ID: 655625
Sample Name:
test@barclays.com.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 11:15:49
Date: 01/07/2022
Version: 35.0.0 Citrine

Table of Contents

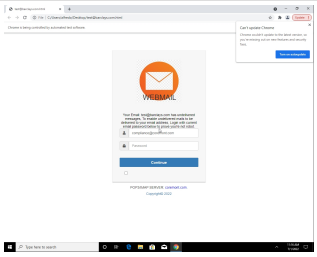
Windows Analysis Report

test@barclays.com.html

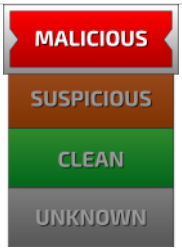
Overview

General Information

Sample Name:	test@barclays.com.html
Analysis ID:	655625
MD5:	3ff5b2d36016905.
SHA1:	ee9774db8ab8b5.
SHA256:	c786576470e647..
Infos:	YARA



Detection



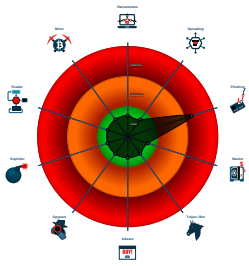
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish44
- HTML body contains low number of …
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 7108 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument C:\Users\alfredo\Desktop\test@barclays.com.html MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 7392 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1708,15171800579801753561,3977679138883550371,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2100 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
test@barclays.com.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish44

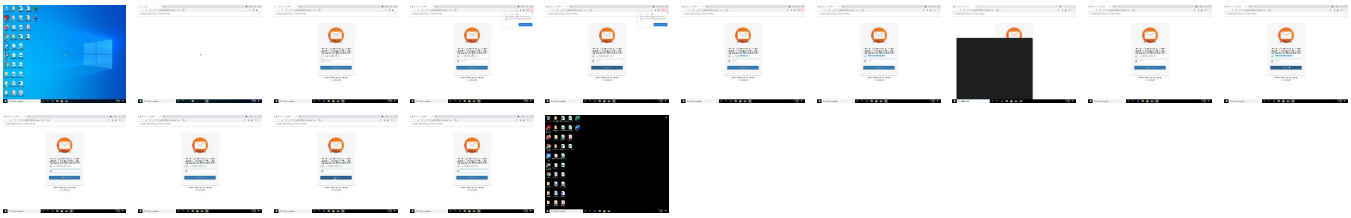
Mitre Att&ck Matrix

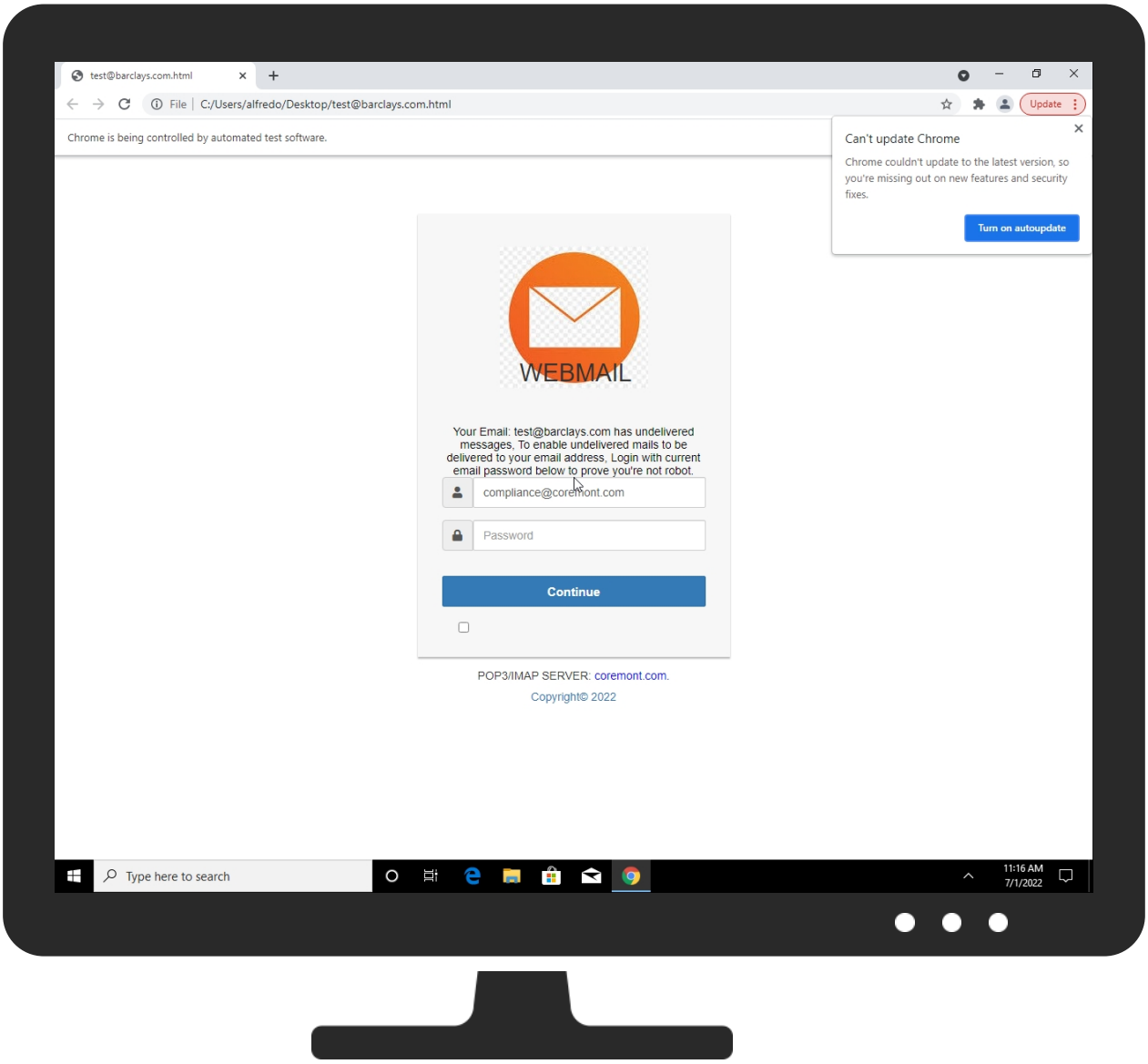
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

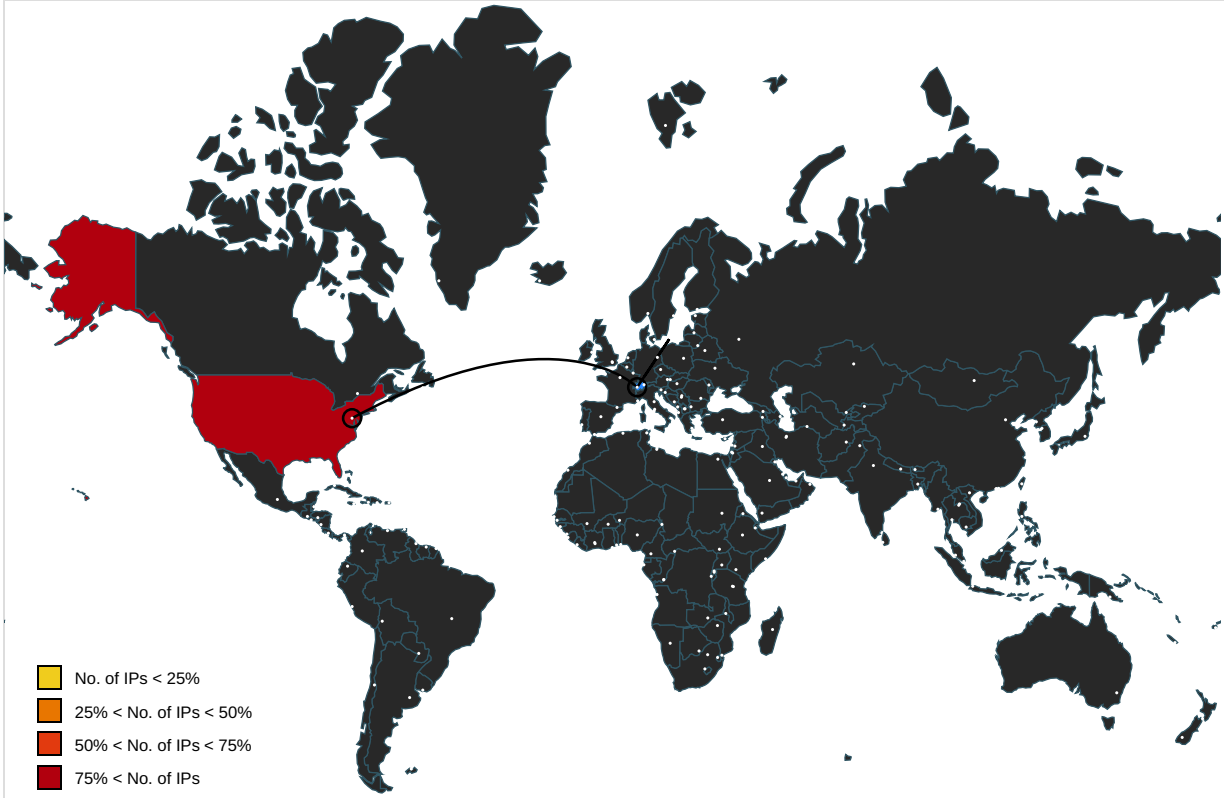
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.35	true	false		high
stackpath.bootstrapcdn.com	188.114.98.173	true	false		high
accounts.google.com	142.250.186.173	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	142.250.185.238	true	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/alfredo/Desktop/test@barclays.com.html	true		low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.35	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
172.67.150.137	unknown	United States		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
216.58.212.131	unknown	United States		15169	GOOGLEUS	false
142.250.186.173	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.187.131	unknown	United States		15169	GOOGLEUS	false
142.250.185.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.170	unknown	United States		15169	GOOGLEUS	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.99	unknown	United States		15169	GOOGLEUS	false
188.114.98.173	stackpath.bootstrapcdn.com	European Union		13335	CLOUDFLARENETUS	false
104.18.23.52	unknown	United States		13335	CLOUDFLARENETUS	false
142.250.186.74	unknown	United States		15169	GOOGLEUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655625
Start date and time: 01/07/202211:15:49	2022-07-01 11:15:49 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test@barclays.com.html
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	15
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
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTML@21/144@8/108
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 142.250.187.131, 69.16.175.42, 69.16.175.10, 142.250.185.170, 104.18.23.52, 104.18.22.52, 142.250.186.74, 34.104.35.123, 172.67.150.137, 104.21.30.41
- Excluded domains from analysis (whitelisted): kit.fontawesome.com.cdn.cloudflare.net, cds.s5x3j6q5.hwcdn.net, fonts.googleapis.com, fs.microsoft.com, ka-f.fontawesome.com.cdn.cloudflare.net, slscr.update.microsoft.com, ajax.googleapis.com, fonts.gstatic.com, clientservices.googleapis.com, edgedl.me.gvt1.com, login.live.com, sls.update.microsoft.com, nexusruleses.officeapps.live.com, glb.sls.prod.dcat.dsp.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 NtSetInformationFile calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\5dd7ae69-e6ad-4a15-a5cb-99a213f83493.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):	112061
Entropy (8bit):	6.032835052530584

Encrypted:	false
SSDEEP:	
MD5:	606BF84462DA3BF118B57CCBCCCA0908
SHA1:	30346F0C2D4E1C67157820B8F3E3AB43A50FB0CA
SHA-256:	663E98BC8873110A1CE0EC471716B51450DA063E329B039D24895E104D936A70
SHA-512:	468F603FC893822104EBF735881A64446FDA9C628A9138F7E314D4E0488C93A4BDC68F502456681DC8A828385FB4D225641C63FDBA26DE099A2B2B1C5C1AC19(
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":1.656699387628812e+12,"network":1.656666988e+12,"ticks":174527904.0,"uncertainty":3036651.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RklezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"last_statistics_update":"13301172985198270"},"profile":{"info_cache":{"Default":{"active_time":1656699386.461558,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\7edfe7eb-47ee-4924-af2b-297a69664551.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95480
Entropy (8bit):	3.761968837842764
Encrypted:	false
SSDEEP:	
MD5:	A43AA409DE92FE3BA54E95FD414EC15E
SHA1:	A88649F9083446794C82BBE241D8CBC17F9F4F55
SHA-256:	4F3281212878C276CFCA43E8C4454B68801ABBA275FB39FCB20B7CEF84C952C8
SHA-512:	65CA44B5FE9C3DED069CBABD64EB2B3DA1C237153CEFB41AB664F2C43D43C7EAA03E2AF44EF993BF301740E1B6E509434A15EA9746186BCEDCD798E1220F3352
Malicious:	false
Reputation:	low
Preview:	.t.....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....`8. ...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.....`8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\934a3bab-1920-40b2-aca2-fff43d1629aa.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):	112080
Entropy (8bit):	6.033130875358341
Encrypted:	false
SSDEEP:	
MD5:	C031A298F7A7058C9A93528C9D1B19B4
SHA1:	6BCF1B8576A1DF903900C92ADB2F76FDDD240D4C
SHA-256:	7CE0C96EF16826731309298F81D1F37B33E42F10DFEB98ABC763A45E98E65B22
SHA-512:	7149A3CC2E592C66105F2901DBFE92894B94A6DB7289685F012A78E6C725D13078D84A9DB260D35AD57BF93C72086933BAA2F1B6D9F50E4F775BA4B0E733E6C
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":1.656699387628812e+12,"network":1.656666988e+12,"ticks":174527904.0,"uncertainty":3036651.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RklezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"last_statistics_update":"13301172985198270"},"profile":{"info_cache":{"Default":{"active_time":1656699386.461558,"avatar_icon":"chrom

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\05f5fc9d-0b67-4173-b3d0-47807686f7eb.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):	5.5735441201447
Encrypted:	false
SSDEEP:	
MD5:	9E98E65F7FF1002C90AE93B9CEC43C8D
SHA1:	F4D33182C4C575EAED4900E608AFD08915D7D873
SHA-256:	9D597ACFFB15A76D486426C6A69692B0D274F6FC36F47D70E2901BB10FB67E30
SHA-512:	4C7F65C89EAE69E1C8D23819B9348F8AEC52D1B9B31BA3F2F96356AA1416412C01552D0CA32882FD19DADFFF082EC94B5D4EDA139C9F1AA5824EB613F1DB9774
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":"13301172985569893","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\425d98ad-f4df-4e13-b8fb-41dff37b5585.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\4b5a2f7e-0423-447f-8da5-5df0d2bb6dd8.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):	18586
Entropy (8bit):	5.558479837229627
Encrypted:	false
SSDEEP:	
MD5:	7D53BA39268087A0445A530F4275C4DF

SHA1:	140E0819A240386FB10258BDC9A72D9809EDAC3B
SHA-256:	593053B93C985AADF42EB393643439922565C6B3CDD719CE16E520F69B37D33E
SHA-512:	B14A119F822A413F380B06B71FBDC7F8892C202D0E57295B46AA11883E7491B428E4C14DC2F21DA3C487B2D7591CB1591E395BAC1A5F6AD74D716AF8F1ABD0E2
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":"13301172985569893","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\52d67da0-d354-4a40-bad6-22c5d5bd7bf3.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...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\592ac4df-946e-4d99-9532-8cb93f7c5a77.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):	16478
Entropy (8bit):	5.571378577833114
Encrypted:	false
SSDEEP:	
MD5:	DEFD43D583EFE7C6727973F1BDF3A4D3
SHA1:	119B8B593A1C9EF3CD18B59D69D98B3B8C30F2AF
SHA-256:	2478AE7B4F76CD06021A86DE4B19E23E6F2637B4CBFB8427D787D171F2770BFA
SHA-512:	D6244EBC6A025692F787CE7E4468D281BE3CE9A9023F3E93ED04693724B1D21AB46B1F21DE672ED228E1537EECF6FA1F25EACD9084747B27EE4A11A5C01AD352
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":"13301172985569893","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\7220f273-efaa-47a9-bdff-54e88e0f464d.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):	3488
Entropy (8bit):	4.943776399173666
Encrypted:	false

SSDEEP:	
MD5:	9FE04B27A90D5BE23E33B81EED767497
SHA1:	1FB3F7142B2999CE980EF49174A16BD2EBC20077
SHA-256:	73D6BB0B8CA6CE08375D79F20F066375BA26474FFD6B0B3CBB04CF3D6FF09963
SHA-512:	EEB94657CC4300A831911C135714AE552FC17E4251C4193E36A667A9511545DB18C5BDAFC3998E883288671EC19E8C2A32601740122AB618EE1FA5E9A7CB1B9A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172986639748","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":2739},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301172986632070"},"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":"87918f8b-68c8-434f-bb4f-34345c3e655b"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"6AD9AD61E0153714185 4BC739159265C","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\7a4b5349-6aec-4abd-8d0f-8d8b0bc4a6a6.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):	16479
Entropy (8bit):	5.571406526074186
Encrypted:	false
SSDEEP:	
MD5:	2A9337176AE2FA7AEAD31965F1F811F7
SHA1:	D574ECABB1BCB5BB0D7CCE2471EAF255F646D01A
SHA-256:	936450830988A4081D48EF78E1D8BE40C8AD1E991801AB0ADF7644DE5F2636E0
SHA-512:	A78EDCE653E58BB509290F670B3760C8D44E5AD9599561296FFB495EBF46108A58A51B68DC821FF43F91F8CA891DFBAEAAAA536AF9A0F424FE4110A563280033
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":"13301172985569893","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\Extension Rules\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.703350913120781
Encrypted:	false
SSDEEP:	
MD5:	2EEF53AE6DE9AD256284DD6755FD531F
SHA1:	261CCFB8513BA731EFDA38A1B282E701F425336F
SHA-256:	F4B932DAC8AE2E0D7E6ECEF3499839A01BDD3E11C6EC85786146546E2C8AF8F5
SHA-512:	7A7FEE95114F58EB82E582D0C397615B1B105305FCB17653D82B9AFDDD067D7010FA9FBB0A99D10B5DA5D79E148D2C5B2D6B2FEE107078132C36DE48A09666
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.139607015814034
Encrypted:	false

SSDEEP:	
MD5:	2F321C3082652B29D4BFD091EFABE973
SHA1:	75EAE53F68851DED6ABE8A63FC77FE757669A7EB
SHA-256:	C5B740E4F55FE9EB88ABBDFF76E806FC229F1D23EEEF0A5211F271AFD1053540
SHA-512:	CEFEC5241B0C0CC894252C7EA04DFCEBEFB7E89AD0CEB30A7CC1F700472DF9B94583F674AB18A2BBEE89BE04560FF65D723DBD5AC5523429AF5372B915CBAF21
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:16:26.661 1da4 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2022/07/01-11:16:26.662 1da4 Recovering log #3.2022/07/01-11:16:26.663 1da4 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.201480325031026
Encrypted:	false
SSDEEP:	
MD5:	ED64AEF0CFB4EBB413973DD729C23441
SHA1:	A1A4CA6FBAA6CB3A8E4F4ADDCD1560338471BD56
SHA-256:	D1BC3ACEB13E1E1FF82C91DE37C82A303ED59A684C0D2107E2A690E25B11EB03
SHA-512:	FFCF60D99E79E7627AEF7688EC4EC51F6970E257C3EB84ADAC9CD894E7006299F20D14583EAB5A8B8681E98453F6084DF9ABFA224459C9CA46D5DA27E875192
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:16:30.476 e28 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2022/07/01-11:16:30.477 e28 Recovering log #3.2022/07/01-11:16:30.478 e28 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018164538716206493
Encrypted:	false

SSDEEP:	
MD5:	DE21D7B08C7B46E96C7227600C2615E7
SHA1:	5D08759EEF7044ED91BD4A3E197C0F94315E9932
SHA-256:	55BFA2933016C9F7B529D2D20E19739DB8DD0D33E7B7EDBB92C136DE998A932C
SHA-512:	6EAC6FD82B59EC30CF613D6A1A9F03F3E7D5D1ED1002CDCC05CF45FB8360FCB8AF5E0436C8038DD2EFA884F58DB0362F36246D02363CD8297BE8791C34C3D54
Malicious:	false
Reputation:	low
Preview:	....

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.)...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...I..U].M.5@.....6...C...@..T....EW..LX..=K..O b..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\History

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.4917652753081512
Encrypted:	false
SSDEEP:	
MD5:	4D943E53BA68D5573BB84E9E004E97AF
SHA1:	A17DC9505818F35F5AF1BDF9A7A3C3F02D0F4BC4
SHA-256:	AACA76BA0C0BE569DCBFF85FB3D661C412633BF913681A0DEE109CDECF8068D7
SHA-512:	7D7E717D7AA5005A2597B6F4811EC8BFE3FD630535CD56187003623EEBBB8C209035B7A9A150CCF1F71A75288B39FED4601DFDF5F336A461E74C4BA76E07242
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.145956800026923
Encrypted:	false
SSDEEP:	
MD5:	F6858E2EB0D9057C7ADDFD95E0388BB7

SHA1:	BF9D2C3D4CC4FD2C856CB5A2CEE376E46DDE334D
SHA-256:	48473C173A2A557AC869EB3592594DACF63142F5B2357B9A7C9D3C54EC9DE78C
SHA-512:	E079EE331CB14A7A6AF0D72D3B64A140C3C3FD3FC76DCDB83340E996B49FAD22CF84CD88A8B2CEA6A21A54C547D05029832755F7E27EE4CFB57E065CAB1A2257
Malicious:	false
Reputation:	low
Preview:	......"?....alfredo..barclays..c..com..desktop..file..html..test..users*c.....alfredo.....barclays.....c.....com.....desktop.....file.....html.....test.....users..2.....a.....b.....c.....d.....e.....f.....h.....i.....k.....l.....m.....o.....p.....r.....s.....t.....u.....y...:S.....B_...[..... .....*7file:///C:/Users/alfredo/Desktop/test@barclays.com.html2.:.....J.....!&/3

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.175123052155276
Encrypted:	false
SSDEEP:	
MD5:	1E962BEFB590B4E940A3603FA8D5BFB2
SHA1:	83A086C37A984D34C8B68E91C7273536A43A9E7C
SHA-256:	B469A0FD3142DCC68CCD84CF58F088263B06259A5BF2202767438654912FF600
SHA-512:	BBF788DDB911BA9DEA7EB5199B5CF62C0865CC70D9AA3433A1476A4B343CE3555C3204F7506D1D45D60ABB5D353108B4AFBC7F4DF08F77A62DC5290323937991
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:16:25.798 1dc8 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2022/07/01-11:16:25.870 1dc8 Recovering log #3.2022/07/01-11:16:25.874 1dc8 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.7766145155282294
Encrypted:	false
SSDEEP:	
MD5:	5BA75311B1B0D6276E298ECCD12B8B07
SHA1:	AD9ABB15695F177530511DFD188EB8C33B8F7929
SHA-256:	AEB7F25D09A00715C768CB87BA66EE544830347F998CCF218DE5C2072C4AAF3E
SHA-512:	B60C61AA8F0448365E90B8076A04BBCF945A289E4B851648925B53F9340B89C97553B28D63753A91E53AD64D34C19DB294913DB159A934DF9B5AFCBF951E0617
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....O}..... ....

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):	4.943776399173666
Encrypted:	false
SSDEEP:	
MD5:	9FE04B27A90D5BE23E33B81EED767497
SHA1:	1FB3F7142B2999CE980EF49174A16BD2EBC20077
SHA-256:	73D6BB0B8CA6CE08375D79F20F066375BA26474FFD6B0B3CBB04CF3D6FF09963
SHA-512:	EEB94657CC4300A831911C135714AE552FC17E4251C4193E36A667A9511545DB18C5BDAFC3998E883288671EC19E8C2A32601740122AB618EE1FA5E9A7CB1B9A
Malicious:	false

Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172986639748","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":2739},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301172986632070"},"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":"87918f8b-68c8-434f-bb4f-34345c3e655b"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"6AD9AD61E0153714185 4BC739159265C","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):	18586
Entropy (8bit):	5.558479837229627
Encrypted:	false
SSDEEP:	
MD5:	7D53BA39268087A0445A530F4275C4DF
SHA1:	140E0819A240386FB10258BDC9A72D9809EDAC3B
SHA-256:	593053B93C985AADF42EB393643439922565C6B3CDD719CE16E520F69B37D33E
SHA-512:	B14A119F822A413F380B06B71FBDC7F8892C202D0E57295B46AA11883E7491B428E4C14DC2F21DA3C487B2D7591CB1591E395BAC1A5F6AD74D716AF8F1ABD0E 2
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":"13301172985569893","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\Session Storage\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	327
Entropy (8bit):	2.5384726236607107
Encrypted:	false
SSDEEP:	
MD5:	A66EFAA590A0D16B1874A35836BA0A4B
SHA1:	BB750C61E162420271F89A90F2B58F43587680E1
SHA-256:	B9AB1ED7609E2254B7D4FB655B57B21B2BE601646C4FF0B207C411E8BDD9E654
SHA-512:	2B1EA0C798B69B360AB1546D14FCCF7D5F9CB224B31BC8430CDB956C8CC570A086E4CFA10E6A843292DEB862F4161DFC9B9ABBC44AFE397FF0EC9563646FFA5
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13301172988058248

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2897
Entropy (8bit):	3.2501537967237804
Encrypted:	false
SSDEEP:	
MD5:	66D7F18B5EE1106295AEB6F7BA114F8A
SHA1:	B89D443CBD8810F0D25D985A67053C591F60D371
SHA-256:	525680BF2EB62A206A2C078BBFAD3EBABFD073097107051768200301847 7CFE8
SHA-512:	5656006AD31A9502F3B2D0A508C43212BA14F6A64FAD6C407F8468243782242D6DA78518B4B342F275E56812BC3A71400346728723173 1CE0015374361CC9F41
Malicious:	false

Reputation:	low
Preview:	SNSS..... .....I.....1...,.....$...e1ddc875_31a9_4fd1_bf6a_53c34c1683a2.....T..... .....i..d.....7...file:///C:/Users/alfredo/Desktop/test@barclays.com.html.....x..... .....Lyb.....Lyb....0.....H.....@.....v...7...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.r.e.d.o./.D.e.s.k.t.o.p./.t.e.s.t.@.b.a.r.c.l.a.y.s.. .c.o.m...h.t.m.l.....8.....0.....8..... .....P...$...9.5.a.2.4.2.5.f.-.f.1.e.b.-.4.b.1.5.- .8.7.4.b.-.0.0.2.3.3.f.6.8.1.b.2.3.....P...$...f.6.2.e.2.7.a.1.-.e.1

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13301172989165152

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8386
Entropy (8bit):	3.1685766946953176
Encrypted:	false
SSDEEP:	
MD5:	5FCEA6CE4F44879903C7B7B219034FAD
SHA1:	229CC2BF13B8554F48E10E9717D4F739D8E78437
SHA-256:	6072BBFA7A2CF8D6F505A59FBBE217949414B5CAE833BFD1C7CDA62F3A54594F
SHA-512:	0A9A7D48F48984962C761DA41A4590625364B4726BAF5001A529999A6ECE71837CC0C0C0CC2E933D4A00689CCD7239BF8A67048D9CEDCD544C05578FACE6D1 6
Malicious:	false
Reputation:	low
Preview:	SNSS.....s.k..''/.M..H.....chrome://welcome/.....W.e.l.c.o.m.e. .t.o. .C.h.r.o.m.e.....x.....p.....l. D.B...m.D.B... .....8.....8.....H.....*.....c.h.r.o.m.e.:././.w.e.l.c.o.m.e./.....o''.route''.landing''.step''.landing{.....8..... ..0.....8..... .....chrome://welcome.....P...$...4.a.a.d.f.5.d.b.-.2.6.5.a.-.4.e.9.f.-.a.1.9.b.-.9.f.f.4.d.3. 5.1.1.6.4.b.....P...$...8.5.e.e.d.4.1.b.-.e.5.c.1.-.4.3.5.0.-.8.2.e.e.-.c.1.4.b.f.d.f.4.c.4.a.1.....chrome://welcome/.....''/.....''/.....''/..... .....chrome://welcome/new-user...>...W.e.l.c.o.m.e. .t.o. .C.h.r.o.m.e. .-. .A.d.d. .b.o.o.k.m.a.r.k.s. .t.o. .y

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.1059338072822555
Encrypted:	false
SSDEEP:	
MD5:	83DE52D6537120C3358301269F132826
SHA1:	D3DC7BEF5FA41F104E0DEE99018B7898C4034D9C
SHA-256:	A5C94A6AE6DCFE12CE6C2737C6A959675DE87A7FCDA6A102619278E494CCABEF
SHA-512:	6CCDBA6A5AD01A72875A68486FA4635A4E72D4791B64ED126D334D34AB2F934B5FEF66E72EC65CE2C3419136B05D056666F61983B08CE8B144D4CD3EF95524A 9
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:16:25.514 1e60 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00 0001.2022/07/01-11:16:25.514 1e60 Recovering log #3.2022/07/01-11:16:25.515 1e60 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Dat a\Default\Site Characteristics Database/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low

Preview:	....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000001.dbtmp

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

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C2375B
Malicious:	false
Reputation:	low
Preview:	.|..".....leveldb.BytewiseComparator.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.1393343230292
Encrypted:	false
SSDEEP:	
MD5:	8FE41E4DB3AB25D3A9DEC47648E5FD88
SHA1:	AEBC93DA47A9A7A42DBCE4171009CAEAF9B56F5B
SHA-256:	7601D002D420632409BA7B9B42DAFBC918B4A4117F1B3594CA6BB3DD33262833
SHA-512:	CD7D31F110D22AB83FCFCD479AFA74F990D397582A44DF0829E0F78E68430843CDEBF9590CB3E13F9045608CA2597ED44DEBC2DCBABBEF9716A2D43ED2102E0
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:17:04.438 1dc8 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2022/07/01-11:17:04.441 1dc8 Recovering log #3.2022/07/01-11:17:04.442 1dc8 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.219241002662272
Encrypted:	false
SSDEEP:	
MD5:	DB77A6ECAAA45C5E2DEA06E59416992E
SHA1:	AEB265427B8C069FBA10301F1937533F82A18625
SHA-256:	0AB7C52814035FB3F8C0122311CF908C938514FCA9F2776036FC9CD4B055269F
SHA-512:	EAECB537FFD25920FE4C0AE8998BBD2753562D56CBD9BC851463A297F01F9B28291A457021AC81B596F214A2A6CF65AB56A1E006DAC913C96D2B9A4F8206041 8
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:16:25.565 19a4 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2022/07 /01-11:16:25.566 19a4 Recovering log #3.2022/07/01-11:16:25.567 19a4 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0033769341339387224
Encrypted:	false
SSDEEP:	
MD5:	932B3CBB4FFEF066B8F4E492F17AA39A
SHA1:	872DD3F75498BE4E61960E85463837293FD06841
SHA-256:	63D24EB3FD5816D83FF649E69621BA0ED54615DECD72408FA70BDAED76A4C0C5
SHA-512:	7AC110540007704E8DF48B013E95C9E5BAE56FD283A2DF0A013F593CD43F7C1C9D3A1BCC34904D17BC08874ABC684D1AA1DB986F76D2A0EB59C025A262FCD 54
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....j....l7..... ....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Web Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2247582786585376
Encrypted:	false
SSDEEP:	
MD5:	6D741023AA69E2D4B124E4436F15E1A8
SHA1:	781C1E2C45C02C80FF693CA15A02525F4BCC91FF
SHA-256:	1D43AA9AAE20BA2B89AAF6101C93FAF4318116B0F0579A5EC04FC103AA978F19
SHA-512:	5CEA97EF5DD03AC7C14F8748D5A00ABDB3CB32AB14ED14C1E765FA0086C68C2A1501AE790DE1B208B44DC375A02EAD586FE4814E08E1E55863E3A767B3627 8F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....-.....&.....O}.....) ....

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\f6839c5e-12a8-4271-8c6e-3b1843bbc857.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):	4092
Entropy (8bit):	4.990395385865642
Encrypted:	false
SSDEEP:	
MD5:	027AA32DDE338A03F559A5BA14CD04D9
SHA1:	095473704A68D1DA87835E9E53BF3A6B515F633D
SHA-256:	F8FE11A8AEE9A82682D4D1C8A18AF32523400B6326DFE142E198EAA3571CA1F8
SHA-512:	D6A06A6AC225D32549E0C832B0F0BA7F297AD120FB0D5087B97D0A9302112913AAD7778B12B640BFC59DA5D2C58AECFCC6C14910CB0D9BA8BBA62BC7F7D21 5D6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172986639748","alternate_error_pages":{"backup":true},"autocomplete":{"retention_pol icy_last_version":92},"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":2739,"this_wee k_services_downstream_foreground_kb":{"115188287":57,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reportin g_timestamp":"13301172986632070"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_versi on":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656699388.47803,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm": {"product_category_for_subtypes":"com.c

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\ffc0ae26-ecd7-4faf-8bc3-14b4ecff9872.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):	4.943994402281553
Encrypted:	false
SSDEEP:	
MD5:	6252C023D5B949049BA78169ED2BED3C
SHA1:	B23D7E17556071E8D07CE01B881AABE15EE0A2BA
SHA-256:	0783F05D811A2BD0499E75892026CC77717328D034E9C709E2BA6939C2C84BC5
SHA-512:	CCBD8F5463FB3C3B8A5607F497D2AD5443947A1700569A75B4B051BCF09FB0F5EAA4988A267E90652E27492CEA16F30875D9721738AE019A5CED4DD0F5EA220 E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301172986639748","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_remov ed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_righ t":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2739},"default_apps_install_state":2,"domain_diversity":{"last_rep orting_timestamp":"13301172986632070"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"prod uct_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"87918f8b-68c8-434f-bb4f-34345c3e655b"}},"intl":{"selected_lang uages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"6AD9AD61E0153714185 4BC739159265C","engagement":{"schema_version":4}},

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):	112219
Entropy (8bit):	6.034089669751341
Encrypted:	false
SSDEEP:	
MD5:	B9FEA487887EE7D470950B1FC6228D29
SHA1:	60C02A858180B7CD5D1FFFA9D99A7E1064D93418
SHA-256:	95F746233B6E090E9503E6DF9AB1E7CC8FB081B5A00890276CD0397BD69D23D9
SHA-512:	A4C82F7B0C82F3B09841CB006F03190D1F7F4AB37A39E79978E02BE8114391701927C7C356A6DC9E341E567C0313095A0C01C32D1079AE36EE4713C34F95D0FC
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":1.656699387628812e+12,"network":1.656666988e+12,"ticks":174527904.0,"uncertainty":3036651.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187567243"},"plugins":{"resource_cache_update":"1656699446.6361

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\a7e5f443-b449-45ad-8e8b-7d84a52d0a3a.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):	112219
Entropy (8bit):	6.034089669751341
Encrypted:	false
SSDEEP:	

MD5:	B9FEA487887EE7D470950B1FC6228D29
SHA1:	60C02A858180B7CD5D1FFFA9D99A7E1064D93418
SHA-256:	95F746233B6E090E9503E6DF9AB1E7CC8FB081B5A00890276CD0397BD69D23D9
SHA-512:	A4C82F7B0C82F3B09841CB006F03190D1F7F4AB37A39E79978E02BE8114391701927C7C356A6DC9E341E567C0313095A0C01C32D1079AE36EE4713C34F95D0FC
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":1.656699387628812e+12,"network":1.656666988e+12,"ticks":174527904.0,"uncertainty":3036651.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187567243"},"plugins":{"resource_cache_update":"1656699446.6361

C:\Users\alfredo\AppData\Local\Temp\1bb9848a-13e0-481e-9182-6f8c10c78242.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):	3110
Entropy (8bit):	7.933903341619943
Encrypted:	false
SSDEEP:	
MD5:	A83A2746B84F1CF573B02965B72ED592
SHA1:	85CC572D6F90029EB99AAFA56297D1BCA494313A
SHA-256:	DF4B53C1C7C48E80753D4945E6EC7847084F51BF57F0ED9D341326C74651D6EC
SHA-512:	C287F479EF572A06FF191C4E9A8A718507C97A2A45CB265D7DC65DD7922B80D36CE7660EC5D7EA9F3D1F1EF71C51C3E4F3D7973754F97A89B4F14D1B1FDE70E
Malicious:	false
Reputation:	low
Preview:	.....ko.7.....J...../..v..... ....zE.\+.T..f..%wW.$.....p8/.....z..\|a...}.#y.`.l..7Kr..T:'.UE,.&.i..Y.....h...B.....gJ....%.\.?.f]1R..@3.jHA..eHi&.Q..`....g.__?'3^...@~X..a8.....UN..%...&.F..K19".Y:.).L.L..WL..xxD>.P@ ...&'..j..)%.Q\..<!.3n.<#....;.gd2.LZ....x.m&.e.`&;.KX..."...<G....8.R.jsd....g.)..?.$=UVT...#.+g.!.....R..1..#D.k...3.Bj3iT.....*.M..L....}..S.K.....zi..n.A{.....n..o.0j..q...w...3.7.N..].>...zK..sr1#.d..Tk..ckB...<....j.a.M1oe.9.jIQ.y+...6.....]....v.X.....q.....a>...2`.WV.v.'..~.3*.4.'8...hkT.H..9SOIF.%...;n.6.U....i!...2v.9/.;.....R..8.(..L.b....aY2ps% ."...x.V..Y[.h.....^.........U.....p.'.&m.....6..%pWE....:..o.k...<.....5....j.I...*9...f..3.....-..0..D;.....*S.td/...........^_.v.)y ..Uf..q>.v2...0....o....Y%5;.5fn..{.....p_.....B..V.....D.Y.I....q 3...sm.b..!..E....a. &.w.-.s..>..M_...`..0..k.!<SH...9$.....V.\A$..}..8....#`...,...3.W..k...\..xH.1).~.Y.L1.O...\.....k.....s..i+.....).0

C:\Users\alfredo\AppData\Local\Temp\cd7b350f-5982-4504-8046-216985eb3307.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	modified
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326688
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\cf3055ee-f737-4238-b99a-ce800a1e765f.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):	5168
Entropy (8bit):	7.956694278195136
Encrypted:	false
SSDEEP:	

MD5:	3E5CCD9B583763AF68E28C5101373167
SHA1:	2005CDC0A8070B65E321A197D576698ECC267496
SHA-256:	41412C0863920BA95E9FDBD3AF000CBE926A73C078997A233DF55379A5C4D274
SHA-512:	04BF4F7320326B085C40527797577D8770A30A1ED24A8587A000A5AE1D8F39E0B7F187DB14603295AC7A2901A4698683CC3BED2C2611539293A1927AB31BEAE1
Malicious:	false
Reputation:	low
Preview:	.....[ks.8..._.....#.,.G..8.;.55;.%..&5$e.....)..d._...%.....s.....+..Uv}...]rq.....luK.).zJh..3.&..Uu...W...s.H. .MV..\U3Ef.\.|...TU.9.z)I...u.+.g3U`Zs.6d...JiJ.rU.IV.".'L\|8 .d..j.J..q.....O."..<,...n...~\|E.dV.u.O..'"...e.uyJ?..?]~.?.....M.,.7...j.,.fz].. >+o.gz....<^(5.Jg_.Ap.U.i.....?.8.....,.*.*./.iQ..8.....A.DO/....?.~..N.~a.-..g.N~.....o.^...L.mW.]:{..... /.....[VkTu[wki.gK...;-.<...\.".3]..}V...)9i.V.P="m?.....V.i...7..S.U.d..(..\....g....bU.....}.....P9$.A...N..ckV..Qz..A....7..{pd.f.7....}6on.....7J;...Y..l>W...H.Z.....j..... Wk9vj+V.W.zAm.....P.oYo..|.....}.g.^.p...Z....l%cT|LN3..H.....{...~.J.%.!k.(.)..."....q.%.V.. d..MZ.`.....o..m3....1.../..jeH.....Q....X...j..o..|.o.r..nVw._...9 .....o...l....!...{....xU5.. }.x.I..3.vT%z.k..o.....^.S*.t(....+r\.u<...G.`.....g...r..?...}7.=.....c~.F.e..w.v$sC/.B.p.D~..J...:....7Vl3w...s.-".....]+..KO.~....%.I..?.&.o...\?.9..

C:\Users\alfredo\AppData\Local\Temp\de7d353a-91ad-46d9-9dca-e1f03ca82a0b.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):	28748
Entropy (8bit):	**7.9918576871001425**
Encrypted:	**true**
SSDEEP:	
MD5:	2A37AD0EC191D53104BB46953AC6C43C
SHA1:	FD23FFC5B7E4A6B45FBD88A486D15FAA51DC07AE
SHA-256:	51F075EB69486CB23B32A0776782B4A1B2AF204429AB94510469E02B115E56CC
SHA-512:	AEB91CB7902A800D7B0C43627EC2B52121BC41BA29A1B6ABEDBFCFA4802254A0594ED239EA7A3F8D40241E43D436428D1E4AC117BD97269D78460F82F9BDCF 68
Malicious:	false
Reputation:	low
Preview:	.....Zms.6...._..p..[.(.b[...M....N{..t ...S.....v...H.q.g:....]...p..6I8_d...C.\p.X$.2.p.g.8I}8.".D)$<..O...}.J9.3..a.i.'...x.....5O...x.....I.M.!.'\.l.2.0.cN.fq....\.....7..,.....>.p...w&. KS.....(O.V>.....O.r..V~J.`....U(..Y..MIy..w..g0e.....D.,L..y..N.+..._....O.h.]...V....r.....O.|.:....Li..>COy.....N.h.....R....Q%.,Xr.y...G8=.A....!8(..L....c....sA....t.Vl:...v...G ;...^.l...#.t.>...k..d..kr...B.....Pb.0*..!..;9.....:~....j;....j.*O..!B.....?....^.]....;...[.g.B...%..'.7;.9.>..gP. p8...:.5l.Y.....Jp..R,.?..b..8O.....h.X(..G.).Cz.C..%....x.ET.....AEi.../..0.. ....k.*t.. .wl..e...H.i.F.....?.....z...?.....(../.O..R.?.4..7...j ..Q.....l..ob!..A..j...@..!).....K...MW.U.N.....W..Bh'8.'.y....Y.[o...PI..W.*...i...r.e..=.k^.WC..Uy.j..687^.z.#u5.4O.....-j.j3..L. 1..F...8.....@l.9.c.aGC.R.&..j.Q-av?...[4.E..T8....u..+9.<.n.Qw.D..N..S..3.D..... .%C.j.7.Y.s(.0wq.ZI.#"#..[K.GJ ....4.....?

C:\Users\alfredo\AppData\Local\Temp\e2101325-4ca1-4db2-95b9-c345399cc004.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):	30948
Entropy (8bit):	**7.99105089802474**
Encrypted:	**true**
SSDEEP:	
MD5:	7F0FCE2F184F63FED8E9929FB106C282
SHA1:	0582EB5BFC7FCCCC1C77A860F00E351E61F5DC67
SHA-256:	7C33F333216849E50AFC9550DA7DA4450D221B837340716ACCEE3766FFD4A62B
SHA-512:	AD1CD5B804C08C4C25BD6F97153D3371156848A83682DF1829B0B113B60ED0B01D67B5CD737CB414C8B825E12C7E0D6B5F9B338F4AF7FC82BE8AAF4CA8E279 BA
Malicious:	false
Reputation:	low
Preview:	.....y..../...*D4e.sH.v.{.....mv9MR...&..b.`.P."........r.....X...9s.s..w..;...>.}8...O.ep....O.]...$KO.tu...2?Yfi.'ove..T.....(.N7.R..<yr....t..}).....>[.....*."....'7.j.....#.n..e1..Fr..... j5xH.~.*...yvw....y.....vl.....IWT..)...\|...\..<=.V.C..}.fF..T.....~.~..:).....i...2./D.}...]..<+3T..Z.Q9*0.....3..7.e..p.:..-.P..n.}j....U...."...\|Gm...AdQ:*...gz%n..:...K.o[..."..n...(V..A...U.D.~ x.Q..X.tw.F..,.Q...k.9.w.....2....t.....XF....E./...Hu.%..]....7.T...X.\$4.~.....`..e\....}.X...`A...J.....k...$IO..OS:...=...R...q.....FE.H.)M..WX/.....6.._..ry..J..`.q.'....x^..[r..Z.Y:..0.. .g.y....#.1.'...F7M.6...S....7.To.G.... `#.....-."...^....;..8..{.6VhL?%uU...K....O9.`Y....b.5.,zP.+\..!.1wK.j.P].....jW.!.j...i3.v.<..n.P..g....~.x..z.8...2^..U.f.bt#.+.U..N.....!.[.!#.C .A.xy.....p...n.mU,.....=.....h .ME..T/....IT\h,.U.....(.U ...Tf.?Zd8.2.V.....*..../....Oyh.j._.I.k..u...).3.r.3...j.....O....+],...

C:\Users\alfredo\AppData\Local\Temp\e6b0db7b-9f08-487a-a9ef-699c08b3ce7f.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):	249577
Entropy (8bit):	**7.998368705248363**
Encrypted:	**true**
SSDEEP:	
MD5:	51055D2BFDA62ADF265DAB3E6F6E9E8D

SHA1:	1B31763846FB99C0638CCBA379C81FCD3B9F8BAF
SHA-256:	D6A7818A7AE6CF87D1164B86CDA2C4A2E8A0E884A9CD7204A758EAD48AB82B30
SHA-512:	52917C81732E0F90B3AC67EFE67E741D6EC987545B864358FA494DFC490F813002C0F06A05350BB9256E38FE4B43D7B1612287653AF2CE56E04718C6C1FD62DA
Malicious:	false
Reputation:	low
Preview:	.....<kw.6...+..HF.,eo....:N.n.g.h.*:.-B.....$(.Nv.i-....g0..o..Q.H~.RAt...X.$_..7~)r.<.....)....`S..@.X....._..bA.....R.T.+....X..%6r..B^...1,.....G.M.P\..#*.....l.BJ.M.. 2`.....B.}....G.s-.M..gh.R..I.mV2.{=.;L...<F*N..(K&q....W.....,b.dj#.. ....gv..6.....oajq1\.y.sv..../....IX....pc..l>.Le ..S'b]"....6&.&...]M.L...,.....|...._.k6ep..HU.W...JT..^.t... .db.Y....n&..W.U....._..g(..&.....AXL$.Cq..2.W..^~!.....q.n..V.).K.C.*..~./c8z.!v<2H<..4..`].+.^k..NE.'.-8.\.....<. -g.!..=...i8.r`..e...J../.4*.$,E.5..S..8...j.q.[.9.$...9\...< ....O.z.....F.K.+....Y.<.....Q.X.U.i..5xS.....Bp.A.....r.zm.....O.N.<}....go..{~...gg/^.}x....1@.H..*a$..v..R.....I:..x.R."NF1..E...A.i...E.X...y".....8..d....P.YEE.NZFy<...?z. %ED;.[jl.f.y.,&.....<$....Ry..T.sV\.U.w)x.....k6.O..$T.....9c...z..}~..*..z...5..s.v[s.7....I...?...Z...n...9..S..\c 7IfX.....di..FA..._r<3.%..'..Q}..H.ZL).vo8.O...

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770 0C
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_dir7108_695416080\CRX_INSTALL_locales\ca\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40

SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\de\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\en\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\es\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\es_419\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\et\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\fil\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6E 7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... ."... },.. "app_name": {.. "message": "Chrome ... ."... },.. "craw_app_unavailable": {.. "messa ge": "..... .. .."... },.. "craw_connect_to_network": {.. "message": "..... ...."... },.. "iap_unavailable": {.. "message": "..-.. ...."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "..... Chrome ... ."... }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 96E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators

Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false

SSDEEP:	
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome .....".. },.. "app_name": {.. "message": "Chrome .....".. },.. "craw_app_unavailable": {.. "message": ".....".. },.. "craw_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED

SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	501
Entropy (8bit):	4.804937629013952
Encrypted:	false
SSDEEP:	
MD5:	8F0168B9A546D5A99FD8A262C975C80E
SHA1:	B0718071BD0B7251D4459E9C87DF50C14622FBD6
SHA-256:	F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F
SHA-512:	A1191CDC496DDD7470BDCFAF186BB9488767159E0CA6A6242D195FA3351704DC8F8BBD03DBEE57D37BBD897C9E8D14B7325FB37D58AC80DEC0F972FF89375B8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er utilgjengelig for \u00f8yeblikket."},"craw_connect_to_network":{"message":"Du m\u00e5 koble til et nettverk."},"app_name":{"message":"Chrome Nettmarked-betalinger"},"app_description":{"message":"Chrome Nettmarked-betalinger"},"iap_unavailable":{"message":"Betaling i app er ikke tilgjengelig for \u00f8yeblikket."},"please_sign_in":{"message":"Du m\u00e5 logge p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8AA7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false

Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "craw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
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_dir7108_695416080\CRX_INSTALL_locales\sk\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC9D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . Chrome ...-.....".. },.. "app_name": {.. "message": "..... . Chrome ...-.....".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... . ...".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. . Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA687 52E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavai lable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\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_dir7108_695416080\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_a pp_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavail able": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\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:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCB F
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_dir7108_695416080\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 compl eted.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\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:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC8D2
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_dir7108_695416080\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:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C809
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_dir7108_695416080\CRX_INSTALL_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwYXRoIjoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6Ik9nUkNIZlVoam9xOU93NHFfaEhvTTQxNzNMelJyYkVpUVdsRXNRSzhscFkifSx7InBhdGgiOiJfbG9jYWxlcy9kYS9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6Il9sb2NhbGVzL2RlL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoIjoiX2xvY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jYWxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd

SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=e||{};e.scope={};e.arrayIteratorImpl=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};e.arrayIterator=function(a){return{next:e.arrayIteratorImpl(a)}};e.ASSUME_ES5=!1;e.ASSUME_NO_NATIVE_MAP=!1;e.ASSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");};e.global=e.getGlobal(this);.e.IS_SYMBOL_NATIVE="func

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\craw_window.js

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\css\craw_window.css

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1741
Entropy (8bit):	4.912380256743454
Encrypted:	false
SSDEEP:	
MD5:	67BF9AABE17541852F9DDFF8245096CD
SHA1:	A4AC74DD258E8E0689034FAA1B15A5C7C56DC3BB
SHA-256:	10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC
SHA-512:	298FA132C6F122798FDB9BC6DE8024915147ADC20355B56A92F0ED9ACCE4549BE6E7F42212E07DCA166E31624D4E66E299565845D4BA1C51CA935050641B61F
Malicious:	false
Reputation:	low
Preview:	html, body {. margin: 0;. overflow: hidden;.}..webview {. width: 100%;. height: 100%;. min-height: 100%;. position: absolute;.}...craw_overlay {. position: absolute;.. left: 0;. top: 0;. right: 0;. bottom: 0;.. background-color: white;.. -webkit-transition: opacity 250ms linear;.. display: -webkit-flex;. -webkit-flex-direction: column;. -webkit-flex: 1 0%;. -webkit-align-items: center;. -webkit-justify-content: center;.. -webkit-app-region: drag;.}...craw_overlay img {. margin: 16px;.}..#loading_overlay {. opacity: 1;.}..#offline_overlay {. opacity: 0;. display: none;.}..#offline_overlay > img {. -webkit-filter: saturate(0%);.}..#offline_overlay > span {. font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif;. font-size: 15px;. line-height: 21px;. color: #8d8d8d;. display: block;.}..#loading_splash {. width: 128px;. height: 128px;.}..#drag_overlay {. position: absolute;. left: 0;. top: 0;. right: 0;. bottom: 0;. pointer-events: none;. -webkit

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\html\craw_window.html

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	810
Entropy (8bit):	4.723481385335562
Encrypted:	false
SSDEEP:	

MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281E FF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/craw_window.css" rel="stylesheet">. <script src="/craw_window.js"></script>. </head>. <body>. <webview> </webview>. . . . . <div cl ass="craw_overlay" id="offline_overlay">. . . <br /span>. . . . . </body>.</html>.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\flapper.gif

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	dropped
Size (bytes):	70364
Entropy (8bit):	7.119902236613185
Encrypted:	false
SSDEEP:	
MD5:	398ABB308EEBC355DA70BCE907B22E29
SHA1:	CFFB77B8A1724B8F81D98C6D6AD0071D10162252
SHA-256:	2B73533F47A99FFEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040
SHA-512:	FC7A56FC8A61A582161874B54ADBAD30A84840190008EDB0B6FBF84F91393CA58E988E3FE446F11A0C3C691C18249B93AEC2904B3D0C4F0857D79034F662385A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....!..NETSCAPE2.0.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:..B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g]]$ueW.Ny Q.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:..B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g]]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m 4..7..!.....,.....'..w=.....\.)._6.k..OF...n.#\~"....2b3..I.)..eu.Q.`.e.....gr.?>.s.l0.....@.~.Tr.[8.+.,.;..EE....S.*f.....,.....B8/D..;.9.q.....ukC...r.I.....j.....BGY...o2J....+O4....X4.....cH%7....I.....0H!.!.....!.,.....p8.a$....hh@.4....X,A.0L..(....JX.j...,.....z.X.Q....jB.d....B..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false
SSDEEP:	
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5
SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC1417091
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:,[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....a i..w38.+....Bf././..]...{.....8...3.....3W~OJ.. /...u6V.C..U.0.+._=.c..9.X.?....L....S@.L...m.0..>.C...L|TF.p5..f4M.,.V....8..a.<...RP..@)E,..E"...h.....!...-....,I..T.....m..._[[{w{{.... {*.^.....M.x..h4.h.....\.R.E....j).7.....h4.A.E.....,. ...iii.Vj?2...=/.B.FK9P..@)=Rj..D".Y...2.B..x.}0...&J...2.....f.O..e.H.....!.J)'I..R....B.....QJ;K..L...L.I".L~mhh.R.@).FFF ~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....],w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b.. aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:..=...r.....E].o...F..P.....i...\....

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE

SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCA5134903E4C1AA3D54BC7C5ED3E65B50C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDAT8...Mk.Q...;... .....F..QW.....F....J.?.w..7~.....'.Q..B]... .QS...M&_w..b&.|`.....p...f.?.D$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N .Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C.._...%..*.^....4.l...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a..".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7y e6X<...'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\|.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\topbar_floating_button.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.475799237015411
Encrypted:	false
SSDEEP:	
MD5:	8803665A6328D23CC1014A7B0E9BE295
SHA1:	9DA6EE729D5A6E9F30658B8EC954710F107A641F
SHA-256:	D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C
SHA-512:	ECD9E71B8BA1ED8BD4CA5A0936CB66A83611C4ABCBDA76C250F4CDF4AD80320212E8F5EEB79A38910718F8346ECC1AD580A3FA835EC2B22BE497F36899FB5930
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...Q..0.....2...(p...~Z.}'.>I%O...V!s...../...`.<..`.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\topbar_floating_button_close.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	252
Entropy (8bit):	6.512071394066515
Encrypted:	false
SSDEEP:	
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D77A64
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..... ..Pp.X....H...b@...|.^LC_.E.BP+.....X.P.....q..~..p/. ..s.....%D^...$.....@.!...<...).? .4{.k.G3...4..[cH..0..l.8.!r..m.R..{.....`.f...#.x.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\topbar_floating_button_hover.png

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\topbar_floating_button_maximize.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.8155898293424775
Encrypted:	false
SSDEEP:	
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A8654
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...HIDATx.....0.CQS.....~..."..........m.v+Sq....<!...M8m...'...@$..0....E.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\images\topbar_floating_button_pressed.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	
MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFB
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....$.<u..[.....h.....M..x(....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir7108_695416080\CRX_INSTALL\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.449026004350873
Encrypted:	false
SSDEEP:	
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED548F
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. },.. "default_locale": "en",.. "description": "__MSG_APP_DESCRIPTION__",.. "display_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png",.. "16": "images/icon_16.png".. },.. "key": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0lV5/lj0wx7zJ/xcibUgDeIxobvv9XD+zO1MdjMWuqJFcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB",.. "manifest_version": 2,.. "minimum_chrome_version": "29",.. "name": "__MSG_APP_NAME__",.. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com",.. "scopes": ["https://www.googleapis.com/auth/sierra", "https://www.googleapis.com/auth/sierrasandbox", "https://www.googleapis.com/auth/chromewebstore", "https://www.googleapis.com/auth/chromewebstore.readonly"].. },.

Static File Info

General

File type:	HTML document, ISO-8859 text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.4407926395140076
TrID:	
File name:	test@barclays.com.html
File size:	431903
MD5:	3ff5b2d36016905e595efd4a6793c17e
SHA1:	ee9774db8ab8b5b156c7ea7933031825d930071e
SHA256:	c786576470e647e9d098001c6a748c17277cc4cf6c2209ce7e4712baff2490dd
SHA512:	bd04db88c60415333ba8b0ce6f01763d581218ab9455b8f46138c2bbab01a414dce2891cd62aa6d7e406f80ceec6cedd4bb9e56697e0647aebe88782655ea571
SSDEEP:	1536:6LFKC9Bu59svDU7jDqlvlx3oc1pT9bfx+Bx2pXKfTuhHv8u4PlwCgYT13K313t31:xuhHv8u4PlwCr1y1d8K
TLSH:	B694A23C6302CC4DAD776A7FFCA46B115018AF57EDCAB7C8086D80972AE09BA35147D6
File Content Preview:	<script language="javascript">.. ..// == Begin Free HTML Source Code Obfuscation Protection from https://snapbuilder.com == //..document.write(unescape('%3C%21%64%6F%63%74%79%70%65%20%68%74%6D%6C%3E%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E%0A

File Icon

Icon Hash:	e8d6a08c8882c461