

ID: 626160
Sample Name:
Markham_remittance71792.html
Cookbook: default.jbs
Time: 16:52:50
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Markham_remittance71792.html 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Yara Signatures 5
HTML 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
Phishing 6
System Summary 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 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 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\37ebb356-1366-4ac9-b9a5-4f155eac2e21.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\4279688c-ccf2-4a52-96e3-28436d78710e.tmp 13
C:\Users\user\AppData\Local\Google\Chrome\User Data\433f349a-f7ce-4d23-9c1c-3f1fa02c644e.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\887a3d81-e417-4014-83b7-f8087fd7a485.tmp 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0496899f-cd98-4d2f-9b3b-e3603b01bf18.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\11e98cfa-321d-41f6-823f-fefa6ca37079.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\17d03284-fb89-4156-a1b7-3f4865b2b8ed.tmp 15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\267e8d7e-444d-499a-84c4-5289dd5ad774.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2828436a-ee9f-4735-a6ad-a02051102669.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp 16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31ea0c81-af9f-4b41-9e5c-b7c8d2cadda9.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40312678-bff8-4148-bcd2-aec63c9a2ebd.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\47c12e3a-fbf5-4753-9359-4b65fd8d3714.tmp 17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\54bfa4ad-47c3-4db3-b006-843b76ca3bf4.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85d19c0a-bca2-4b8b-9c8f-79b31e2aa9d9.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a31a281-cb7a-4212-9ea7-735ee4c55af3.tmp 18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG 19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1 21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy) 21

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\c5039d67-d38e-4985-b555-d03b10443522.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\38463f5c-f0ae-4961-b50e-b31b5bd37c0a.tmp 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy) 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a05a10cc-8075-4cd6-8f41-2deaa10cc9c1.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a3d9393e-36fb-4927-823e-50c67327139a.tmp 23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\befd7c60-6fb7-444e-a8dc-fc136b20ec59.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c9eb0dea-8c9b-47f9-8596-911f4768b7e9.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce7730a1-d52a-4a76-b1f9-df40c1420311.tmp 24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\eef68339-c70d-4d3d-beec-75dad9362ba2.tmp 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser 25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy) 26
C:\Users\user\AppData\Local\Google\Chrome\User Data\ab8decf5-124e-4475-98d9-7482911fcbac.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\ae15c89e-7c5b-4b52-8104-188ae82c9efa.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\b84d0014-63e2-4691-82e6-cb5324ea59b4.tmp 27
C:\Users\user\AppData\Local\Google\Chrome\User Data\c4bfec7f-f4f5-49bc-8146-3d6c32104213.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\df0d930c-be85-420f-b26b-87e2c24d5fa6.tmp 28
C:\Users\user\AppData\Local\Google\Chrome\User Data\ea7e5bfe-bdbb-410d-973a-176203aab36a.tmp 28
C:\Users\user\AppData\Local\Temp\7136_816727225_metadata\verified_contents.json 29
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_pnacl_json 29
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o 29
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o 30
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_crtend_o 30
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe 30
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a 31
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a 31
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a 31
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a 32
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 32
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe 32
C:\Users\user\AppData\Local\Temp\7136_816727225\manifest.fingerprint 33
C:\Users\user\AppData\Local\Temp\7136_816727225\manifest.json 33
C:\Users\user\AppData\Local\Temp\b3e55fe4-20c7-4d63-81d0-442d72ecb023.tmp 33
C:\Users\user\AppData\Local\Temp\e0dde7fa-2d92-4e6d-8669-76373e8b1211.tmp 33
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\bg\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\ca\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\cs\messages.json 34
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\da\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\de\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\el\messages.json 35
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\en\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\en_GB\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\es\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\es_419\messages.json 36
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\et\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\fi\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\fil\messages.json 37
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\fr\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\hi\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\hr\messages.json 38
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\hu\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\id\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\it\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\ja\messages.json 39
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\ko\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\lt\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\lv\messages.json 40
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\nb\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\nl\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\pl\messages.json 41
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\pt_BR\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\pt_PT\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\ro\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\ru\messages.json 42
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\sk\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\sl\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\sr\messages.json 43
C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\sv\messages.json 44
Static File Info 44
General 44
File Icon 44
Network Behavior 44
Network Port Distribution 44
TCP Packets 45

UDP Packets 47
DNS Queries 47
DNS Answers 48
HTTP Request Dependency Graph 49
HTTPS Proxied Packets 49
Statistics 59
Behavior 59
System Behavior 59
Analysis Process: chrome.exePID: 7136, Parent PID: 4128 59
General 59
File Activities 60
Registry Activities 60
Key Value Modified 60
Analysis Process: chrome.exePID: 4228, Parent PID: 7136 60
General 60
File Activities 60
Disassembly 61

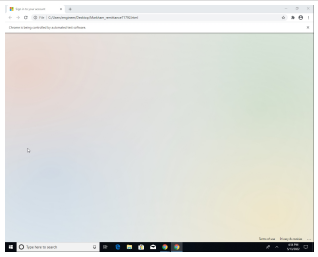
Windows Analysis Report

Markham_remittance71792.html

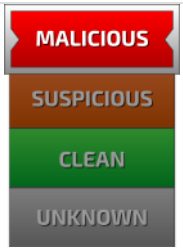
Overview

General Information

Sample Name:	Markham_remittance71792.html
Analysis ID:	626160
MD5:	fe3defd33424d60.
SHA1:	32e53b9fb508f8a.
SHA256:	82f0a546917da9..
Infos:	



Detection



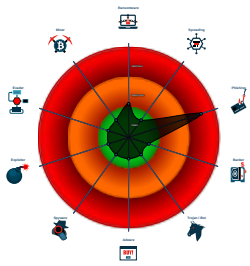
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- HTML document with suspicious na…
- Phishing site detected (based on im…
- None HTTPS page querying sensitiv…
- No HTML title found
- JA3 SSL client fingerprint seen in co…
- HTML body contains low number of …
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 7136 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\Markham_remittance71792.html MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4228 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,8452305244807070825,17752714670138375518,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

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

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

System Summary



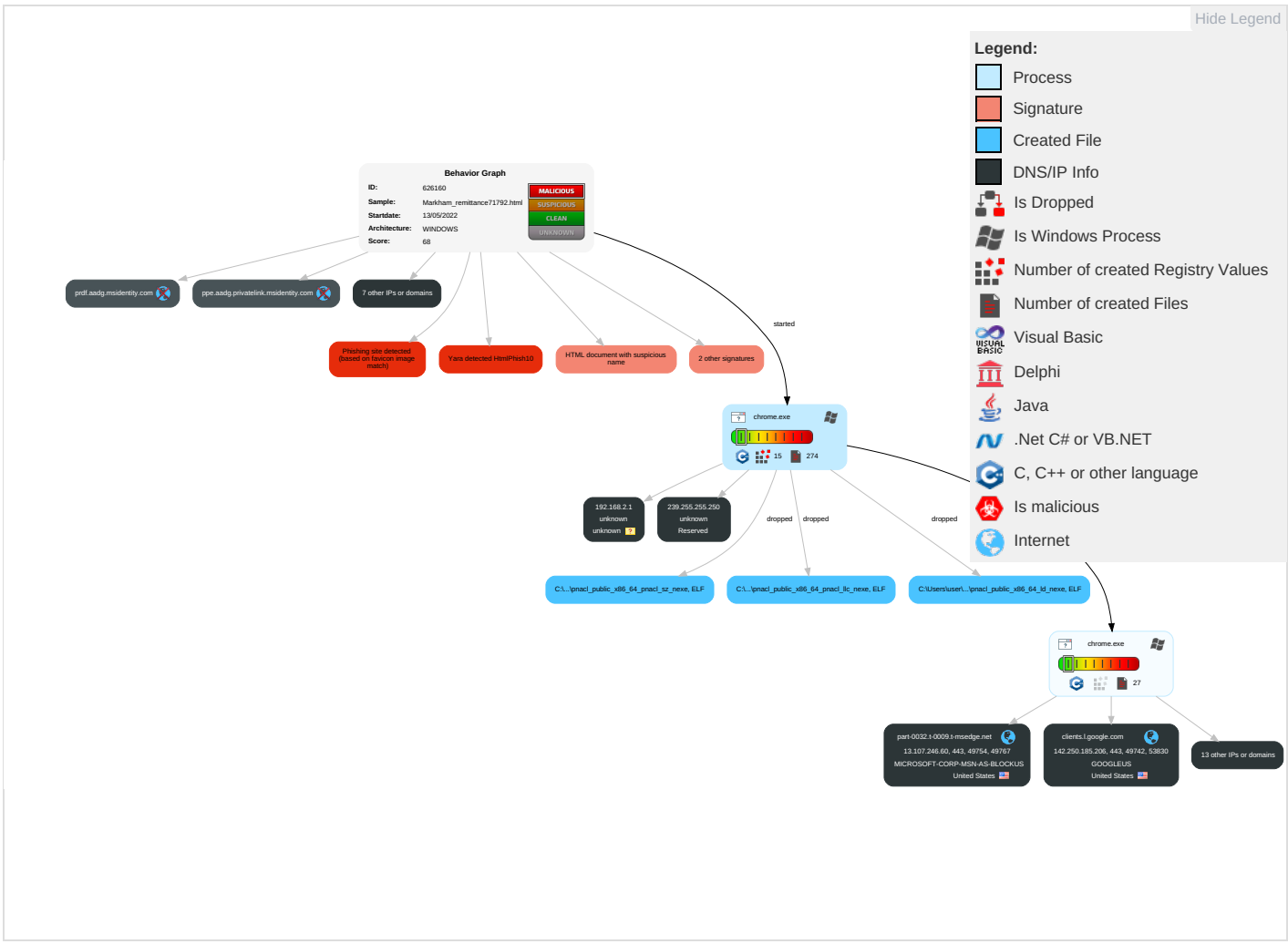
HTML document with suspicious title

HTML document with suspicious name

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	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

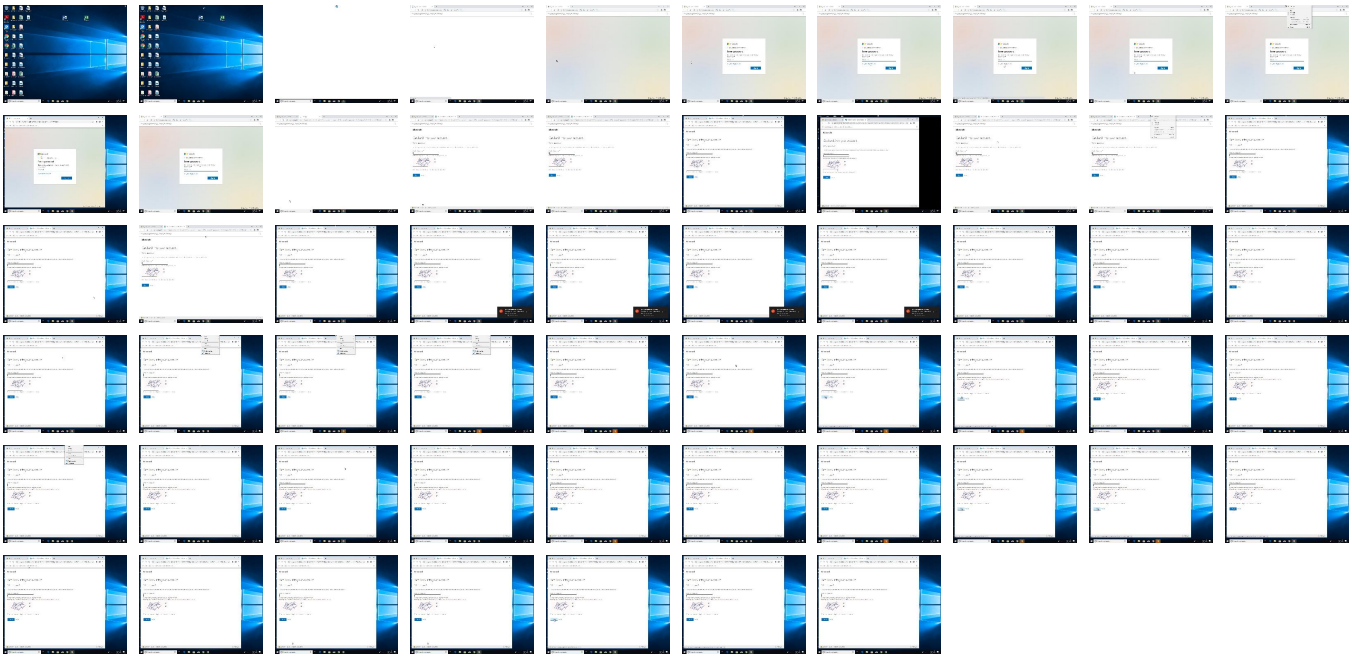
Behavior Graph

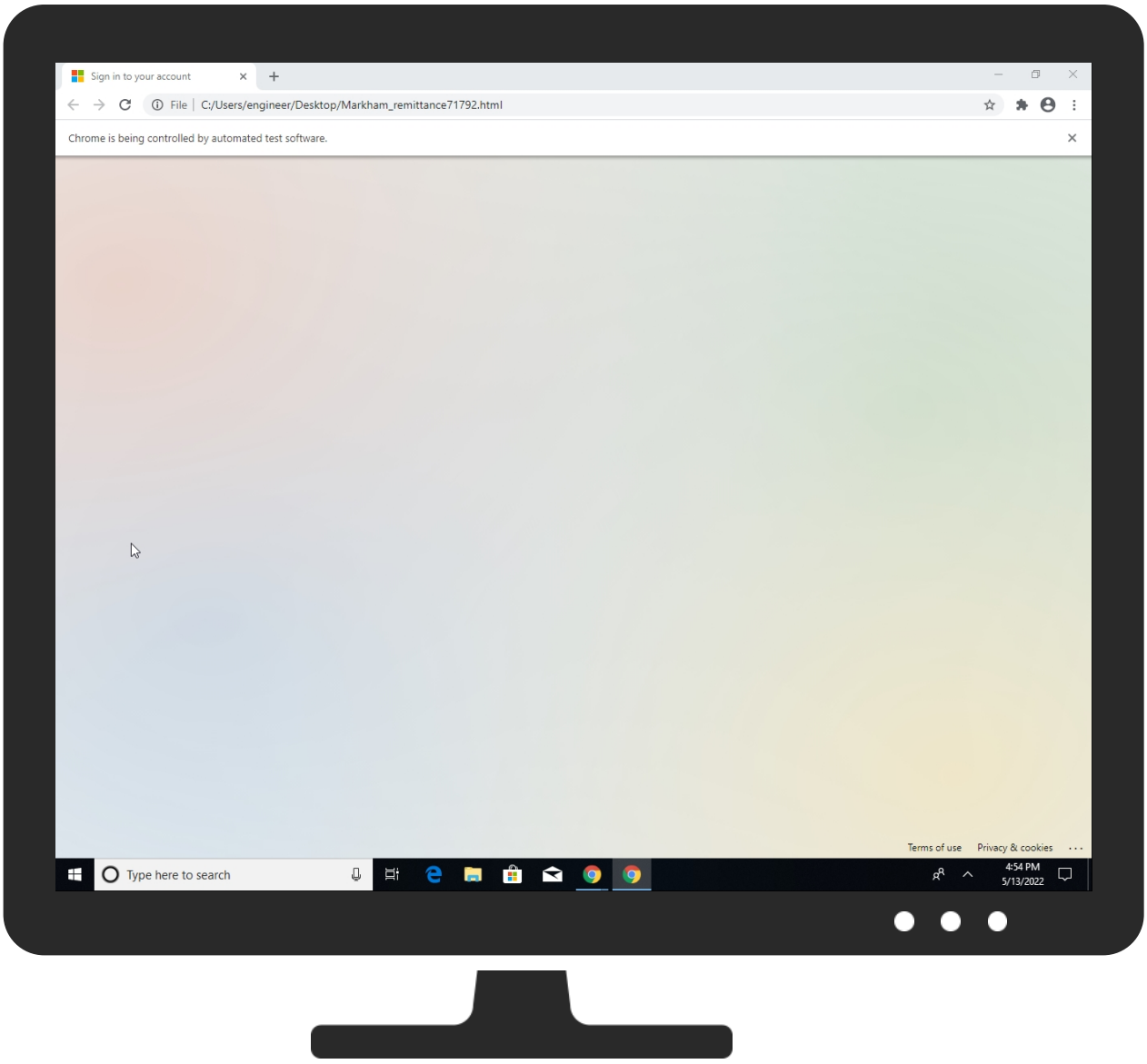


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Markham_remittance71792.html	7%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
part-0032.t-0009.t-msedge.net	0%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.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/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_szor2ujtsn_b-ik0b744ha2.js	0%	Virustotal		Browse
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_szor2ujtsn_b-ik0b744ha2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	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	142.250.186.77	true	false		high
part-0032.t-0009.t-msedge.net	13.107.246.60	true	false	• 0%, Virustotal, Browse	unknown
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.185.206	true	false		high
passwordreset.microsoftonline.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

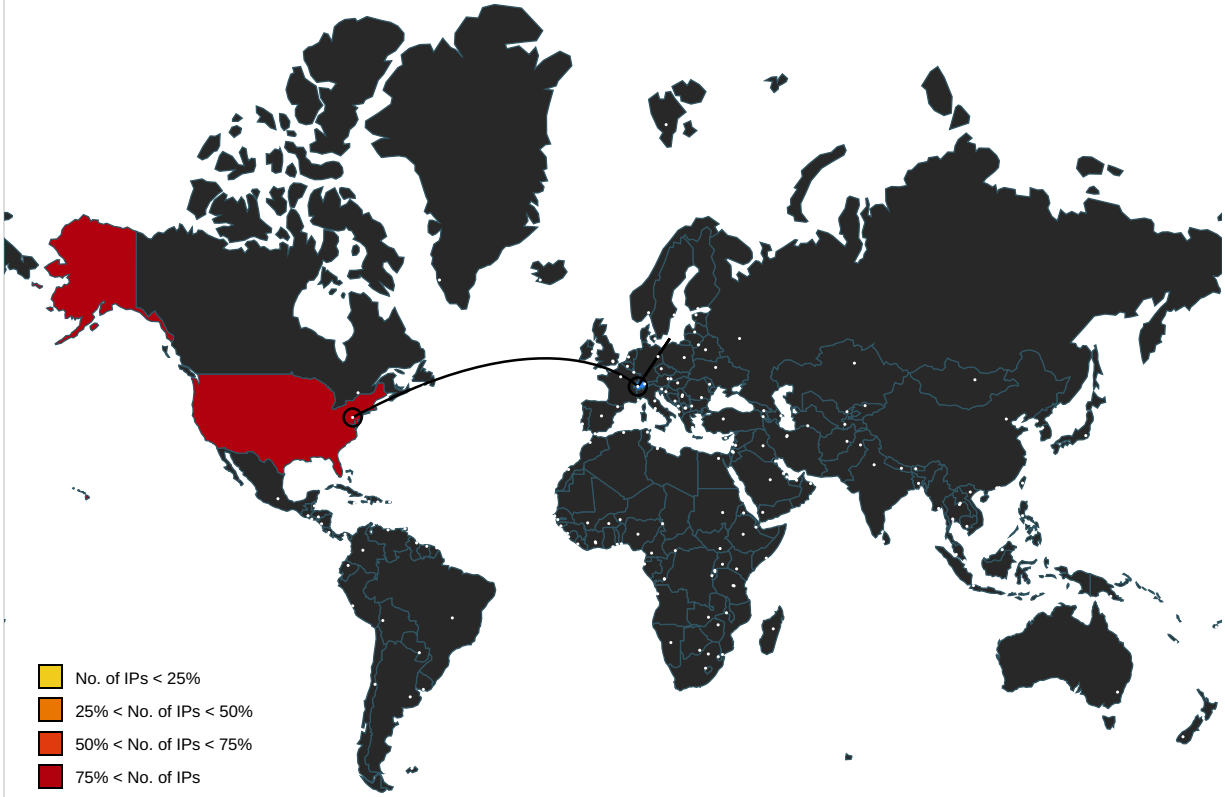
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Markham_remittance71792.html	true		low
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg	false	• URL Reputation: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwlT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBol5aflAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAYvvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uqOZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwIfgZzH_eiV3vvafOv8B0&mkt=en-GB&hosted=0&device_platform=Windows+10	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_szor2ujtsn_b-ik0b744ha2.js	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	38463f5c-f0ae-4961-b50e-b31b5bd37c0a.tmp.1.dr, 30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.tmp.1.dr, c5039d67-d38e-4985-b555-d03b10443522.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	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.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	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.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	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.tmp.1.dr	false		high
http://https://apis.google.com	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.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	30c72336-9917-4d7a-b81f-63e5d1d6225c.tmp.1.dr, 11e98cfa-321d-41f6-823f-fefa6ca37079.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json0.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
13.107.246.60	part-0032.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
142.250.186.77	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626160
Start date and time: 13/05/202216:52:50	2022-05-13 16:52:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Markham_remittance71792.html
Cookbook file name:	default.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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Copyright Joe Security LLC 2022

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.winHTML@26/121@8/8
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%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBol5aflAaJlBS qrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05 m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mV XuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqlTz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVo LOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAY vvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uq OZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwlfgZzH_eiV3vvafOv8B0&mkt=en-GB&hosted=0&device_platform=Windows+10

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.206, 69.16.175.10, 69.16.175.42, 173.194.160.71, 142.250.185.99, 173.194.160.72, 40.126.32.66, 40.126.32.129, 40.126.32.6, 40.126.32.131, 152.199.19.160, 20.190.159.16, 172.217.16.138, 142.250.186.163, 142.250.185.195, 74.125.108.199
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, cds.s5x3j6q5.hwcdn.net, r2.sn-1gi7znek.gvt1.com, clientservices.googleapis.com, arc.msn.com, www.ppetm.aadg.akadns.net, r3---sn-1gi7znes.gvt1.com, mscomajax.vo.msecnd.net, redirector.gvt1.com, login.live.com, r2.sn-1gi7znes.gvt1.com, update.googleapis.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, www.ppetm.aadg.trafficmanager.net, client.ppe.repmap.microsoft.com, client.wns.windows.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, cs22.wpc.v0cdn.net, www.tm.f.prd.aadg.akadns.net, lgincdnvzeuno.ec.azureedge.net, aadcdn.msauth.net, r2---sn-1gi7znek.gvt1.com, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, r2---sn-1gi7znes.gvt1.com, www.tm.f.prd.aadg.trafficmanager.net, store-images.s-microsoft.com, lgincdn.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, r3.sn-1gi7znes.gvt1.com
- 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:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	high, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\37ebb356-1366-4ac9-b9a5-4f155eac2e21.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):	407439
Entropy (8bit):	6.047101758556116
Encrypted:	false
SSDEEP:	6144:CssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Csh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	39FE554D1FE189B154F2CD657FF9FBE0
SHA1:	C855D6A3464939665666000919 9FCEB244FA6262
SHA-256:	F861CD558773FFE3208F5890186561FA8F319454342683FDB439EE4CFC7A1D1E
SHA-512:	3FFF4B2A723911198538EF3751E5F4F6D66B0E6A158244B7D101E48E7B835DF345872300A939DAEBAA8813D919EC649709698897B7C1635B892D410841EE5086
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4279688c-ccf2-4a52-96e3-28436d78710e.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):	407439
Entropy (8bit):	6.047102023365469
Encrypted:	false
SSDEEP:	6144:NssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Nsh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	1B3B93E47271BB4631CC3278EE7324DC
SHA1:	E9567AA7407AD0FC319A49C87FC1EE3BBC42E45B
SHA-256:	8E35A969BE3065222EF67D1F59C6674CF6E2E94552AA375514A14339B5D57E80
SHA-512:	C8AAC33FF9D687B1F678E6F5E76D7A44106E6636BCA1D369D48E61E7EA0494DB471875F000D5B430F18C524DD5207907B6863A8AC613F5CAFAFC45741838971
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\433f349a-f7ce-4d23-9c1c-3f1fa02c644e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7437878002958587
Encrypted:	false
SSDEEP:	384:h3tSK0vtQXgOVHZWJN6rfvum3FOwdHYNGxIrTwu8x9oEwHrP2mjATAK62pOokaNC:xG+5ZqIRJAenAKUov3m+KYm652
MD5:	68911738802B4B76C789C3160C6600CF
SHA1:	EEF9B05CD5EEB0F0614E98D187F5DAA310DC555D
SHA-256:	C813923D3D05977653D4B6E4B175D856C3B6181ACC9D7B7A4F91D1737F348A89
SHA-512:	85B35915E2DA2CACF857F6DCC1C6A2C05E0F1229AAE46CA5BE1B9E68C56C228792A8E3EAA504ADE1C6564DA905E5530945E8BABC88E7304388F8CE76D5AD1B9F
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\887a3d81-e417-4014-83b7-f8087fd7a485.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.743604743823655
Encrypted:	false
SSDEEP:	384:R3tSK0vtQXgOVHZWJN6rfvum3FOwdHYNGxIrTwu8x9oEwHrP2mjX9TAK62pOokax:BG+5ZqIsJAenAKUov3m+KYm65z
MD5:	34581C0BC33791ED0F213F2A49BC0AEF
SHA1:	9814829BDC0CDB20867649EDC059F81ADAF702FA
SHA-256:	9CA9BD2895B044A9D2D8AD84BC49282C0A23F9FBF0D205F9A4B3FAA6C3ABBBDA
SHA-512:	7C6B15047D338CE21B4D7DF6D251A24E3ABCF1E9843A18035FA1D35DCA12529A44CC0D2CB8C08981E9B69172B2CDF28DFB603313200F49BFB1C022FA41D880B
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\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:FkXEwozZHn:+EwozZHn
MD5:	BEBB369FF4A565B19D5E0BC83CD176AE
SHA1:	A6F07666F8DDDF61E5AACE533129BFB541A8A769
SHA-256:	8018F98553432706436A31FFD1E743018C3B7F1AA8D34B2FA18F494A4CFCEB19
SHA-512:	5D2F9F6E9502517AFF4673C3157D57046D4E38D70B5E228F468FB820363E559087D1A2F2E4006B4589BF3F175A4507F1FA3D7BE5FC34F9FA39EB17757DAEC17F
Malicious:	false
Preview:	sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0496899f-cd98-4d2f-9b3b-e3603b01bf18.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):	4936
Entropy (8bit):	4.952920716406454
Encrypted:	false
SSDEEP:	48:YczUklSyklX6gctqAxiqTlYD1lQKHoTw0r/ad8C1Nfct/9BhUJo3KhmeSnpNGzsa:nzXbXcO1paAKIQxk0JCKL8robOTQVuwn
MD5:	23AB93E9403E41810538D2F9918064C3
SHA1:	6BDA68776FB171B1FCDB35EECD161C1C382F050B
SHA-256:	22722F61B9444BFFD2EDD58D10A175F5777F564B4A11CF01838000A248223D5D
SHA-512:	8E33D0DEAD4AFD7B56F125240B69428EBDFFE88B27EC8D33963EF055C15589193F5C1CC39AD228FDD1CDC8349B84C9A8E817FDB4C6277A5230A2A36719891E A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","

Encrypted:	false
SSDEEP:	48:YczUklSyklX6gctqAxiqTlYD1lQKHoTw0r/ad8C1Nfct/9BhUJo3KhmeSnpNGzsa:nzXbXcO1paAKlQxk0JCKL8robOTQVuwn
MD5:	23AB93E9403E41810538D2F9918064C3
SHA1:	6BDA68776FB171B1FCDB35EECD161C1C382F050B
SHA-256:	22722F61B9444BFFD2EDD58D10A175F5777F564B4A11CF01838000A248223D5D
SHA-512:	8E33D0DEAD4AFD7B56F125240B69428EBDFFE88B27EC8D33963EF055C15589193F5C1CC39AD228FDD1CDC8349B84C9A8E817FDB4C6277A5230A2A36719891E A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","

SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31ea0c81-af9f-4b41-9e5c-b7c8d2cadda9.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):	4963
Entropy (8bit):	4.958125917521853
Encrypted:	false
SSDEEP:	48:YczUklSyklX6gcebBqAxiqTlYD1lQKHoTw0r/ad8C1Nfct/9BhUJo3KhmeSnpNGf:nzXbXLO1paAKIQxk0JCKL8rGbOTQVuwn
MD5:	ECA2F63E1FE53F5AA4CD82A09DFF10F2
SHA1:	4E0954A6759113EE3245E09BF80B0260CCFB0DCD
SHA-256:	E65A102FB9E77F70F774B586136265B98A7570F21A75A45ACD32F7C88A4109E0
SHA-512:	44A0D0D953B82498C965D2D62FA5A33254C915E0E0DE196E4A2BB01A70F29FFA8661341DA99A0FABF718A80A3FEF32F62B6E6BC9369FCFC57E7153097A2C7D7C
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","

SHA1:	871866790D9F5DBE76CDA0B696350BFD5685E012
SHA-256:	D61C547DBDE5870CB58D57851411FB9BD938DB2711CF5D9AAE2799110547B611
SHA-512:	BC5570EB0DEFC959BC25721E1B0E5112DB9C2B927332B978A7720C7CD13E91E2E8E4C1C14CB8D4EE1BBCD0225EC14D099ECE8B61AB10C581C3C8B0EFB1053F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

SHA-256:	D61C547DBDE5870CB58D57851411FB9BD938DB2711CF5D9AAE2799110547B611
SHA-512:	BC5570EB0DEFC959BC25721E1B0E5112DB9C2B927332B978A7720C7CD13E91E2E8E4C1C14CB8D4EE1BBCD0225EC14D099ECE8B61AB10C581C3C8B0EFB1053F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

Preview:	2022/05/13-16:54:32.377 1c2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/13-16:54:32.378 1c2c Recovering log #3.2022/05/13-16:54:32.379 1c2c 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):	378
Entropy (8bit):	5.247778683488692
Encrypted:	false
SSDEEP:	6:AFl4bQ+q2PN723iKKdK25+Xqx8chI+IFUtqVfFl1BgZmwYVfFl24SQVkwON723ib:Ajt+vVa5KkTXfchI3FUtijE/Ij2UV5Op
MD5:	5AEBB64D623681B742E71D5620ED77D2
SHA1:	69250F34BF40F9DBFC948011895973C4763CD12B
SHA-256:	45D86BF64F57712AE0DE33C9CAFD026815992CC13B382D3B76AA00FA75684C26
SHA-512:	8F8869C88E1E0CB33EE0A9937E08B8006348A7ED0A844FFA48F463DC03D67124361F7D502AE70FDB64A641E56FA0CBBF3B39416B8ABE05C626908E76CE3F0333
Malicious:	false
Preview:	2022/05/13-16:54:32.377 1c2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/13-16:54:32.378 1c2c Recovering log #3.2022/05/13-16:54:32.379 1c2c 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):	788
Entropy (8bit):	5.249290001859071
Encrypted:	false
SSDEEP:	24:4seKJJgRbvArohsWNDcq8jDY78BJgskfa9yBDOBfaQt9iB0Y81:4srJJksmHFF8jHU62k1
MD5:	548A26C149F42DD06A460DAFFB9EF33D
SHA1:	49EFD6CADB2BA6945E781944A1F3A482E85B2D19
SHA-256:	66D0DBEE3A75DBE072FC9AFFDA1180B7F0C31257BFC5F109AC28966429DBEEF2
SHA-512:	9DBB528CFD34E6FD7AE8D11718379F266B34B2B0438538E01D8C5028D34B0FC4B3FFCE5B44E69ED39CEC1EBB4E8933269A4B2609E348C65E0E325F90EFD378A
Malicious:	false
Preview:	......"b....account..c..desktop..user..file..html..in..markham..remittance71792..sign..to..users..your*.....account.....c.....desktop.....user.....file.....html.....in.....markham.....remittance71792.....sign.....to.....users.....your..2.....1.....2.....7.....9.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....y...:w.....B}...y..... .....*>file:///C:/Users/user/Desktop/Markham_remittance71792.html2.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):	2147
Entropy (8bit):	4.8957316282209655
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qyvTCXDHz5sSBGsSxRLsSvStssST5sS9MHrYhbG:2lNnOa+TCXDHz5BoxxqtGT59GshS
MD5:	0D5306978243185A2D99CB38707EC714
SHA1:	F712CDEF46A912CC9C7116C66B6D810E4F1F6611
SHA-256:	803CC6EDBA78ECC2914B89F83E0E6997802862845311343FF6C3DAB054A0EDF6
SHA-512:	09382EB6A9226FB73ADC9FD84EAF67F148572EA94991A9B057519A794A0798E72CF32EB2AE59A1AA01EC4C5D481449AAAA1A250A2397DFA84575A7B5F08F4BDB
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"

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):	5244
Entropy (8bit):	4.985037885820804
Encrypted:	false
SSDEEP:	96:nzXbOCO1paAKIQxk0JCKL8AgsQklXRSbOTQVuwn:nzXbA1p9q4K+klBo
MD5:	6E9E254DACB5B78DAF7E8B0774BAD54B
SHA1:	4A14E2061966BF51EEF1F7FA95A93EF48F587F30
SHA-256:	1F3DA196267AE1FA49D3DDBEDBFA8B506080F9A6B576535AFB27178537BDF285
SHA-512:	D33BAC0B3CE0CC076E51191D13BC97F73014D7AD3C9A5034C1465DCF04BDB342BCE76A294E401D4ADD57888A2266644ED6C67D229783E1EB7BF0ECBCF3A5E CB0
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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\c5039d67-d38e-4985-b555-d03b10443522.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):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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\38463f5c-f0ae-4961-b50e-b31b5bd37c0a.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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E40653950
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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\a05a10cc-8075-4cd6-8f41-2deaa10cc9c1.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):	5244
Entropy (8bit):	4.985827312732892
Encrypted:	false
SSDEEP:	96:nzXbOCO1paAKIQxk0JCKL8AgspkthjGbOTQVuwn:nzXbA1p9q4K/ktB0
MD5:	9E2C42D4924530F808365C784FF62274
SHA1:	1DFA59E78A577D2643D3515F6A7A8F4FCC6B36BB
SHA-256:	BC374B471B2FC5198D6DA2CEDDD616EF198611AC48041232748313DA59A54177
SHA-512:	606FE9A5132940041B2F7EB5291A3BEAC2D4EDD163D2441B63CA38EF958EA0B1EADCE37A2D16ACDE4005FC533E83B556A1950FEB59665B83D5D2B470531B181E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","

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":"13296959649141377","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\befd7c60-6fb7-444e-a8dc-fc136b20ec59.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19792
Entropy (8bit):	5.564194169382681
Encrypted:	false
SSDEEP:	384:Mz4tiLl4eX91kXqKf/pUZNCgVLH2HfDVrUYHGRO9ilB4Lt:WLlx91kXqKf/pUZNCgVLH2HfprUMGCia
MD5:	7E280A6B1C086998B9CB9DD0EBB7E908
SHA1:	B017A6A4C492DD159427EFF813C39ACA4236BBE1
SHA-256:	BFC352EEA8FC5EBA0CFE69DAB59C5A79893EB115C52289F533C6E2E4FA367EAE
SHA-512:	34E40C051A13B45412D22CEB7692CABA828EE53F4E02E07029D1FE3152D1508D6978F7054CA0F4CF1461F144932CEDC15B9E8CB0DB565A96D8455883093AC5C
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":"13296959649141377","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\c9eb0dea-8c9b-47f9-8596-911f4768b7e9.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):	5244
Entropy (8bit):	4.985827312732892
Encrypted:	false
SSDEEP:	96:nzXbOCO1paAKIQxk0JCKL8AgspkthjGbOTQVuwn:nzXbA1p9q4K/ktB0
MD5:	9E2C42D4924530F808365C784FF62274
SHA1:	1DFA59E78A577D2643D3515F6A7A8F4FCC6B36BB
SHA-256:	BC374B471B2FC5198D6DA2CEDDD616EF198611AC48041232748313DA59A54177
SHA-512:	606FE9A5132940041B2F7EB5291A3BEAC2D4EDD163D2441B63CA38EF958EA0B1EADCE37A2D16ACDE4005FC533E83B556A1950FEB59665B83D5D2B470531B181E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

Preview:	.

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\Default\eef68339-c70d-4d3d-beec-75dad9362ba2.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):	4964
Entropy (8bit):	4.958375952471822
Encrypted:	false
SSDEEP:	48:YczUklSykSX6gcebBqAxiqTlYD1lQKHoTw0r/ad8C1Nfct/9BhUJo3KhmeSnpNGf:nzXbOLO1paAKIQxk0JCKL8rGbOTQVuwn
MD5:	63CFE50F3A4867D7AE59E1F627C03CF4
SHA1:	871866790D9F5DBE76CDA0B696350BFD5685E012
SHA-256:	D61C547DBDE5870CB58D57851411FB9BD938DB2711CF5D9AAE2799110547B611
SHA-512:	BC5570EB0DEFC959BC25721E1B0E5112DB9C2B927332B978A7720C7CD13E91E2E8E4C1C14CB8D4EE1BBCD0225EC14D099ECE8B61AB10C581C3C8B0EFB105 3F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296959650108127","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"c ountryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl: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):	399051
Entropy (8bit):	6.026856721087679
Encrypted:	false
SSDEEP:	6144:dssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:dsh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	B192F46F578674C1B6C8F2AB2FEDAF93
SHA1:	44D8FFE2AFC0A4D9B403EB16115DF41766B1103E
SHA-256:	03B72D4F875D3A911421EF1799E7D10B3E9F83173ABB012F1C8A8081A2436176
SHA-512:	4FA24EB75FB83106AF721793411132B52DF0BC86892265094AE7CB879332B56B92A1E7FC8F9DE29F5CA1A740E98D5E286CCA63333326678897E63891941ABF90
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.743604743823655
Encrypted:	false
SSDEEP:	384:R3tSK0vtQXgOVHZWJN6rfvum3FOwdHYNGxIrTwu8x9oEwHrP2mjX9TAK62pOokax:BG+5ZqIsJAenAKUov3m+KYm65z
MD5:	34581C0BC33791ED0F213F2A49BC0AEF
SHA1:	9814829BDC0CDB20867649EDC059F81ADAF702FA
SHA-256:	9CA9BD2895B044A9D2D8AD84BC49282C0A23F9FBF0D205F9A4B3FAA6C3ABBBDA
SHA-512:	7C6B15047D338CE21B4D7DF6D251A24E3ABCF1E9843A18035FA1D35DCA12529A44CC0D2CB8C08981E9B69172B2CDF28DFB603313200F49BFB1C022FA41D880B
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\ab8decf5-124e-4475-98d9-7482911fcbac.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):	407439
Entropy (8bit):	6.0471013753448375
Encrypted:	false
SSDEEP:	6144:AssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Ash3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	8922544F44EAB13727D5D7CD5F86A748
SHA1:	3E759957EE509997B5B9D351F9C233E2D0468010
SHA-256:	7C196CFF48B6503EB6D9867AEA33DCB5ABF949FB4BE88321D2FEF0991FF392B4
SHA-512:	1BAE04F3BEBD89FB9E0C0610367222A1548F3DDF9711696F77CBE33B603A9E1D024BCC5930753218525F84879948343ED2BDB1CAC822F0927B7C6C40A360F7F
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ae15c89e-7c5b-4b52-8104-188ae82c9efa.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):	398957
Entropy (8bit):	6.026687297767612
Encrypted:	false
SSDEEP:	6144:KssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Ksh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	7CFDC20145EFD8D7EB84BF5EA5A7E871
SHA1:	DF129662B546180BCE32F181F81459D3952741DB
SHA-256:	1ABC29CC04AC317D35EA12FEAE87245B39366A828B5EF39523BBFAA1EFDC44BA
SHA-512:	26B1DB2A43D88CD8BE79D83C4F7FEA5107D0D2D49CA88EF96A2A9689D3FDD263B48D94CB1BD087ED8A186EF2720E10EAC80FDA4D844B8556E7B47A3F2A96A8EA
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\b84d0014-63e2-4691-82e6-cb5324ea59b4.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):	398957
Entropy (8bit):	6.026687297767612
Encrypted:	false
SSDEEP:	6144:KssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Ksh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	7CFDC20145EFD8D7EB84BF5EA5A7E871
SHA1:	DF129662B546180BCE32F181F81459D3952741DB
SHA-256:	1ABC29CC04AC317D35EA12FEAE87245B39366A828B5EF39523BBFAA1EFDC44BA
SHA-512:	26B1DB2A43D88CD8BE79D83C4F7FEA5107D0D2D49CA88EF96A2A9689D3FDD263B48D94CB1BD087ED8A186EF2720E10EAC80FDA4D844B8556E7B47A3F2A96A8EA
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\c4bfec7f-f4f5-49bc-8146-3d6c32104213.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):	398957
Entropy (8bit):	6.026687129164415
Encrypted:	false
SSDEEP:	6144:1ssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:1sh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	34E9C8823BFA91A93ABD3E55BAF6DC6F
SHA1:	AE04406288617CECE55413BBEFC49A4403C673BB
SHA-256:	4EF3E2CAF0CFE848284C232CB58E0B634883BFC77D9B48BF514DEEAC625CF488
SHA-512:	1D1457322815D3DA42512B14F98A296630A69ECABA3F81AD29F6E47BD351AC5953AD1C45682E485EA791D59853466D2F7B63E4CD979A648E5139BF33E3840589
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\df0d930c-be85-420f-b26b-87e2c24d5fa6.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):	399051
Entropy (8bit):	6.026856721087679
Encrypted:	false
SSDEEP:	6144:dssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:dsh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	B192F46F578674C1B6C8F2AB2FEDAF93
SHA1:	44D8FFE2AFC0A4D9B403EB16115DF41766B1103E
SHA-256:	03B72D4F875D3A911421EF1799E7D10B3E9F83173ABB012F1C8A8081A2436176
SHA-512:	4FA24EB75FB83106AF721793411132B52DF0BC86892265094AE7CB879332B56B92A1E7FC8F9DE29F5CA1A740E98D5E286CCA633333266788897E63891941ABF90
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230364634526"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ea7e5bfe-bdbb-410d-973a-176203aab36a.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):	407439
Entropy (8bit):	6.047101758556116
Encrypted:	false
SSDEEP:	6144:CssvoWpYtR9rOKeSMyI92G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinS:Csh3XSJShrGNPUZ+w7wJHyEtAWL
MD5:	39FE554D1FE189B154F2CD657FF9FBE0
SHA1:	C855D6A3464939665660009199FCEB244FA6262
SHA-256:	F861CD558773FFE3208F5890186561FA8F319454342683FDB439EE4CFC7A1D1E
SHA-512:	3FFF4B2A723911198538EF3751E5F4F6D66B0E6A158244B7D101E48E7B835DF345872300A939DAEBAA8813D919EC6497096988897B7C1635B892D410841EE5086
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652486051895305e+12,"network":1.652453654e+12,"ticks":181856995.0,"uncertainty":4394892.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\7136_816727225_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":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19waWdnaWVkZWxfcGF0aC5wYXRoI

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\7136_816727225_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 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\7136_816727225_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.....!..... ....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\7136_816727225_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:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 96
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • 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\7136_816727225_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:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A63 4E
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`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.n acl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4 xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@. A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\7136_816727225_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:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
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.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false

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\7136_816727225_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
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\7136_816727225_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...J...G..`I..

C:\Users\user\AppData\Local\Temp\7136_816727225_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\7136_816727225\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\7136_816727225\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\b3e55fe4-20c7-4d63-81d0-442d72ecb023.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\e0dde7fa-2d92-4e6d-8669-76373e8b1211.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770 0C
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_dir7136_1905944538\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CI B4
Malicious:	false
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_dir7136_1905944538\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_dir7136_1905944538\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_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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_dir7136_1905944538\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
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_dir7136_1905944538\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
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_dir7136_1905944538\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
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_dir7136_1905944538\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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 comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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 r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 12
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_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 co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
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_dir7136_1905944538\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_dir7136_1905944538\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_dir7136_1905944538\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+WYpU344Hlx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU: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".. },.. "craw_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 completed.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
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_dir7136_1905944538\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59D
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC09D
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir7136_1905944538\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_dir7136_1905944538\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.".. }..}..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	2.892921658564605
TrID:	
File name:	Markham_remittance71792.html
File size:	221056
MD5:	fe3defd33424d60e303716f443d24070
SHA1:	32e53b9fb508f8a1e3211a197aeaae8625caccd0
SHA256:	82f0a546917da921f6c1e70b4087a78f625a2c14a6de603448fe05e5eb76eda6
SHA512:	d6303079f4f5f5712e3a814bcf2a7fa709774700bf4667dba3ddf6524dc3108983194ca1dd032f6684501acaeab6ae9e5868d7bd99de121912ccff50edfba351
SSDEEP:	384:QnSM1SFhzMiZnSM1SFhzMiCBoWKpPkh3w2eL410GdO/5pwLCT6RuJ+f+S8c6oH92:2teW/s8
TLSH:	7E242FAF432F8D6ED43599048C35FD0D94B0AEB14A5BF1BAEB9738D4CBA91E04F40259
File Content Preview:	<script type='text/javascript'>document.write('\u003C\u0073\u0063\u0072\u0069\u0070\u0074\u003E\u000D\u0076\u0061\u0072\u0020\u005A\u0078\u0054\u0054\u0052\u0075\u0075\u0068\u0068\u0020\u003D\u0020\u0027dGxld2luYmVyZ0BtYXJraGFtLmNh\u0027\u003B\u000D\u0076

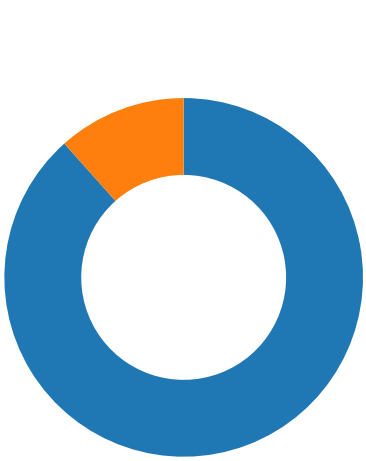
File Icon



Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:54:12.589010000 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:12.589042902 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:12.589123011 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:12.589394093 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.589416027 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.589478016 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.601423979 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:12.601450920 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:12.601680040 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.601696968 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.647145033 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:12.647181034 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:12.647257090 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:12.647633076 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:12.647645950 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:12.653641939 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.654201984 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.654256105 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.654762983 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.654834986 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.656146049 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:12.656204939 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:12.666559935 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:12.671961069 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:12.671989918 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:12.674315929 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:12.674422979 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:12.704435110 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:12.704972029 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:12.704993963 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:12.706844091 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:12.706953049 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:13.113910913 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:13.114073038 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:13.114581108 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:13.114602089 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:13.115406036 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:13.115668058 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.115701914 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.115813971 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.115959883 CEST	49744	443	192.168.2.6	142.250.186.77

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:54:13.115981102 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.116111040 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.116123915 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139295101 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139318943 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139539957 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.139590979 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139667034 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139700890 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.139862061 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139883995 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.139961958 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.139981031 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.140079975 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.147361040 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:13.147450924 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:13.147468090 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:13.147515059 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:13.149030924 CEST	49742	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:13.149068117 CEST	443	49742	142.250.185.206	192.168.2.6
May 13, 2022 16:54:13.156102896 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.156133890 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.156240940 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.156256914 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.156280994 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.156322956 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.156337976 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.156389952 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.156418085 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.157419920 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.157454014 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.157531023 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.157592058 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.157601118 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.157632113 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.157685041 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.157728910 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.168605089 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.168689013 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:13.168709993 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.168725967 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.168785095 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:13.173089981 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.173192024 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:13.173198938 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.173243046 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.189125061 CEST	49744	443	192.168.2.6	142.250.186.77
May 13, 2022 16:54:13.189150095 CEST	443	49744	142.250.186.77	192.168.2.6
May 13, 2022 16:54:13.225069046 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.230957031 CEST	49741	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:13.230995893 CEST	443	49741	152.199.23.37	192.168.2.6
May 13, 2022 16:54:14.004225016 CEST	49750	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:14.004307032 CEST	443	49750	152.199.23.37	192.168.2.6
May 13, 2022 16:54:14.004420996 CEST	49750	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:14.006865025 CEST	49751	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:14.006968021 CEST	443	49751	152.199.23.37	192.168.2.6
May 13, 2022 16:54:14.007077932 CEST	49751	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:14.010380983 CEST	49750	443	192.168.2.6	152.199.23.37
May 13, 2022 16:54:14.010420084 CEST	443	49750	152.199.23.37	192.168.2.6

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:54:12.536966085 CEST	61607	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:12.537982941 CEST	56550	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:12.539438009 CEST	52858	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:12.540575027 CEST	50029	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:12.557322025 CEST	53	61607	8.8.8.8	192.168.2.6
May 13, 2022 16:54:12.566458941 CEST	53	52858	8.8.8.8	192.168.2.6
May 13, 2022 16:54:12.568862915 CEST	53	50029	8.8.8.8	192.168.2.6
May 13, 2022 16:54:16.576579094 CEST	62643	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:16.597887993 CEST	53	62643	8.8.8.8	192.168.2.6
May 13, 2022 16:54:17.862430096 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:17.888613939 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.889334917 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:17.914954901 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.914994001 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.915019035 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.915055037 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.950047016 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:17.957449913 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:17.968894958 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:17.968934059 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.055109978 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.055414915 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.056869984 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.061125994 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.067222118 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.088148117 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.098089933 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.098118067 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.098134995 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.138510942 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.160581112 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.236193895 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.452019930 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.453125954 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.453198910 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:18.468791962 CEST	443	53830	142.250.185.206	192.168.2.6
May 13, 2022 16:54:18.536472082 CEST	53830	443	192.168.2.6	142.250.185.206
May 13, 2022 16:54:38.618551016 CEST	49520	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:39.007193089 CEST	65526	53	192.168.2.6	8.8.8.8
May 13, 2022 16:54:40.844736099 CEST	52125	53	192.168.2.6	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 16:54:12.536966085 CEST	192.168.2.6	8.8.8.8	0x2b01	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 13, 2022 16:54:12.537982941 CEST	192.168.2.6	8.8.8.8	0x7cd1	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 13, 2022 16:54:12.539438009 CEST	192.168.2.6	8.8.8.8	0x4072	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 13, 2022 16:54:12.540575027 CEST	192.168.2.6	8.8.8.8	0x4c4e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 13, 2022 16:54:16.576579094 CEST	192.168.2.6	8.8.8.8	0xe60a	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 13, 2022 16:54:38.618551016 CEST	192.168.2.6	8.8.8.8	0xc10	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)
May 13, 2022 16:54:39.007193089 CEST	192.168.2.6	8.8.8.8	0xcb48	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 16:54:40.844736099 CEST	192.168.2.6	8.8.8.8	0x44f3	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
May 13, 2022 16:54:12.557322025 CEST	8.8.8.8	192.168.2.6	0x2b01	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:12.557322025 CEST	8.8.8.8	192.168.2.6	0x2b01	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 13, 2022 16:54:12.557480097 CEST	8.8.8.8	192.168.2.6	0x7cd1	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:12.566458941 CEST	8.8.8.8	192.168.2.6	0x4072	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:12.566458941 CEST	8.8.8.8	192.168.2.6	0x4072	No error (0)	clients.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)
May 13, 2022 16:54:12.568862915 CEST	8.8.8.8	192.168.2.6	0x4c4e	No error (0)	accounts.google.com		142.250.186.77	A (IP address)	IN (0x0001)
May 13, 2022 16:54:14.025681019 CEST	8.8.8.8	192.168.2.6	0x92dc	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 13, 2022 16:54:14.040992975 CEST	8.8.8.8	192.168.2.6	0x537a	No error (0)	dual.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:14.040992975 CEST	8.8.8.8	192.168.2.6	0x537a	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)
May 13, 2022 16:54:14.040992975 CEST	8.8.8.8	192.168.2.6	0x537a	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)
May 13, 2022 16:54:16.597887993 CEST	8.8.8.8	192.168.2.6	0xe60a	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:16.597887993 CEST	8.8.8.8	192.168.2.6	0xe60a	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 13, 2022 16:54:16.707976103 CEST	8.8.8.8	192.168.2.6	0xd81b	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 13, 2022 16:54:16.732816935 CEST	8.8.8.8	192.168.2.6	0x51c4	No error (0)	dual.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:16.732816935 CEST	8.8.8.8	192.168.2.6	0x51c4	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)
May 13, 2022 16:54:16.732816935 CEST	8.8.8.8	192.168.2.6	0x51c4	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)
May 13, 2022 16:54:38.641088963 CEST	8.8.8.8	192.168.2.6	0xc10	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:38.641088963 CEST	8.8.8.8	192.168.2.6	0xc10	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:38.641088963 CEST	8.8.8.8	192.168.2.6	0xc10	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:39.030081987 CEST	8.8.8.8	192.168.2.6	0xcb48	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:39.376394033 CEST	8.8.8.8	192.168.2.6	0xe4a5	No error (0)	ppe.aadg.privatelink.msidentity.com	www.ppetm.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:40.872279882 CEST	8.8.8.8	192.168.2.6	0x44f3	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:40.872279882 CEST	8.8.8.8	192.168.2.6	0x44f3	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:54:40.872279882 CEST	8.8.8.8	192.168.2.6	0x44f3	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 16:54:40.993489027 CEST	8.8.8.8	192.168.2.6	0xdd86	No error (0)	ppe.aadg.privatelink.msidentity.com	www.ppetm.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- aadcdn.msftauth.net
- logincdn.msauth.net
- aadcdn.msauth.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49742	142.250.185.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:13 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-13 14:54:13 UTC	34	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-Ug4vaL02fz9tt6aKPAnNzg' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 13 May 2022 14:54:13 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5611 X-Daystart: 28453 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-13 14:54:13 UTC	35	IN	Data Raw: 33 36 64 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 31 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 38 34 35 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: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5611" elapsed_seconds="28453"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:13 UTC	35	IN	Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-05-13 14:54:13 UTC	36	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49744	142.250.186.77	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:13 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-13 14:54:13 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-05-13 14:54:13 UTC	100	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 13 May 2022 14:54:13 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-S4_5ioThHL6ZCQz0Qu7y6Q' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-S4_5ioThHL6ZCQz0Qu7y6Q' '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 Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-13 14:54:13 UTC	101	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",[]]
2022-05-13 14:54:13 UTC	101	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49765	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:16 UTC	180	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
2022-05-13 14:54:16 UTC	184	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: 26393293 Cache-Control: public, max-age=31536000 Content-MD5: DhdidjYrlCeaRJJRG/y9mA== Content-Type: image/svg+xml Date: Fri, 13 May 2022 14:54:16 GMT Etag: 0x8D7B007297AE131 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (frc/8FE5) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000 x-ms-version: 2009-09-19 Content-Length: 1864 Connection: close
2022-05-13 14:54:16 UTC	185	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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49767	13.107.246.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:16 UTC	204	OUT	GET /ests/2.1/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.msauth.net
2022-05-13 14:54:16 UTC	204	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=604800 Content-Length: 276 Content-Type: image/svg+xml Content-Encoding: gzip Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Last-Modified: Fri, 02 Nov 2018 20:25:09 GMT ETag: 0x8D64101494758DF Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 91d75960-a01e-0035-2365-659168000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0qxV9YgAAAABqhbpDd2g0R40wVAcDbpTNQU1TMDRFREdFMTkxMAAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= X-Azure-Ref: 0GHF+YgAAAADe1sV6HTWpT6uH9AmIwbPvRlJBMzFFREdFMDkxNwAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= Date: Fri, 13 May 2022 14:54:16 GMT Connection: close
2022-05-13 14:54:16 UTC	205	IN	Data Raw: 1f 8b 08 00 00 00 00 00 04 00 95 51 3d 6f c3 20 10 fd 2b 88 ae e6 e0 08 d8 b8 b2 3d 74 ca 90 ae 1d ba 45 8a 6b 5b 22 1f aa 91 c9 cf 2f 67 3b 6e 87 2c 15 f0 80 bb 7b ef 9e a0 1a a7 8e dd cf fe 32 d6 bc 0f e1 f6 2a 65 8c 11 e2 0e ae df 9d d4 4a 29 99 2a 38 8b c3 29 f4 35 d7 86 b3 be 1d ba 3e 2c e7 69 68 e3 db f5 5e 73 c5 14 d3 26 4d de 54 61 08 be 6d 8e e3 d8 86 b1 92 cb ad ba 1d 43 cf 4e 35 7f 47 97 21 82 2d dc 04 ce 98 7d 01 39 16 7e 07 a5 c6 8c d0 09 b0 a5 a1 75 c8 33 d4 de 40 69 8c 98 71 4b cc 9c 55 e5 93 b3 af c1 fb 9a bf 18 45 83 cb bf bd 14 f1 b2 02 94 cd fd 53 fa 1e ff ef e3 ac 04 a0 41 01 aa c0 b4 0e 36 95 97 a4 47 9b 05 67 1d 11 d6 2c 66 33 67 c1 35 46 1b b1 49 9d da d8 47 40 3c 0e 98 4c 2e 3a 60 b5 4e 26 01 3f 52 03 93 0c cf 89 64 b4 b0 28 08 37 Data Ascii: Q=o +=tEk["/g;n,{2*eJ)*8)5>,ih^s&MTamCN5G!-}9~u3@iqKUESA6Gg,f3g5FIG@<L.:`N&?Rd(7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49777	192.229.221.185	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:27 UTC	206	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: logincdn.msauth.net If-Modified-Since: Wed, 22 Jan 2020 00:32:50 GMT If-None-Match: 0x8D79ED29CF0C29A
2022-05-13 14:54:27 UTC	206	IN	HTTP/1.1 304 Not Modified Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 29223781 Cache-Control: public, max-age=31536000 Date: Fri, 13 May 2022 14:54:27 GMT Etag: 0x8D79ED29CF0C29A Last-Modified: Wed, 22 Jan 2020 00:32:50 GMT Server: ECAcc (frc/8E9E) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: ae00a5ef-301e-0050-690f-5d9d0f000000 x-ms-version: 2009-09-19 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49778	13.107.246.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:27 UTC	206	OUT	GET /ests/2.1/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.msauth.net If-Modified-Since: Fri, 02 Nov 2018 20:25:09 GMT If-None-Match: 0x8D64101494758DF
2022-05-13 14:54:27 UTC	207	IN	HTTP/1.1 304 Not Modified Cache-Control: public, max-age=604800 Content-Type: image/svg+xml Content-Encoding: gzip Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Last-Modified: Fri, 02 Nov 2018 20:25:09 GMT ETag: 0x8D64101494758DF Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 91d75960-a01e-0035-2365-659168000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0qxV9YgAAAABqhbpDd2g0R40wVAcDbpTNQU1TMDRFREdFMTkxMAAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= X-Azure-Ref: 0I3F+YgAAAADigW7vpfYtSbnN7iME+D/2RlJBMzFFREdFMDkyMAAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= Date: Fri, 13 May 2022 14:54:27 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49779	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:28 UTC	208	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 If-Modified-Since: Wed, 12 Feb 2020 22:01:50 GMT If-None-Match: 0x8D7B007297AE131

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:28 UTC	208	IN	HTTP/1.1 304 Not Modified 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: 26393305 Cache-Control: public, max-age=31536000 Date: Fri, 13 May 2022 14:54:28 GMT Etag: 0x8D7B007297AE131 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (frc/8FE5) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000 x-ms-version: 2009-09-19 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49741	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:13 UTC	1	OUT	GET /ests/2.1/content/cdnbundles/converged.v2.login.min_rayhgcterrtxpnvapp3erg2.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-US,en;q=0.9
2022-05-13 14:54:13 UTC	1	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: 28561869 Cache-Control: public, max-age=31536000 Content-MD5: +rPQJ6BWMovrMLNrlexvKQ== Content-Type: text/css Date: Fri, 13 May 2022 14:54:13 GMT Etag: 0x8D88DD061D3546B Last-Modified: Sat, 21 Nov 2020 03:49:00 GMT Server: ECAcc (frc/8FAB) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 9bf8b192-801e-000e-2214-631f6b000000 x-ms-version: 2009-09-19 Content-Length: 107668 Connection: close
2022-05-13 14:54:13 UTC	2	IN	Data Raw: 2f 2a 21 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 20 2a 2f 2f 2a 21 0a 2d 2d 2d

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:13 UTC	36	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
2022-05-13 14:54:13 UTC	52	IN	Data Raw: 6c 6f 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 Data Ascii: low-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,.tab
2022-05-13 14:54:13 UTC	68	IN	Data Raw: 63 22 2c Data Ascii: c",
2022-05-13 14:54:13 UTC	68	IN	Data Raw: 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 69 61 6e 20 42 61 69 74 69 22 2c 22 4d 56 20 42 6f 6c 69 22 2c 22 4d 79 61 6e 6d 61 72 20 54 65 78 74 22 2c 22 43 61 6d 62 72 69 61 20 4d 61 74 68 22 7d 2e 49 45 5f 4d 37 20 75 6c 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 7d 2e 49 45 5f 4d 37 20 69 6e 70 75 74 5b 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 5d 2c 2e 49 45 5f 4d 37 20 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 Data Ascii: "Estrangelo Edessa","Microsoft Himalaya","Microsoft New Tai Lue","Microsoft PhagsPa","Microsoft Tai Le","Microsoft Yi Baiti","Mongolian Baiti","MV Boli","Myanmar Text","Cambria Math"}.IE_M7 ul{margin-left:0}.IE_M7 input[type="button"],.IE_M7 input[type="s
2022-05-13 14:54:13 UTC	84	IN	Data Raw: 2d 77 69 64 74 68 3a 31 30 30 25 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 77 68 69 74 65 2d 73 70 61 63 65 3a 6e 6f 77 72 61 70 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 74 65 78 74 2d 6f 76 65 72 66 6c 6f 77 3a 65 6c 6c 69 70 73 69 73 3b 74 6f 75 63 68 2d 61 63 74 69 6f 6e 3a 6d 61 6e 69 70 75 6c 61 74 69 6f 6e 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 62 6f 72 64 65 72 2d 73 74 79 6c 65 3a 73 6f 6c 69 64 3b 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 32 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 33 32 70 78 3b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 63 Data Ascii: -width:100%;text-align:center;white-space:nowrap;overflow:hidden;vertical-align:middle;text-overflow:ellipsis;touch-action:manipulation;color:#000;border-style:solid;border-width:2px;border-color:transparent;min-height:32px;border:none;background-color:#c
2022-05-13 14:54:13 UTC	101	IN	Data Raw: 6c 61 73 73 3d 22 72 61 64 69 6f 22 5d 3a 66 69 72 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 7d 2e 66 6f 72 6d 2d 67 72 6f 75 70 2d 74 6f 70 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 36 70 78 7d 64 69 76 5b 72 6f 6c 65 3d 6c 69 73 74 69 74 65 6d 5d 2c 2e 6c 69 73 74 2d 69 74 65 6d 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 32 30 70 78 3b 64 69 73 70 6c 61 79 3a 6c 69 73 74 2d 69 74 65 6d 3b 6c 69 73 74 2d 73 74 79 6c 65 3a 63 69 72 63 6c 65 3b 6c 69 73 74 2d 73 74 79 6c 65 2d 74 79 70 65 3a 64 69 73 63 7d 2e 70 68 6f 6e 65 43 6f 75 6e 74 72 79 43 6f 64 65 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 77 69 64 74 68 3a 31 30 30 25 3b 6c 65 66 74 3a 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 34 70 78 3b 68 65 69 67 68 74 3a 33 36 70 Data Ascii: lass="radio"]:first-child{margin-top:0}.form-group-top{margin-top:16px}div[role=listitem],.list-item{margin-left:20px;display:list-item;list-style:circle;list-style-type:disc}.phoneCountryCode{position:absolute;width:100%;left:0;padding:6px 4px;height:36p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49751	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	110	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-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	111	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: 26393291 Cache-Control: public, max-age=31536000 Content-MD5: DhdidjYrlCeaRJJRG/y9mA== Content-Type: image/svg+xml Date: Fri, 13 May 2022 14:54:14 GMT Etag: 0x8D7B007297AE131 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (frc/8FE5) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1528e04b-101e-0063-5ccd-76af16000000 x-ms-version: 2009-09-19 Content-Length: 1864 Connection: close
2022-05-13 14:54:14 UTC	112	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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49750	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	111	OUT	GET /ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_szor2ujtsn_b-ik0b744ha2.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-13 14:54:14 UTC	114	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: 18879449 Cache-Control: public, max-age=31536000 Content-MD5: 6Qvaph3XjGlz0gTgNQb8QQ== Content-Type: application/x-javascript Date: Fri, 13 May 2022 14:54:14 GMT Etag: 0x8D8B274B724F769 Last-Modified: Wed, 06 Jan 2021 18:56:03 GMT Server: ECAcc (frc/8FA5) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 4fabead7-501e-0003-3f24-bb2de5000000 x-ms-version: 2009-09-19 Content-Length: 41194 Connection: close
2022-05-13 14:54:14 UTC	115	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 35 29 2c 72 3d 69 28 37 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(5),r=i(7),a=r.Strin

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	131	IN	Data Raw: 74 Data Ascii: t
2022-05-13 14:54:14 UTC	131	IN	Data Raw: 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 61 63 63 6f 75 6e 74 20 74 6f 20 61 20 47 69 74 48 75 62 20 61 63 63 6f 75 6e 74 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 32 3d 22 59 6f 75 20 63 61 6e 27 74 20 75 73 65 20 74 68 69 73 20 6f 70 74 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 77 6f 72 6b 20 6f 72 20 73 63 68 6f 6f 6c 20 72 65 73 6f 75 72 63 65 73 2e 22 2c 65 2e 43 54 5f 53 54 52 5f 44 69 61 6c 6f 67 5f 43 6c 6f 73 65 42 75 74 74 6f 6e 3d 22 43 6c 6f 73 65 22 2c 65 2e 43 54 5f 50 57 44 5f 53 54 52 5f 53 77 69 74 63 68 54 6f 43 72 65 64 50 69 63 6b 65 72 5f 4c 69 6e 6b Data Ascii: ion, you must have previously linked your personal Microsoft account to a GitHub account.",e.CT_ST R_GitHubDialog_Desc2="You can't use this option to access work or school resources.",e.CT_STR_Dialog_CloseButt on="Close",e.CT_PWD_STR_SwitchToCredPicker_Link
2022-05-13 14:54:14 UTC	151	IN	Data Raw: 50 5f 45 5f 4d 45 4d 42 45 52 5f 4c 43 4b 45 44 3a 22 38 30 30 34 31 30 31 31 22 2c 50 50 5f 45 5f 42 41 44 5f 50 41 53 53 57 4f 52 44 3a 22 38 30 30 34 31 30 31 32 22 2c 50 50 5f 45 5f 4d 49 53 53 49 4e 47 5f 4d 45 4d 42 45 52 4e 41 4d 45 3a 22 38 30 30 34 31 30 33 31 22 2c 50 50 5f 45 5f 4d 49 53 53 49 4e 47 5f 50 41 53 53 57 4f 52 44 3a 22 38 30 30 34 31 30 33 32 22 2c 50 50 5f 45 5f 46 45 44 45 52 41 54 49 4f 4e 5f 49 4e 4c 4f 47 49 4e 5f 44 49 53 41 4c 4c 4f 57 45 44 3a 22 38 30 30 34 37 38 41 43 22 2c 50 50 5f 45 5f 50 45 5f 52 55 4c 45 46 41 4c 53 45 3a 22 38 30 30 34 34 39 30 43 22 2c 50 50 5f 45 5f 4d 4f 42 49 4c 45 43 52 45 44 53 5f 50 48 4f 4e 45 4e 55 4d 42 45 52 5f 42 4c 41 4e 4b 3a 22 38 30 30 34 35 38 30 31 22 2c 50 50 5f 45 Data Ascii: P_E_MEMBER_LOCKED:"80041011",PP_E_BAD_PASSWORD:"80041012",PP_E_MISSING_MEMBERN AME:"80041031",PP_E_MISSING_PASSWORD:"80041032",PP_E_FEDERATION_INLINELOGIN_DISALLOWED:"80 0478AC",PP_E_PE_RULEFALSE:"8004490C",PP_E_MOBILECREDS_PHONENUMBER_BLANK:"80045801",PP_E

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49753	192.229.221.185	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	114	OUT	GET /shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 Host: logincdn.msauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: 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-US,en;q=0.9
2022-05-13 14:54:14 UTC	147	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: 29223768 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Fri, 13 May 2022 14:54:14 GMT Etag: 0x8D79ED29CF0C29A Last-Modified: Wed, 22 Jan 2020 00:32:50 GMT Server: ECAcc (frc/8E9E) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: ae00a5ef-301e-0050-690f-5d9d0f000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2022-05-13 14:54:14 UTC	148	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
6	192.168.2.6	49754	13.107.246.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	160	OUT	GET /ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 Host: aadcdn.msauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: 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-US,en;q=0.9
2022-05-13 14:54:14 UTC	160	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=604800 Content-Length: 276 Content-Type: image/svg+xml Content-Encoding: gzip Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Last-Modified: Fri, 02 Nov 2018 20:25:09 GMT ETag: 0x8D64101494758DF Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 X-Cache: TCP_HIT x-ms-request-id: 91d75960-a01e-0035-2365-659168000000 x-ms-version: 2009-09-19 x-ms-lease-status: unlocked x-ms-blob-type: BlockBlob Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Access-Control-Allow-Origin: * X-Azure-Ref-OriginShield: 0qxV9YgAAAABqhbpDd2g0R40wVAcDbpTNQU1TMDRFREdFMTkxMAAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= X-Azure-Ref: 0FnF+YgAAAAAQVXbt6pamRpqBlIR5X1NPRlJBMzFFREdFMDkxMAAzOWExMmY3ZS04OTlmLTQ2Y2YtYTZkMC0yNGJiYmEyN2Q5NTY= Date: Fri, 13 May 2022 14:54:13 GMT Connection: close
2022-05-13 14:54:14 UTC	161	IN	Data Raw: 1f 8b 08 00 00 00 00 00 04 00 95 51 3d 6f c3 20 10 fd 2b 88 ae e6 e0 08 d8 b8 b2 3d 74 ca 90 ae 1d ba 45 8a 6b 5b 22 1f aa 91 c9 cf 2f 67 3b 6e 87 2c 15 f0 80 bb 7b ef 9e a0 1a a7 8e dd cf fe 32 d6 bc 0f e1 f6 2a 65 8c 11 e2 0e ae df 9d d4 4a 29 99 2a 38 8b c3 29 f4 35 d7 86 b3 be 1d ba 3e 2c e7 69 68 e3 db f5 5e 73 c5 14 d3 26 4d de 54 61 08 be 6d 8e e3 d8 86 b1 92 cb ad ba 1d 43 cf 4e 35 7f 47 97 21 82 2d dc 04 ce 98 7d 01 39 16 7e 07 a5 c6 8c d0 09 b0 a5 a1 75 c8 33 d4 de 40 69 8c 98 71 4b cc 9c 55 e5 93 b3 af c1 fb 9a bf 18 45 83 cb bf bd 14 f1 b2 02 94 cd fd 53 fa 1e ff ef e3 ac 04 a0 41 01 aa c0 b4 0e 36 95 97 a4 47 9b 05 67 1d 11 d6 2c 66 33 67 c1 35 46 1b b1 49 9d da d8 47 40 3c 0e 98 4c 2e 3a 60 b5 4e 26 01 3f 52 03 93 0c cf 89 64 b4 b0 28 08 37 Data Ascii: Q=o +=tEk["/g;n,{2*eJ)*8)5>,ih^s&MTamCN5G!-}9~u3@iqKUESA6Gg,f3g5FIG@<L.:`N&?Rd(7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49758	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	161	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-US,en;q=0.9
2022-05-13 14:54:14 UTC	162	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: 29069171 Cache-Control: public, max-age=31536000 Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Content-Type: image/x-icon Date: Fri, 13 May 2022 14:54:14 GMT Etag: 0x8D8731240E548EB Last-Modified: Sun, 18 Oct 2020 03:02:30 GMT Server: ECAcc (frc/8F98) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 0f49f9d8-001e-006f-0f77-5e6395000000 x-ms-version: 2009-09-19 Content-Length: 17174 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:14 UTC	162	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 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

Timestamp	kBytes transferred	Direction	Data
2022-05-13 14:54:16 UTC	187	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: 29069173 Cache-Control: public, max-age=31536000 Content-MD5: EuPayFgGHQiAI7K9SOL6lg== Content-Type: image/x-icon Date: Fri, 13 May 2022 14:54:16 GMT Etag: 0x8D8731240E548EB Last-Modified: Sun, 18 Oct 2020 03:02:30 GMT Server: ECAcc (frc/8F98) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 0f49f9d8-001e-006f-0f77-5e6395000000 x-ms-version: 2009-09-19 Content-Length: 17174 Connection: close
2022-05-13 14:54:16 UTC	187	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 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

Start time:	16:54:06
Start date:	13/05/2022
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\Markham_remittance71792.html
Imagebase:	0x7ff6220c0000
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

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	7FF6220FFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **4228**, Parent PID: **7136**

General

Target ID:	1
Start time:	16:54:08
Start date:	13/05/2022
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=1564,8452305244807070825,17752714670138375518,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8
Imagebase:	0x7ff6220c0000
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.

Copyright Joe Security LLC 2022

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