ID: 612082
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 14:48:42
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

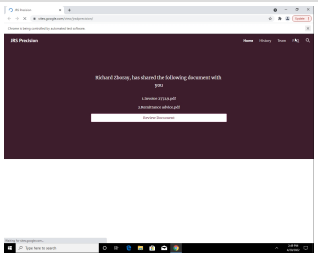
Windows Analysis Report

https://sites.google.com/view/jrsdprecision/

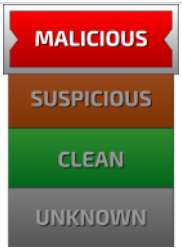
Overview

General Information

Sample URL:	https://sites.google.com/view/jrsdprecision/
Analysis ID:	612082



Detection

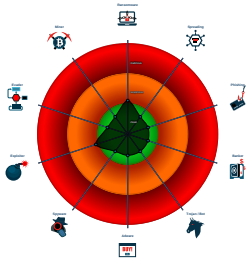


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for dom...

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 7748 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument https://sites.google.com/view/jrsdprecision/ MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 5296 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1732,8493929056398251142,18182367843663010915,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2192 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

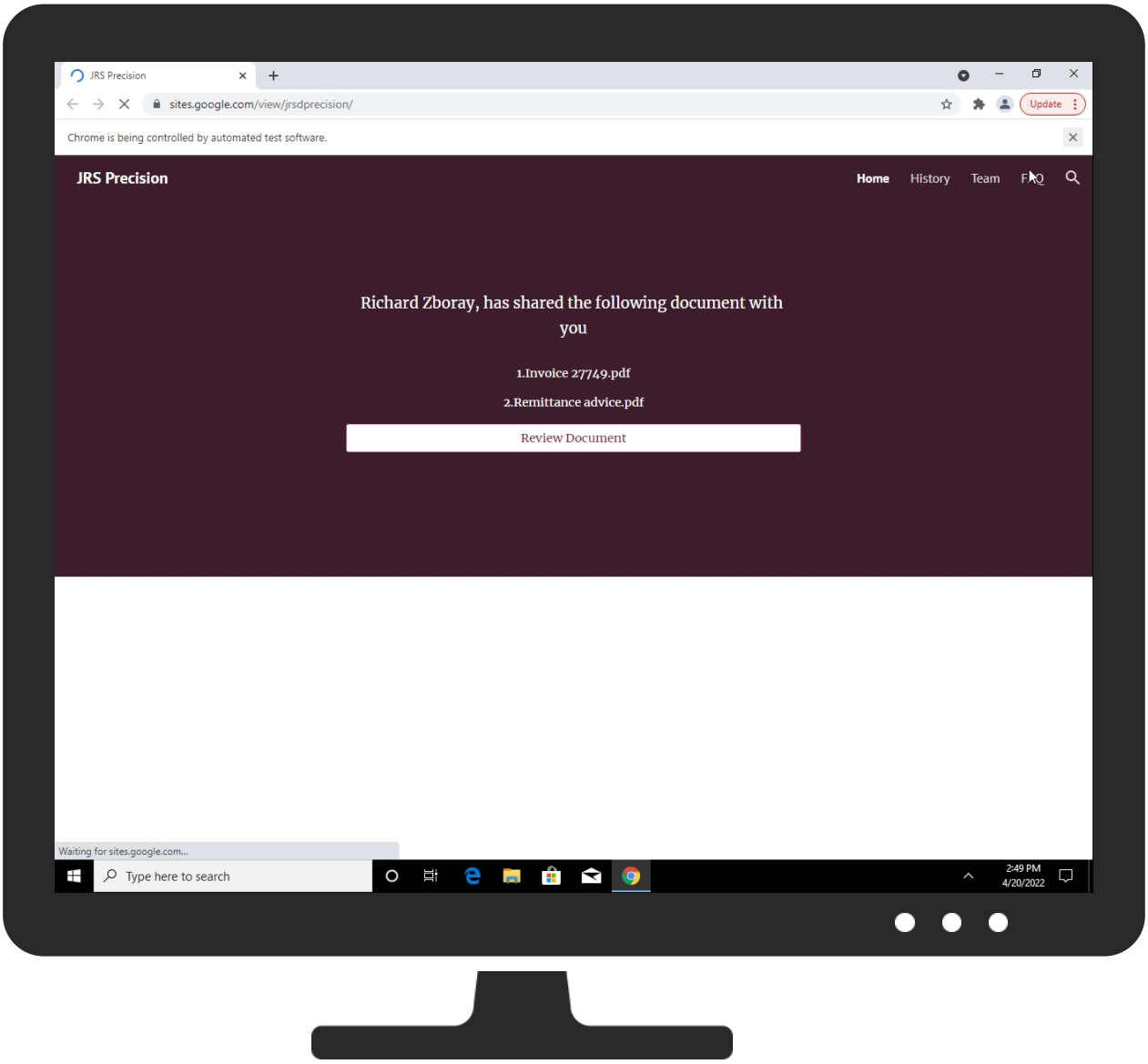
Mitre Att&ck Matrix

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	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 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	1 Extra Window Memory Injection	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 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)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
https://sites.google.com/view/jrsdprecision/	0%	Virustotal		Browse
https://sites.google.com/view/jrsdprecision/	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
lively-field-031627803.1.azurestaticapps.net	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
https://lively-field-031627803.1.azurestaticapps.net/	17%	Virustotal		Browse

Domains and IPs

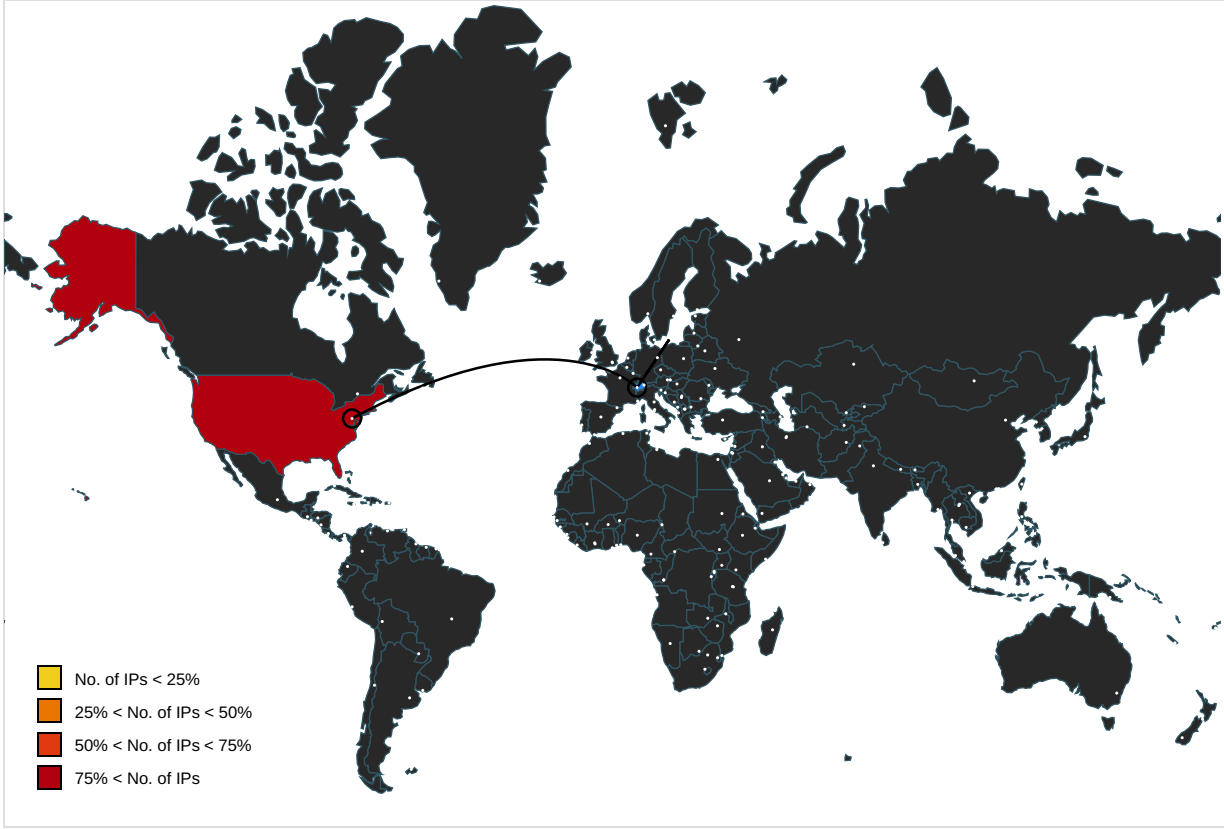
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.74.195	true	false		high
accounts.google.com	142.250.185.205	true	false		high
plus.l.google.com	142.250.185.78	true	false		high
waws-prod-am2-5ecab9f3.sip.p.azurewebsites.windows.net	20.50.153.39	true	false		high
sites.google.com	142.250.185.206	true	false		high
www.google.com	142.250.185.228	true	false		high
clients.l.google.com	142.250.184.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.65	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
lh5.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
lively-field-031627803.1.azurestaticapps.net	unknown	unknown	true	• 16%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high
lh4.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://www.google.com/url?q=https%3A%2F%2Flively-field-031627803.1.azurestaticapps.net%2F&sa=D&sntz=1&usg=AOvVaw1FCGTlHeY_IG3uPBB2uOGm	false		high
https://lively-field-031627803.1.azurestaticapps.net/	true	• 17%, Virustotal, Browse	unknown
https://sites.google.com/view/jrsdprecision/	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.195	unknown	United States		15169	GOOGLEUS	false
20.50.153.39	waws-prod-am2-5ecab9f3.sip.p.azurewebsites.windows.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.78	plus.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.206	sites.google.com	United States		15169	GOOGLEUS	false
142.250.185.228	www.google.com	United States		15169	GOOGLEUS	false
152.199.19.161	unknown	United States		15133	EDGECASTUS	false
152.199.19.160	unknown	United States		15133	EDGECASTUS	false
173.194.187.10	unknown	United States		15169	GOOGLEUS	false
142.250.185.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.185.202	unknown	United States		15169	GOOGLEUS	false
142.250.186.106	unknown	United States		15169	GOOGLEUS	false
172.217.23.97	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.195	unknown	United States		15169	GOOGLEUS	false
142.250.186.142	unknown	United States		15169	GOOGLEUS	false
142.250.184.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.74.195	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false
142.250.184.234	unknown	United States		15169	GOOGLEUS	false
142.250.185.65	googlehosted.l.googleusercontent.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:	612082
Start date and time: 20/04/202214:48:42	2022-04-20 14:48:42 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://sites.google.com/view/jrsdprecision/
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Detection:	MAL
Classification:	mal48.win@32/73@12/198
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.160.2, 20.190.160.134, 20.190.160.73, 20.190.160.75, 20.190.160.67, 20.190.160.8, 20.190.160.6, 20.190.160.69
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, login.live.com, www.tm.lg.prod.aadmsa.akadns.net, nexusrules.officeapps.live.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\9695e3c4-56db-4cc7-992a-45713eb00888.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):	102985
Entropy (8bit):	6.067985025828186
Encrypted:	false
SSDEEP:	
MD5:	AD4AB88173AE19A8D7D56F145E29E960
SHA1:	FA207E7995A5B02CBC4EF1B793D11C050868B467
SHA-256:	1CB69CAF63A46C2F4F0D713135022613C218D94744AFC92C4DE88088C2E60F90
SHA-512:	D05C9C7F6B170B9DFC812AE64B5DF4F257D721F5E787A56069B80ED814B87BE2B4BBC71F4570FFA321C7BB9CECA50CAA7F70886436E89E79C819AF3A17F01502
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.650491361310381e+12,"network":1.650458962e+12,"ticks":171224455.0,"uncertainty":2244175.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187279872"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40

Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	
MD5:	FA7200D6F80CD1757911C45559E59C0E
SHA1:	89C6E99BAEC4EBB3E9A97B928FB473D1498EBA88
SHA-256:	D9779EA4D6DD544A23C2A1C53146B6A4E596927F47DFA0680B0A7EE751D43BB2
SHA-512:	71D9B2DA8EAF404063D918812BA61C3EFB6A23A283B0332180A38C8137FBB21D7977C008D5A57A74469776945CD4ED42C0BCC09F923EDEC52D8F7FE90FA2D14
Malicious:	false
Reputation:	low
Preview:	sdPC.....A.>'..M..,.,.-.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\161e6ebd-0964-45b3-80a3-af19e4bb1e75.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:	
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\469fbbcb-77ca-4e71-946f-c05cb4ea6336.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .2v...M..(..... ....]..X\.).H...>..Z.....\..._....V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[.....z...`...J....9...E...k...R.D.....G...A....;...E...h..XKd..KW.....D...>...=..X....GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`...\...K...D...A...;.....3...\...e...V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...l..U].M.5@.....6...C...@..T....EW..LX..=K..Ob..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\4b055950-271c-4d74-a193-0dc12f543316.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):	3488
Entropy (8bit):	4.94330612618446
Encrypted:	false
SSDEEP:	
MD5:	E1918D61209AE6F53A03A9FCC0C76D21
SHA1:	7A2CDE0C55D09A8502BF81DE4DB3ADDA63EAD401
SHA-256:	2F29400F8CBE9AE83904C34E24DEA79A0C7192FB117AC75F4F28C45F831F0F4F

SHA-512:	DED660A34A72D3CA0C20874FE37564EBEC187610071895C9A6FF62016E73BE2D965ED1FCEAEEC423156B4E4E8032FB8DE652942B7453DFBD2FCB7835C25D5E33
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13294964960676105","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2728},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13294964960674368"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"53f343c8-20c8-4b87-a62a-4cb92b110c96"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"0017C9EB5DB27B3A25D082EB844D073A","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\9f0933e2-de68-4d1c-8c9e-2fed691b823b.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):	15765
Entropy (8bit):	5.573274961139714
Encrypted:	false
SSDEEP:	
MD5:	E57899E0E8BFD5FA0020DA4832D4FF9E
SHA1:	56A01EA7B995FAD40DC0E3263FA6B197F5393261
SHA-256:	34661BF5C7D6BD16955B42F5322B93B223A8AA1AF588BF4521A09A3B8F06E997
SHA-512:	6CB421647EC2F341CF1AEA950ED13F9239367423FF2CA691587A01E726B59E76701B3585F7B085FE55C91619A637ACAF2AD64CC0B25F8E2909B03DB7DF97C47
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13294964959289746","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11336
Entropy (8bit):	6.0707244876366575
Encrypted:	false
SSDEEP:	
MD5:	2E2110A99AD3AE9721A458C95C64C868
SHA1:	72AE17599EDC0B2DC61C41D946E3E296864F2CBA
SHA-256:	BB46BA705D5F6F43F66B07EA5DA4CC7CC0BF8FE635CCC4EBBA30A5D4A54158DE
SHA-512:	29D95D043F3E529DD33F73B3207A9167D479D9FC404209497B53229CF68AA634CB8A1FE3FD08512FD7F48AFB567144DB873FBBDAD8171D42968B97357F06BC1
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["8D+nOE33nrpuAnTVcJlgMPWVo79reBkp3Z22WTJi5B8="],"block_size":4096,"path":"_locales/nb/messages.json"},{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\9221.427.0.1_0_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	26178

Entropy (8bit):	6.060546316291638
Encrypted:	false
SSDEEP:	
MD5:	E7FC5462366916AA507D0D350BF1BE86
SHA1:	0D250D97A4FAA070DCE2BE246F14656800EE6561
SHA-256:	84F230EAF1D18C25F8336F3ADEB490847D2ABFF6D4B30E7744C0D2B5790F84F6
SHA-512:	F07D080196055AAD3AF5F0231C05AE6EF54FFA4C035775C7CE32B0A57EF254A79A05FB7ACED60D3F0F5A785C6846E675949F99161C32F81B977EB25ABEFAAB18
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["fM6wUoU96QmdAMMJqhyPQdILY6QXE2cfpXivMNd/kSg=","GmZUfDhlvU+1ByKQxZIcQZm+8bSFENyNk79q9fsZu3o=","X0hU8nolnxRmTiwIKtHtUeSjEP4YaSRtnpXvJQrqg8I="],"block_size":4096,"path":"_locales/nb/messages.json"},{"block_hashes":["/0XLYLvR7GDi1lXEsqI5OOorLaHGVkQU9sW9wrxd/qs=","ugdSYfR9jET/5OpIYWZUycWy9FcBX/jb/7/hmW5DVR0=","Z2vShQRg9avHHQwTkYjAyfnFnhHQ6Ce+ob00hRV0V2Q=","Ilb7yaoAR7pQ0ZDpBU1ZzIKa+hURf3edJBILNvUO6lk=","5mpQSSRBXvBC9O0QpFoDxFGOcDS5Iua0gICy3D+t0UM=","EkWgzDTb1zblDgz7APE/G19fsHn/TJJuw3JbNsqGNCY=","Mb/n/cgw5oibXHqBfMwXremke8GY9oWJPhuY1Y2CrpQ=","cb+9vKl/3iDYu97Gc5yEsJnJ2QWd4dpd1E3pt/3yaqQ=","17+40sjnss/mFRm6idVmlEZTl+kWrR1GSzedHRD8yZI=","fTKSj8L49Jxlk/4helP5XYq

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... ....N..... .(....D..... .2v...M..(..... .....]..X\.).H...>..Z.....\..._...V...F...A...A.....^..Wb...f.)...I...v.M...B...@..Wc...[.....z...`...J.....9...E...k...R.D.....G...A.....;...E...h..XKd..KW.....D...>...=..X....GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`..\...K...D...A...;.....3...\...e...V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...I..U].M.5@.....6...C...@..T....EW..LX..=K..Ob..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

C:\Users\alfredo\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):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\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):	3488
Entropy (8bit):	4.9432370233519975
Encrypted:	false
SSDEEP:	
MD5:	FEFAA6678A43550781F1164BE58FD855
SHA1:	C333BD4F0DDFB545D50CF128F00761EC0E9F1342
SHA-256:	C01D5F0A535D06FE04E58A453D7D2C49FFC108A7E4EE63069D5C246B78332B37
SHA-512:	30CB36A3558BEE5743510CC34792C26529BB3ED4AFEF88C5B5F0F1B181F773503EF671A7395D6E8927DB4FB4A0733EA8B36493200459FD6156965AE3806770F0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13294964960676105","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2728},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13294964960674368"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"53f343c8-20c8-4b87-a62a-4cb92b110c96"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"0017C9EB5DB27B3A25D082EB844D073A","engagement":{"schema_version":4}},

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15765
Entropy (8bit):	5.573274961139714
Encrypted:	false
SSDEEP:	
MD5:	E57899E0E8BFD5FA0020DA4832D4FF9E
SHA1:	56A01EA7B995FAD40DC0E3263FA6B197F5393261
SHA-256:	34661BF5C7D6BD16955B42F5322B93B223A8AA1AF588BF4521A09A3B8F06E997
SHA-512:	6CB421647EC2F341CF1AEA950ED13F9239367423FF2CA691587A01E726B59E76701B3585F7B085FE55C91619A637ACAF2AD64CC0B25F8E2909B03DB7DF97C47
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13294964959289746","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\b3c90246-77bd-47f0-8977-1ced11f1db4f.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):	3488
Entropy (8bit):	4.9432370233519975
Encrypted:	false
SSDEEP:	
MD5:	FEFAA6678A43550781F1164BE58FD855
SHA1:	C333BD4F0DDFB545D50CF128F00761EC0E9F1342
SHA-256:	C01D5F0A535D06FE04E58A453D7D2C49FFC108A7E4EE63069D5C246B78332B37
SHA-512:	30CB36A3558BEE5743510CC34792C26529BB3ED4AFEF88C5B5F0F1B181F773503EF671A7395D6E8927DB4FB4A0733EA8B36493200459FD6156965AE3806770F0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13294964960676105","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2728},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13294964960674368"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"53f343c8-20c8-4b87-a62a-4cb92b110c96"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"0017C9EB5DB27B3A25D082EB844D073A","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\c1178d0d-9d91-49fa-98ab-d6260f75eda0.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):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\c8bb9053-4812-4961-87c6-2a46025a1966.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):	18568
Entropy (8bit):	5.558163077271108
Encrypted:	false
SSDEEP:	
MD5:	E7EDA950949825F231A110EA343A0F66
SHA1:	95B9701C4CCAEE15E102DB72F0DA62071C5FA778
SHA-256:	BEA96051DDD994E8C2EE944B00230D406B95063026A8039150430FF5192AF24D
SHA-512:	E5D810AD67AC586ED3FB7127E372AF4209798A3DA168A805ED732F76075FAA8BC8466C7342D72691DD863F98C752E072CDB70CD0FE5AE22A7528EC561E77894E
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13294964959289746","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000006.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:	
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1(
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

C:\Users\alfredo\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:	
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1(
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

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

C:\Users\alfredo\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):	2.873140679513133
Encrypted:	false
SSDEEP:	
MD5:	3A0E5D4F452CF99191634D0FFAB744A0
SHA1:	F115BBB898EEFF640D8D19AD44A86C3FCDFFC0AD
SHA-256:	B9D528D3AE283039F4700C7E4E790744C58A26353A91B536DD91CBA4F648A35F
SHA-512:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528A
Malicious:	false
Reputation:	low
Preview:	92.0.4515.107

C:\Users\alfredo\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):	98417
Entropy (8bit):	6.036978354962259
Encrypted:	false
SSDEEP:	
MD5:	517703416513B89BDD69F435CBBF23F7
SHA1:	FACD8114B88FC11737088A713AA891EC6FA169DD
SHA-256:	E9F99398B89834F9C783B7EE711D11AE0A7F3CED3EDFC052364C93694DEBC097

SHA-512:	D3C31C16E6E92FB18BE5038FFB26CB5ADFCD57088A1C371B93E0769572DF91A997A1621ECF0E8021329C3402BBE507A90B744E1E7DBAD2901E0A5944680DA54 7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.650491361310381e+12,"network":1.650458962e+12,"ticks":171224455.0,"uncertainty":2244175.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2IIZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13294964958472636"},"profile":{"info_cache":{"Default":{"active_time":1650491360.342553,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\bf2272fb-bcd7-437c-ba8e-7aaad0ed459f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.7620072177897192
Encrypted:	false
SSDEEP:	
MD5:	524A7C231BB2CD0FF09F4E85CA296B53
SHA1:	7FF2D4C1E9E86DAF19A3B5DF9CE8E01BE1D41D3A
SHA-256:	D683902320B8E4F13854B39097800C2B929F463945C6DF3AD365E2014CF36642
SHA-512:	71FA3619B99F38E3679BE3DBFBB2B434DAB921990E9277F068B62107B90D6625603445E30AE2495EA4584EEE7655695524A0705792D8D8A4DAD043C18A060C80
Malicious:	false
Reputation:	low
Preview:	4}.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....Y8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....Y8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\c3dc22aa-a5e4-4a42-bcfa-b281a0b5c11a.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):	98417
Entropy (8bit):	6.036978354962259
Encrypted:	false
SSDEEP:	
MD5:	517703416513B89BDD69F435CBBF23F7
SHA1:	FACD8114B88FC11737088A713AA891EC6FA169DD
SHA-256:	E9F99398B89834F9C783B7EE711D11AE0A7F3CED3EDFC052364C93694DEBC097
SHA-512:	D3C31C16E6E92FB18BE5038FFB26CB5ADFCD57088A1C371B93E0769572DF91A997A1621ECF0E8021329C3402BBE507A90B744E1E7DBAD2901E0A5944680DA54 7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.650491361310381e+12,"network":1.650458962e+12,"ticks":171224455.0,"uncertainty":2244175.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2IIZGHfAdJRwvbkapN4/FWvwMAAAAPz8l/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13294964958472636"},"profile":{"info_cache":{"Default":{"active_time":1650491360.342553,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Temp\049638ac-3685-4c42-a568-2ed63fd69a27.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	101891
Entropy (8bit):	**7.9971613680976565**
Encrypted:	**true**
SSDEEP:	
MD5:	173CA02E5B06065771DEB2F28E4E5A9E

SHA1:	20F1774FB280C94C13082A255C27D7A786EFD5C7
SHA-256:	634557AE2916F2FAA0CBF2557F8F96E26845ABE94D2784FD73B169EC5618B186
SHA-512:	D947E3ED56BE1F3C668943E8F066F39650D2E0D76BF64BAD167E100B8B1066B88D8E851346AFBD9777E90445F41C5108A0A2F1514A3F28F02D4EC39978121E71
Malicious:	false
Reputation:	low
Preview:	.....{..0.....&xqH.....zyIBv9....=...+.....I6....3#.l.@..9.s].W7...h4..H...7.^.....Bg.....`.;.S...P.....z.3.....9~.P..{..-.z.....b.:.....>..'....I8.....'v.M'E.?bA...N8.'.8I.._...< v&.pT{.L'Ne...#.S!].T.-+...r)5.j.U.8q....X..VPo.....F.o..A.~~.?.w.....eNJ..a)....i....:?._^..v.<=ei...i.....Q...8k.....~j.c.W.....~...Q.yq..^9..z.....S..b.E..L3|.9S.pa...a....5...J.\. 2l..s..4.....S.u..o.|.Q.K.0.=.....0....xj.4....Mie..C..3..... .....WN.....4Vs.B..N.bD...VK%...mb...{{....pd..7..G.....}.J;''..4,.....A.R|0d..)..M.....;;.8.h.C.u..pkM..Z@.....r..U....H.. .],..l:~p..8`....3....5.*.t../S{.{`.^kB=f.....ZR..L.$t..D%I..xB../.{rb..h8.!.....Z.0.....{PuK%Vv...RR.*.....j.vw.[B..$..|&..eZEW.Z[&..d>.o.....@..t.z.O.12C.....Kk..oS.[.0.M...<.z q#*g.r....."0+.[.....Tb.E....F...U..U0...G.....t!.+...&K.@.N.#R.]...+.;.M[..x,...J.l.....&y.n.....j>..0.|W.+.S.0X.S.E..L....R.....W.u.g.S.&^.g..N/..

C:\Users\alfredo\AppData\Local\Temp\1f43297c-be93-4252-860f-1a5fa54dd691.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:	
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F33260 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|..A..L.+.=...kP.!.1..

C:\Users\alfredo\AppData\Local\Temp\3309d7c3-39e0-4234-9afb-e778f5a58874.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	826470
Entropy (8bit):	**7.993386298864445**
Encrypted:	**true**
SSDEEP:	
MD5:	BB2058E728F79C67137BDFCFCEEC72D4
SHA1:	0AE586E5DD08EA7BECD5618DA868E7FA94910F60
SHA-256:	9107E42F7F892FECD9A0A8CB05FEDAE7D9E045442FB17AF11A77F6F7253B66B7
SHA-512:	E35C7CC13C58748D3A3970BD5DA5D2568220EA939CB16FDB6E68078C198AFF78FDF06BC4EFAF564186FBA82E4E427CDA9EB08CCCC2984E66D725D7388D402 4B
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....b.._..+.....e..'.q<.iJ.....]m.....L.3..O....u{..+..&..;....]..)....b._.Ut._.....B .Q.X.C.._....,...x.^.....8B..n....}. Q.u;..>6....B.....a...Y..j1.<..b...m..@...y..&.".7..+a%{`..|...).:.7j.*k.0...(7...U.4Q.b'..._;.e.z...v.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3. \"...,g.c...6)..(.E...U...#.i.a.:....N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....e8....:._i..4.r#...@3.F.:....!0...{..s.....)v3-....S.G.I.;.....c$.*.....-...p&..,.....i) {G....6.L?.....c.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!..\...`.M..\..3.....2g.7.

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA

SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F502
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
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%
Reputation:	low
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\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	0CE951B216FCF76F754C9A845700F042

SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Reputation:	low
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.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A......D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333BA
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `....;...|.....4...x..#...-...4I..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....".*...1...:...D...K...T...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt_abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1B38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....__pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git 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\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `....._pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....!.....!.....'.....G.....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i.....0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."..."..."..."......@.....`..... ...@..`..... ...@..`..... ...@..`..... ...@..`.....`... ...@..`.....`...`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046_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:	
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`... ...@...@.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046\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:	
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\alfredo\AppData\Local\Temp\7748_1216091046\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:	
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
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\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome ....."... },.. "app_name": {.. "message": "..... Chrome ....."... },.. "craw_app_unavailable": {.. "message": "....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "..... Chrome"... }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B

SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "craw_app_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavailable": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ...-..... Chrome".. },.. "app_name": {.. "message": "..... ...-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\vi\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):	695
Entropy (8bit):	4.855375139026009
Encrypted:	false
SSDEEP:	
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AEAEAB246FF8987F4D992B48D47BE
SHA-256:	051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04
SHA-512:	74FD267CF7E299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "app_name": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "craw_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.".. },.. "craw_connect_to_network": {.. "message": "Vui l.ng k.t n.i v.i m.ng.".. },.. "iap_unavailable": {.. "message": "Thanh to.n trong .ng d.ng hi.n kh.ng kh. d.ng.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\zh_CN\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):	5.210259193489374
Encrypted:	false
SSDEEP:	
MD5:	BB73BF561BB79F89D9BF7C67C5AE5C65
SHA1:	2FADD3A1959B29C44830033A35C637D0311A8C9C
SHA-256:	D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
SHA-512:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC68D2
Malicious:	false

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL_locales\zh_TW\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):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C80 9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome .....".. },.. "app_name": {.. "message": "Chrome .....".. },.. "craw_app_unavailable": {.. "message": ".. .....".. },.. "craw_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message ": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "... Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_206036005\CRX_INSTALL\manifest.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\kn\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20406
Entropy (8bit):	5.312117131662377
Encrypted:	false
SSDEEP:	
MD5:	2E3239FC277287810BC88D93A6691B09
SHA1:	FC5D585DA00ADC90BF79109C7377BD55E6653569
SHA-256:	5FC705AD19761204D8604EA069936A23731B055D51E7836CAAF16AC7719FBEEA
SHA-512:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF 3479
Malicious:	false
Reputation:	low

Preview:	{.. "1018984561488520517": {.. "message": "..... .....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "1 28276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "180276274658 9457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... $

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\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):	15480
Entropy (8bit):	5.617756574352461
Encrypted:	false
SSDEEP:	
MD5:	E303CD63AD00EB3154431DED78E871C4
SHA1:	3B1E5B8E2CF5EBDF5D33656EF80A46563F751783
SHA-256:	FDE602BFDB1AFD282682DA5338C4F91D8A2F6CB5411DB8F62F4583D629CE67A6
SHA-512:	18BA1D5A25FBC1829AD957A531B0CC490AFCBD20AC22181021363AA3CFB916270B8732E824463C9B0897220E8AE86EB1BE561D6540E6C625F08F228F61DDFFA 3
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": ".. . .. .?".. },.. "128276876460319075": {.. "message": ".. ..".. },.. "1428448869078126731": {.. "message": "... ..".. },.. "1522140683318860351": {.. "message": ".... ....".. },.. "15509 04064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "...".. },.. "180276274658 9457177": {.. "message": "...".. },.. "185039 7500312020388": {.. "message": "$START_LINK$Google Home .END_LINK. Chromecast. .....? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15802
Entropy (8bit):	5.354550839818046
Encrypted:	false
SSDEEP:	
MD5:	93BBBE82F024FBCB7FB18E203F253429
SHA1:	83F4D80F64FA2ADCE6C515C5F663BD38A76C51DB
SHA-256:	E7A8570922CCC4F2CA3721C4E61F426158C4E7BC90274FBC8BE4040FF8B6CA9B
SHA-512:	B7E7878106B466CE95069141DF1DE387E847348B62E9C4D548006452F3E164B3AD842E9673A56DC011A5ECC3346B5863E2034EE477A9D1F3E0ABD76B2D0F640A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Stringa".. },.. "1213957982723875920": {.. "message": "Kuris i. toliau pateikt. teigini. geriausiai apib.dina j.s. tinkl. ?".. },.. "128276876460319075": {.. "message": ".renginio suradimas".. },.. "1428448869078126731": {.. "message": "Vaizdo .ra.o sklandumas".. },.. " 1522140683318860351": {.. "message": ".vyko ry.io klaida. Bandykite dar kart..".. },.. "1550904064710828958": {.. "message": "Leid.iama skland.iai".. },.. "1636686747687494376": {.. "message": "Puiki".. },.. "1802762746589457177": {.. "message": "Garsumas".. },.. "1850397500312020388": {.. "message": "Ar .Chromecast. rodomas $START_LINK$programoje .Google Home.END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15891
Entropy (8bit):	5.36794040601742
Encrypted:	false
SSDEEP:	
MD5:	388590CE5E144AE5467FD6585073BD11
SHA1:	61228673A400A98D5834389C06127589F19D3A30
SHA-256:	05CA14196CA5D90B228C0F03684E03EBE403A3E7B513AE0A059244AE12B51164
SHA-512:	BF83AC90BC56CEB1CA12DCB47BCE542FB8CFE0BC14E34DE4FE1A84F7CDB4B54E36C125CEA7EE06EA6244F7795A0957A8A20DB30CA4C60FC6E96EF2A73544 8521
Malicious:	false
Reputation:	low

Preview:	{.. "1018984561488520517": {.. "message": ".lesald.ts. att.ls".. },.. "1213957982723875920": {.. "message": "Kur. no t.l.k min.tajiem apgalvojumiem vislab.k raksturo j.su t.klu?".. },.. "128276876460319075": {.. "message": "Ier.ces atra.ana".. },.. "1428448869078126731": {.. "message": "Video vienm.r.ba".. },.. "1522140683318860351": {.. "message": "Neizdev.s izveidot savienojumu. L.dzu, m..iniet v.lreiz.".. },.. "1550904064710828958": {.. "message": "Vienm.r.gs a tt.ls".. },.. "1636686747687494376": {.. "message": "Nevainojama".. },.. "1802762746589457177": {.. "message": "Ska.ums".. },.. "1850397500312020388": {.. "message": "Vai j.su Chromecast ier.ce ir redzama $START_LINK$lietotn. Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2"..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\ml\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20995
Entropy (8bit):	5.346788032166745
Encrypted:	false
SSDEEP:	
MD5:	0CBE2A5C0798516F665F06BC46373B6D
SHA1:	12AE7DDF4BA59B0324DE1E2EA10BBDCEC1495753
SHA-256:	41179A3582BE3DE2CB8A569AF22EC97AF2A42403D75E250BCAE853DBF7DDE598
SHA-512:	72B4B8E24152569AAF582115FAF7DE83ED51DC796AB5BEBA27F1BE4B0520F1280A4EDFDAB13DD9AA2B144B4E52A2F920162C6B34F738802AEA9458C141C2AD A4
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message"

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\mr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19625
Entropy (8bit):	5.311040089989635
Encrypted:	false
SSDEEP:	
MD5:	E4D38794005291B3AB72389F7C959E8C
SHA1:	D19AAAAC79EF703FFE78371B44D9F3681414E1EA
SHA-256:	915D323B9F7DB9E13BD50A75426B750C93EBC8699C523E72A37CB818CC33292B
SHA-512:	F1C502582D581C088F06E95309CBD5125D6E0EA3EE0AB82DB561AAC91A9E52B361FBFD93B63BF7A73026FEDC76B8B77483AA6AD1A54760DC20496F8666897E 8
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".... ....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "..... $START_LINK$ Goo

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\ms\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15330
Entropy (8bit):	5.193447909498091
Encrypted:	false
SSDEEP:	
MD5:	09D75141E0D80FBD3E9E92CE843DA986
SHA1:	B24EAB4B1242C31B69514D77BC1DB36A3F648F40
SHA-256:	8F1DBDEFD910AD88BEEC7956619CDB34391D6E69254C3A7497E8F87134AE8B5C
SHA-512:	935C69481F1555787FCB9A5490B3188B348284B600359239742A7D802ADD5CC8A30CC1F0942D52E620DFB388787FCD69B548BBAC590110245DF5763367A2DD5A
Malicious:	false
Reputation:	low

Preview:	{.. "1018984561488520517": {.. "message": "Tidak bergerak".. },.. "1213957982723875920": {.. "message": "Antara yang berikut, manakah yang terbaik menggambarkan rangkaian anda?".. },.. "128276876460319075": {.. "message": "Penemuan Peranti".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Sila cuba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Kelantangan".. },.. "1850397500312020388": {.. "message": "Adakah anda dapat melihat Chromecast anda dalam $START_LINK$ apl Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15321
Entropy (8bit):	5.221228928144735
Encrypted:	false
SSDEEP:	
MD5:	6DDB73E39B89687181221341448D2365
SHA1:	FA71231ACE49AEBAD99AF747E173CCC6C7FF0126
SHA-256:	21CAB8AF7F2ABF337CC33C51E9F4FD33A3AF08603CDDB74A30D4A05654F020FF
SHA-512:	FD25E3DCC8DEB8B5EB2FBCAE5C2F0FDD07F507EB2BC3B8AF83CE64DC4C4B4B15D4B73903E73C9668716C609F98A8083AFD44EA59833265CCACCE958CECA 5410
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Loopt vast".. },.. "1213957982723875920": {.. "message": "Welke beschrijving past het beste bij je netwerk?".. },.. "128276876460319075": {.. "message": "Apparaatdetectie".. },.. "1428448869078126731": {.. "message": "Vloeiendheid van de video".. },.. "152214 0683318860351": {.. "message": "Kan geen verbinding maken. Probeer het opnieuw.".. },.. "1550904064710828958": {.. "message": "Vloeiend".. },.. "1636686 747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Zie je je Chromecast in de $START_LINK$Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15418
Entropy (8bit):	5.346020722930065
Encrypted:	false
SSDEEP:	
MD5:	8254020C39A5F6C1716639CC530BB0D6
SHA1:	A97A70427581ADA902CA73C898825F7B4B4FAC8F
SHA-256:	2F4E4FC6AEB4A8E7F0E0DCE220D66E763F4EBF1FA79985834D636C6692FEA3E8
SHA-512:	9A2CD0F061A943CE04789FF259ECE5B3CCA11EBB6C1DF16C703F70394A5F89415E8EFB79CFB4646FC07FD261170A74602644FFF02ABD38548895CDF7DAB68E 6
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zatrzymuje si.".. },.. "1213957982723875920": {.. "message": "Kt.ra z tych opcji najlepiej opisuje Twoj. sie.?".. },.. "128276876460319075": {.. "message": "Wykrywanie urz.dze.".. },.. "1428448869078126731": {.. "message": "P.ynno.. obrazu".. },.. "1522140683 318860351": {.. "message": "Nie uda.o si. nawi.za. po..czenia. Spr.buj ponownie.".. },.. "1550904064710828958": {.. "message": "P.ynna".. },.. "1636686747 687494376": {.. "message": "Idealna".. },.. "1802762746589457177": {.. "message": "G.o.no..".. },.. "1850397500312020388": {.. "message": "Czy Chromecasta wida. w.$START_LINK$aplikacji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\pt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15475
Entropy (8bit):	5.239856689212255
Encrypted:	false
SSDEEP:	
MD5:	FABD5D64267F0E6D7BE6983AB8704F8C
SHA1:	D4DAAD0FF5C461C51E6C1FD22B86AFC5B13E123F
SHA-256:	D82DCA262FF005668B252B478DEDAAC4A5C1E417AF9DE57C22F169A6680183AE
SHA-512:	AD8B2129DCB4F232AEDD7A2B90AF2EFA43497F9118C27AB843D279F7B0EDF70AF95251B46C8098AA831FEC0B2AF6AB0308D3DCFD9AE87BEA8AD9E0D1032E F8B

Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congela".. },.. "1213957982723875920": {.. "message": "Qual das seguintes alternativas melhor descreve sua rede?".. },.. "128276876460319075": {.. "message": "Detec..o de dispositivos".. },.. "1428448869078126731": {.. "message": "Suavidade da reprodu..o do v.deo".. },.. "1522140683318860351": {.. "message": "Falha na conex.o. Tente novamente.".. },.. "1550904064710828958": {.. "message": "Suave".. },.. "1636686747687494376": {.. "message": "Perfeita".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": ". poss.vel encontrar seu Chromecast no $START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15655
Entropy (8bit):	5.288239072087021
Encrypted:	false
SSDEEP:	
MD5:	75E16A8FB75A9A168CFF86388F190C99
SHA1:	C27CE4C1DB3DF2D232925C73DC9AC1FA24DAD396
SHA-256:	9C4716FF42A730F1E7725F0D9E703F311E79FDA31F85B4BB0B8863FC3C27AB9D
SHA-512:	9E0BF56560B1D73F9706FF6AA2D5628CBE58EFCE197899A7EE686B2395D0FA2F9927538DD9B7B152CE2DED4708A210DA3DD6F5350E62AF853E809782997B192
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Redare cu bloc.ri".. },.. "1213957982723875920": {.. "message": "Care dintre urm.toarele descrie cel mai bine r e.eaua ta?".. },.. "128276876460319075": {.. "message": "Descoperirea dispozitivelor".. },.. "1428448869078126731": {.. "message": "Calitatea red.rii vi deoclipului".. },.. "1522140683318860351": {.. "message": "Conexiunea nu s-a stabilit. .ncerca.i din nou.".. },.. "1550904064710828958": {.. "message": "Redare lin.".. },.. "1636686747687494376": {.. "message": "Redare perfect.".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500 312020388": {.. "message": "Chromecastul dvs. apare .n $START_LINK$ aplica.ia Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17686
Entropy (8bit):	5.471928545648783
Encrypted:	false
SSDEEP:	
MD5:	8EF94823972EA8D2FC9BB7EC09AB1846
SHA1:	4171DC9CE9D82FDA5A280517A1FE58C907D75CE3
SHA-256:	1009DB9FFA64E411B31E0780EBA43B9C9F8B05B5AC8CCA9A38514650261ABB0A
SHA-512:	83CEC6CF43F4A5A998B987DA6B6F236B36078C560F1CD79366AEBF2950ECD881F0B3ECC1C0769D911381B4A1D5901121E3620CA1AC2401BDE12642BE64EFD6 A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "........".. },.. "1213957982723875920": {.. "message": "..... .. ..?".. },.. "12 8276876460319075": {.. "message": "........ . ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": ".. ....".. },.. "1550904064710828958": {.. "message": "....... .....".. },.. "1636686747687494376": {.. "message": "........".. },.. "1802762746589457177": {.. "message": "........".. },.. "1850397500312020388": {.. "message": ".. .... Chromecast . $START_LINK$. .....

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15733
Entropy (8bit):	5.409011445299871
Encrypted:	false
SSDEEP:	
MD5:	9FDFFDD627F96DF699EC9F9D3625502F
SHA1:	04B830F3C7DA394EEA6063B7405FA12B23E151CA
SHA-256:	73B21C2BD165AA33724EABF134AF52ADD9A7C202A1462F0BEDEA3BC6701DD470
SHA-512:	9B135A8430244EDD5ABDAB2537029765EA33468627EFC39477AFBC8429907DC307A1E5C06E2178472C7D46AE049B7C1F5112B91019056126451023FD2AD66325

Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zam.za".. },.. "1213957982723875920": {.. "message": "Ktor. z nasleduj.cich skuto.nost. najlep.ie popisuj. va.u sie.?".. },.. "128276876460319075": {.. "message": "Vyh.ad.vanie zariaden.".. },.. "1428448869078126731": {.. "message": "Plynulos. videa".. },.. "1522140683318860351": {.. "message": "Pripojenie zlyhalo. Sk.ste to znova.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "V.born.".. },.. "1802762746589457177": {.. "message": "Hlasitos.".. },.. "1850397500312020388": {.. "message": "Vid.te svoj Chromecast v.$START_LINK$aplik.cii Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15628
Entropy (8bit):	5.292871661441512
Encrypted:	false
SSDEEP:	
MD5:	F60AB4E9A79FD6F32909AFAC226446B3
SHA1:	07C9E383D4488BEBE316CA86966FC728F55A2E32
SHA-256:	CDE581E6E7CF0136B003B45549E3BBEE7B67B74ADD786A8D5607BFDAD1DE7B87
SHA-512:	F6A7673A8EFDB7FF74D7B83DD4BCB3683031DB7FBFE6654F6311CBA53EC42F3E45CE2B42A6E385F868271BBDD348272ACF9CE304E2DB52A10B36D24C7B0311 4F
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzne".. },.. "1213957982723875920": {.. "message": "Kaj od tega najbolje opi.e va.e omre.je?".. },.. "12 8276876460319075": {.. "message": "Odkrivanje naprav".. },.. "1428448869078126731": {.. "message": "Teko.e predvajanje videoposnetka".. },.. "1522140683 318860351": {.. "message": "Vzpostavitev povezave ni uspela. Poskusite znova.".. },.. "1550904064710828958": {.. "message": "Teko.e".. },.. "16366867476 87494376": {.. "message": "Odli.no".. },.. "1802762746589457177": {.. "message": "Glasnost".. },.. "1850397500312020388": {.. "message": "Ali je Ch romecast viden v $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17766
Entropy (8bit):	5.432888569680161
Encrypted:	false
SSDEEP:	
MD5:	127A5422BE8B58668A9502DC03C1639C
SHA1:	77603F93079A203D104CFF2806C55330658578FC
SHA-256:	C7B9ECE155924B9FA60662CDC1D1736A210018BD16E4B3E3613A2EE17782F0D6
SHA-512:	2421046C4E921F2181E5B8D4E478332BB74E561E7924D37EB7AB171847EA1D2748C94BB632198F0A78888F6F14EB5F1951B99EFA0AA0DC32A9C8E293CB4C3DC 6
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... ..".. },.. "1213957982723875920": {.. "message": ".... .. ..?".. },.. "12827687646 0319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "... .....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15135
Entropy (8bit):	5.258962752997426
Encrypted:	false
SSDEEP:	
MD5:	897DAE6B0CF0FDE42648F0B47CB26E06
SHA1:	E1F5F5F65AF34FF9484AB2B01E571EAF19BA23D0
SHA-256:	52656C24F6F6D0F3B3FC01E9504C4D5CEB85624F1B22E974CA675DD0E94EB82D

SHA-512:	399DEACFE61F4AF9B24AAA0357D30149CC49DA7825295933D3AE006714B5DE7AC5FCB9EC5340B0E3AB4ABF25641032BBBB5B7D578CD204F4EDEAFE6E08C55663
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fastnar tillf.lligt".. },.. "1213957982723875920": {.. "message": "Vilket av f.ljande beskriver ditt n.tverk b.st?".. },.. "128276876460319075": {.. "message": "Enhetsidentifiering".. },.. "1428448869078126731": {.. "message": "J.mn videouppspelning".. },.. "1522140683318860351": {.. "message": "Det gick inte att ansluta. F.rs.k igen.".. },.. "1550904064710828958": {.. "message": "Flyter p.".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Volym".. },.. "1850397500312020388": {.. "message": "Visas din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\sw\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15156
Entropy (8bit):	5.216902945207334
Encrypted:	false
SSDEEP:	
MD5:	EC233129047C1202D87DC140F7BA266D
SHA1:	537E4C887428081365D028F32C53E3C92F29AAA6
SHA-256:	28EDBC5C4858217811D45CAA215710E452C8926E4DE99F810001AD664D08BE0D
SHA-512:	2E3F9BA1EA9EEF921E76B46B5EF2404B3B77B61F18CF67CC78C23C62202227F678A3DBE9C730E42A310800914DC53F25E8B2FBF461839DE33D3501B0BCB4ECD
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Inasita kucheza".. },.. "1213957982723875920": {.. "message": "Ni gani kati ya zifuatazo inaelezea mtandao wako vizuri?".. },.. "128276876460319075": {.. "message": "Kupata Kifaa".. },.. "1428448869078126731": {.. "message": "Ulaini wa Kutiririsha Video".. },.. "1522140683318860351": {.. "message": "Imeshindwa kuunganisha. Tafadhali jaribu tena.".. },.. "1550904064710828958": {.. "message": "Laini".. },.. "1636686747687494376": {.. "message": "Bora".. },.. "1802762746589457177": {.. "message": "Sauti".. },.. "1850397500312020388": {.. "message": "Je, unaweza kuona Chromecast yako katika $START_LINK$ programu ya Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\ta\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20531
Entropy (8bit):	5.2537196877590056
Encrypted:	false
SSDEEP:	
MD5:	C50C5D2EDFC79DBDCBD5A58A027A3231
SHA1:	14314D760A18C39F06CD072CF5843832AFB86689
SHA-256:	EEB0E89D5AD92B80FF08F88533A111DB3416D7C3860C64227D1CC8B7C2B58298
SHA-512:	A241084C44260C239CB8E6736AB7F7D1988142DDA6CAAD9F907FB42970BE56EC8DA6956BFBE97F926C6EFA32B750F1F57815980494BC31D27DF609C04421AD4
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... ....."..},.. "1213957982723875920": {.. "message": "..... ... .?"..},.. "128276876460319075": {.. "message": "..... ....."..},.. "1428448869078126731": {.. "message": "..... ...."..},.. "1522140683318860351": {.. "message": "..... ...."..},.. "1550904064710828958": {.. "message": "..... ....."..},.. "1636686747687494376": {.. "message": "....."..},.. "1802762746589457177": {.. "message": "....."

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\te\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20496
Entropy (8bit):	5.301173454436774
Encrypted:	false
SSDEEP:	
MD5:	28425862224952A50E881BFA19475ECC
SHA1:	BDAEC83C2988AFE15D886FE5428FA7870FF1FAF4
SHA-256:	793A422E88496566E3EF1E22F30784268716613EBB56C58DC5C0F4B5344F87BF

SHA-512:	16AECF9768E72D3654A6D9CD21EB57693EBCCB15C60B20CE0F722C24627CC64F3BB9BD5951112A1A8933AD65E1ACDD1013D4F1BB433A4170A99B19003FDE9 9F
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "........".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "12827 6876460319075": {.. "message": "..... ....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "..... ....".. },.. "1802762746589457177": {.. "message": "........".. },.. "185039750031202038

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18849
Entropy (8bit):	5.3815746250038305
Encrypted:	false
SSDEEP:	
MD5:	9F926FCB8BAEA23453B99EA162CCDEA1
SHA1:	04D1E45591C0435A39DCA00A81E83E68585E8B64
SHA-256:	100463C587F549C964A4EB21EA38EA1B4ADEF11E927FAC8FF884623B77202C02
SHA-512:	F226278DDF2D1995961690895361AB7B5D221C5E36D7767BBA71F36716C27B28210F85DC7DB4D2FC61B048FE2D058EE76EFBF2AD2A9714375149C4D09E18BE2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...."... },.. "1213957982723875920": {.. "message": "..... ....."... },.. "128276876460319075": {.. "message": "....."... },.. "1428448869078126731": {.. "message": "....."... },.. "1522140683318860351": {.. "message": "..... ...."... },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "....."... },.. "1802762746589457177": {.. "message": "....."... },.. "1850397500312020388": {.. "message": "..... Chromecast ..... $

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15542
Entropy (8bit):	5.336342457334077
Encrypted:	false
SSDEEP:	
MD5:	B0420F071E7C6C2DE11715A0BF026C63
SHA1:	F41CC696786B18805DB8DC9E1E476146C0D6BE90
SHA-256:	309F946F753DF6AF5C255D772EA0D429462152F78ABA4A96A2E369707A2C6B67
SHA-512:	67B42FC962AB70FFF86777E5057047EF4CFFDA4BED040F9D45BB5DB0275C3B5F21B17924AE5C51C71E8B078AB88AE3001C70CDB4E1994D4C8A20DEFC3A1D3 FA
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Donuyor".. },.. "1213957982723875920": {.. "message": "A..n.z. a.a..dakilerden hangisi en iyi .ekilde tan.mlar?".. },.. "128276876460319075": {.. "message": "Cihaz Bulma".. },.. "1428448869078126731": {.. "message": "Videonun D.zg.n Oynat.lmas."... },.. "15221 40683318860351": {.. "message": "Ba.lant. ba.ar.s.z oldu. L.tfen tekrar deneyin."... },.. "1550904064710828958": {.. "message": "D.zg.n".. },.. "16366867 47687494376": {.. "message": "M.kemmel".. },.. "1802762746589457177": {.. "message": "Ses d.zeyi".. },.. "1850397500312020388": {.. "message": "Chr omecast'inizi $START_LINK$Google Home uygulamas.ndaEND_LINK g.rebiliyor musunuz? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_L INK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17539
Entropy (8bit):	5.492873573147444
Encrypted:	false
SSDEEP:	
MD5:	FF06E78C06E8DFF4A422EA24F0AB3760
SHA1:	A434D1CE22DE0D2FD1842E94F5815F7B1972D1EE
SHA-256:	E209FDEF12CCEC03B4E0D5B9464F90D527E62C5BC4DD565C680661D7F282AB02
SHA-512:	8EADCC918F51A946A68AAF4D9DD7F3894BE470FD0A0550E4160D609F30C78BD55508B3DF4D62A28C0813D83C5C10F9A7BFE656A4CF519E4CC814FFB07F1E9F 3B

Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".. . ...?".. },.. "1282768764 60319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": ".. ....".. },.. "1550904064710828958": {.. "message": "..... .....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802 762746589457177": {.. "message": "......".. },.. "1850397500312020388": {.. "message": ".. .... Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeho

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\vi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16011
Entropy (8bit):	5.466848470908827
Encrypted:	false
SSDEEP:	
MD5:	05A2C5EED47B155AA9EC9BC3DC15D6A5
SHA1:	09E795DC1FDF80B5E96728C8B1C701B8194DCF97
SHA-256:	EE794AD0D6BAD28C783962EA92CA2E7CDA8E374FFDF083711B03149EFB2A7D32
SHA-512:	38A10B8357D6A6BEA1BFCB760F2103D2B271477D71811ACD86761B70D4B6C8BD7A80E157CF658D751F8BB169725EBCC748EA2D90AAECC42708064D49DA9695 5
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "D.ng h.nh".. },.. "1213957982723875920": {.. "message": "Tr..ng h.p n.o sau ..y m. t. ..ng nh.t m.ng c.a b.n?".. },.. "128276876460319075": {.. "message": "Kh.m ph. thi.t b.".. },.. "1428448869078126731": {.. "message": ".. m..t c.a video".. },.. "1522140683318860351": {.. "message": "K.t n.i kh.ng th.nh c.ng. Vui l.ng th. l.i.".. },.. "1550904064710828958": {.. "message": "M..t m.".. },.. "1636686747687494376": {.. "message": "Ho.n h.o".. },.. "1802762746589457177": {.. "message": ".m l..ng".. },.. "1850397500312020388": {.. "message": "B.n c. th. nh.n th.y Chromecast c.a m.nh tro ng $START_LINK$.ng d.ng Google HomeEND_LINK kh.ng? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "conte

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\zh\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):	14773
Entropy (8bit):	5.670562029027517
Encrypted:	false
SSDEEP:	
MD5:	D4513639FFC58664556B4607BF8A3F19
SHA1:	65629BC4CBBACA498F4082DD5884C8D3D7DDDC8A
SHA-256:	C6D49997A9B4FF7FE701EC3644B1A523679A27778FB4BD39B7DBCA9F1ACCE595
SHA-512:	16260FAC30D57EBFD577833F45D52FEA446ABE877D0D4015EF47C5C9072B81DDA71ED4E5E7DAFDEBE82B26556A4477EA4BFCDEC227058E381B9812DAB1F43 79B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..".. },.. "1213957982723875920": {.. "message": "..".. },.. "128276876460319075": {.. "message": "....".. },.. "1428448869078126731": {.. "message": ".....".. },.. "1522140683318860351": {.. "message": ".....".. },.. "1550904064710828958": {.. "message": "..".. },.. "1636686747687494376": {.. "message": "..".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "... $START_LINK$Google Home ..END_LINK..... Chromecast ..$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START_SPAN": {.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL_locales\zh_TW\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):	14981
Entropy (8bit):	5.7019494203747865
Encrypted:	false
SSDEEP:	
MD5:	494CE2ACB21A426E051C146E600E7564
SHA1:	D045ECC2A69C963D5D34A148FE4A7939DE6A1322
SHA-256:	A1053F9496ED7FA3C625C94347F07A5E760F514FD8EE142EC9EE64E86B9C063D
SHA-512:	DE2C8498B55749B4D35CF2627E55271F7F09E4560FA16D7094EFB4085CF1E5FAE36F067AAC01AE120548C00DC8AA530EE96079B5CC3E322DF9FF8592799AEB3 F

Malicious:	false
Reputation:	low
Preview:	{.. "10198456148852051 7": {.. "message": "....".. },.. "12139579827238759 20": {.. "message": "..............".. },.. "128276876460319075": {.. "message": "....".. },.. "14284488690781267 31": {.. "message": ".....".. },.. "15221406833188603 51": {.. "message": "..........".. },.. "15509040647108289 58": {.. "message": "..".. },.. "16366867476874943 76": {.. "message": "..".. },.. "18027627465894571 77": {.. "message": "..".. },.. "18503975003120203 88": {.. " message": ".... $START_LINK$Google Home ....END_LINK..... Chromecast ..$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7748_327753163\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1980
Entropy (8bit):	4.855422406261543
Encrypted:	false
SSDEEP:	
MD5:	30B78A52B000FF35C18C3D435CA15075
SHA1:	3DEB89546193DA52C8843D90325290496C6E47DD
SHA-256:	0A20B0B88FEBE7464BC199663D5DBC2BEA252394C69D352C091E0C7C1538E90F
SHA-512:	B8C705C21F61362060CF4374210802B4701DA2BE64318D2C766848364BE6B33535BE333F31D23CA854A73F1344204A2AE0DFC97B1BD081DC39199C3CE937BD7
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "background": {. "persistent": false,. "scripts": [. "common.js",. "mirroring_common.js",. "background_script.js".]. },. "content_security_policy": "default-src 'self'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; script-src 'self' https://apis. google.com https://feedback.googleusercontent.com https://www.google.com https://www.gstatic.com; child-src https://accounts.google.com https://content.googleap is.com https://www.google.com; connect-src 'self' http://*:* https://*:*; font-src https://fonts.gstatic.com;",. "default_locale": "en",. "description": "Provider for discovery and services for mirroring of Chrome Media Router",. "externally_connectable": {. "ids": [. "idmofbkcelhplfjnmmdolenpigiiiecc",. "ggedfkijiiammpnbdadhllnehap omdge",. "njjegkblellcjnakomndbaloifhcoccg".]. },. "manifest_version": 2,. "minimum_chrome_version": "37",. "name": "

C:\Users\alfredo\AppData\Roaming\Microsoft\Spelling\en-US\default.dic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	low
Preview:	..

Static File Info

No static file info