a 20 7b 20 5c 27 62 6f 69 6c 65 72 Data Ascii: BoilerPlateText" class="wrap-content" data-bind="\n htmlWithMods: tenantBranding.BoilerPlateText,\n ht mlMods: { filterLinks: svr.fIsHosted },\n css: { \'transparent-lightbox\': tenantBranding.UseTransparentLightBox },\n externalCss: { \'boiler

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49800	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2192	OUT	GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2210	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control ,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 10267848 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:09 GMT Etag: 0x8D79A1B9F5E121A Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (muc/332D) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: bce65af5-b01e-0072-7d60-2fee33000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-06-30 20:52:09 UTC	2211	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title> <path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37 .3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49802	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2214	OUT	GET /shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: aadcdn.msftauth.net
2022-06-30 20:52:09 UTC	2215	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control ,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 16993043 Cache-Control: public, max-age=31536000 Content-MD5: DhdidjYrlCeaRJJRG/y9mA== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:09 GMT Etag: 0x8D7B007297AE131 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (muc/3327) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: f043b268-b01e-0016-2336-f2876c000000 x-ms-version: 2009-09-19 Content-Length: 1864 Connection: close
2022-06-30 20:52:09 UTC	2215	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 39 32 30 22 20 68 65 69 67 68 74 3d 22 31 30 38 30 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 3e 3c 67 20 6f 70 61 63 69 74 79 3d 22 2e 32 22 20 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 45 29 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 36 36 2e 34 20 31 37 39 35 2e 32 63 39 35 30 2e 33 37 20 30 20 31 37 32 30 2e 38 2d 36 32 37 2e 35 32 20 31 37 32 30 2e 38 2d 31 34 30 31 2e 36 53 32 34 31 36 2e 37 37 2d 31 30 30 38 20 31 34 36 36 2e 34 2d 31 30 30 38 2d 32 35 34 2e 34 2d 33 38 30 2e 34 38 32 2d 32 35 34 2e 34 20 33 39 33 2e 36 73 37 37 30 2e 34 32 38 20 31 34 30 31 2e 36 20 31 37 32 30 2e 38 20 31 34 30 31 2e 36 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip- path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-3 80.482-254.4 393.6s770.428 1401.6 1720.8 1401.6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49801	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:09 UTC	2215	OUT	GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: aadcdn.msftauth.net
2022-06-30 20:52:09 UTC	2217	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 27327272 Cache-Control: public, max-age=31536000 Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:09 GMT Etag: 0x8D79A1B9B05915D Last-Modified: Thu, 16 Jan 2020 00:32:45 GMT Server: ECAcc (muc/3318) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5eeef1c9-501e-0046-1939-94c4e6000000 x-ms-version: 2009-09-19 Content-Length: 513 Connection: close
2022-06-30 20:52:09 UTC	2218	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 32 34 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 34 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 31 38 2c 31 31 2e 35 37 38 76 2e 38 34 34 48 37 2e 36 31 37 6c 33 2e 39 32 31 2c 33 2e 39 32 38 2d 2e 35 39 34 2e 35 39 34 4c 36 2c 31 32 6c 34 2e 39 34 34 2d 34 2e 39 34 34 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 38 5a 22 20 66 69 6c 6c 3d 22 23 34 30 34 30 34 30 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 31 30 2e 39 34 34 2c 37 2e 30 35 36 6c 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49755	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	1	OUT	GET /shared/1.0/content/js/asyncchunk/convergedlogin_ppassword_2fbf6b08b73b1ba49bfa.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	37	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 10929283 Cache-Control: public, max-age=31536000 Content-MD5: AaS3I4gSE2QaaYyNSkR92w== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D92D15182F3F21 Last-Modified: Fri, 11 Jun 2021 20:11:27 GMT Server: ECAcc (muc/3340) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 9fc8fe46-f01e-0033-575c-29ec9c000000 x-ms-version: 2009-09-19 Content-Length: 19397 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	38	IN	Data Raw: 2f 2a 21 0a 20 2a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 53 54 41 52 54 20 4f 46 20 54 48 49 52 44 20 50 41 52 54 59 20 4e 4f 54 49 43 45 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0a 20 2a 20 0a 20 2a 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 62 61 73 65 64 20 6f 6e 20 6f 72 20 69 6e 63 6f 72 70 6f 72 61 74 65 73 20 6d 61 74 65 72 69 61 6c 20 66 72 6f 6d 20 74 68 65 20 70 72 6f 6a 65 63 74 73 20 6c 69 73 74 65 64 20 62 65 6c 6f 77 20 28 54 68 69 72 64 20 50 61 72 74 79 20 49 50 29 2e 20 54 68 65 20 6f 72 69 67 69 6e 61 6c 20 63 6f 70 79 72 69 67 68 74 20 6e 6f 74 69 63 65 20 61 Data Ascii: /*! * -- START OF THIRD PARTY NOTICE -- * * This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice a
2022-06-30 20:52:03 UTC	54	IN	Data Raw: 20 Data Ascii:
2022-06-30 20:52:03 UTC	54	IN	Data Raw: 20 20 20 20 20 20 20 20 20 5c 78 33 63 21 2d 2d 20 6b 6f 20 69 66 6e 6f 74 3a 20 75 73 65 45 76 69 63 74 65 64 43 72 65 64 65 6e 74 69 61 6c 73 20 2d 2d 5c 78 33 65 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 5c 78 33 63 21 2d 2d 20 6b 6f 20 63 6f 6d 70 6f 6e 65 6e 74 3a 20 7b 20 6e 61 6d 65 3a 20 22 63 72 65 64 2d 73 77 69 74 63 68 2d 6c 69 6e 6b 2d 63 6f 6e 74 72 6f 6c 22 2c 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 72 61 6d 73 3a 20 7b 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 72 76 65 72 44 61 74 61 3a 20 73 76 72 2c 5c 6e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: \x3c!-- ko ifnot: useEvictedCredentials --\x3e\n \x3c!-- ko component: { name: "cred-switch-link-control",\n params: {\n serverData: svr,\n

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49756	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	2	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-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	2	OUT	Data Raw: 20 Data Ascii:
2022-06-30 20:52:03 UTC	425	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 30 Jun 2022 20:52:03 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-I2UGWCFUWoUx8CNXA-1iqg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-I2UGWCFUWoUx8CNXA-1iqg' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 20:52:03 UTC	427	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-06-30 20:52:03 UTC	427	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49757	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	2	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-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%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-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	284	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-QyWwHPSCAeynP-UUA4Dudw' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 30 Jun 2022 20:52:03 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5659 X-Daystart: 49923 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-06-30 20:52:03 UTC	285	IN	Data Raw: 33 31 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 35 39 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 39 39 32 33 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5659" elapsed_seconds="49923"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-06-30 20:52:03 UTC	286	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-06-30 20:52:03 UTC	286	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49752	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	3	OUT	GET /ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min__vnug8v1o1-mkptmkuydsg2.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	105	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 1815804 Cache-Control: public, max-age=31536000 Content-MD5: 8VdQovyys05wHikC7akm0w== Content-Type: application/x-javascript Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D9279B443DE09D Last-Modified: Fri, 04 Jun 2021 20:56:46 GMT Server: ECAcc (muc/3371) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: fde63933-a01e-0059-303f-7c442d000000 x-ms-version: 2009-09-19 Content-Length: 43198 Connection: close
2022-06-30 20:52:03 UTC	114	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 6e 29 7b 69 66 28 69 5b 6e 5d 29 72 65 74 75 72 6e 20 69 5b 6e 5d 2e 65 78 70 6f 72 74 73 3b 76 61 72 20 74 3d 69 5b 6e 5d 3d 7b 65 78 70 6f 72 74 73 3a 7b 7d 2c 69 64 3a 6e 2c 6c 6f 61 64 65 64 3a 21 31 7d 3b 72 65 74 75 72 6e 20 65 5b 6e 5d 2e 63 61 6c 6c 28 74 2e 65 78 70 6f 72 74 73 2c 74 2c 74 2e 65 78 70 6f 72 74 73 2c 6f 29 2c 74 2e 6c 6f 61 64 65 64 3d 21 30 2c 74 2e 65 78 70 6f 72 74 73 7d 76 61 72 20 69 3d 7b 7d 3b 72 65 74 75 72 6e 20 6f 2e 6d 3d 65 2c 6f 2e 63 3d 69 2c 6f 2e 70 3d 22 22 2c 6f 28 30 29 7d 28 5b 66 75 6e 63 74 69 6f 6e 28 65 2c 6f 2c 69 29 7b 69 28 32 29 3b 76 61 72 20 6e 3d 69 28 31 29 2c 74 3d 69 28 34 29 2c 72 3d 69 28 35 29 2c 61 3d 72 2e 53 74 72 69 6e Data Ascii: !function(e){function o(n){if(i[n])return i[n].exports;var t=i[n]={exports:{},id:n,loaded:!1};return e[n].call(t.exports,t,t.exports,o),t.loaded=!0,t.exports}var i={};return o.m=e,o.c=i,o.p="",o(0)}([function(e,o,i){i(2);var n=i(1),t=i(4),r=i(5),a=r.Strin
2022-06-30 20:52:03 UTC	130	IN	Data Raw: 72 64 20 62 79 20 75 73 69 6e 67 20 57 69 6e 64 6f 77 73 20 48 65 6c 6c 6f 20 6f 72 20 61 20 73 65 63 75 72 69 74 79 20 6b 65 79 2e 22 2c 65 2e 43 54 5f 53 54 52 5f 46 69 64 6f 44 69 61 6c 6f 67 5f 44 65 73 63 5f 43 72 6f 73 73 50 6c 61 74 66 6f 72 6d 3d 22 53 69 67 6e 20 69 6e 20 77 69 74 68 6f 75 74 20 61 20 75 73 65 72 6e 61 6d 65 20 6f 72 20 70 61 73 73 77 6f 72 64 20 62 79 20 75 73 69 6e 67 20 61 20 73 65 63 75 72 69 74 79 20 6b 65 79 2e 22 2c 65 2e 43 54 5f 53 54 52 5f 47 69 74 48 75 62 44 69 61 6c 6f 67 5f 44 65 73 63 3d 22 54 6f 20 75 73 65 20 74 68 69 73 20 6f 70 74 69 6f 6e 2c 20 79 6f 75 20 6d 75 73 74 20 68 61 76 65 20 70 72 65 76 69 6f 75 73 6c 79 20 6c 69 6e 6b 65 64 20 79 6f 75 72 20 70 65 72 73 6f 6e 61 6c 20 4d 69 63 72 6f 73 6f 66 74 20 Data Ascii: rd by using Windows Hello or a security key.",e.CT_STR_FidoDialog_Desc_CrossPlatform="Sign in without a username or password by using a security key.",e.CT_STR_GitHubDialog_Desc="To use this option, you must have previously linked your personal Microsoft
2022-06-30 20:52:03 UTC	146	IN	Data Raw: 72 64 Data Ascii: rd
2022-06-30 20:52:03 UTC	274	IN	Data Raw: 3a 31 31 2c 46 65 64 65 72 61 74 69 6f 6e 3a 31 33 2c 53 48 41 31 3a 31 35 2c 53 74 72 6f 6e 67 41 75 74 68 3a 31 38 2c 53 74 72 6f 6e 67 41 75 74 68 54 4f 54 50 3a 31 39 2c 4c 57 41 43 6f 6e 73 65 6e 74 3a 33 30 2c 50 61 73 73 77 6f 72 64 49 6e 6c 69 6e 65 3a 32 30 2c 52 65 6d 6f 74 65 4e 47 43 3a 32 31 2c 53 65 73 73 69 6f 6e 41 70 70 72 6f 76 61 6c 3a 32 32 2c 4e 47 43 3a 32 33 2c 4f 74 63 4e 6f 50 61 73 73 77 6f 72 64 3a 32 34 2c 52 65 6d 6f 74 65 43 6f 6e 65 63 74 5f 4e 61 74 69 76 65 50 6c 61 74 66 6f 72 6d 3a 32 35 2c 4f 54 43 3a 32 37 2c 4b 6d 73 69 3a 32 38 7d 2c 6f 2e 55 73 65 72 50 72 6f 70 65 72 74 79 3d 7b 55 53 45 52 4e 41 4d 45 3a 22 6c 6f 67 69 6e 22 2c 45 52 52 4f 52 5f 43 4f 44 45 3a 22 48 52 22 2c 45 52 52 5f 4d 53 47 3a 22 45 72 72 Data Ascii: :11,Federation:13,SHA1:15,StrongAuth:18,StrongAuthTOTP:19,LWAConsent:30,PasswordInline:20,RemoteNGC:21,SessionApproval:22,NGC:23,OtcNoPassword:24,RemoteConnect_NativePlatform:25,OTC:27,Kmsi:28},o.UserProperty={USERNAME:"login",ERROR_CODE:"HR",ERR_MSG:"Err

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49759	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	658	OUT	GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	658	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 10267842 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D79A1B9F5E121A Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (muc/332D) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: bce65af5-b01e-0072-7d60-2fee33000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-06-30 20:52:03 UTC	659	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 30 38 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 30 38 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49760	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	663	OUT	GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	664	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 27327266 Cache-Control: public, max-age=31536000 Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D79A1B9B05915D Last-Modified: Thu, 16 Jan 2020 00:32:45 GMT Server: ECAcc (muc/3318) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5eeef1c9-501e-0046-1939-94c4e6000000 x-ms-version: 2009-09-19 Content-Length: 513 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	664	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 32 34 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 34 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 31 38 2c 31 31 2e 35 37 38 76 2e 38 34 34 48 37 2e 36 31 37 6c 33 2e 39 32 31 2c 33 2e 39 32 38 2d 2e 35 39 34 2e 35 39 34 4c 36 2c 31 32 6c 34 2e 39 34 34 2d 34 2e 39 34 34 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 38 5a 22 20 66 69 6c 6c 3d 22 23 34 30 34 30 34 30 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 31 30 2e 39 34 34 2c 37 2e 30 35 36 6c 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.57

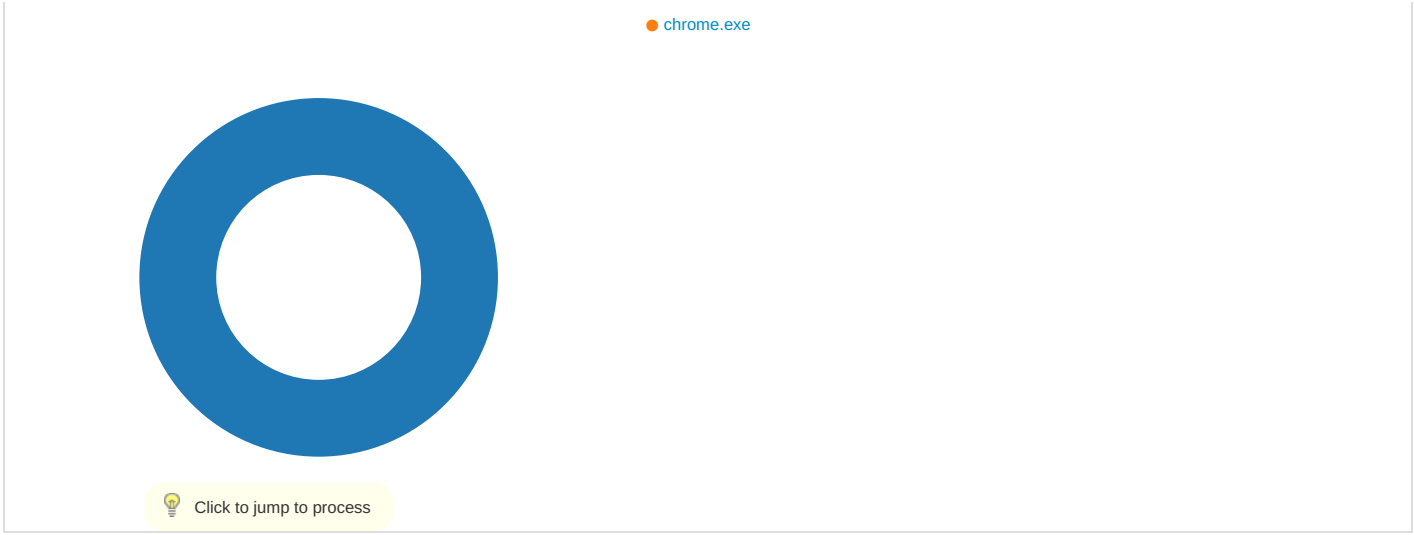
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49761	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 20:52:03 UTC	663	OUT	GET /shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-06-30 20:52:03 UTC	665	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 16993037 Cache-Control: public, max-age=31536000 Content-MD5: DhdidjYrlCeaRJJRG/y9mA== Content-Type: image/svg+xml Date: Thu, 30 Jun 2022 20:52:03 GMT Etag: 0x8D7B007297AE131 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (muc/3327) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: f043b268-b01e-0016-2336-f2876c000000 x-ms-version: 2009-09-19 Content-Length: 1864 Connection: close
2022-06-30 20:52:03 UTC	665	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 39 32 30 22 20 68 65 69 67 68 74 3d 22 31 30 38 30 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 3e 3c 67 20 6f 70 61 63 69 74 79 3d 22 2e 32 22 20 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 45 29 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 36 36 2e 34 20 31 37 39 35 2e 32 63 39 35 30 2e 33 37 20 30 20 31 37 32 30 2e 38 2d 36 32 37 2e 35 32 20 31 37 32 30 2e 38 2d 31 34 30 31 2e 36 53 32 34 31 36 2e 37 37 2d 31 30 30 38 20 31 34 36 36 2e 34 2d 31 30 30 38 2d 32 35 34 2e 34 2d 33 38 30 2e 34 38 32 2d 32 35 34 2e 34 20 33 39 33 2e 36 73 37 37 30 2e 34 32 38 20 31 34 30 31 2e 36 20 31 37 32 30 2e 38 20 31 34 30 31 2e 36 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6

Statistics

Behavior

● chrome.exe



System Behavior

Analysis Process: chrome.exe PID: **5056**, Parent PID: **3600**

General

Target ID:	0
Start time:	22:51:58
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 "C:\Users\user\Desktop\lmax_SUMMARY.html
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Copyright Joe Security LLC 2022

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	7FF7964FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **3964**, Parent PID: **5056**

General

Target ID:	1
Start time:	22:52:00
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=1588,11292151676533456628,2741544286314243644,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Copyright Joe Security LLC 2022