ID: 458871
Cookbook: browseurl.jbs
Time: 20:21:31
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

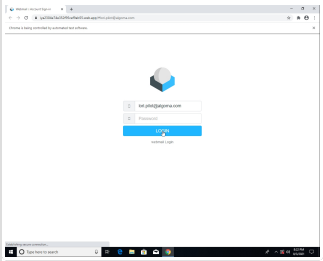
Windows Analysis Report https://iya2304e74e352f95cef…

Overview

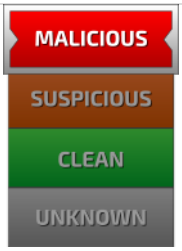
General Information

Sample URL:	http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com
Analysis ID:	458871
Infos:	

Most interesting Screenshot:



Detection



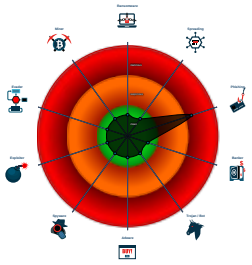
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- HTML body contains low number of …
- No HTML title found
- URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6604 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6772 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,13940740740856333051,3351174129214579356,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1792 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

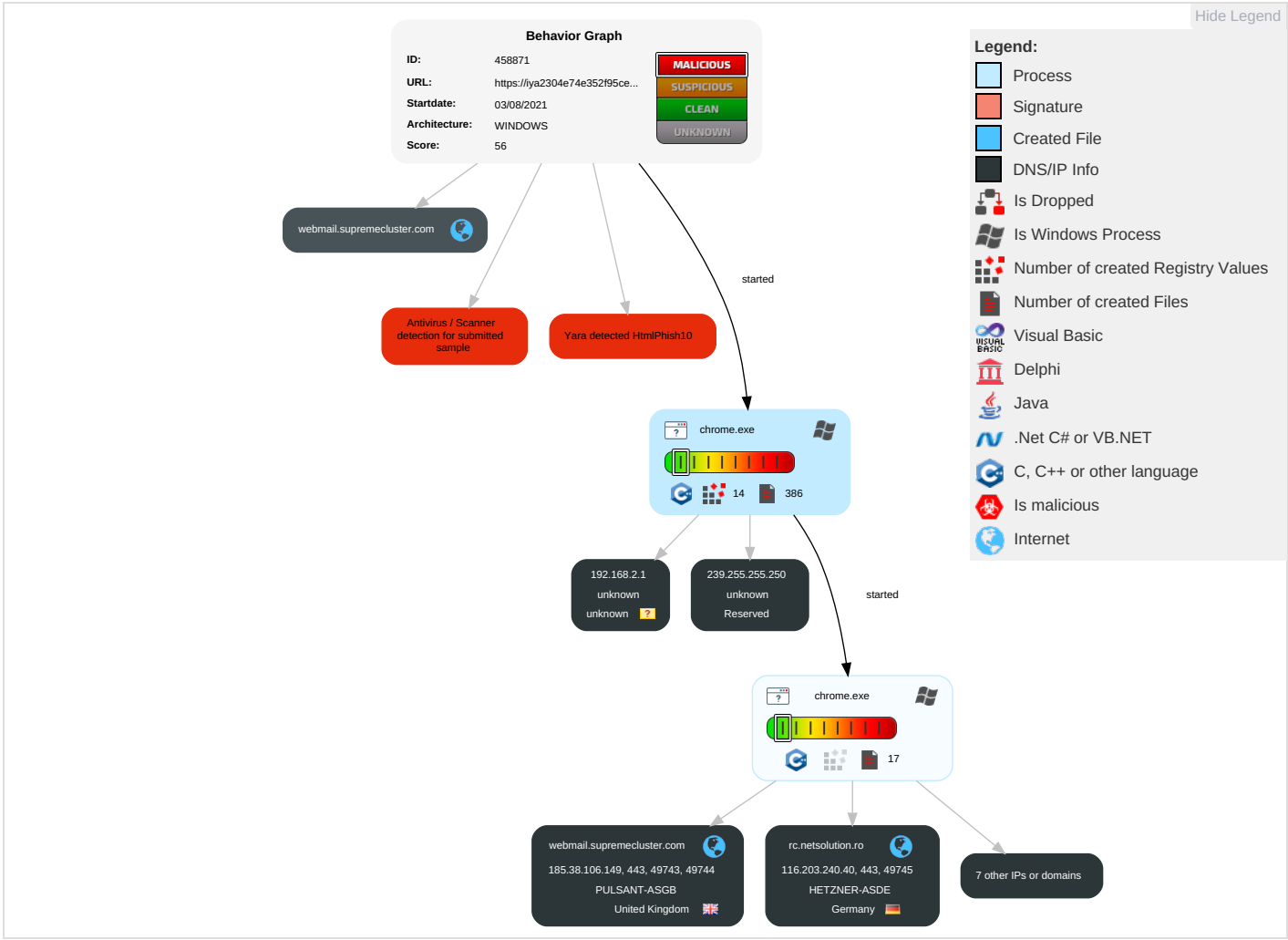
Phishing:

Yara detected HtmlPhish10

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	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

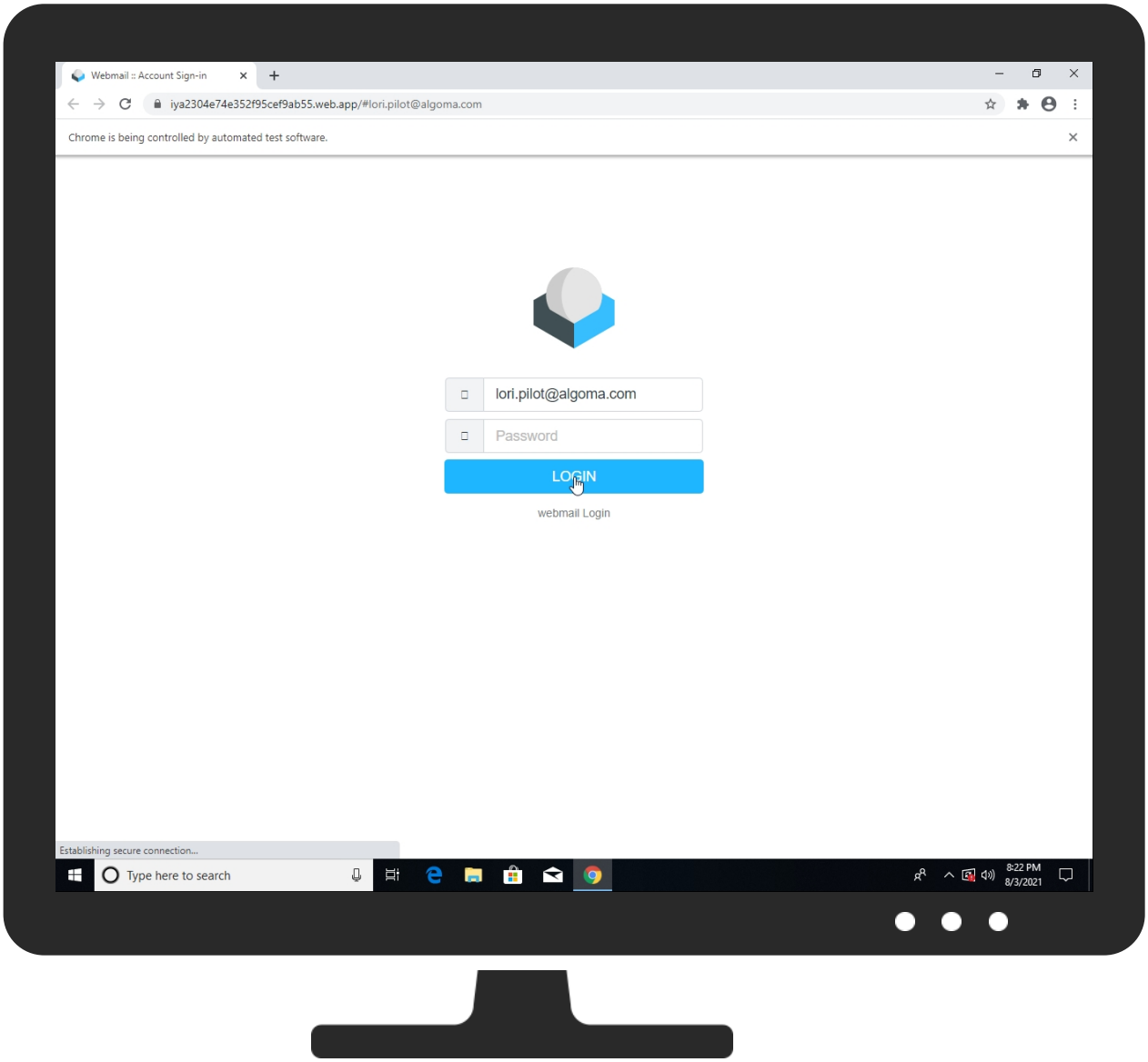
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com	0%	Avira URL Cloud	safe	
http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot	0%	Avira URL Cloud	safe	
http://https://rc.netsolution.ro/program/js/jquery.min.js?s=1525002594	0%	Avira URL Cloud	safe	
http://https://iya2304e74e352f95cef9ab55.web.app/4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rc.netsolution.ro	116.203.240.40	true	false		unknown
accounts.google.com	216.58.205.77	true	false		high
iya2304e74e352f95cef9ab55.web.app	151.101.65.195	true	false		unknown
webmail.supremecluster.com	185.38.106.149	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
185.38.106.149	webmail.supremecluster.com	United Kingdom		12703	PULSANT-ASGB	false
116.203.240.40	rc.netsolution.ro	Germany		24940	HETZNER-ASDE	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
151.101.65.195	iya2304e74e352f95cef9ab55.web.app	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458871
Start date:	03.08.2021
Start time:	20:21:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@28/200@7/9
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C5 9
Malicious:	false
Reputation:	low
Preview:	sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\22226983-57fe-405a-93b3-3c1bda2db0d4.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):	5794
Entropy (8bit):	5.181031330269843
Encrypted:	false
SSDEEP:	96:niLXr9UzIKIgK/5k0JCKL8aku1GbOTlVuHn:niLb96IOyh4KrkuI
MD5:	567B46439ADB962EF69E708F2BC6615D
SHA1:	B46550A3F500314FB02FED2DB1B5F1B50EEB6A1B
SHA-256:	4AF7C0F735A2FAE1DB049D8BA71EBFEC436FB735A846687B2D216CEAA5D676DC
SHA-512:	6E0A2D2A72B14CA94CD4E410384BD293847BC8D0D2FD1A90B61AE06619EF1451D3B155034A45603E05AEE7EB77AD7B29F35307D5B2D4D4A4D4D0DEF669E9D2 D4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272488537319285","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\311ee518-3911-49a9-a442-30d7f7a71c2c.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):	22602
Entropy (8bit):	5.536234280832976
Encrypted:	false
SSDEEP:	384:BcLtkLlryXW1kXqKf/pUZNCgVLH2HfDMrUvHGMnZ5mRSp4U:ZLl0W1kXqKf/pUZNCgVLH2HfgrUfGMnF
MD5:	36EA886EE7B6C2EAB71995F1E7C2893D
SHA1:	E9A4E6103E4A6FC48F62018D82FEA0D44E3BEDEE
SHA-256:	9A1A7C2F2409B6B3E6D942BAEEBB3FF13019228EC2493828A05F0A16EEAE045F
SHA-512:	BB39F6D05769897B96811664B2A57FFB8B92465F348E1526926BADB05680CDE609C3046FC3A24051FDDC642663B2C72F5F6E5B1D01338FCD45953E8A15DCFE9A
Malicious:	false
Reputation:	low
Preview:	{"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":"13272488537031826","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b644c3b-e9c8-4057-971c-2659fd9b7b15.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b644c3b-e9c8-4057-971c-2659fd9b7b15.tmp	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d0af136-2c8d-4134-87ee-046aeb5662ee.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):	22601
Entropy (8bit):	5.536440230406649
Encrypted:	false
SSDEEP:	384:BcLtkLlryXW1kXqKf/pUZNCgVLH2HfDMrUvHGznZ5mR2p4b:ZLl0W1kXqKf/pUZNCgVLH2HfgrUfGzna
MD5:	C90E6898C42581C0723856E612449851
SHA1:	2CB561FA2269A284F1A37483EC771991B4F40224
SHA-256:	F2A24C8A03B1C3A2CA6806AEDFE3F14586C2F11E2C08BF5FD7EE3CDBA4C4C6F1
SHA-512:	2EF2CDD217F86BFF8F1F6A6DF2E599EB1E216A61E769B6946D02E36BC82A10A207879F047B91015D5ADC7C4564871C99E24A4C1B67E686944497E7383C0AB5C
Malicious:	false
Reputation:	low
Preview:	{"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":"13272488537031826","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\97c913ce-31ac-4b54-8f42-1f3a0a6e5605.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):	5198
Entropy (8bit):	4.971884908512879
Encrypted:	false
SSDEEP:	96:niLat9pIKIgK/5k0JCKL8aku1GbOTlVuHn:niL69pIOyh4KrkuI
MD5:	3D78FC1F72868BCA448CA75F9DD1645F
SHA1:	14ACA3A4A92EFEB59787DFC47059135F8243ADF9
SHA-256:	F5023EBCB2544D4C9916E21EAC2AD2B33C6355D33D7BDAEDEE1F04EDA20E35B9
SHA-512:	1B5D2CAFD7D7F14AE5A03E9F130305C0D5842AB96176A70E485B1307FAAD83FE212A9E891E5EDE9F6DCD762C57EB735CBE14CD07DEC8169DB010D7DAE41F1 EE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272488537319285","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.175654707412731
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
SSDEEP:	6:mRXStoM+q2Pwkn23iKKdK9RXXTZIFUtpmXSvLmZmwPmXSvzMVkwOwkn23iKKdK9l:2u+vYf5Kk7XT2FUtpm4m/PmxV5Jf5KkT
MD5:	1D48A1A6246BEC9ECC6342BF60B1C2A1
SHA1:	D57ED95E066CBB161F4288DAB6A3FECF8AE56482
SHA-256:	D1D3ECA7C6B15B6CB3CFFE1C18CDBF9B7296AADD504C7C112EC5D007EF39FECA
SHA-512:	31ACBBBCC8BE275E53F5BA1E1043A2F35BB46F35F0954C9E1FDFBE424F14A5AB69F02DA517AABD19E07EA8F61FDBA5E14301B50DD11E5C75AC7462F8F1F8A8EF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.785 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:22:29.791 1a1c Recovering log #3.2021/08/03-20:22:29.793 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.175654707412731
Encrypted:	false
SSDEEP:	6:mRXStoM+q2Pwkn23iKKdK9RXXTZIFUtpmXSvLmZmwPmXSvzMVkwOwkn23iKKdK9l:2u+vYf5Kk7XT2FUtpm4m/PmxV5Jf5KkT
MD5:	1D48A1A6246BEC9ECC6342BF60B1C2A1
SHA1:	D57ED95E066CBB161F4288DAB6A3FECF8AE56482
SHA-256:	D1D3ECA7C6B15B6CB3CFFE1C18CDBF9B7296AADD504C7C112EC5D007EF39FECA
SHA-512:	31ACBBBCC8BE275E53F5BA1E1043A2F35BB46F35F0954C9E1FDFBE424F14A5AB69F02DA517AABD19E07EA8F61FDBA5E14301B50DD11E5C75AC7462F8F1F8A8EF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.785 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:22:29.791 1a1c Recovering log #3.2021/08/03-20:22:29.793 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.171425583161632
Encrypted:	false
SSDEEP:	6:mRXS+M+q2Pwkn23iKKdKyDZIFUtpmXSvNZmwPmXSWMVkwOwkn23iKKdKyJLJ:2W+vYf5Kk02FUtpms/PmmV5Jf5KkWJ
MD5:	B5B058305AECE7F2F39EA35F0B64A106
SHA1:	454115CE4D9C22C03C062070CFB2BE02CE1D8EE8
SHA-256:	F7DB8E852F3B069705F8B9C707DA456BB986B93DF39667292FD9A6D813F96026
SHA-512:	D8A1D86A4BE63ED40AF06C509DE4E5B7DCCAEE27725C730EC4238E28045081E3D21BAA0172569B3759E532ABC8B64FBB2869DDA718F59E5DEAF4A33F5859D140
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.697 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:22:29.729 1a1c Recovering log #3.2021/08/03-20:22:29.749 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.171425583161632
Encrypted:	false
SSDEEP:	6:mRXS+M+q2Pwkn23iKKdKyDZIFUtpmXSvNZmwPmXSWMVkwOwkn23iKKdKyJLJ:2W+vYf5Kk02FUtpms/PmmV5Jf5KkWJ
MD5:	B5B058305AECE7F2F39EA35F0B64A106
SHA1:	454115CE4D9C22C03C062070CFB2BE02CE1D8EE8
SHA-256:	F7DB8E852F3B069705F8B9C707DA456BB986B93DF39667292FD9A6D813F96026
SHA-512:	D8A1D86A4BE63ED40AF06C509DE4E5B7DCCAEE27725C730EC4238E28045081E3D21BAA0172569B3759E532ABC8B64FBB2869DDA718F59E5DEAF4A33F5859D140
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Preview:	2021/08/03-20:22:29.697 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:22:29.729 1a1c Recovering log #3.2021/08/03-20:22:29.749 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\454755fc887d0a8b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.651581779541641
Encrypted:	false
SSDEEP:	6:m8YEAR4KPDcnjrQQ3hKyxh1SBGvAuhK6t:ePD8QShlvN
MD5:	A8834E14C1021999123652220128BDE6
SHA1:	BBFF4D515C78D99C93E5583300ED8258ED233A86
SHA-256:	D20971B509845B38E1A2177D2994EB072463A3596A66929139111231CE5D730A
SHA-512:	45C79CE800FA1BEF6A60B389945693AEECC37D0F299D771290D42EF9E04EE483930655E161ECA0FB9E310B7FCCBEFF748DB2C5E7E793DD9C94558FAA559328F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...S..G...._keyhttps://rc.netsolution.ro/program/js/jquery.min.js?s=1525002594 .https://iya2304e74e352f95cef9ab55.web.app/4...B'/.....@.....@.]....?C..-.....CF..lp.#....A..Eo.....m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	4.795438597273673
Encrypted:	false
SSDEEP:	3:kCHFj/LlHldrg0zT9Iptlll5/lOptlllKL8ftlll0l0qxzUsR8ftlllwAfvqDLVi:jF1ZzdcTxzPawAfyDn2C+n
MD5:	6B923D3DAFD76257840B196E3CBA0C2F
SHA1:	B719AC0AF4AC128B915A04CE3F0A43035744E75D
SHA-256:	D682DDB77F37114AB5E73FCB174C30A8A4E4A677A76930B84B9E049319FD27BB
SHA-512:	0F3AD91B67F441C6B623875DD479E388B5FBF417184463AF70FEA90F77DAFC1288B4438788AC1AED5CB5A38CF3A50AB80DD775D5273CFE036CBD5B1D6C6E9CF6
Malicious:	false
Reputation:	low
Preview:	.....+..oy retne.....}..UGE.O..B'/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....B'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index?. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	264
Entropy (8bit):	4.795438597273673
Encrypted:	false
SSDEEP:	3:kCHFj/LlHldrg0zT9Iptlll5/lOptlllKL8ftlll0l0qxzUsR8ftlllwAfvqDLVi:jF1ZzdcTxzPawAfyDn2C+n
MD5:	6B923D3DAFD76257840B196E3CBA0C2F
SHA1:	B719AC0AF4AC128B915A04CE3F0A43035744E75D
SHA-256:	D682DDB77F37114AB5E73FCB174C30A8A4E4A677A76930B84B9E049319FD27BB
SHA-512:	0F3AD91B67F441C6B623875DD479E388B5FBF417184463AF70FEA90F77DAFC1288B4438788AC1AED5CB5A38CF3A50AB80DD775D5273CFE036CBD5B1D6C6E9CF6
Malicious:	false
Reputation:	low
Preview:	.....+..oy retne.....}..UGE.O..B'/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....B'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9734152769670368
Encrypted:	false
SSDEEP:	24:7e9H6pf1H1oNVfqLbJLbXaFpEO5bNmISHn06Uw/8:7bfvoNhq5LLOpEO5J/Kn7U08
MD5:	9F5810D971759957F6B71EE0C6881DC5
SHA1:	5F33AFCC1A65D920CE33B2D7B9C815C97A1FFBA3
SHA-256:	AA1D00FD9E35300E4022DA25A4E987272D80D27901113E2189CB451CC5D7EAB2
SHA-512:	CF039501C33AC7BFD38968C5525C99DEA04DDD9CF4945D557E5D4EBC2159258E6D525E621CDC69914789A070386BAEB55A37A7A970949917E60FAEDCE0841B6
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1577
Entropy (8bit):	3.40184325370072
Encrypted:	false
SSDEEP:	24:34SIBRlrlJhMteyGjnJ+uXyLBUcYn9ATMtQitzlLlL:34rBDx1nJ+ukBatJRL
MD5:	ABC8CDD4C8B2D6CBE1B278191B0E95D6
SHA1:	1484F398AB8A4A04416219C606CC4B4CF1622D09
SHA-256:	2F4089111DF10591F49732B94F6DA058604B59491B8B884ACBA12F09A59CDEBD
SHA-512:	D00300403B8ED5F7716C1209CFFFB776A63A41EF2CCD6376BDCA8E18E19176F62F541EFA0F6BAADE223663A80D6F801F7F66F5C5DB7903562A4F2802DE77424
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...4c1005ac_7afa_43b1_a968_8758f99c7a1d..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....@...https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com.. ..W.e.b.m.a.i.l. .:.:. .A.c.c.o.u.n.t. .S.i.g.n.-.i.n.....h.....`.....6.....6.....@...h.t.t.p.s.:. /./.i.y.a.2.3.0.4.e.7.4.e.3.5.2.f.9.5.c.e.f.9.a.b.5.5...w.e.b...a.p.p./.#.l.o.r.i...p.i.l.o.t.@.a.l.g.o.m.a...c.o.m.....@.....8.....0.....H..... h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\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):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\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):	320
Entropy (8bit):	5.171992917017907
Encrypted:	false
SSDEEP:	6:mRXXTF+q2Pwkn23iKKdK8aPrqIFUtpmXXTEZmwPmXXTH3VkwOwkn23iKKdK8amLJ:2TF+vYf5KkL3FUtpmTE/PmTXV5Jf5Kkc
MD5:	50F88DB07C0D5D05C5754394AFE1FDBA
SHA1:	E7ACB261B0C809471283B0DC342D142A5945B253
SHA-256:	93CF16EE41C6641C2E046CE71923CC248555DA6A4E24476433A1D04F59223718
SHA-512:	82F60196355BBE141CF73EA995279B74B9997A62999814165B6AD37FFDCC179508AA97B994E976AE09D16CD5C685CCD4589D558EA3B309633D98120D7BD9EF2I
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.315 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-20:22:17.316 1a4c Recovering log #3.2021/08/03-20:22:17.317 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.171992917017907
Encrypted:	false
SSDEEP:	6:mRXXTF+q2Pwkn23iKKdK8aPrqIFUtpmXXTEZmwPmXXTH3VkwOwkn23iKKdK8amLJ:2TF+vYf5KkL3FUtpmTE/PmTXV5Jf5Kkc
MD5:	50F88DB07C0D5D05C5754394AFE1FDBA
SHA1:	E7ACB261B0C809471283B0DC342D142A5945B253
SHA-256:	93CF16EE41C6641C2E046CE71923CC248555DA6A4E24476433A1D04F59223718
SHA-512:	82F60196355BBE141CF73EA995279B74B9997A62999814165B6AD37FFDCC179508AA97B994E976AE09D16CD5C685CCD4589D558EA3B309633D98120D7BD9EF2I
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.315 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-20:22:17.316 1a4c Recovering log #3.2021/08/03-20:22:17.317 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.185307021302351
Encrypted:	false
SSDEEP:	6:mRXZ1zXFlL+q2Pwkn23iKKdK8NIFUtpmXZKGz1ZmwPmXZ0LVkwOwkn23iKKdK8+Q:2p9OvYf5KkpFUtpmp9z1/Pmp05Jf5Kk2
MD5:	4173EF45084705B7097DB88547554876
SHA1:	784AC0867E760B28E0D045A2F04A9636AC5DB02C
SHA-256:	EF8485D6E1F4114EB9177430130B96EC670529E8BA5BE367499F3680940297B5
SHA-512:	383DE2AE0461EAEF6C99F94328A3ECF7D31CBBF5411D47075E4BD6BD01F68E847543629C63FB2A1F1D1CA13E157DC1CF4529A2EB35830ED4E55B62FA6E8713 1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:19.467 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-2 0:22:19.472 1a98 Recovering log #3.2021/08/03-20:22:19.473 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.185307021302351
Encrypted:	false
SSDEEP:	6:mRXZ1zXFlL+q2Pwkn23iKKdK8NIFUtpmXZKGz1ZmwPmXZ0LVkwOwkn23iKKdK8+Q:2p9OvYf5KkpFUtpmp9z1/Pmp05Jf5Kk2
MD5:	4173EF45084705B7097DB88547554876
SHA1:	784AC0867E760B28E0D045A2F04A9636AC5DB02C
SHA-256:	EF8485D6E1F4114EB9177430130B96EC670529E8BA5BE367499F3680940297B5
SHA-512:	383DE2AE0461EAEF6C99F94328A3ECF7D31CBBF5411D47075E4BD6BD01F68E847543629C63FB2A1F1D1CA13E157DC1CF4529A2EB35830ED4E55B62FA6E8713 1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:19.467 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-2 0:22:19.472 1a98 Recovering log #3.2021/08/03-20:22:19.473 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Reputation:	low
Preview:	{"file_hashes":[{"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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.0347016918638543
Encrypted:	false
SSDEEP:	24:LLitYxh0GY/l1rWR1PmCx9fZjsBX+T6Uw0tjcJjHL4MXinmPsS5n2sBFtOO/QEmc:tBmw6fULMX+mPsxUV5TWSwMs6kdGb+Jo
MD5:	C6F2621B712FEDC597F1A9934DE7EFCD
SHA1:	7F86111DDD756503FB112060414C1FD22FFA7511
SHA-256:	943EDCADA90E796EB68F0AA935B46139E1AA8873EC7C70A0235C5F2878843157
SHA-512:	025DDAD3A2C09B688EAA51A6EAE41DB0067A8E5B5D11FC44E8EA335EC83BD9F4A5D5C226B7FB0E794C5991D10F96B0AB4122808918C7A21BF913CB7D8F9BDC15
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.8141974779000543
Encrypted:	false
SSDEEP:	24:RqnUni/olO4/KQnsSfRyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6Uwh3n:Rk684OeKOs0RCBmw6fU+3n
MD5:	43A037524681A2DCFEFE0FDCD7C933C5
SHA1:	B1434E1B540ED0C3C47A5D087D379E0EBB80D8AD
SHA-256:	68103DBD5BAA3C77940AB1BCFED8BD8686819E82C4871438C5A6541D709890D6
SHA-512:	644F727E8A7A283ACEDFAA5B05505F1017199C7AB1A41436195FA93B7D8BA5CA7FBB591196C9C3B9F3E80E7493B395AEFB7C371C2519A71AC730FD890A069E8D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.22305653304618
Encrypted:	false
SSDEEP:	6:mRXSDspM+q2Pwkn23iKKdK25+Xqx8chI+IFUtpmXSD0NZmwPmXSboMVkwOwkn23U:2K+vYf5KkTXfchI3FUtpmz/PmWRV5Jfk
MD5:	C08C1B505E9D9EA87824DD325C1AC9A8
SHA1:	0EDC1545DE68626E6A7AD516878590B1622B671E
SHA-256:	2CBC0C251205AA57E62EC869E185E8CF5AAA827F2C4A06B3C8E5AEF8122F33D8
SHA-512:	A562AD2FD62F6B4B20225A69120867CEECC48D984177D9192FA30698B437E64EFD69F66A5E52A2E9DBF5F5C111DAB3F45DBEAB84243ADF42AB35D6E88F1DC7C6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.536 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:22:29.539 1a1c Recovering log #3.2021/08/03-20:22:29.545 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.22305653304618
Encrypted:	false
SSDEEP:	6:mRXSDspM+q2Pwkn23iKKdK25+Xqx8chI+IFUtpmXSD0NZmwPmXSboMVkwOwkn23U:2K+vYf5KkTXfchI3FUtpmz/PmWRV5Jfk
MD5:	C08C1B505E9D9EA87824DD325C1AC9A8
SHA1:	0EDC1545DE68626E6A7AD516878590B1622B671E
SHA-256:	2CBC0C251205AA57E62EC869E185E8CF5AAA827F2C4A06B3C8E5AEF8122F33D8
SHA-512:	A562AD2FD62F6B4B20225A69120867CEECC48D984177D9192FA30698B437E64EFD69F66A5E52A2E9DBF5F5C111DAB3F45DBEAB84243ADF42AB35D6E88F1DC7C6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.536 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:22:29.539 1a1c Recovering log #3.2021/08/03-20:22:29.545 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.160325241660105
Encrypted:	false
SSDEEP:	6:mRXSTGqM+q2Pwkn23iKKdK25+XuoIFUtpmXSx/ZmwPmXSwpMVkwOwkn23iKKdK28:27+vYf5KkTXYFUtpmQ//PmeV5Jf5KkTZ
MD5:	570BF54989AB04F9332F3ABF52EE29A3
SHA1:	7151E70FE1ECEECC86C338288C678910AF877CF3
SHA-256:	7174E528DD330AF767CE6648CFAC396C3B7B0154CD2A94CEFB9E0BCF2E5F77FB
SHA-512:	F9EF264316EDC04459F08B4438838589DFEF29EF8EB1295F5611AFF505A1A14126058A0DE7F7DEF669BF37AF91CC51727B298EF212B3E730E7ADC55BEFF593A0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.492 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:22:29.497 1a1c Recovering log #3.2021/08/03-20:22:29.499 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.160325241660105
Encrypted:	false
SSDEEP:	6:mRXSTGqM+q2Pwkn23iKKdK25+XuoIFUtpmXSx/ZmwPmXSwpMVkwOwkn23iKKdK28:27+vYf5KkTXYFUtpmQ//PmeV5Jf5KkTZ
MD5:	570BF54989AB04F9332F3ABF52EE29A3
SHA1:	7151E70FE1ECEECC86C338288C678910AF877CF3
SHA-256:	7174E528DD330AF767CE6648CFAC396C3B7B0154CD2A94CEFB9E0BCF2E5F77FB
SHA-512:	F9EF264316EDC04459F08B4438838589DFEF29EF8EB1295F5611AFF505A1A14126058A0DE7F7DEF669BF37AF91CC51727B298EF212B3E730E7ADC55BEFF593A0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.492 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:22:29.497 1a1c Recovering log #3.2021/08/03-20:22:29.499 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\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):	330
Entropy (8bit):	5.220809397999253
Encrypted:	false
SSDEEP:	6:mRXShUpM+q2Pwkn23iKKdKWT5g1IdqIFUtpmXSwXZmwPmXSiMVkwOwkn23iKKdKn:2di+vYf5Kkg5gSRFUtpmV/PmeV5Jf5Kg
MD5:	0E517DDFE2C2AE37733971F02192B175
SHA1:	4067D1023B529516449892C6976127DCDA281FFD
SHA-256:	459EF01410371B6A41B9C2451CE51B8EED8BF5A0FC9B007D933D15A563E0C819
SHA-512:	F3442B53A937789C6B33A38BA66C7456A0CB0FB4D0A6F882179F38CC1B643D4DFBA93818A1F336B39B41CF92243B5FC220F782FE5C07136C89ED0ECBA1A4261
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.475 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:22:29.476 1a1c Recovering log #3.2021/08/03-20:22:29.477 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.220809397999253
Encrypted:	false
SSDEEP:	6:mRXShUpM+q2Pwkn23iKKdKWT5g1IdqIFUtpmXSwXZmwPmXSiMVkwOwkn23iKKdKn:2di+vYf5Kkg5gSRFUtpmV/PmeV5Jf5Kg
MD5:	0E517DDFE2C2AE37733971F02192B175
SHA1:	4067D1023B529516449892C6976127DCDA281FFD
SHA-256:	459EF01410371B6A41B9C2451CE51B8EED8BF5A0FC9B007D933D15A563E0C819
SHA-512:	F3442B53A937789C6B33A38BA66C7456A0CB0FB4D0A6F882179F38CC1B643D4DFBA93818A1F336B39B41CF92243B5FC220F782FE5C07136C89ED0ECBA1A4261
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Reputation:	low
Preview:	2021/08/03-20:22:29.475 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:22:29.476 1a1c Recovering log #3.2021/08/03-20:22:29.477 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\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 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.1301498652100469
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvYlO6f+jrQQ3A/qes/7oOo/lCxthiZA/TWGCxC+/eri/CtjrQQA:TL+A/KO6fEQSA67oNuQa7WGI/DWQSQ
MD5:	A7B6BB6D48A40FB862CC90DA0C528495
SHA1:	BEB136B959FF2F189B23596026605741EE46E57B
SHA-256:	A663434073BD500210EF036924030016F084C7FDAC988CA41D3C987F59D21710
SHA-512:	3B1A0A3D2D086E402BC632BA96A893A88FCD9B5EC7B089924B1CD2522F2B7523CDF9BAB0C2E084B768A227CFC53CCEC67849398E1CF5365D3FF9A2B8C60EC EA
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	807
Entropy (8bit):	5.346310065352662
Encrypted:	false
SSDEEP:	24:vbz+thYbwziAqkjPqOLh9lf9iCdKtIY78BJgskfa9yBD11tEn:+YbwzOONf9rYtOUm
MD5:	E1B2BA54839316DD7868D676B7BDDD2D
SHA1:	FB4BC056AEFB032BB8BCACB634ADCA99F60BEBA1
SHA-256:	697BB8750CDC8C08FB4803C494150563F102B1779F79F6CDEC09D0B2A7C40937
SHA-512:	69A9066D6CA704BC74C1870F306E2C52C890F50E9CE41E0BFBCE5D45B9AECB3653D12A5654722AD5DA0B981D6AE850DE66A21F018EDB595F9D3F711CA1FCB 76
Malicious:	false
Reputation:	low
Preview:	....."d....account..algoma..app..com..https..in..iya2304e74e352f95cef9ab55..lori..pilot..sign..web..webmail*.....account.....algoma.....app.....com.....https.....in. .....iya2304e74e352f95cef9ab55.....lori.....pilot.....sign.....web.....webmail..2.....0.....2.....3.....4.....5.....7.....9.....a.....b.....c.....e.....f.....g..... ...h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w.....y...:n.....B .....~..... .....*@https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com2.Webmail :: Account Sign-in:.....J....."&+06=.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04761656801783401
Encrypted:	false
SSDEEP:	3:dwn3llu/fll92Nll9v/fll9HNll9GFll9v/fll98Fll9kpMRgSWbNFl/l/4ltNlw:0b/4qg9bNFlWCj/l5eEl3n
MD5:	D16A79DD5F0787BFF6EB7B9900E1AE53
SHA1:	51A257607813F0023AF2433A90DE43BE47F85F57
SHA-256:	EAC3034C047D96A51EB2718171F97D7B959DB50310347EFA555506BC4677EF63
SHA-512:	28FCD8F803A36707E1057539D46342B8D97AEC8F6AD897064D8FD4D9F84D453E9D7DF0CC4DC12A369CDBBBA281439EE57360E782E3F20EA6C9B5B609888347E
Malicious:	false
Reputation:	low
Preview:	.....N..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session% (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1577
Entropy (8bit):	3.40184325370072
Encrypted:	false
SSDEEP:	24:34SIBRlrlJhMteyGjnJ+uXyLBUcYn9ATMtQitzlLlL:34rBDx1nJ+ukBatJRL
MD5:	ABC8CDD4C8B2D6CBE1B278191B0E95D6
SHA1:	1484F398AB8A4A04416219C606CC4B4CF1622D09
SHA-256:	2F4089111DF10591F49732B94F6DA058604B59491B8B884ACBA12F09A59CDEBD
SHA-512:	D00300403B8ED5F7716C1209CFFFB776A63A41EF2CCD6376BDCA8E18E19176F62F541EFA0F6BAADE223663A80D6F801F7F66F5C5DB7903562A4F2802DE77424
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...4c1005ac_7afa_43b1_a968_8758f99c7a1d.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....@...https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com..W.e.b.m.a.i.l. .:.:. .A.c.c.o.u.n.t. .S.i.g.n.-.i.n.....h.....`.....6.....6.....@...h.t.t.p.s.:././.i.y.a.2.3.0.4.e.7.4.e.3.5.2.f.9.5.c.e.f.9.a.b.5.5...w.e.b...a.p.p./.#.l.o.r.i...p.i.l.o.t.@.a.l.g.o.m.a...c.o.m.....@.....8.....0.....H.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.467730658251141
Encrypted:	false
SSDEEP:	48:1FGaDa74MD8dbuNdzbQSefgGiNrS0U9RdiN9L:/a74MQdbuNdzbQ5fgGurS0l
MD5:	19351A33B398690EA2FDB739E3DB503C
SHA1:	4530307DDC5CCAA94944B67A87892F72093C382C
SHA-256:	1E147A51EEE2F9DC02E74B26DFA4C5BF378DF052BE5EAA813C198108ADFC8B08
SHA-512:	68E5510B9B6D890D846931B0797ADEAB2F034742FC2EADA42E3D3E96A771622290D5534FC1417F749D76EED3DC824B8D83613F6B6A84BB4CDE9C7CBD3C252E0
Malicious:	false
Reputation:	low
Preview:	g.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..445771000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 20:22:33.14][INFO][mr.Init] MR instance ID: 796b747b-50ed-4919-910b-2a9fdc231d21\n","[2021-08-03 20:22:33.14][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 20:22:33.14][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 20:22:33.14][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 20:22:33.14][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 20:22:33.14][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 20:22:33.14][INFO][mr.CloudProvider]

C:\Users\user\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):	332
Entropy (8bit):	5.131171609039625
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:mRXXor+q2Pwkn23iKKdK8a2jMGIFUtpmXXSubZmwPmXX6liVkwOwkn23iKKdK8as:2or+vYf5Kk8EFUtpm3/Pm/V5Jf5Kk8bJ
MD5:	B3EC82D4218C93FDEDF7CCBF257E5321
SHA1:	3AE3423388626C42AC07ED58189EB7E25A4468DB
SHA-256:	404467BBD98B0818FE23D121A14F5C72DAB49F62DBE03C3B69B807D0EAFDB87B
SHA-512:	8740FB55D2A3F16956B8D897A653E8473063136CCB852DAAB75939A6B423E925B814C383FBB3DD1C77046F5898C4FB4BE94789779C6DB6DAC61189764A41B6DE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.105 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:17.106 1a4c Recovering log #3.2021/08/03-20:22:17.120 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.131171609039625
Encrypted:	false
SSDEEP:	6:mRXXor+q2Pwkn23iKKdK8a2jMGIFUtpmXXSubZmwPmXX6liVkwOwkn23iKKdK8as:2or+vYf5Kk8EFUtpm3/Pm/V5Jf5Kk8bJ
MD5:	B3EC82D4218C93FDEDF7CCBF257E5321
SHA1:	3AE3423388626C42AC07ED58189EB7E25A4468DB
SHA-256:	404467BBD98B0818FE23D121A14F5C72DAB49F62DBE03C3B69B807D0EAFDB87B
SHA-512:	8740FB55D2A3F16956B8D897A653E8473063136CCB852DAAB75939A6B423E925B814C383FBB3DD1C77046F5898C4FB4BE94789779C6DB6DAC61189764A41B6DE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.105 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:17.106 1a4c Recovering log #3.2021/08/03-20:22:17.120 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State74 (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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.173104151622641
Encrypted:	false
SSDEEP:	6:mRXXXCGpyq2Pwkn23iKKdKgXz4rRIFUtpmXXXQG11ZmwPmXXX2+RkwOwkn23iKK2:2XdMvYf5KkgXiuFUtpmXQG11/PmX95JZ
MD5:	A45862BD70F9B5349EEEDC878970DD50
SHA1:	6E6D2F9D83AE0DF26680CA545104EA238AF02558
SHA-256:	D2905731865F4A81D7F3A3AF9D86D9D7E70E303BD0D9F84C0AE0115805BD75FB
SHA-512:	7FED801988C7481AB3861CEB2DC25022E80A042EF25DF496370947FD0E67904FFC3E97B69E557164072EC6560260EF3C3BEA69CECCEDA7B83F9FCF7D507B9EE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/08/03-20:22:17.353 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:17.355 1aa4 Recovering log #3.2021/08/03-20:22:17.357 1aa4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldes (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.173104151622641
Encrypted:	false
SSDEEP:	6:mRXXXCGpyq2Pwkn23iKKdKgXz4rRIFUtpmXXXQG11ZmwPmXXX2+RkwOwkn23iKK2:2XdMvYf5KkgXiuFUtpmXQG11/PmX95JZ
MD5:	A45862BD70F9B5349EEEDC878970DD50
SHA1:	6E6D2F9D83AE0DF26680CA545104EA238AF02558
SHA-256:	D2905731865F4A81D7F3A3AF9D86D9D7E70E303BD0D9F84C0AE0115805BD75FB
SHA-512:	7FED801988C7481AB3861CEB2DC25022E80A042EF25DF496370947FD0E67904FFC3E97B69E557164072EC6560260EF3C3BEA69CECCEDA7B83F9FCF7D507B9EI E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.353 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:17.355 1aa4 Recovering log #3.2021/08/03-20:22:17.357 1aa4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5198
Entropy (8bit):	4.971884908512879
Encrypted:	false
SSDEEP:	96:niLat9pIKIgK/5k0JCKL8aku1GbOTlVuHn:niL69pIOyh4KrkuI
MD5:	3D78FC1F72868BCA448CA75F9DD1645F
SHA1:	14ACA3A4A92EFEB59787DFC47059135F8243ADF9
SHA-256:	F5023EBCB2544D4C9916E21EAC2AD2B33C6355D33D7BDAEDEE1F04EDA20E35B9
SHA-512:	1B5D2CAFD7D7F14AE5A03E9F130305C0D5842AB96176A70E485B1307FAAD83FE212A9E891E5EDE9F6DCD762C57EB735CBE14CD07DEC8169DB010D7DAE41F1 EE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272488537319285","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesTM (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):	5794
Entropy (8bit):	5.181031330269843
Encrypted:	false
SSDEEP:	96:niLXr9UzIKIgK/5k0JCKL8aku1GbOTlVuHn:niLb96IOyh4KrkuI
MD5:	567B46439ADB962EF69E708F2BC6615D
SHA1:	B46550A3F500314FB02FED2DB1B5F1B50EEB6A1B
SHA-256:	4AF7C0F735A2FAE1DB049D8BA71EBFEC436FB735A846687B2D216CEAA5D676DC
SHA-512:	6E0A2D2A72B14CA94CD4E410384BD293847BC8D0D2FD1A90B61AE06619EF1451D3B155034A45603E05AEE7EB77AD7B29F35307D5B2D4D4A4D4D0DEF669E9D2 D4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272488537319285","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.536234280832976
Encrypted:	false
SSDEEP:	384:BcLtkLlryXW1kXqKf/pUZNCgVLH2HfDMrUvHGMnZ5mRSp4U:ZLl0W1kXqKf/pUZNCgVLH2HfgrUfGMnF
MD5:	36EA886EE7B6C2EAB71995F1E7C2893D
SHA1:	E9A4E6103E4A6FC48F62018D82FEA0D44E3BEDEE
SHA-256:	9A1A7C2F2409B6B3E6D942BAEEBB3FF13019228EC2493828A05F0A16EEAE045F
SHA-512:	BB39F6D05769897B96811664B2A57FFB8B92465F348E1526926BADB05680CDE609C3046FC3A24051FDDC642663B2C72F5F6E5B1D01338FCD45953E8A15DCFE9A
Malicious:	false
Reputation:	low
Preview:	{"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":"13272488537031826","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesTM (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):	16745
Entropy (8bit):	5.577712921951887
Encrypted:	false
SSDEEP:	384:BcLtdLlryXW1kXqKf/pUZNCgVLH2HfDMrUhXR3p4tF:2Ll0W1kXqKf/pUZNCgVLH2HfgrUhXtpQ
MD5:	76DA4D4E5BD01516EFBF0BEF613D2979
SHA1:	A8844D4ECB9D040381C781D2529883644DD78F4C
SHA-256:	17D66CB6F57814E1B81D3E3B00BB288948639054F1548AA250110064696D8AD9
SHA-512:	893BF4B7661A2B3300E4DC3CD6E7E5BEFE7AD81B9EE605F105DC58BE5F989027EA55AEAC9B70C8FBA0ED01068CE8584A720C7D1C95B0FB88C0BC1A57684F5A6
Malicious:	false
Reputation:	low
Preview:	{"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":"13272488537031826","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\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):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Entropy (8bit):	5.132602584456675
Encrypted:	false
SSDEEP:	6:mRXXXmRN9+q2Pwkn23iKKdKrQMxIFUtpmXXXZ3JZmwPmXXXAL9VkwOwkn23iKKd0:22MvYf5KkCFUtpmpZ/Pmi5Jf5KktJ
MD5:	0740ABEFA000EFBD0186E8D111458AFC
SHA1:	C41402143F5384E5340DABDE33CC94FF85BD19F9
SHA-256:	6565403F0117156CEF8285E5766C9D89DAA94260D92A5374E7A6EC8B152A04FB
SHA-512:	51B94F443DC13A693E3D6572BCE860B6C5D45A6B5590480AC974807D5CF3AB2BB9AB843548A8E2AD74C775DCF1EE1578EAAC140D44A7F71C06430A7AFDCF4E E2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.274 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-2 0:22:17.275 1a48 Recovering log #3.2021/08/03-20:22:17.276 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.132602584456675
Encrypted:	false
SSDEEP:	6:mRXXXmRN9+q2Pwkn23iKKdKrQMxIFUtpmXXXZ3JZmwPmXXXAL9VkwOwkn23iKKd0:22MvYf5KkCFUtpmpZ/Pmi5Jf5KktJ
MD5:	0740ABEFA000EFBD0186E8D111458AFC
SHA1:	C41402143F5384E5340DABDE33CC94FF85BD19F9
SHA-256:	6565403F0117156CEF8285E5766C9D89DAA94260D92A5374E7A6EC8B152A04FB
SHA-512:	51B94F443DC13A693E3D6572BCE860B6C5D45A6B5590480AC974807D5CF3AB2BB9AB843548A8E2AD74C775DCF1EE1578EAAC140D44A7F71C06430A7AFDCF4E E2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.274 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-2 0:22:17.275 1a48 Recovering log #3.2021/08/03-20:22:17.276 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\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):	348
Entropy (8bit):	5.117464045351927
Encrypted:	false
SSDEEP:	6:mRXXVnq2Pwkn23iKKdK7Uh2ghZIFUtpmXXVUZmwPmXXVUkwOwkn23iKKdK7Uh2gd:2VnvYf5KkIhHh2FUtpmVU/PmVU5Jf5KF
MD5:	F767F11C09ED242BAA7CFF3F06E47703
SHA1:	B238F5A2CCF1AC0BA0836F1E163B29CD22B3AD48
SHA-256:	5E144A0BAE31195A01CD1DA0725EE88F91AAA2727BE206E0384E931DB1538524
SHA-512:	464AB0E78DB3A2E856C210F301A4F46F3C2F6CD0B62A6850B07C4210FBD0DD524355FD429725B3D86319A63515708B1CB1F3764EEB592FEDE0DCA16AAF6B37A E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.014 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-20:22:17.016 1a44 Recovering log #3.2021/08/03-20:22:17.016 1a44 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.117464045351927
Encrypted:	false
SSDEEP:	6:mRXXVnq2Pwkn23iKKdK7Uh2ghZIFUtpmXXVUZmwPmXXVUkwOwkn23iKKdK7Uh2gd:2VnvYf5KkIhHh2FUtpmVU/PmVU5Jf5KF
MD5:	F767F11C09ED242BAA7CFF3F06E47703
SHA1:	B238F5A2CCF1AC0BA0836F1E163B29CD22B3AD48
SHA-256:	5E144A0BAE31195A01CD1DA0725EE88F91AAA2727BE206E0384E931DB1538524
SHA-512:	464AB0E78DB3A2E856C210F301A4F46F3C2F6CD0B62A6850B07C4210FBD0DD524355FD429725B3D86319A63515708B1CB1F3764EEB592FEDE0DCA16AAF6B37A E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.014 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-20:22:17.016 1a44 Recovering log #3.2021/08/03-20:22:17.016 1a44 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5cb0294c-75df-4b0c-83dd-580615f45446.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.215433891706196
Encrypted:	false
SSDEEP:	6:mRXXVVlL+q2Pwkn23iKKdKusNpV/2jMGIFUtpmXXf81ZmwPmXX4YLVkwOwkn23i3:2jIvYf5KkFFUtpmf81/Pmh5Jf5KkOJ
MD5:	2BE1C9EA9ADEA195F3D5A8F0027D4F75
SHA1:	F66961033B24EEB00D77D61608E2DDAED911C7B2
SHA-256:	DFFD9D36748D3D516A18A581BECA3A688E0E85062E7AC96CAA00C699EE02674E
SHA-512:	3424EB9399FB525E50090D97C35A5CD6BEC58423D8A79055B6503EDA05AC28373F40553C5999E56575A6E635446774273D84AF47F388A2AF8454E7DD762BA22F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.302 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:17.303 1a98 Recovering log #3.2021/08/03-20:22:17.304 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Size (bytes):	430
Entropy (8bit):	5.215433891706196
Encrypted:	false
SSDEEP:	6:mRXXVVlL+q2Pwkn23iKKdKusNpV/2jMGIFUtpmXXf81ZmwPmXX4YLVkwOwkn23i3:2jlvYf5KkFFUtpmf81/Pmh5Jf5KkOJ
MD5:	2BE1C9EA9ADEA195F3D5A8F0027D4F75
SHA1:	F66961033B24EEB00D77D61608E2DDAED911C7B2
SHA-256:	DFFD9D36748D3D516A18A581BECA3A688E0E85062E7AC96CAA00C699EE02674E
SHA-512:	3424EB9399FB525E50090D97C35A5CD6BEC58423D8A79055B6503EDA05AC28373F40553C5999E56575A6E635446774273D84AF47F388A2AF8454E7DD762BA22F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.302 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:17.303 1a98 Recovering log #3.2021/08/03-20:22:17.304 1a98 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.266356052588021
Encrypted:	false
SSDEEP:	12:2qvYf5KkmiuFUtpmX7cHz1/PmXFT5Jf5Kkm2J:2QYf5KkSgIXaIXFFJf5Kkr
MD5:	7F1B1D8F164C9AB532DEEB22A84A1417
SHA1:	9840BDC4882F713D097E39A67D6412098DB4E9E2
SHA-256:	9F92619630B003C734C1D8D14655D5055533ABB8E77BFECE6124437AE48120DC
SHA-512:	B686B66D558C8F632131A3EE20D6B9E976FC337F4A967FD6DA0007EDDE3D6C942BAA6059BC1EA9D01302E085CCDF6F63D6E7111E52651B8E801FBCD61CAB74 9D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.348 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:17.352 1a98 Recovering log #3.2021/08/03-20:22:17.353 1a98 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.266356052588021
Encrypted:	false
SSDEEP:	12:2qvYf5KkmiuFUtpmX7cHz1/PmXFT5Jf5Kkm2J:2QYf5KkSgIXaIXFFJf5Kkr
MD5:	7F1B1D8F164C9AB532DEEB22A84A1417
SHA1:	9840BDC4882F713D097E39A67D6412098DB4E9E2
SHA-256:	9F92619630B003C734C1D8D14655D5055533ABB8E77BFECE6124437AE48120DC
SHA-512:	B686B66D558C8F632131A3EE20D6B9E976FC337F4A967FD6DA0007EDDE3D6C942BAA6059BC1EA9D01302E085CCDF6F63D6E7111E52651B8E801FBCD61CAB74 9D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.348 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:17.352 1a98 Recovering log #3.2021/08/03-20:22:17.353 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.231901264801008
Encrypted:	false
SSDEEP:	6:mRXfX9+q2Pwkn23iKKdKusNpZQMxIFUtpmXiJZmwPmXOQ39VkwOwkn23iKKdKusx:2vovYf5KkMFUtpms/Pm+Qz5Jf5KkTJ
MD5:	625B1CB75C0AAADD8F9FCD115F11CF95
SHA1:	5AF202863911B0AB5CBE0BE362801BFC79208BB1
SHA-256:	86EB84EA425A2CA5FCBA9078B9E67182904E3DA6A58949431F7A3D6209B76C19
SHA-512:	155EF93021118141F011D7FA7229812DCC494E44718F8C4F845B19E00BFE74258655EED0C62E9E274BE1ADE328FC6C980012E597F89E28D2F27EC0CEDC739AB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:33.943 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-20:22:33.944 1a48 Recovering log #3.2021/08/03-20:22:33.945 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.231901264801008
Encrypted:	false
SSDEEP:	6:mRXfX9+q2Pwkn23iKKdKusNpZQMxIFUtpmXiJZmwPmXOQ39VkwOwkn23iKKdKusx:2vovYf5KkMFUtpms/Pm+Qz5Jf5KkTJ
MD5:	625B1CB75C0AAADD8F9FCD115F11CF95
SHA1:	5AF202863911B0AB5CBE0BE362801BFC79208BB1
SHA-256:	86EB84EA425A2CA5FCBA9078B9E67182904E3DA6A58949431F7A3D6209B76C19
SHA-512:	155EF93021118141F011D7FA7229812DCC494E44718F8C4F845B19E00BFE74258655EED0C62E9E274BE1ADE328FC6C980012E597F89E28D2F27EC0CEDC739AB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:33.943 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-20:22:33.944 1a48 Recovering log #3.2021/08/03-20:22:33.945 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\9fe7292e-9654-4798-8d33-22d0f39078e7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\9fe7292e-9654-4798-8d33-22d0f39078e7.tmp	
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'...(.....

C:\Users\user\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):	430
Entropy (8bit):	5.140468974633114
Encrypted:	false
SSDEEP:	12:2w/+vYf5KkkGHArBFUtpm7/PmuV5Jf5KkkGHAryJ:2nYf5KkkGgPgIKIJf5KkkGga
MD5:	58C8AD30EE96FE842B375C51F4B79E39
SHA1:	0A32C711A6F23F926785AD928FE06EE33325E1E0
SHA-256:	87034FDA1D6C10DC0B2D3A7B633B97E7D27D25548F9982E26FECB1FE451BBF0F
SHA-512:	FAE3F3A78E7839222DEDC0E5C7C8CA3B06E59D5159D1D415D546FFF52F9313BCE5C89948D09EB690F744352F6465251397A1857B7D833C9B04D68B8419F51BB3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:30.049 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:30.239 1a4c Recovering log #3.2021/08/03-20:22:30.243 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.140468974633114
Encrypted:	false
SSDEEP:	12:2w/+vYf5KkkGHArBFUtpm7/PmuV5Jf5KkkGHAryJ:2nYf5KkkGgPgIKIJf5KkkGga
MD5:	58C8AD30EE96FE842B375C51F4B79E39
SHA1:	0A32C711A6F23F926785AD928FE06EE33325E1E0
SHA-256:	87034FDA1D6C10DC0B2D3A7B633B97E7D27D25548F9982E26FECB1FE451BBF0F
SHA-512:	FAE3F3A78E7839222DEDC0E5C7C8CA3B06E59D5159D1D415D546FFF52F9313BCE5C89948D09EB690F744352F6465251397A1857B7D833C9B04D68B8419F51BB3
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old.. (copy)	
Reputation:	low
Preview:	2021/08/03-20:22:30.049 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:22:30.239 1a4c Recovering log #3.2021/08/03-20:22:30.243 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent Statemp (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.159145707908489
Encrypted:	false
SSDEEP:	12:2wOSQ+vYf5KkkGHArqiuFUtpmPG1/PmzfQV5Jf5KkkGHArq2J:2DMYf5KkkGgCgIZzqJf5KkkGg7
MD5:	76B2B617E11CFCD6ECBC15F512E0C29D
SHA1:	2271982D8866E9EF98DE97A8C39EB5ECBE03BBF4
SHA-256:	AC12BCE170D406851836C7D65A65186CFD43C1690583A6BE07B075D20FCFB76B
SHA-512:	1FDDFED6A473799BF2869E08E48B9622907B9C1233D4D4824BB9CF1C5CA6EB85472F3FB3AFAA7B483434F1F6770816AC84002056E71A3C8A69EB607269198FDE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:30.050 1a9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:30.240 1a9c Recovering log #3.2021/08/03-20:22:30.244 1a9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.159145707908489
Encrypted:	false
SSDEEP:	12:2wOSQ+vYf5KkkGHArqiuFUtpmPG1/PmzfQV5Jf5KkkGHArq2J:2DMYf5KkkGgCgIZzqJf5KkkGg7
MD5:	76B2B617E11CFCD6ECBC15F512E0C29D
SHA1:	2271982D8866E9EF98DE97A8C39EB5ECBE03BBF4
SHA-256:	AC12BCE170D406851836C7D65A65186CFD43C1690583A6BE07B075D20FCFB76B
SHA-512:	1FDDFED6A473799BF2869E08E48B9622907B9C1233D4D4824BB9CF1C5CA6EB85472F3FB3AFAA7B483434F1F6770816AC84002056E71A3C8A69EB607269198FDE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:30.050 1a9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:22:30.240 1a9c Recovering log #3.2021/08/03-20:22:30.244 1a9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.205413580205271
Encrypted:	false
SSDEEP:	12:2klvYf5KkkGHArAFUtpmKZ/PmKz5Jf5KkkGHArfJ:2BYf5KkkGgkgIKMKlJf5KkkGgV
MD5:	164AAFE24C12D8058E0390E1A54B1DAE
SHA1:	62B404021C86781F1B4885F67BEDB22636B53C3D
SHA-256:	5E8F9B116CB0DFE5CF5938F75EDFEB2D5B0B4BA6F33278AA3055B00FC3CA0581
SHA-512:	CF9F2F9AC4ABB4C5E0AF708A2C602B2AA622A473C0BC4CDA4D849C5CF51C8D0522A7A86363D32E685317D04F467E7A6ACCF57816B95F35DD572961DDDD4C470
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:45.635 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-20:22:45.637 1a48 Recovering log #3.2021/08/03-20:22:45.637 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.205413580205271
Encrypted:	false
SSDEEP:	12:2klvYf5KkkGHArAFUtpmKZ/PmKz5Jf5KkkGHArfJ:2BYf5KkkGgkgIKMKlJf5KkkGgV
MD5:	164AAFE24C12D8058E0390E1A54B1DAE
SHA1:	62B404021C86781F1B4885F67BEDB22636B53C3D
SHA-256:	5E8F9B116CB0DFE5CF5938F75EDFEB2D5B0B4BA6F33278AA3055B00FC3CA0581
SHA-512:	CF9F2F9AC4ABB4C5E0AF708A2C602B2AA622A473C0BC4CDA4D849C5CF51C8D0522A7A86363D32E685317D04F467E7A6ACCF57816B95F35DD572961DDDD4C470
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:45.635 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-20:22:45.637 1a48 Recovering log #3.2021/08/03-20:22:45.637 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\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):	324
Entropy (8bit):	5.144307401283357
Encrypted:	false
SSDEEP:	6:mRXXVxN+q2Pwkn23iKKdKpIFUtpmXXV75ZmwPmXXVFgdFNVkwOwkn23iKKdKa/Wd:2VxIvYf5KkmFUtpmV1/PmVCF5Jf5KkaQ
MD5:	D18BFE891C1FFCD4C2599497CFACA538
SHA1:	9EF3CFDC3B1041F486B448750F6B882C2E3ABAE8
SHA-256:	4BAFC4459DDD6FA3A65BF489DB458E4CEE29EA2F0DCA1E115408A7B2A5C9C194
SHA-512:	7050F3CF7C50F4455AD5EC4D82159AA0570BA13F5961BF08DD440F8346A954634A410093D4607A2413772AAB5BA666AF546AB389FB5CE97F5D88127B434816C3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.016 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:22:17.018 1a18 Recovering log #3.2021/08/03-20:22:17.019 1a18 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.144307401283357
Encrypted:	false
SSDEEP:	6:mRXXVxN+q2Pwkn23iKKdKpIFUtpmXXV75ZmwPmXXVFgdFNVkwOwkn23iKKdKa/Wd:2VxIvYf5KkmFUtpmV1/PmVCF5Jf5KkaQ
MD5:	D18BFE891C1FFCD4C2599497CFACA538
SHA1:	9EF3CFDC3B1041F486B448750F6B882C2E3ABAE8
SHA-256:	4BAFC4459DDD6FA3A65BF489DB458E4CEE29EA2F0DCA1E115408A7B2A5C9C194
SHA-512:	7050F3CF7C50F4455AD5EC4D82159AA0570BA13F5961BF08DD440F8346A954634A410093D4607A2413772AAB5BA666AF546AB389FB5CE97F5D88127B434816C3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:17.016 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:22:17.018 1a18 Recovering log #3.2021/08/03-20:22:17.019 1a18 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.2430151028552165
Encrypted:	false
SSDEEP:	12:2FovYf5KkkOrsFUtpmh/Pmy5Jf5KkkOrzJ:2FaYf5Kk+gIU8Jf5Kkn
MD5:	49D7D5D7345A4F6598B7B7D2E02BA123
SHA1:	13D9672D8F25F99A6A4282949BE46A97E0EDC2EB
SHA-256:	DBAC9051BFBD23E2D20309FE10CC012377131A4B14E49D0F77F4F25766013484
SHA-512:	7EAC6987976B7BFCA28EEFEC02C3B3569EF587F8D417A62F4A4BFF0BFFA83C86A8AD21D41E87712DBB44BE94AF249A6DF86F087D34987E4D2CCC576146D0B4 E1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:33.109 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:22:33.110 1a48 Recovering log #3.2021/08/03-20:22:33.111 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.oldn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.oldn (copy)	
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.2430151028552165
Encrypted:	false
SSDEEP:	12:2FovYf5KkkOrsFUtpmh/Pmy5Jf5KkkOrzJ:2FaYf5Kk+gIU8Jf5Kkn
MD5:	49D7D5D7345A4F6598B7B7D2E02BA123
SHA1:	13D9672D8F25F99A6A4282949BE46A97E0EDC2EB
SHA-256:	DBAC9051BFBD23E2D20309FE10CC012377131A4B14E49D0F77F4F25766013484
SHA-512:	7EAC6987976B7BFCA28EEFEC02C3B3569EF587F8D417A62F4A4BFF0BFFA83C86A8AD21D41E87712DBB44BE94AF249A6DF86F087D34987E4D2CCC576146D0B4E1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:33.109 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:22:33.110 1a48 Recovering log #3.2021/08/03-20:22:33.111 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (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):	1041
Entropy (8bit):	5.565926414537616
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe8hUts7wUeE4sRUeiQ:Ym6UUhyKUeiYqPeUekUez6wUecUeP
MD5:	D859304B0966B4B0ADF91735927AFCAE
SHA1:	9A5ABE26BE6AC3576A176B74E36DF6A8DC1F43D6
SHA-256:	24033DA68B3090CC85B76E615EBC0CFDB7B86D85E6C840DC9BFC67D076D3A959
SHA-512:	1B4D8C53AAB012624A8FE77B66997AC00DB0D3AC39119D6A2848432F512DD0590DA7625A61E1480578337329BDF67796BF7A15D52E26DEA1992296645AD779E9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1632987013.793603,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.793607},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:CFSn:GS
MD5:	4B79B6171D3C8D9A16E5130125049271
SHA1:	8252FE216A15CB3578E26ED58FE959A6C91DCB76
SHA-256:	4F8064FC4DABD23CBFB7062ADDF425014D6897D8F65FB1BE36615D350F32761F
SHA-512:	EE2973EDC52C0C3DF7CCA50240E9EDA7787D3DEEBE6BA0F32D4B87C1F338AACF2817E5F64F890CEBBA7EAF34C5E4597134EA0A23683E1364F49191181BD881B
Malicious:	false
Reputation:	low
Preview:	....f NQ.^..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd9f09bf-7c77-4c82-8123-38a0495c5c1d.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):	16745
Entropy (8bit):	5.577712921951887
Encrypted:	false
SSDEEP:	384:BcLtdLlryXW1kXqKf/pUZNCgVLH2HfDMrUhXR3p4tF:2Ll0W1kXqKf/pUZNCgVLH2HfgrUhXtpQ
MD5:	76DA4D4E5BD01516EFBF0BEF613D2979
SHA1:	A8844D4ECB9D040381C781D2529883644DD78F4C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd9f09bf-7c77-4c82-8123-38a0495c5c1d.tmp	
SHA-256:	17D66CB6F57814E1B81D3E3B00BB288948639054F1548AA250110064696D8AD9
SHA-512:	893BF4B7661A2B3300E4DC3CD6E7E5BEFE7AD81B9EE605F105DC58BE5F989027EA55AEAC9B70C8FBA0ED01068CE8584A720C7D1C95B0FB88C0BC1A57684F5 A6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272488537031826","location":5,"manifest":{"a pp":{"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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d6eb9130-5fa9-49b7-a668-27067febd4bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"adverti sed_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","s upports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{ "srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTTM (copy)	
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.415045899639168
Encrypted:	false
SSDEEP:	3:tUK6zXSFWfZmwv3IzXSRNjV8sIzXSeFJcmWGv:mRXSFUZmwPmXS/VvmXSeFSmtv
MD5:	131D94A56A20ADB75E5A8EFA5DC300B7
SHA1:	6CDBA504BBEF7DCF6A17F3E5376DEE4C3173A744
SHA-256:	559768C56D8559A7906702DE64003E7D701419D4CB9D4AFBDE09B7F1A7AC12B0
SHA-512:	213F1A73715F751A41E0F1B37E5E5CDD562856A4A7D17FC681EE7AF570468833FB50BBBAEF797BD5E278596628C77786747A5D6A82F5EF77C0EDD5251B2DCFCB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.193 159c Recovering log #3.2021/08/03-20:22:29.277 159c Delete type=0 #3.2021/08/03-20:22:29.278 159c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.olddf (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.415045899639168
Encrypted:	false
SSDEEP:	3:tUK6zXSFWfZmwv3IzXSRNjV8sIzXSeFJcmWGv:mRXSFUZmwPmXS/VvmXSeFSmtv
MD5:	131D94A56A20ADB75E5A8EFA5DC300B7
SHA1:	6CDBA504BBEF7DCF6A17F3E5376DEE4C3173A744
SHA-256:	559768C56D8559A7906702DE64003E7D701419D4CB9D4AFBDE09B7F1A7AC12B0
SHA-512:	213F1A73715F751A41E0F1B37E5E5CDD562856A4A7D17FC681EE7AF570468833FB50BBBAEF797BD5E278596628C77786747A5D6A82F5EF77C0EDD5251B2DCFCB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.193 159c Recovering log #3.2021/08/03-20:22:29.277 159c Delete type=0 #3.2021/08/03-20:22:29.278 159c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ff3e7189-ba5c-4f26-b9eb-999a01e0fe48.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):	1041
Entropy (8bit):	5.565926414537616
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe8hUts7wUeE4sRUeiQ:Ym6UUhyKUeiYqPeUekUez6wUecUeP
MD5:	D859304B0966B4B0ADF91735927AFCAE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ff3e7189-ba5c-4f26-b9eb-999a01e0fe48.tmp	
SHA1:	9A5ABE26BE6AC3576A176B74E36DF6A8DC1F43D6
SHA-256:	24033DA68B3090CC85B76E615EBC0CFDB7B86D85E6C840DC9BFC67D076D3A959
SHA-512:	1B4D8C53AAB012624A8FE77B66997AC00DB0D3AC39119D6A2848432F512DD0590DA7625A61E1480578337329BDF67796BF7A15D52E26DEA1992296645AD779E9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1632987013.793603,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.793607},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.167766273918841
Encrypted:	false
SSDEEP:	6:mRXStNOq2Pwkn23iKKdKfrzAdIFUtpmXStyZmwPmXStrzkwOwkn23iKKdKfrzILJ:2UNOvYf5Kk9FUtpmUy/PmU35Jf5Kk2J
MD5:	0058AFA986BBFAABE4E3223B989C3F0B
SHA1:	8200ADD08948FCDD88C17C45865904FAFB4E6CDF
SHA-256:	0F3F9881F80FCB3BCD0B53204C65180D9ECD4FB6941FFC62BCFAE0EA91135ED4
SHA-512:	A353EB6EA4991091940DDC097483AA82B7DBDE7B3D2C7E654581D90A4A8E5583B0202FD465C293EECADBA290263F5956344AA7C9BA0FFF88433BF41CE054345 0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.991 1a94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/08/03-20:22:29.994 1a94 Recovering log #3.2021/08/03-20:22:29.995 1a94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.167766273918841
Encrypted:	false
SSDEEP:	6:mRXStNOq2Pwkn23iKKdKfrzAdIFUtpmXStyZmwPmXStrzkwOwkn23iKKdKfrzILJ:2UNOvYf5Kk9FUtpmUy/PmU35Jf5Kk2J
MD5:	0058AFA986BBFAABE4E3223B989C3F0B
SHA1:	8200ADD08948FCDD88C17C45865904FAFB4E6CDF
SHA-256:	0F3F9881F80FCB3BCD0B53204C65180D9ECD4FB6941FFC62BCFAE0EA91135ED4
SHA-512:	A353EB6EA4991091940DDC097483AA82B7DBDE7B3D2C7E654581D90A4A8E5583B0202FD465C293EECADBA290263F5956344AA7C9BA0FFF88433BF41CE054345 0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-20:22:29.991 1a94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/08/03-20:22:29.994 1a94 Recovering log #3.2021/08/03-20:22:29.995 1a94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174471
Entropy (8bit):	6.079631732743056
Encrypted:	false
SSDEEP:	3072:c+VGaYTJQE+mugy9+QV1T7IRwdfLSNPJFcbXafIB0u1GOJmA3iuRN:xAxaV+QfT7GSmhHaqfllUOoSiuRN
MD5:	5DB61013220B41377D692BAE876265B6
SHA1:	6C816851207458DC177690C418F333C43B2DE39B
SHA-256:	F7B52310FC0A86B9422F2957D9A579CCD3D1BDE4CEBA99B0271D300FEB5C9104
SHA-512:	B5B2500FE17A4214D3B8A89CBE88781EAE8A4C07FB3A8ECEE68B339A730188097115A0F1192E3CB99067520F1B0C074CA98D951590BF850BD2F26DDC013622A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628014940044469e+12,"network":1.628014942e+12,"ticks":7262765691.0,"uncertainty":4436387.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174471
Entropy (8bit):	6.079630828791983
Encrypted:	false
SSDEEP:	3072:s+VGaYTJQE+mugy9+QV1T7IRwdfLSNPJFcbXafIB0u1GOJmA3iuRN:hAxaV+QfT7GSmhHaqfllUOoSiuRN
MD5:	AE227F46D6A429C3B336F81DBD26012B
SHA1:	3414EE3B2E0D4B789C90A9EE0C09ED2D737EAA69
SHA-256:	C7D2846C96965A6FC35308219584F73CAA0E20675FFDCAF06657D6E694FD3026
SHA-512:	EE61A8263D61B0210232C25FA5DA97788EA82A65468AA3A2576E7E01EEC4962F57380795EA9FBC0228289D9E694F0B680921D19631E91A7C3A3499F38E1E24B4
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628014940044469e+12,"network":1.628014942e+12,"ticks":7262765691.0,"uncertainty":4436387.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715020141"},"plugins":{"metadata":{"adobe-flash-player":{"

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7496855485485643
Encrypted:	false
SSDEEP:	384:H7XEU25D+mBgjNMrdvl03HEyDHeTGzmrRmUmx3Kyq1rhsm1C1WEAoTOW6gNp1UNP:tqVpKKn30efSISUHPeAKWYgBW
MD5:	FE41D8EC7C3FEA1B004A8EBAD3192B67
SHA1:	BE68EB354866B9990ECB2CB50ED852526476FF49
SHA-256:	FD7907690B3DF29387A2696C0700D61B9D945C69E2A49EDDBC0A38C71D37BF0F
SHA-512:	B146CA79BAB361BCF1C89A1ED26812FC366CCE1583220B3E8CA6C8F48E52C1BEF79512703DCE26CC7B0F963ED564B7A2AEA8B3EDD45EED9716249DB058FA3 78B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\b967fc3c-2fba-46f8-86bb-43b27344cbfe.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):	174471
Entropy (8bit):	6.079631431763681
Encrypted:	false
SSDEEP:	3072:cAZGaYTJQE+mugy9+QV1T7IRwdfLSNPJFcbXafIB0u1GOJmA3iuRN:3UxaV+QfT7GSmhHaqfIlUOoSiuRN
MD5:	76AA28853ED4C7865D181A58CE51AD94
SHA1:	CB187F4DD141987582D75B3C4B22D7B1E2AB22E4
SHA-256:	7F9520FB53B8950A327F4C81ABDBE03014330D559BE9BCF4F011EA4AE18E74EB
SHA-512:	EB23E5CB6C88B8D92F13808131645687F574D1E8DCF03C658048E419A60907547DE45D0CC63678CDEFBF5536FAE6F6C9F8C030BDA520D788E6C8EE01D4F8BA D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628014940044469e+12,"network":1.628014942e+12,"ticks":7262765691.0,"uncertainty":4436387.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\ba79ef51-fc57-4874-9606-772a69da670f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7496855485485643
Encrypted:	false
SSDEEP:	384:H7XEU25D+mBgjNMrdvl03HEyDHeTGzmrRmUmx3Kyq1rhsm1C1WEAoTOW6gNp1UNP:tqVpKKn30efSISUHPeAKWYgBW
MD5:	FE41D8EC7C3FEA1B004A8EBAD3192B67
SHA1:	BE68EB354866B9990ECB2CB50ED852526476FF49
SHA-256:	FD7907690B3DF29387A2696C0700D61B9D945C69E2A49EDDBC0A38C71D37BF0F
SHA-512:	B146CA79BAB361BCF1C89A1ED26812FC366CCE1583220B3E8CA6C8F48E52C1BEF79512703DCE26CC7B0F963ED564B7A2AEA8B3EDD45EED9716249DB058FA3 78B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\c9e8b14e-47fd-42e7-ab68-db19dcf80d8c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified

C:\Users\user\AppData\Local\Google\Chrome\User Data\c9e8b14e-47fd-42e7-ab68-db19dcf80d8c.tmp

Size (bytes):	174471
Entropy (8bit):	6.079630828791983
Encrypted:	false
SSDEEP:	3072:s+VGaYTJQE+mugy9+QV1T7IRwdfLSNPJFcbXafIB0u1GOJmA3iuRN:hAxaV+QfT7GSmhHaqfIlUOoSiuRN
MD5:	AE227F46D6A429C3B336F81DBD26012B
SHA1:	3414EE3B2E0D4B789C90A9EE0C09ED2D737EAA69
SHA-256:	C7D2846C96965A6FC35308219584F73CAA0E20675FFDCAF06657D6E694FD3026
SHA-512:	EE61A8263D61B0210232C25FA5DA97788EA82A65468AA3A2576E7E01EEC4962F57380795EA9FBC0228289D9E694F0B680921D19631E91A7C3A3499F38E1E24B4
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628014940044469e+12,"network":1.628014942e+12,"ticks":7262765691.0,"uncertainty":4436387.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715020141"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\dce05fd3-ccfa-43c3-8aae-a213c2a67c95.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):	174471
Entropy (8bit):	6.079631732743056
Encrypted:	false
SSDEEP:	3072:c+VGaYTJQE+mugy9+QV1T7IRwdfLSNPJFcbXafIB0u1GOJmA3iuRN:xAxaV+QfT7GSmhHaqfIlUOoSiuRN
MD5:	5DB61013220B41377D692BAE876265B6
SHA1:	6C816851207458DC177690C418F333C43B2DE39B
SHA-256:	F7B52310FC0A86B9422F2957D9A579CCD3D1BDE4CEBA99B0271D300FEB5C9104
SHA-512:	B5B2500FE17A4214D3B8A89CBE88781EAE8A4C07FB3A8ECEE68B339A730188097115A0F1192E3CB99067520F1B0C074CA98D951590BF850BD2F26DDC013622A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628014940044469e+12,"network":1.628014942e+12,"ticks":7262765691.0,"uncertainty":4436387.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:22:20.291594982 CEST	192.168.2.4	8.8.8.8	0x7c21	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:20.303503990 CEST	192.168.2.4	8.8.8.8	0x3bdf	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:20.307668924 CEST	192.168.2.4	8.8.8.8	0x7527	Standard query (0)	iya2304e74e352f95cef9ab55.web.app	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:21.240627050 CEST	192.168.2.4	8.8.8.8	0x179f	Standard query (0)	webmail.supremecluster.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:21.245049000 CEST	192.168.2.4	8.8.8.8	0xcdb2	Standard query (0)	rc.netsolution.ro	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:22.602606058 CEST	192.168.2.4	8.8.8.8	0xc1e4	Standard query (0)	webmail.supremecluster.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:30.107064009 CEST	192.168.2.4	8.8.8.8	0xea68	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:22:20.324103117 CEST	8.8.8.8	192.168.2.4	0x7c21	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:22:20.324103117 CEST	8.8.8.8	192.168.2.4	0x7c21	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:20.338613033 CEST	8.8.8.8	192.168.2.4	0x3bdf	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:20.348613024 CEST	8.8.8.8	192.168.2.4	0x7527	No error (0)	iya2304e74e352f95cef9ab55.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:20.348613024 CEST	8.8.8.8	192.168.2.4	0x7527	No error (0)	iya2304e74e352f95cef9ab55.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:21.288343906 CEST	8.8.8.8	192.168.2.4	0xcdb2	No error (0)	rc.netsolution.ro		116.203.240.40	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:21.289697886 CEST	8.8.8.8	192.168.2.4	0x179f	No error (0)	webmail.supremecluster.com		185.38.106.149	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:22.635193110 CEST	8.8.8.8	192.168.2.4	0xc1e4	No error (0)	webmail.supremecluster.com		185.38.106.149	A (IP address)	IN (0x0001)
Aug 3, 2021 20:22:30.139915943 CEST	8.8.8.8	192.168.2.4	0xea68	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:22:30.139915943 CEST	8.8.8.8	192.168.2.4	0xea68	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTPS Packets

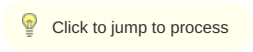
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 20:22:21.340770006 CEST	116.203.240.40	443	192.168.2.4	49745	CN=rc.netsolution.ro CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jul 27 11:05:45 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Oct 25 11:05:43 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 20:22:22.705054045 CEST	185.38.106.149	443	192.168.2.4	49762	CN=webmail.supremecluster.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Jul 02 07:12:00 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Sep 30 07:11:59 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6604 Parent PID: 2440

General

Start time:	20:22:16
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://iya2304e74e352f95cef9ab55.web.app/#lori.pilot@algoma.com'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6772 Parent PID: 6604

General

Start time:	20:22:17
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,13940740740856333051,3351174129214579356,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1792 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly