ID: 364055
Sample Name: %F0%9F%93%A9-Tina_Cfisd_HP29VF.htm
Cookbook: default.jbs
Time: 19:12:30
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

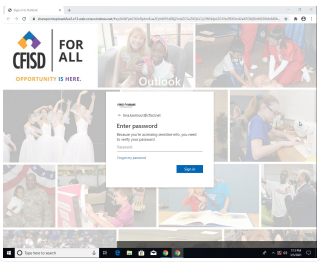
Analysis Report %F0%9F%93%A9-Tina_Cfisd_HP29VF.h…

Overview

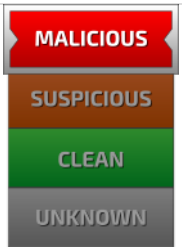
General Information

Sample Name:	%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm
Analysis ID:	364055
MD5:	55e8459fd775c23.
SHA1:	e7a99dbb445083..
SHA256:	bd841306b786d4..
Infos:	

Most interesting Screenshot:



Detection



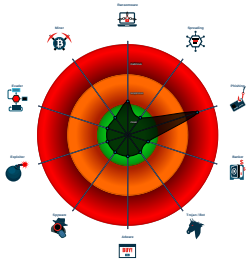
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish_10
- Yara detected obfuscated html page
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid 'forgot password' link found
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6396 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6580 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1520,6376799053035196430,7750294235629446408,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

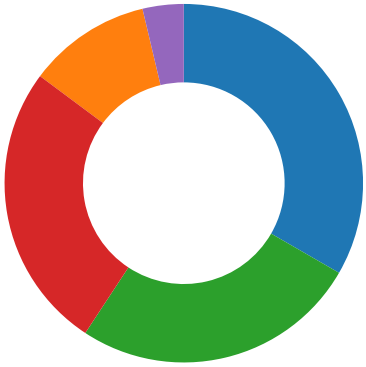
Initial Sample

Source	Rule	Description	Author	Strings
%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Phishing
- Compliance
- Networking
- System Summary
- Persistence and Installation Behavior

Click to jump to signature section

Phishing:

Yara detected HtmlPhish_10

Yara detected obfuscated html page

Compliance:

Creates a directory in C:\Program Files

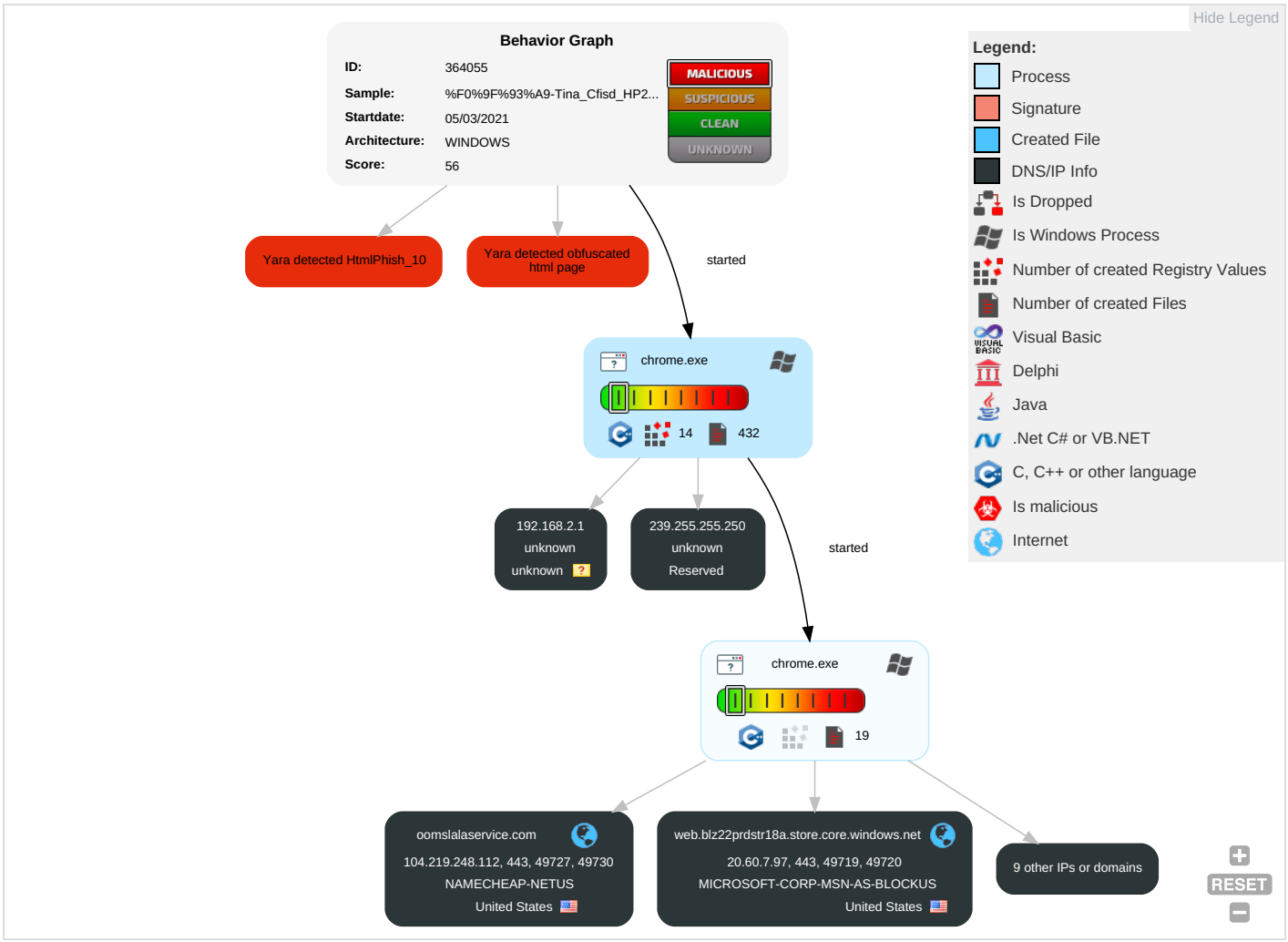
Creates license or readme file

Uses secure TLS version for HTTPS connections

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 3	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

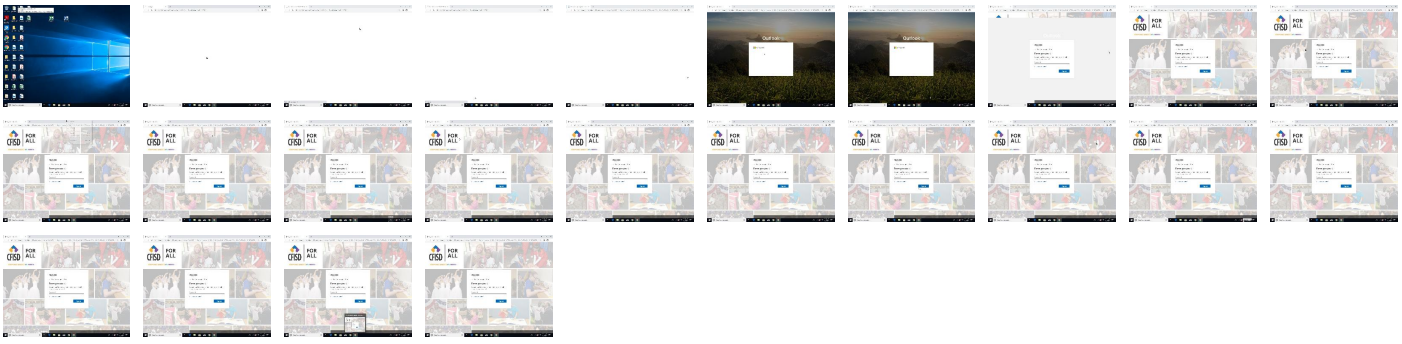
Behavior Graph

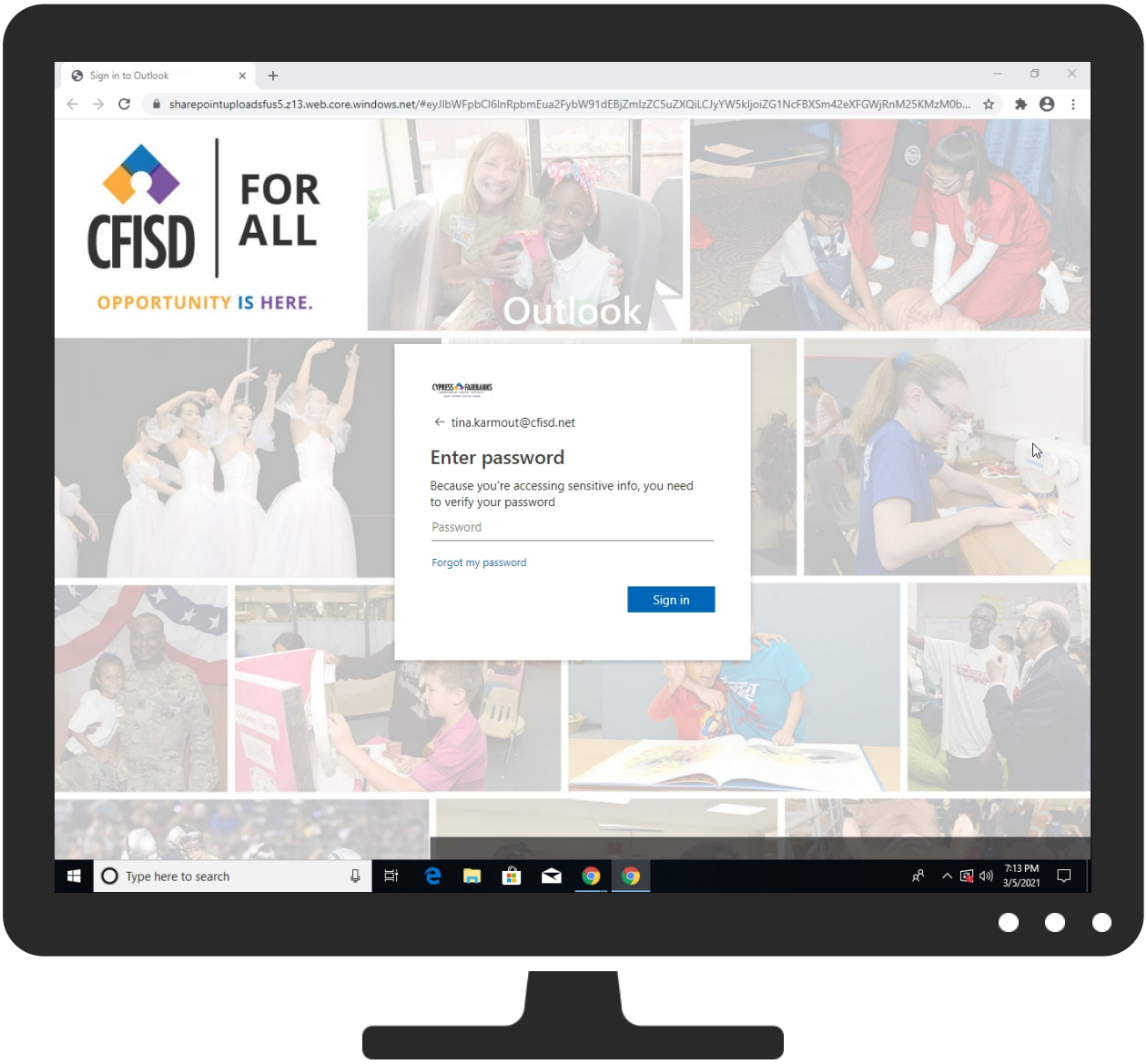


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
oomslalaservice.com	0%	Virustotal		Browse
t.dripemail2.com	0%	Virustotal		Browse
cs1025.wpc.upsiloncdn.net	0%	Virustotal		Browse
convoy.app	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://convoy.app/search?routeType=Offers&~channel=repeat_request_reload_email&~email_feature=repea	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net	0%	Avira URL Cloud	safe	
http://https://t.dripemail2.com	0%	Avira URL Cloud	safe	
http://https://oomslalaservice.com	0%	Avira URL Cloud	safe	
http://https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpa	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
web.blz22prdstr18a.store.core.windows.net	20.60.7.97	true	false		high
oomslalaservice.com	104.219.248.112	true	false	• 0%, Virustotal, Browse	unknown
t.dripemail2.com	34.192.142.116	true	false	• 0%, Virustotal, Browse	unknown
cnvy.app.link	13.224.193.100	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false	• 0%, Virustotal, Browse	unknown
convoy.app	52.52.65.159	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.23.65	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
aadcdn.msauthimages.net	unknown	unknown	false		unknown
sharepointuploadsfus5.z13.web.core.windows.net	unknown	unknown	false		high

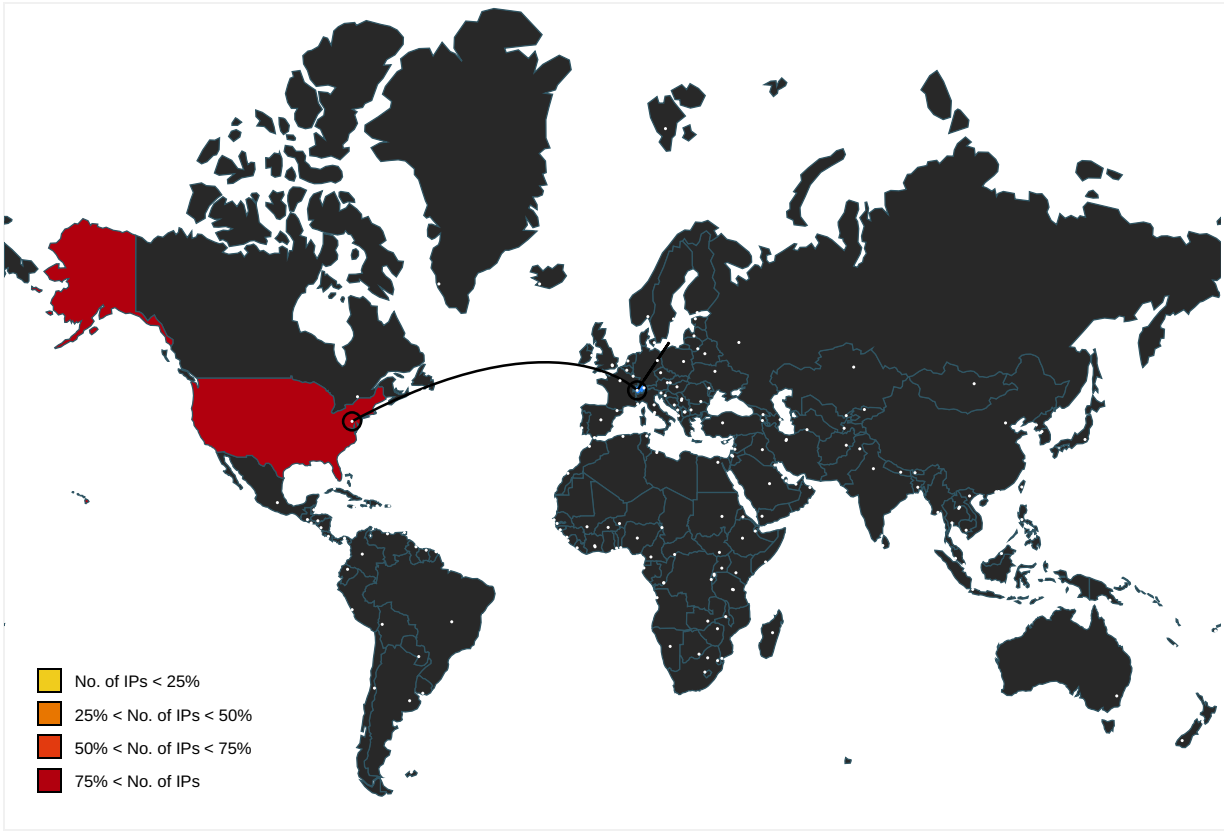
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sharepointuploadsfus5.z13.web.core.windows.net/#eyJlbWFpbCI6InRpbmEua2FybW91dEBjZmlzZC5uZXQiLCJyYW5kIjoiZG1NcFBXSm42eXFGWjRnM25KMzM0bDZ3OHlZMzZlOWlHbTlMa0RQSFdGbHoxN1RoM0RRNGtUNmx6aGpyIn0=	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	004b85ab-df46-44d4-b943-340acdc4ef9b.tmp.1.dr, 432b2f1f-5519-4732-b9e6-7a8d72085144.tmp.1.dr, 372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp.1.dr, 750e1841-fc76-49f9-a83d-9675ea47ac15.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://convoy.app/search?routeType=Offers&~channel=repeat_request_reload_email&~email_feature=repea	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	432b2f1f-5519-4732-b9e6-7a8d72085144.tmp.1.dr, 372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp.1.dr	false		high
http://https://aadcdn.msauthimages.net	372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.dripemail2.com	372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cnvy.app.link/O9lDJUMI3U?routeType=Offers&~channel=repeat_request_reload_email&~email_featur	History.0.dr	false		high
http://https://sharepointuploadsfus5.z13.web.core.windows.net/#	Current Session.0.dr	false		high
http://https://oomslalaservice.com	372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://sharepointuploadsfus5.z13.web.core.windows.net/#eyJlbWFpbCI6InRpbmEua2FybW91dEBjZmlzZC5uZXQi	History.0.dr	false		high
http://https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpa	History.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
104.219.248.112	oomslalaservice.com	United States		22612	NAMECHEAP-NETUS	false
20.60.7.97	web.blz22prdstr18a.store.core.windows.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.52.65.159	convoy.app	United States		16509	AMAZON-02US	false
34.192.142.116	t.dripemail2.com	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.224.193.100	cnvy.app.link	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	364055
Start date:	05.03.2021
Start time:	19:12:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.winHTM@35/175@7/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.211.6.115, 104.43.193.48, 172.217.20.238, 172.217.22.237, 172.217.22.206, 173.194.187.170, 74.125.173.39, 52.255.188.83, 172.217.23.80, 172.217.22.240, 216.58.207.176, 172.217.20.240, 172.217.23.48, 216.58.207.163, 172.217.20.234, 172.217.23.42, 172.217.23.74, 172.217.22.202, 216.58.207.138, 216.58.207.170, 93.184.221.240, 104.42.151.234, 13.64.90.137, 13.88.21.125, 51.11.168.160, 184.30.24.56, 40.88.32.150, 172.217.20.227, 173.194.182.198, 92.122.213.194, 92.122.213.247, 20.54.26.129, 74.125.173.28, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, storage.googleapis.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, r1---sn-4g5e6nlk.gvt1.com, clients2.google.com, audownload.windowsupdate.nsatc.net, aadcdn.ec.azureedge.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, content-autofill.googleapis.com, r1---sn-4g5e6nss.gvt1.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, r5---sn-4g5e6nz7.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r1.sn-4g5e6nss.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, r6.sn-4g5e6nld.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wu.azureedge.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, aadcdn.azureedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, r5.sn-4g5e6nz7.gvt1.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, r1.sn-4g5e6nlk.gvt1.com, skypedataprdcoleus17.cloudapp.net, r6---sn-4g5e6nld.gvt1.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:13:25	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.199.23.72	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	
	http://rmqi89xr.gocapitalswift.biz/Qo4UguRqu/bGF1cmEuZ29uemFsZXpAc3luZ2VudGEuY29t	Get hash	malicious	Browse	
	http://https://pydevelopment.com/wpvnote/Y2hyaXNfcHVsbGlnQGJheWxvci5lZHU=	Get hash	malicious	Browse	
	http://https://axirouteprevention.fr/images/to/TO/abuse@aptum.com	Get hash	malicious	Browse	
	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXIxLmNvbQ==	Get hash	malicious	Browse	
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	
	http://email.balluun.com/ls/click?upn=vAgQonvqwvuwOYm-2FeLk6JoFNFg3eRlAI8QIEVntBAuI-2BvU3e7BCgAWK4gND5sUFzaOsmo7sSmVoKwCcIxTg-2BFixi2xkEEW0oX1nuZ00rbDRxhHyjyRDdAxKojA59O-2B4AFSpNTWqqEs1z6j5wzlR2-2FBqayO2J83qvH4QoQ-2F3anf0VFAroZ5d-2BXoNmQDglJ5pwxxVoZatBhZPngQRjuQTxew-3D-3DzH4L_3j-2BjdnCo31g6AoJOEEgYaF9xlWteAa1K0Qa8qq9OD9qW7sjFhUMmultTO5jBWtQpNUDwj6PE1qUa9-2BpzdXtC1dfajoy6E591rXly0ybZJZAn8Vxq-2Fq0s46eH6TVCm1b6N0WF6m2Ciw6XuwKQM6-2FvOhmnealyeWsQT6Pbejkt1oPtkbgT9bDnxj2sxfWzdY-2F9GQwHNqRuoi-2FmHeLH7KOkDQ-3D-3D	Get hash	malicious	Browse	
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	
	http://rwiqipwvnklaqkuu.ltiliqhting.com/asci/SmFjcXVlbGluZS5TY2hyYWRlckByYWJvYmFuay5jb20=	Get hash	malicious	Browse	
	http://https://igainc-my.sharepoint.com/:o:/p/tcarr/elepnwd2-bzfsjpud_cugcwbjnnx2pfug1t1x3dcvlcytq?e=ylqh7j	Get hash	malicious	Browse	
	http://nueawbjavdjkdyq.centralcs.org/cope/YW5keS5wZXR0ZXJzb25AYXB0dW0uY29t#616e64792e706574746572736f6e40617074756d2e636f6d	Get hash	malicious	Browse	
	http://citacademiesuk-my.sharepoint.com	Get hash	malicious	Browse	
	http://49.120.66.34.bc.googleusercontent.com/osh?email=bob@microsoft.com	Get hash	malicious	Browse	
	http://https://fra1.digitaloceanspaces.com/monna/index.html#judith.russell@centrica.com	Get hash	malicious	Browse	
239.255.255.250	audio_cheri.riley@treetop.com_file.htm	Get hash	malicious	Browse	
	March 4, 2021, 055038 PM.HTM	Get hash	malicious	Browse	
	MRS.exe	Get hash	malicious	Browse	
	equinitiTicket#51347303511505986.htm	Get hash	malicious	Browse	
	_evm5437345.htm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	March 4, 2021, 021638 PM.HTM	Get hash	malicious	Browse	
	PaymentConfirmation_9QE1-NSSB8U-CHF3.htm	Get hash	malicious	Browse	
	New Invoice.PDF.htm	Get hash	malicious	Browse	
	Intruder.exe	Get hash	malicious	Browse	
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies .com.html	Get hash	malicious	Browse	
	holla.htm	Get hash	malicious	Browse	
	UPS Delivery Notification, Receiver susiej@johnsto ncompanies.com.html	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	remit726498.htm	Get hash	malicious	Browse	
	Xero from wellbeingsoftware.htm	Get hash	malicious	Browse	
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKe ep.htm	Get hash	malicious	Browse	
	#Ud83d#UdcdeMichelle.bloxham.htm	Get hash	malicious	Browse	
	selfassessment.doc	Get hash	malicious	Browse	
	Xeros from ecommpay.htm	Get hash	malicious	Browse	
104.219.248.112	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	
	http://https://raubax.com/php/login/	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cs1025.wpc.upsiloncdn.net	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKe ep.htm	Get hash	malicious	Browse	• 152.199.23.72
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 152.199.23.72
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	• 152.199.23.72
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	• 152.199.23.72
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 152.199.23.72
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 152.199.23.72
	http://rmqi89xr.gocapitalswift.biz/Qo4UguRqu/bGF1cmEuZ29uemFsZXpAc3luZ2VudGEuY29t	Get hash	malicious	Browse	• 152.199.23.72
	http://https://pydevelopment.com/wpvnote/Y2hyaXNfcHVsbGlnQGJheWxvci5lZHU=	Get hash	malicious	Browse	• 152.199.23.72
	http://https://axirouteprevention.fr/images/to/TO/abuse@aptum.com	Get hash	malicious	Browse	• 152.199.23.72
	http://gomterly.tk/nomter/YW5nZWxvLmRlc2FudGlzQGNvZ2Vjb3BlZXlxLmNvbQ==	Get hash	malicious	Browse	• 152.199.23.72
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 152.199.23.72
	http://email.balluun.com/ls/click?upn=vAgQonvqwvuwOYm-2FeLk6JoFNFg3eRlAI8QIEVntBAuI-2BvU3e7BCgAWK4gND5sUFzaOsmo7sSmVoKwCcIxTg-2BFixi2xkEEW0oX1nuZ00rbDRxhHyjyRDdAxKojA59O-2B4AFSpNTWqqEs1z6j5wzlR2-2FBqayO2J83qvH4QoQ-2F3anf0VFAroZ5d-2BXoNmQDglJ5pwxxVoZatBhZPngQRjuQTxew-3D-3DzH4L_3j-2BjdnCo31g6AoJOEEgYaF9xlWteAa1K0Qa8qq9OD9qW7sjFhUMmultTO5jBWtQpNUDwj6PE1qUa9-2BpzdXtC1dfajoy6E591rXly0ybZJZAn8Vxq-2Fq0s46eH6TVCm1b6N0WF6m2Ciw6XuwKQM6-2FvOhmnealyeWsQT6Pbejkt1oPtkbgT9bDnxj2sxfWzdY-2F9GQwHNqRuoi-2FmHeLH7KOkDQ-3D-3D	Get hash	malicious	Browse	• 152.199.23.72
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 152.199.23.72
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 152.199.23.72
	http://rwiqipwvnklaqkuu.ltiliqhting.com/asci/SmFjcXVlbGluZS5TY2hyYWRlckByYWJvYmFuay5jb20=	Get hash	malicious	Browse	• 152.199.23.72
	http://https://igainc-my.sharepoint.com/:o:/p/tcarr/elepnwd2-bzfsjpud_cugcwbjnnx2pfug1t1x3dcvlcytq?e=ylqh7j	Get hash	malicious	Browse	• 152.199.23.72

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://nueawbjavdjkdyq.centralcs.org/cope/YW5keS5wZXR0ZXJzb25AYXB0dW0uY29t#616e64792e706574746572736f6e40617074756d2e636f6d	Get hash	malicious	Browse	• 152.199.23.72
	http://citacademiesuk-my.sharepoint.com	Get hash	malicious	Browse	• 152.199.23.72
	http://49.120.66.34.bc.googleusercontent.com/osh?email=bob@microsoft.com	Get hash	malicious	Browse	• 152.199.23.72
	http://https://fra1.digitaloceanspaces.com/monna/index.html#judith.russell@centrica.com	Get hash	malicious	Browse	• 152.199.23.72
t.dripemail2.com	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 54.158.2.202
	http://https://adclick.g.doubleclick.net/pcs/click?xai=AKAOjsuAdmpMchmoFdZDPbMXBlokocyA_LFtEyj9kJY954hC5mJGurXSs_N79OI-jzZY21N1pvAVIRDTNCj-DpiT4wnZ7H859vPYQmUDOy5YE9XRInzUtCGUGws-aNdZNyo_E9D_JNeMzTzZse3INUS-7omiEswmHVST-wCMaGYDJIiAdKI9UjKZBrrVjaEu7oNGvSqFpE3PGs-p4IKKri-p-WNFq_dRzb1BGFC3Q6ZKO0qQJEtNrtiwcDEkGTac9EixKyFfAZ3S-BGTECCM65NeVM22UvJq2dKcpa_7MdcyOmwsF-YnWH2T&sai=AMfl-YQiO-7a_XQE9aG1TZlVlihyreoscJk-Lr9xc18RB4LLZiH1wF1vCyOqwg6Ien7x26hweDGC9jn4p3WUZ1F0ccNM-jq4TaKv3AMKg6gGo1dCe9ifPmbb2gYjIH-1DqcgwT3b&sig=Cg0ArKJSzF6saN_I3E13EAE&urlfix=1&adurl=https://email.ratemyagent.com/Email/RedirectToURL?URL=https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpaTdhcmgiLCJ1cmwiOiJodHRwczovL3N0b3JhZ2UuZ29vZ2xlYXBpcy5jb20vc2hteGNwZ2JveHJveTEuYXBwc3BvdC5jb20vaW5kZXguaHRtbCJ9#Z2VuYS5kcmFrZUBibXMuY29t	Get hash	malicious	Browse	• 34.227.187.212
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https://reporting.sainsburys-online.com/cgi-bin/rr/nobook:2648901,nosent:322556,nosrep:175447/https%3A%2F%2Fzutwholesale.com/tools/emails/click/order-confirmation/1/button/view-order-status?url=https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpaTdhcmgiLCJ1cmwiOiJodHRwczovL3N0b3JhZ2UuZ29vZ2xlYXBpcy5jb20vc2hteGNwZ2JveG5sYTEuYXBwc3BvdC5jb20vaW5kZXguaHRtbCJ9#dG9ueUBmb2ltcy5jb20=	Get hash	malicious	Browse	• 34.196.43.244
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https://reporting.sainsburys-online.com/cgi-bin/rr/nobook:2648901,nosent:322556,nosrep:175447/https%3A%2F%2Fzutwholesale.com/tools/emails/click/order-confirmation/1/button/view-order-status?url=https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpaTdhcmgiLCJ1cmwiOiJodHRwczovL3N0b3JhZ2UuZ29vZ2xlYXBpcy5jb20vc2hteGNwZ2JveGtpbDEuYXBwc3BvdC5jb20vaW5kZXguaHRtbCJ9#YmVubEBhdXN0cmFsaWFuYmFsbGV0LmNvbS5hdQ==	Get hash	malicious	Browse	• 52.73.138.76
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https://reporting.sainsburys-online.com/cgi-bin/rr/nobook:2648901,nosent:322556,nosrep:175447/https%3A%2F%2Fzutwholesale.com/tools/emails/click/order-confirmation/1/button/view-order-status?url=https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpaTdhcmgiLCJ1cmwiOiJodHRwczovL3N0b3JhZ2UuZ29vZ2xlYXBpcy5jb20vc2hteGNwZ2JveG1vbjEuYXBwc3BvdC5jb20vaW5kZXguaHRtbCJ9#bW9uYS5ndWxicmFuc2VuQG9wcGVnYXJkLmtvbW11bmUubm8=	Get hash	malicious	Browse	• 52.73.138.76
	http://tr.subscribermail.com/cc.cfm?sendto=http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https%3a%2f%2fzutwholesale.com/tools/emails/click/order-confirmation/1/button/view-order-status?url=https://t.dripemail2.com/c/eyJhY2NvdW50X2lkIjoiNDgxODMzMSIsImRlbGl2ZXJ5X2lkIjoibTllYTV3NTFkdWFsbWJpaTdhcmgiLCJ1cmwiOiJodHRwczovL3N0b3JhZ2UuZ29vZ2xlYXBpcy5jb20vZXlldHNmYmhmYmtpbDIuYXBwc3BvdC5jb20vaW5kZXguaHRtbCJ9#amFuZXRAdmlhc2VhdGluZy5jb20=	Get hash	malicious	Browse	• 34.199.211.214
oomslalaservice.com	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	zmR8OHKFzs.exe	Get hash	malicious	Browse	• 198.54.122.60
	kLRqBDRRQp.exe	Get hash	malicious	Browse	• 199.193.7.228
	87iQnkqmHE.rtf	Get hash	malicious	Browse	• 199.193.7.228
	Order.doc	Get hash	malicious	Browse	• 198.54.122.60
	Request for Quotation RFQ.doc	Get hash	malicious	Browse	• 198.54.122.60
	TYPEDESC.exe	Get hash	malicious	Browse	• 199.193.7.228
	Datos factura.doc	Get hash	malicious	Browse	• 162.0.236.110
	Confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• 198.54.125.250
	8877.exe	Get hash	malicious	Browse	• 198.54.117.197
	KK7wD2vDmF.exe	Get hash	malicious	Browse	• 198.54.117.212
	Transfer Confirmation.exe	Get hash	malicious	Browse	• 198.54.117.197
	2021_03_04.exe	Get hash	malicious	Browse	• 198.54.117.215
	#Uc138#Uae08 #Uacc4#Uc0b0#Uc11c.exe	Get hash	malicious	Browse	• 198.54.117.215
	Request for Qouation.exe	Get hash	malicious	Browse	• 198.54.116.236
	20210303948387477467,pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	Machines BID 8100250147_purchase requirements.exe	Get hash	malicious	Browse	• 63.250.37.200
	dwg.exe	Get hash	malicious	Browse	• 198.54.117.215
	Invoice #0023228 PDF.exe	Get hash	malicious	Browse	• 104.219.248.70
	k26agg1xUj.exe	Get hash	malicious	Browse	• 198.54.122.60
	a16i5VgAvi.exe	Get hash	malicious	Browse	• 198.54.122.60
EDGECASTUS	Paid561571.htm	Get hash	malicious	Browse	• 152.199.23.37
	Remittance0434.htm	Get hash	malicious	Browse	• 152.199.23.37
	603e0ffd2eeb9.tar.dll	Get hash	malicious	Browse	• 192.229.221.206
	remit726498.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	• 152.199.23.72
	Gewinncode-32532404.docm	Get hash	malicious	Browse	• 152.199.21.141
	2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx	Get hash	malicious	Browse	• 152.199.21.175
	Xeros from condor.htm	Get hash	malicious	Browse	• 93.184.220.70
	Payment.html	Get hash	malicious	Browse	• 152.199.23.37
	Remittance advice.htm	Get hash	malicious	Browse	• 152.199.23.37
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	• 152.199.23.37
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 152.199.23.37
	Z4fYo3NwC0.exe	Get hash	malicious	Browse	• 93.184.220.29
	602b97e0b415b.png.dll	Get hash	malicious	Browse	• 192.229.221.215
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 8%3A1%3A54 a.m., _20210209080154.8E45EAA12FF8DC21@sophiajoyas.cl_.html	Get hash	malicious	Browse	• 192.229.221.185
	Farie PO.doc	Get hash	malicious	Browse	• 192.229.221.185
	5DktGbEvIA.apk	Get hash	malicious	Browse	• 68.232.34.193
	February Payroll.xls.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37
MICROSOFT-CORP-MSN-AS-BLOCKUS	FileZilla_3.50.0_win32-setup.exe	Get hash	malicious	Browse	• 52.155.217.156
	com.totallymoney.account-1.14.0-sameapk.com.apk	Get hash	malicious	Browse	• 52.232.209.85
	com.totallymoney.account-1.14.0-sameapk.com.apk	Get hash	malicious	Browse	• 52.177.138.113
	inquiry10204168.xlsx	Get hash	malicious	Browse	• 23.101.8.193
	FileZilla_3.50.0_win64-setup.exe	Get hash	malicious	Browse	• 52.155.217.156
	GFT_457425442_1889647017.xls	Get hash	malicious	Browse	• 22.2.28.70
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies.com.html	Get hash	malicious	Browse	• 23.101.203.117
	XT032401329TS.vbs	Get hash	malicious	Browse	• 52.142.149.244
	lsass(1).exe	Get hash	malicious	Browse	• 40.79.78.1
	wzdu53.exe	Get hash	malicious	Browse	• 52.239.137.4
	wzdu53.exe	Get hash	malicious	Browse	• 52.239.137.4
	2AWamkLYry.exe	Get hash	malicious	Browse	• 13.68.173.197
	6Sux9KdbL8.exe	Get hash	malicious	Browse	• 40.124.50.181
	E72rgYhTgU.exe	Get hash	malicious	Browse	• 52.148.154.111
	epObj56UzE.xls	Get hash	malicious	Browse	• 13.94.141.24
	epObj56UzE.xls	Get hash	malicious	Browse	• 13.94.141.24
	VC6gnk46VQ.xls	Get hash	malicious	Browse	• 13.94.141.24
	epObj56UzE.xls	Get hash	malicious	Browse	• 13.94.141.24

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VC6gnk46VQ.xls	Get hash	malicious	Browse	• 13.94.141.24
	VC6gnk46VQ.xls	Get hash	malicious	Browse	• 13.94.141.24

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	March 4, 2021, 055038 PM.HTM	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	_evm5437345.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	March 4, 2021, 021638 PM.HTM	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Intruder.exe	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies .com.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	UPS Delivery Notification, Receiver susiej@johnsto ncompanies.com.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	wzdu53.exe	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	wzdu53.exe	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKe ep.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	selfassessment.doc	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	BL.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Xeros from condor.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	BL.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	_vm54959395930.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Malone3388_001.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	xerox for hycite.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116
	VM859-7757.htm	Get hash	malicious	Browse	• 52.52.65.159 • 34.192.142.116

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Reputation:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.116981173650867
Encrypted:	false
SSDEEP:	6:kKTzilkwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:LziywTJ6HkPlE99SNxAhUe0ht
MD5:	E79C78AECCD0A6F3ED36BC530BD66E08
SHA1:	1EC78D71D4A3FF1DB0E61DA123BD40D5C7DD96E1
SHA-256:	EE6E1AF5CE841E8FCF2D20D2B2825177CD2676EF1A0AA45CC2F53DC9520308B9
SHA-512:	B89CDEE8E19893109635CC7ED6F48480C924DE39D8F8AE423844328751A61319441D25EDE8CE2CBF42519DD335A857D1B72D7D4EC23FD67F36652FDA8A95CAB
Malicious:	false
Reputation:	low
Preview:	p..... .....6...(..... ....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\00ad58fa-9dbd-42bb-8e2e-f60a82cfa666.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	156705
Entropy (8bit):	6.051628322249181
Encrypted:	false
SSDEEP:	3072:x6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:pAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	6DC97D981CEFB00062AC8B63EC413571
SHA1:	C19676139620626A951FAC56E62A3B715F55F653
SHA-256:	67AC4018B4371D1BEBDE8FA9BE65CEAF1F27F8073C640E56F37D4C7A3BBA3A04
SHA-512:	EF77B7CF914A6E740FEB6ACF48EBF41EC062407C9F972E4CD0251119BAEA8084D3BF4EDC686A2DFEB3BA46A11BCDB6A0C40882CD03123A585B4DC925D0D23A31
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\00ad58fa-9dbd-42bb-8e2e-f60a82cfa666.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016318593"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ffc0a3c-1490-49e9-90e6-550f8a199135.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):	156507
Entropy (8bit):	6.051031528878209
Encrypted:	false
SSDEEP:	3072:K6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:kAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	530543D9C6B000F6B9B22795FE6251CB
SHA1:	627F11755397B2703E1E31A0A600710361360025
SHA-256:	09AF81DB210FCDE19EE59140027A9525275DB0EDEC2E10D8445D86E8C27C4404
SHA-512:	59D0C4A4A1B67284D5C2B6C300C2E31C719E8D70F7E6B367F1372427FDE367A9B9E01CC0D08C4CCC77159AB6211C50D32701E8537B36D6A518D2C8DD258CF7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016318593"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\377b400c-7ea5-49d4-9b7a-d40ce25bcffe.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):	156601
Entropy (8bit):	6.051318081375612
Encrypted:	false
SSDEEP:	3072:C6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:sAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	524ED6182C4C8223BF6890810D2A37D1
SHA1:	83283CC08E7A86F1B3C4BF10A3576ACFA53E11AA
SHA-256:	7EB0B1EFC4611D153EB36AE44587C74D2E8521C688BDE1A7FF33730F09EA09F7
SHA-512:	DD7ACB6090A32D2DDEE85BFF9585B1485D754A3B967A8F96F76B575C03C5FE68C6F6EFB905E85B3599A22282024B1CB4538D60E0770741E0FBB3276C92C9AAA9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016318593"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e01fc06-660b-49b7-bdeb-7bab0827968a.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):	156507
Entropy (8bit):	6.051031528878209
Encrypted:	false
SSDEEP:	3072:K6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:kAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	530543D9C6B000F6B9B22795FE6251CB
SHA1:	627F11755397B2703E1E31A0A600710361360025
SHA-256:	09AF81DB210FCDE19EE59140027A9525275DB0EDEC2E10D8445D86E8C27C4404
SHA-512:	59D0C4A4A1B67284D5C2B6C300C2E31C719E8D70F7E6B367F1372427FDE367A9B9E01CC0D08C4CCC77159AB6211C50D32701E8537B36D6A518D2C8DD258CF7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e01fc06-660b-49b7-bdeb-7bab0827968a.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016318593"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f309005-1121-499d-b5c9-6341fed8896e.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):	164995
Entropy (8bit):	6.081437493486914
Encrypted:	false
SSDEEP:	3072:fxU6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:piAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	CB038560B062DFAD7F1F9B7860273370
SHA1:	A4BA23D5120E046399B5CECE4055C203730DC21D
SHA-256:	2F7DCDEDC11F7C1B71AB534D7FD93964C2AEDEA7B61318166489B543E62B3D56
SHA-512:	36A4BAFBFA7EA93F5FB799186A1D5FC8F2DAD8E234A0B7A85099694B543D22320F61AD9B14A74D8B0D9411E004D217E0F56EA6D522E4A650305FA350F5CF438
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\812116f8-a97e-473e-ba19-12d006bf92ff.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):	164995
Entropy (8bit):	6.0814374425343045
Encrypted:	false
SSDEEP:	3072:pxU6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:HiAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	B58216D3F70E6B6FF91FA9C360D75D4D
SHA1:	954164CCFC4FC2D56585EFADC6339C040EADA73F
SHA-256:	F825AA51FE1EFF8B6A3EC0E48BF209897FFC4AF123E62D2FD8275234C3890651
SHA-512:	B3EB1E2B56B7E4FCD85D7C7A2A12BEE121F46F0C30A634CDF09B18886F8ADF6911AC9C510FC536AAD16B5AD00CB39E92FF45B4DB7E6F5F816084A2206FAEA43D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016318593"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\8ad6a739-9c68-4493-b13a-f510cd7943fe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7369661814667814
Encrypted:	false
SSDEEP:	384:1/OlZnoGfQzLVU6poN5rCv9X3mpTyHjSGadrYLxxxmzfj+r8Rmc/oHZJx2Ov3JNa:tm2hNunG+EenJLjIvDi3KZfdFq
MD5:	74A8011414843B4D5598DDBC923CF849
SHA1:	C48C2AB0BCDE21CB868FA1479BF2C61F92326209
SHA-256:	B5F1AD9B288179002461BCE57D2254857AF9E24BC42F2DA76F9AF9181D8E04D8
SHA-512:	38D09AB189B6B987FD262155D05B466BE7083E9DB77B0BA0CC99C4DC8E875F120DBBAFEA3E6A6873B8C4F04E39ACBFA65B482FFFCED9A9CA9F7F6F8187211535
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\8ad6a739-9c68-4493-b13a-f510cd7943fe.tmp	
Preview:	.q.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.......g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...s38.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\9c927333-9f4a-4b9e-8dda-54e61b3922e5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7365802603094695
Encrypted:	false
SSDEEP:	384:l/OlZnoGfQzLVU6poN5rCv9X3mpTyHjSGadrYLxxxmzfj+r8RmcIaoHZJx2Ov3JT:9m2hNuns+EenJLjIvDi3KZfdF5
MD5:	3D502865DC03A1737F25CB6C4E5D110D
SHA1:	06A9761BAA6E18E54F159A6178A5237EFCE35E4B
SHA-256:	1C0D2B6C6D5361DE96E7E3696E6D26AD2478D3A1B70FE8AEAEE0CB6D38C89119
SHA-512:	BE2ED7E5BB9EDC6F64CD24ACB926655BC60F3817EF85549169DD4427239510ED74E4137F5D700186960B82CDC303EED3EAE2E1D8623FC3C424471D9F76F31A4 A
Malicious:	false
Reputation:	low
Preview:	.t.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...s38.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\...... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\275c338d-ba00-4753-a572-0adc8821400e.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):	5892
Entropy (8bit):	5.190197928422971
Encrypted:	false
SSDEEP:	96:ng9PRKG46aNcVGok0JC0M7yRWL8GkahJbOTQVuwn:ngeG46qcn40bYpkan
MD5:	A689E0E99C16A8699965ECDE4596A2AC
SHA1:	8662649D1EFD6A011C76DDBA77242582917ED261
SHA-256:	CE961B8D1691229D1D9AD311993D23BF177D404CEB1ED50538C2353B1F03A613
SHA-512:	E1F566B0A0DF89D0510AC0B191B5394CA2361ECCBFA32B5245BDF12002406ED0F69302F7E414225C90FB5D17035EC329491EDB7966B53434523C5420E4AA990F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259473996555258","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\372e50c5-ba47-47e8-9a8b-c80a5d221ffc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2713
Entropy (8bit):	4.879178137071292
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5shiRLshEDshkTshShHRtdshL5yvh3sh36Mbzsh53qIzshZMHTgM:JTnOCXGDHzDprnc+O6MiaI2GdhH
MD5:	2E870D80BAA2B02A8065DA32171412F1
SHA1:	54718A222C829D1140652C785C5720DDF4910511
SHA-256:	62716E6AA9DF463C050C5C68AAAB8C25FD3647EA8B50E45C169A74CAC8245F71
SHA-512:	96A1E595E311BC4AAFDE7040B51E5353AEC432825FB206C7971F1C8846E97AD8A03B007662012BE8E9709C35766980CCF8A02645A58D035EF74B698806834F6A
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13262065999219632","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13262065999235522","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3b65280d-4512-41ce-9319-72ada5c3e3f3.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):	22614
Entropy (8bit):	5.536006726500715
Encrypted:	false
SSDEEP:	384:p1Ht0LlTvX/1kXqKf/pUZNCgVLH2HfDcrU6HG5nTcKtiaXlI4u:CLlb/1kXqKf/pUZNCgVLH2HflrUKG5ns
MD5:	7705870D9348489C977880EE9E026437
SHA1:	FA2D63983ADACCD014FBEE4A9EB97BECCB14EF8B
SHA-256:	DB89B19683BB5BF85688EF537C426BACBF8FDB8B90B6545004FF8DE3D4C1C746
SHA-512:	751282D0F689EB3E61077FCEE35B07089D01BCE0E3BE9243E3FF6BE5902C45CA7C61B271CF7DD497209764A649FE075BC21F8949CC35A895B772280DDFAB05F
Malicious:	false
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":"13259473996358642","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\432b2f1f-5519-4732-b9e6-7a8d72085144.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ee82313-0eee-4155-bacf-38dfa3897257.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):	22612
Entropy (8bit):	5.535853352548068
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ee82313-0eee-4155-bacf-38dfa3897257.tmp	
SSDEEP:	384:p1HtdLlTvX/1kXqKf/pUZNCgVLH2HfDcrU6HGenT9tiaZlI40:7Llb/1kXqKf/pUZNCgVLH2HfIrUKGen0
MD5:	CE5059AFA582AFD9FE4E2DEBF0C77C17
SHA1:	E7B541387644865F3751FE5B72297E2D842CDBB2
SHA-256:	04548A8BA419754DABAF0BF346266FDBA20C3FC0A1933D52071E41E341D9436F
SHA-512:	74470691D239CA3B0648A07D76C0F7AF2C0DCF4AF98D81EF44B76E982BED6CEC3169017CAD1FBACE989286D43F216FACECDAFABE2230C4C7F2E9AA1D56850 93
Malicious:	false
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":"13259473996358642","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\62400abb-6762-45cc-a5a1-8d8b5407db77.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):	5866
Entropy (8bit):	5.1889020276797
Encrypted:	false
SSDEEP:	96:ng9PEKG46aNcVGok0JC0M7yRWL8GkahfbOTQVuwn:ngxG46qcn40bYpkaB
MD5:	A4F1999E426E83F55B57E24EB4AB1136
SHA1:	722F7B46376307F7673EF3D9A9669D3650C4F731
SHA-256:	3648788CF2CBDE0EAB040F93A854F1F0141B83598F7B5299A82BA80B50DF42DA
SHA-512:	BDA38D1A7F05F3325673CCEF7934CEE5A5AD7E876167D43762ABF7943214EC5636A46DC65DCEA4318A71E484A03E612F5FA61DD25A072CBF74657F4E05BB39E 5
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259473996555258","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b724efc-229b-484f-8071-6e3162acf7e5.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):	1039
Entropy (8bit):	5.564724392927681
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv5C7wUs/RUenHQ:YI6UUhVseKUewqPeUer2UefiwUspUenw
MD5:	972161A2E737F31AA18AC60D3CC8CF46
SHA1:	5DFD73BE175817C7ECB2077008BFB2E12AAD94A0
SHA-256:	76F1B68F17531A5EBB5F49911CF9F7B0EA9E43A05C242AE5D21EFC04D9DF9FED
SHA-512:	75138ECAFF7C54D22F772FF8A8E47697ED17A4170568C02E45A419385FA681C03DC44553936936A4D7C2609111B702E627365371245FBEB61CFC1EF198716C0B
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1646536399.219749,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1615000399.219751},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

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):	331
Entropy (8bit):	5.246875252473121
Encrypted:	false
SSDEEP:	6:mnmD+q2PWXp+N23iKKdK9RXXTZIFUtpwA0WZmwPwv9VkwOWXp+N23iKKdK9RXX5d:v+va5Kk7XT2FUtpJ0W/PyV5f5Kk7XVJ
MD5:	D94B66E22A7B094CAE4E27C12970BBED
SHA1:	09FD7D117052EBDC1EB900A08C4127310830F289
SHA-256:	51C4C18A3FB25CAD5349460B758499E3212142D5CE1B33E1EE7B5611A9F6FF72

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
SHA-512:	B22639C351EB54F07738740B54114A6379B307D62A770E5D871FC35240D7F019B06C3A780E2149FF8E05A19DC2847EBDD2D77EB2F6E52397036769462F50D311
Malicious:	false
Preview:	2021/03/05-19:13:18.861 2ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/03/05-19:13:18.863 2ec Recovering log #3.2021/03/05-19:13:18.864 2ec 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):	315
Entropy (8bit):	5.19941938799038
Encrypted:	false
SSDEEP:	6:mnXFD+q2PWXp+N23iKKdKyDZIFUtpwHWZmwPwVFDVkwOWXp+N23iKKdKyJLJ:oD+va5Kk02FUtpCW/Pq1V5f5KkWJ
MD5:	57FF8245336C60E2A9B72053D1DAB231
SHA1:	735C420F5BD7C2477FEAA677D84B0621164D86CD
SHA-256:	C21D558F22D0267AD33A2056B55CCB3B65D633FB11449E308717DFBBEB9B1008
SHA-512:	8B726AC6F4C1DE4F2B2FFA5F2E315809EB30F045B6C103C0AA3983CEC91474481F96E2F3A5AAEC1860B3AA6C3E233DC49CE88A725EC116F754602A5C3D306D6
Malicious:	false
Preview:	2021/03/05-19:13:18.851 2ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/03/05-19:13:18.852 2ec Recovering log #3.2021/03/05-19:13:18.853 2ec 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\Cookies	
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):	12288
Entropy (8bit):	1.309994157111725
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U1BibMxr3QyuzJNOZ05mZ:dNwMMReXOJ
MD5:	AECE2BDECF245CC7227760357CE70C4A
SHA1:	5DC6376AC4D1F1880904B4E6D63339ADC77880E9
SHA-256:	F8DB8A3F145DDBD3F9FD42326BC766A93546D065460D4BB6DEFAECB8CDF4DF36
SHA-512:	B40D5D23B8AA90BB8778987566F141A5516C7A1EA3E5107288B3056FA1793F586FBFE874E63E520AD96CE89DA403475958E98E7227A2223272E518CFE8E4C78D
Malicious:	false
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):	0.9672245872240701
Encrypted:	false
SSDEEP:	24:dcLgAZOZD/gNiqLbJLbXaFpEO5bNmISHn06UwTt8:d8NOZeiq5LLOpEO5J/Kn7UMt8
MD5:	509630A1DA408F7F1A52534108752B64
SHA1:	BBD79487CFAD23BC42256E88DF4DA067B1741BE7
SHA-256:	BA017B43705DBC202D7F1C9EBA64C35B4F50FAAB787C63B19079853E68D503BF
SHA-512:	285A51F984CC478AEA491CD4A2DE9B3ADBADE4AC9D26A240E1DAC318080249E208038E181BD8CC9CA0A640AF4ED18DA0C140D394376F3A18B2586A1C816CB71
Malicious:	false
Preview:	.....(.v..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Size (bytes):	3934
Entropy (8bit):	3.857219682635605
Encrypted:	false
SSDEEP:	48:34/2KE7xU/g7sw5MUvE/lJtQ37/9QlTWfycM1tQ31Z/9QlTWfy18/98alMBRr:34gO6sGvEm3b6tcMc3n6tkWsMX
MD5:	397C422EC3B6E59970D8D57D1CFEBF76
SHA1:	A3220DCF89B929C2D05CEF8DC36AB504B88B892C
SHA-256:	BEFD8124CE635B5ED14915AA6EE60800D55DC234370C776403B8C766E3EDE17A
SHA-512:	77713133C9D9D8955EEED5BC196E3CBA55C5873781223F7290181381896F05C5DDC76089BD99720527FD8653C6EEEC8217CE02097DB6400C26D6DEE00360AC8
Malicious:	false
Preview:	SNSS.....I.....1.,.....$...3b26f315_715c_4663_b58b_27c1a79e6ad6.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....I...file:///C:/Users/user/Desktop/%25F0%259F%2593%25A9-Tina_Cfisd_HP29VF.htm.....h.....`.....h.....h.....@.....X.....I...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.%.2.5.F.0.%.2.5.9.F.%.2.5.9.3.%.2.5.A.9.-.T.i.n.a._.C.f.i.s.d._.H.P.2.9.V.F...h.t.m.....8.....0.....8.....I...file:///C:/Users/user/Desktop/%25F0%259F%2593%25A9-Tina_Cfisd_HP29V

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
Malicious:	false
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
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):	5.239153895145504
Encrypted:	false
SSDEEP:	6:mnuJ5Iq2PWXp+N23iKKdK8aPrqIFUtpwuCDZmwPwuXFzkwOWXp+N23iKKdK8amLJ:JJKva5KkL3FUtpZE/PZXF5f5KkQJ
MD5:	5634139A8936048760338FE48EF69163
SHA1:	333AEDFE22BD8CB81FFD4C6B15C0B9BFC32AFB72
SHA-256:	ECA059C9F4742EB1186F381E423496FF2B78AF4732A42E2A4ABD3208C9E9A0A1
SHA-512:	97328F94B86FF8E594207EBF1E1814032989A4656D9E4A92EB28B6FA13CD5F2F01060D660F1F5C9AB02619FDE8CCD9F83395E378EFDC2931172D81D8E7BD71FA
Malicious:	false
Preview:	2021/03/05-19:13:16.561 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/03/05-19:13:16.562 1994 Recovering log #3.2021/03/05-19:13:16.563 1994 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
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
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.....

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):	5.208854475125429
Encrypted:	false
SSDEEP:	6:mnM3Iq2PWXp+N23iKKdK8NIFUtpwUMGXZmwPwUAkwOWXp+N23iKKdK8+eLJ:L3Iva5KkpFUtpVD/PVA5f5KkqJ
MD5:	C87EFD38D8720E2BD4DE6E2DDFEE68E5
SHA1:	BD16BD157F8F5BF3DF467E28F36B925BBDBF3597
SHA-256:	60192F0D34A27F11D0F01671AEA312CF6E801FAD6B044A1C7ED06C68494FD229
SHA-512:	8C312ABD8205AC6ED58200901D1831BF76438C8E695D67265A68590584E4E5B9FD7C3192186F2FCB89FDDCB34671A7F70E659BEB6F0391C48F75597C3FEAE0E
Malicious:	false
Preview:	2021/03/05-19:13:18.719 19f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/03/05-1 9:13:18.720 19f0 Recovering log #3.2021/03/05-19:13:18.721 19f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/0000 03.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\comput ed_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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\c omputed_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:7dOscSRKc1nGRSklhEw6M1tf7SNyb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+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=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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
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):	369
Entropy (8bit):	5.288402028607754
Encrypted:	false
SSDEEP:	6:mneZi+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpweF2WZmwPweT9VkwOWXp+N23iKG:Bi+va5KkTXfchI3FUtpAW/PRV5f5KkTM
MD5:	F1F083ECA3A41295227F157241193257
SHA1:	615E2E3F2D8B03B48AB659301F7372DD504F3179
SHA-256:	7E786BBBAE1D41C6A7752D871730D5A92089DA8EA57D4D0AFD5D44F2DAF1DB48
SHA-512:	2DEC0D304A964360E71E2378928631E614552475AC1E6F1F3C856027086C1F83CED941957CF61983C19FB43FFEF88C874865D3D9CECBBE964BE9A67A1B7D6067
Malicious:	false
Preview:	2021/03/05-19:13:18.783 2ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/03/05-19:13:18.784 2ec Recovering log #3.2021/03/05-19:13:18.786 2ec 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
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.234778792050438
Encrypted:	false
SSDEEP:	6:mnR9+q2PWXp+N23iKKdK25+XuoIFUtpw0tAXWZmwPw0tAiVkwOWXp+N23iKKdK28:0+va5KkTXYFUtpHyXW/PHyiV5f5KkTXp
MD5:	AF49D9C1BC4854E2266E59F6338E2B28
SHA1:	691A77D5657E0E395D50DCD9E3FE81C569FE3CBF
SHA-256:	A3680A445EE2ABFA3665025AA0CF9238476811A90C289CCB199CC4F3C2194844
SHA-512:	5439607DCFF940C1AD934A7403A67BB4E8BF94787328511EC551C3DB46E4028F19916E486FB086366986D4BA67ED5F306825AAD6511C3799D9CA0A5711BF5AD1
Malicious:	false
Preview:	2021/03/05-19:13:18.776 2ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/03/05-19:13:18.777 2ec Recovering log #3.2021/03/05-19:13:18.777 2ec 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):	327
Entropy (8bit):	5.291350528305955
Encrypted:	false
SSDEEP:	6:mnSj59+q2PWXp+N23iKKdKWT5g1IdqIFUtpwSDXWZmwPwSJJ39VkwOWXp+N23iKN:T+va5Kkg5gSRFUtpvW/PtJNV5f5Kkg5i
MD5:	1CED11D5D48E15BE0BBDA8FC0DFA7835
SHA1:	5B1BC0B5F962903CE8608F74803A697F7647A811
SHA-256:	376ED7BEDC16D35B54B0C698325226553AF031CFFF076B73CDDE7A9DB43FC21F
SHA-512:	3F17D78BCE97A3212AEE69B099C78A6A569F54194E036AB09CF86F9E963FEB64E4C272912C328ECE9DF9D07DFA6AA087C805D7B4DCAF12744E29E8879712F90
Malicious:	false
Preview:	2021/03/05-19:13:18.744 2ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/03/05-19:13:18.745 2ec Recovering log #3.2021/03/05-19:13:18.746 2ec 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflfkD/t:8l
MD5:	493D2538EFCAC7319030307CB7787516
SHA1:	1E0EEE3166D4788B6B790D3C685BF221CF514D16
SHA-256:	3D56519477C374066F99D35DD2A5AF6336B8FA88D5ADC0564EC1EDDEA85F4684
SHA-512:	97DB6968061541A20A8970521D9B0C3F58AAE96007C586E2FC8B5C6288FEB9DB44B5A2E3F1D3ED94AB91E202E47CF15706FF68E6E2FB780313077D488C76BF9E
Malicious:	false
Preview:	.'..(.....A.k./.....

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):	1.2642474183867827
Encrypted:	false
SSDEEP:	48:Tkr/Z3VVtQ3c3UMUPW31uRk9TW3x1RANW3ljaRAJW3ysM7v2XtQ3HMUPzuRk9TVf:She3cEMUuwhl1eCrrh3HMUUgz
MD5:	CC539A3AC1C0C30055C8E56BF989EAFA
SHA1:	4307732CBE22D6EE7A84C1280F7E2EA6F9490A73
SHA-256:	84E8EE7CF21FE86925F45F47125A8C9B204FA54A98D67CA27161F2E4DD01AAFE
SHA-512:	77B03F64C0CCAECC34FD5777A1CBC5FDFECD790F06E0E1387D9485A52A9C2DB568FA4101C400894DDDED5DA6F8AD2D0F9FB01D11641445C3F2407CAFD7557EE
Malicious:	false
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):	717
Entropy (8bit):	5.308532402408565
Encrypted:	false
SSDEEP:	12:KkE9f3Tj52q5GVG3Osc1vgEeU24GXP13y0q6noFBk778B/xgskZBa9sNiyDRkn1R:KkE1Tj5TsM3d+vP1t413y0q6oDY78BJN
MD5:	7AB18F53672E3EEED9D96D949B4E14E1
SHA1:	275A5C5BDD641520A269F3580F51292A556F4600
SHA-256:	4887947982C141B92B1742AD67475B2841477C8B6D28154BC6C2247647C94AB5
SHA-512:	D23501578D1B867592164C72B4FEA5AD05C37D56163E672BE855C56D8908BCDF8F06CEB4C7370CC2E29C74959D8FD061AA1EECF960E5398D66CC09FE012657
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Preview:	.....''L.....93..9f..a9..c..cfisd..desktop..f0..file..user..hp29vf..htm..tina..users*.....93.....9f.....a9.....c.....cfisd.....desktop.....f0.....file.....user.....hp29vf.....htm.....tina.....users..2.....0.....2.....3.....9.....a.....c.....d.....e.....f.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....z...:w.....Bq...m..... .....*Ifile:///C:/Users/user/Desktop/%25F0%259F%2593%25A9-Tina_Cfisd_HP29VF.htm2.:.....J..... #&),17>

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):	42076
Entropy (8bit):	0.116393421789357
Encrypted:	false
SSDEEP:	6:qOqfOhpOvaOvoOuAOtoOj4yOng9bNFlWCj/laKl3l94/fMt76Y4QZVRtRex99pGX:U2LJgRqLBj/h3l94nMWQA9LOBQZ8fOY
MD5:	CBCA7CCFCFF416EFAFD84E1EE3DEFCCC
SHA1:	FA2D55B28BB2ED570C1D54B5EFBC000CFA357436
SHA-256:	C5C0C06C8C5F94CC527FB5B7B0E5006BE91AB74FED52154AF123BEAF9E4BC90D
SHA-512:	8BF16A8BFE717791F7AF5DD19471BCA61AACD605A8E605D87C742D42E6219DB8AF19ACC66F99DF1902AF039F545CD0EA6570D75F25581C1DFB16C0A7A28590 8
Malicious:	false
Preview:	....

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):	5.468607211231562
Encrypted:	false
SSDEEP:	48:jTZ/G0ha7JMs8dbju+rgbQSefgGkCNrS0U9RdiN9G:jTVa7JM/dbju+rgbQ5fgGDrS0Y
MD5:	7CFD38FC1367CAC2C503F99B0C18FE97
SHA1:	2C80C74300F435423FC19C0D425043B3F6603252
SHA-256:	BECE89356A9B6FA631A7413D8053DFFBECBBDBB95AD30E94C6031900B028857A
SHA-512:	9122EFE39B9207B3AA117AD2B9F6B70C38C0F099308E33606A41EDE6D8A3A1292216EDD38D7FFE9E0686D16785678B8DC33A00E05F858FB86BE3968A0C07B792
Malicious:	false
Preview:	#..j...*.....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..535113000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-03-05 19:13:22.11][INFO][mr.Init] MR instance ID: 747c19bf-e6c7-4654-b5bc-7454302f90b1\n","[2021-03-05 19:13:22.12][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-03-05 19:13:22.12][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-03-05 19:13:22.12][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-03-05 19:13:22.12][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-03-05 19:13:22.12][INFO][mr.CastProvider] Query enabled: true\n","[2021-03-05 19:13:22.12][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):	5.175360633869416
Encrypted:	false
SSDEEP:	6:mnogKq2PWXp+N23iKKdK8a2jMGIFUtpwoKFZZmwPwo/kwOWXp+N23iKKdK8a2jM4:YKva5Kk8EFUtpC/Pn5f5Kk8bJ
MD5:	5552DABAA7DB6F21E7466171A6105263
SHA1:	6D2E468CE082C883BA455D893DCF2053AA6B472D
SHA-256:	854D1FA5FD81997451F9C7AA11860DA07881238C854B86D33205F65C488C1F19
SHA-512:	2C7A741F49341795B3D9D88282CBCF41C3930AAA2163CE8D75C94C7EE2C047879DA7AA28F6855E2266B4F08453E44E5FC2F9ABDE56C787D098D6CC42CA9720
Malicious:	false
Preview:	2021/03/05-19:13:16.396 19d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:13:16.398 19d0 Recovering log #3.2021/03/05-19:13:16.399 19d0 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\Platform Notifications\LOG	
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\Platform Notifications\LOG	
Size (bytes):	334
Entropy (8bit):	5.225445198490205
Encrypted:	false
SSDEEP:	6:mnujq2PWXp+N23iKKdKgXz4rRIFUtpwudDhZmwPwuU7kwOWXp+N23iKKdKgXz4qG:Jjva5KkgXiuFUtpZD/PZA5f5KkgX2J
MD5:	6F23B22DAA6E95AFC32AC96440E20646
SHA1:	D17A262EF776435FB46ED34BF269B5B5495A4736
SHA-256:	DC61478E77E544E574F32C2FB0640BD37E7849E8A880E0261FEDBE68A8066C7E
SHA-512:	5BD3AFDE3597D8A17C9AF7F156BCCFC5C065B47CD4A8C245289FFDAE0796C81586F189A9AE715BC6C32EEAC75522692CD8CAE6B8D06D2E5AB18715D45CC69A72
Malicious:	false
Preview:	2021/03/05-19:13:16.581 19f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/03/05-19:13:16.582 19f0 Recovering log #3.2021/03/05-19:13:16.583 19f0 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\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:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
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
Entropy (8bit):	5.213663237045455
Encrypted:	false
SSDEEP:	6:mnuYIq2PWXp+N23iKKdKrQMxIFUtpwuuXZmwPwuuFkwOWXp+N23iKKdKrQMFLJ:J5va5KkCFUtpZ+/PZy5f5KktJ
MD5:	43476344A159CD43D180E2F6FEB559C1
SHA1:	CFE61E4BDA69A6C6B4706134F04229C65AE6CAD5
SHA-256:	37DA4A5918C91BCC17E77CE9BE39DB1D1583516B34DC2999F0362E4951674EB3
SHA-512:	73B48ADAEFC2D04ED21BC8573D360FAD598C9AD4AE6BDDFCF0201A710A413BB3ECF4697345AFACB2DDAD7BEE3BCE4C2B1E09A7322F971BFD5ECBC5AF5AC1FD71
Malicious:	false
Preview:	2021/03/05-19:13:16.512 1984 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/03/05-19:13:16.514 1984 Recovering log #3.2021/03/05-19:13:16.514 1984 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/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):	5.200301916996006
Encrypted:	false
SSDEEP:	6:mnoQq2PWXp+N23iKKdK7Uh2ghZIFUtpwolZZmwPwolzkwOWXp+N23iKKdK7Uh2gd:ova5KkIhHh2FUtp9Z/P9z5f5KkIhHLJ
MD5:	9B998670DE5F8D5DB0251BC07FA51E28
SHA1:	3C32B8112966C76C75AA57CF9D4B8E60CA90F15B
SHA-256:	186EE20F2730B248AE702567B22CD52FD35597D85D13F1FC981B08A197C98C0B
SHA-512:	A747484E643704F63E61347E7E659F7739C3B5CC991524337800F1F765067E53F377E3156C295F50B2AAFB3ED4ED253B40B7452D74D400B67BA1713CA645C67F
Malicious:	false
Preview:	2021/03/05-19:13:16.333 1984 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/03/05-19:13:16.335 1984 Recovering log #3.2021/03/05-19:13:16.335 1984 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\004b85ab-df46-44d4-b943-340acdc4ef9b.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","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
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):	5.3148383372255985
Encrypted:	false
SSDEEP:	6:mnuqjlq2PWXp+N23iKKdKusNpV/2jMGIFUtpwubcZmwPwubckwOWXp+N23iKKdKK:JqjIva5KkFFUtpZA/PZo5f5KkOJ
MD5:	32F0DD860D10081277A09C4B819FCB17
SHA1:	A5E2F55A0E7AC53932091FF4F6BA75B2CE4B4843
SHA-256:	AE020BAA8167FB3D796A4956D8FF5E7E34FF8A0D7268C185247C56893FB9E9DE
SHA-512:	3C8100ADAB7A89690339991246CEAAA75643F9C7AA1C568CB1B63842ED544ED26C63D62D26C83056AA6283AC72D019F267335379500CF7F56F0387875CA68B7A
Malicious:	false
Preview:	2021/03/05-19:13:16.547 1984 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:13:16.549 1984 Recovering log #3.2021/03/05-19:13:16.549 1984 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.333732456577356
Encrypted:	false
SSDEEP:	6:mnuvQMq2PWXp+N23iKKdKusNpqz4rRIFUtpwufZZmwPwu8kwOWXp+N23iKKdKusX:Jtva5KkmiuFUtpZR/PZ85f5Kkm2J
MD5:	1033A5B436D299D00492B264C33196AF
SHA1:	66F71B0DBB450D01BCB6559153F1FAB0280ABAB4
SHA-256:	B50D0B8474D80369F526B035C5E46BB1A58D8BBDA6A24700A95A49BEC38FE386
SHA-512:	C9B7C58A68E3B6B1C5B3F5509833DBF01CB703B1FC43E29E143E0D487F91A63DB8C3B50DE937132049C742BE096E21AAE2BDE5933978BB4005F5B0FCF4EC5BCB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Preview:	2021/03/05-19:13:16.579 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/03/05-19:13:16.583 1994 Recovering log #3.2021/03/05-19:13:16.584 1994 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
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):	5.311112500525346
Encrypted:	false
SSDEEP:	6:mnHbq2PWXp+N23iKKdKusNpZQMxIFUtpwHi5ZZmwPwHi5zkwOWXp+N23iKKdKusx:abva5KkMFUtpq4Z/Pq4z5f5KkTJ
MD5:	125463F2A25FC75D1E42A0D9D7F104C0
SHA1:	B709FA9FF48163F0D34035D50657F563C22A705A
SHA-256:	C931FEB585C7394BB8521E5E1CDE30886678969D33896B3CD3AF47636DB8890C
SHA-512:	31C57F53406597D2E6F91A14DB4E6D279D9246640A6504A9606AA62F3F143D23C4C43C6BE7C3AF6A827081EC5293CF78B36D9AF848447B25E6C0E4F3DAE79FF
Malicious:	false
Preview:	2021/03/05-19:13:32.866 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/03/05-19:13:32.868 1994 Recovering log #3.2021/03/05-19:13:32.868 1994 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\750e1841-fc76-49f9-a83d-9675ea47ac15.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
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):	5.2441726688371855
Encrypted:	false
SSDEEP:	12:8va5KkkGHArBFUtpnX/P+5f5KkkGHAryJ:Ga5KkkGgPgqf5KkkGga
MD5:	F24E4F09F2C7D21F10A49D58A5D852A0
SHA1:	212A22F05573CE79648264651D2B2F768587AD74
SHA-256:	84018EDD48659CE2A18FF83BA53354DFD155333337C852C19CD2D797185A06D0
SHA-512:	EE742CFE3881846492968C999E919CB45D02122D29A0E8D683DDBB3EB7E7EF099CBD4273FC7FDAD186B44747D0781EB2C1D02C9B1DDBEF9973D9E9EE0639C B3
Malicious:	false
Preview:	2021/03/05-19:13:20.662 1984 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:13:20.668 1984 Recovering log #3.2021/03/05-19:13:20.670 1984 Reusing old log C:\Users\user\A ppData\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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.236876952640159
Encrypted:	false
SSDEEP:	12:6HM+va5KkkGHArqiuFUtpy/P4MV5f5KkkGHArq2J:uda5KkkGgCgf2f5KkkGg7
MD5:	4E0F7980B0C4B5ECACA69D19036A3037
SHA1:	93931112757FA0C966B99BF287AB9ADFA0F2E04F
SHA-256:	7D61A016641C4DBA00C6A3DFF5294F968318521B80F9EF66F55AB06B73D97A82
SHA-512:	715826573A8DA6840A04C4CAD80F40183D3597ACA0FDFABD7F90E7B313C14DCD598490EAF1AC8E46191EB24C4E85394F4002AC8A3BAB500BB750E3FD62B4F7 F
Malicious:	false
Preview:	2021/03/05-19:13:20.676 198c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/03/05-19:13:20.680 198c Recovering log #3.2021/03/05-19:13:20.681 198c 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
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
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):	5.2242896997602095
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SSDEEP:	12:GAIva5KkkGHArAFUtpWGUD/PWX5f5KkkGHArfJ:G9a5KkkGgkgQeJf5KkkGgV
MD5:	4E8A642E7D50BD715FA41EB531EDC1B6
SHA1:	EBC8413835A0C98076E1D9E86CF9A5B2365D0199
SHA-256:	1E32E6F1813F4E4CF0F97CB218E6668164019C42ADF92C8F3007989AA1ADA29F
SHA-512:	D989D14497979343F3FAA6E319AF031B4CAE0925E434B45F817D3D5C3390FC61BF98427955D24E97D6CE4BA60D7FF1571A2F82473947390EC3DFB6A6BD65A5D(
Malicious:	false
Preview:	2021/03/05-19:13:36.068 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/03/05-19:13:36.069 1994 Recovering log #3.2021/03/05-19:13:36.070 1994 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
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
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):	5.275843077500945
Encrypted:	false
SSDEEP:	6:mnoAq2PWXp+N23iKKdKpIFUtpwoTZmwPwosPkwOWXp+N23iKKdKa/WLJ:Yva5KkmFUtpL/Pu5f5KkaUJ
MD5:	04425CF1F46F84A07742E7E9B4AEE622
SHA1:	84A212239CF82427FB558FD4E5C848D30379E815
SHA-256:	F2C54D114AA76F6B4331FBE10C554DFCBE89527CBB0B3C2EF60AECAC261DF8D1
SHA-512:	F4AAAB8D2F78B948EB5DA7A41EF0B5674505AA5ACEF4F53EAD8A09AA79E75D830E80DF5115E0CBE87170C760679BAC09BD709DA5632DC598E23541B6BF5E61 49
Malicious:	false
Preview:	2021/03/05-19:13:16.351 1984 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/03/05-19:13:16.353 1984 Recovering log #3.2021/03/05-19:13:16.354 1984 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):	5.328161609757539
Encrypted:	false
SSDEEP:	6:mnaq2PWXp+N23iKKdKks8Y5JKKhdIFUtpwcZZmwPwLkwOWXp+N23iKKdKks8Y5JF:rva5KkkOrsFUtpR/P45f5KkkOrzJ
MD5:	ADC36FEA4927EA41F83A4B47C244FA22
SHA1:	E249FB38E8892EC62942127A818F28C7ED984878
SHA-256:	D88DF2F3685220FEC40832578385762C5FD2AC74E81179EC301F4BDF52B0CB1F
SHA-512:	EAB94E0390D450C8471B85860480696AB290E5CE308784F3A84C78D7494429863E63853A6436C92A3D418E31C8198C70FD2DA153A1840FB8E4EBF9A35371485B
Malicious:	false
Preview:	2021/03/05-19:13:22.080 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/03/05-19:13:22.081 1994 Recovering log #3.2021/03/05-19:13:22.082 1994 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\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.960777084415068
Encrypted:	false
SSDEEP:	3:6m//lvDuKmawCs2Ah/n:R/l7uKzwKAZ
MD5:	E046D2367999C279913FE688523F84D3
SHA1:	518382B859FED5C37ACC36211F130AAE0725FE4F
SHA-256:	7A10269C72AE005A46CED1158723498CE577A4298F191105BFCE77552BA0528A
SHA-512:	62207BAF8CFF5FA60AB106DAC0FB7B7F26DFCFC79E478187106D0D23A2ED21C8FAB4DE4EE6A28BECA4010407A4429CE98BAC4F33EE0FC0F971361386AE404B 81
Malicious:	false
Preview:	....._.`...+.....{..w.......'E...b)..............k6}S.]w....Ex.Z...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ab7cacf6-4aa5-4c39-9156-14c31c6efd10.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):	5573
Entropy (8bit):	5.174962981617731
Encrypted:	false
SSDEEP:	96:ng9PEKG46aNcVGok0JC0M7yRWL8VbOTQVuwn:ngxG46qcn40bY6
MD5:	CF724E73865566729A77934878922880
SHA1:	A4879BB441C80809C7102FCF5FAF4C2CE125A494
SHA-256:	22C47180AD91DA788E2ED8E49C8CAD423D14BC211E6BA045DBE30AF64CB47B07
SHA-512:	7781433DF81E4B3CEA14C7ABAD04CC3E4FED645A975084E3905AA360D0A3C926596E69CF1D7A59846A5C604C1E0194325ED65643C992CAE67E1C536DC6958E4 E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259473996555258","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

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
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):	136
Entropy (8bit):	4.513842200668168
Encrypted:	false
SSDEEP:	3:tUK98fE2WZmwv37897V8s78Ih7WGv:mnfE2WZmwPwZVvwIVtv
MD5:	9F2AF596871B4C418E83AE641825B85B
SHA1:	25E8A6AB24C2F71B2DE54BD7923DE61BC2C68042
SHA-256:	A6235C3AC65F70195A94237E6662ECFC6FE9E13CBF58049B9B263D22FFC16134
SHA-512:	600106838977AA319F586B50FE6F4519F6E669D4149D5FD42385E8E4F348B0FD15209424B771F7580C4B55576B7F7C0F96DD44F22BF9318AE1B24F9CF6361D3E
Malicious:	false
Preview:	2021/03/05-19:13:18.614 2ec Recovering log #3.2021/03/05-19:13:18.655 2ec Delete type=0 #3.2021/03/05-19:13:18.656 2ec 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e82f27e5-ae8f-490d-892b-421fbfea43bc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\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):	5.219214849063019
Encrypted:	false
SSDEEP:	6:mnxYq2PWXp+N23iKKdKfrzAdIFUtpwSZmwPwzTXkwOWXp+N23iKKdKfrzILJ:yYva5Kk9FUtpP/P6X5f5Kk2J
MD5:	B8F6C817752E4CB4DAC6B7DD0141774C
SHA1:	BA40C28BA4BBA86617A3E84BA9CAA0CBDE9245A4
SHA-256:	39B2AF68FDFB949359B536D70BA24C6753AC242857E9ABF5541A563C6A5096CF
SHA-512:	A8A9C79998E4CBDC5EDD95A0E41BF017671357C582B92EE2E8234BC0CEBC47A450D0B68B1DD39177D452EEF050DAB74EA696CA4E76974D2F711479A503777A9
Malicious:	false
Preview:	2021/03/05-19:13:18.871 19f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/03/05-19:13:18.872 19f0 Recovering log #3.2021/03/05-19:13:18.873 19f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false

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
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Efl0s1:8S
MD5:	63A923748629371E65C9D396A9CBE7E3
SHA1:	28F25CDDB5E611085026904B80DA57E131E9C15A
SHA-256:	4C1817093A3250DA88A3ECD1F0F5F50F5F6C64581E38529E60BFC5006DBD02BD
SHA-512:	8B95050AC359EC3CF1A657FB952C710ABA7EAC91D9B1D9DFEA96E8E2217F2AC14489FB91ABC8B8B1C40FAB815FC2BF938227018F2F717B14316170766D6149E E
Malicious:	false
Preview:	.'..(.....=.k. /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.19.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6396_1373984923\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223592
Entropy (8bit):	4.9638585725691575
Encrypted:	false
SSDEEP:	3072:SRztNSIhnVr91m7Y+VFwPmqSqm2+Sc4Q2PRbKbG5uu5hrExzu6KyGbx+9Omzpj:ShNZDE7nxPC5cVr6xE
MD5:	FCCFC2303ACCE4945A4E5B17FEB074D6
SHA1:	314086BBE1D350CB8850C76D89C00EC6D4E7B0BE
SHA-256:	6139961F1E07AE33628E913D3551469AFB1AD57A29F0520B2281879A44CBC92F
SHA-512:	7F8E9D7919C5A4896113EBFDACC5B9728DC9F56138B163FD92E9CC82B393890B125FADE7586B3A4373B9930311035E5581B14705167070A28FDB5D42D69EA14E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir6396_1373984923\Ruleset Data	
Preview:	.....d.....5..... .....`...D.....|.....t...p.....h...d...`.....t...L...T...8...@...<...8...4.....,...(.....uocca.....&.....ozama.....3.. 0.....0iupb.....@_..H.....g.bat.....`.....onwod.....x.....ennab.....d.....nozam.....(v.....geips.....rekoj.....lgoog.....`.....uotpo..... lreko.....o.....x7.....x.....tf.....H...,.....P...L.....@...<...t...4...0...P...(...0... .....h.....H.....(..... .....l.....H.....(.....t.....l...h...d...`.....T...P...L...H...X...@...<...8...4...0...,...(...$... .....d.....@..... ....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\bd308b8c-7456-42bc-b8c7-f4e5596666f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.736352495920218
Encrypted:	false
SSDEEP:	384:7/OlZnoGrzMpoN5rCv9X3mpTyHjSGadrYLxxxmzfj+r8Rmc/oHZJx2Ov3JNU1Bo9:m2hNunG+EenJLjlvDi3KZfdFx
MD5:	BA933B42DA3BC8D7E168ADC5A7997621
SHA1:	A170B7B112856577A13DF7A13EEDBD36EAF2C61B
SHA-256:	7736F0E9FCC5C3B0122A620C00DF85B373083D35940053B82F83E15CE4EEF367
SHA-512:	93B631A825F45E7B1CBEBFEAF2D0699B578CE36A7254AEA9F5087EFBB77F01B7FABABC993E46A561A3E2859B5BA00C046FCFAD936C0DCAEE6DA9F920E3588DB7
Malicious:	false
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...s38.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\c265e242-f18b-4a23-9278-57b589bfa16a.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):	164995
Entropy (8bit):	6.081437493486914
Encrypted:	false
SSDEEP:	3072:fxU6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:piAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	CB038560B062DFAD7F1F9B7860273370
SHA1:	A4BA23D5120E046399B5CECE4055C203730DC21D
SHA-256:	2F7DCDEDC11F7C1B71AB534D7FD93964C2AEDEA7B61318166489B543E62B3D56
SHA-512:	36A4BAFBFA7EA93F5FB799186A1D5FC8F2DAD8E234A0B7A85099694B543D22320F61AD9B14A74D8B0D9411E004D217E0F56EA6D522E4A650305FA350F5CF438
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\cc6ed88d-4e6f-4685-8dcb-66c4f43266fb.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):	156601
Entropy (8bit):	6.051318081375612
Encrypted:	false
SSDEEP:	3072:C6we9QSr571ljD6v2CcDPvZaerIihFcbXafIB0u1GOJmA3iuRt:sAQwh1xFTJ4CaqfIlUOoSiuRt
MD5:	524ED6182C4C8223BF6890810D2A37D1
SHA1:	83283CC08E7A86F1B3C4BF10A3576ACFA53E11AA
SHA-256:	7EB0B1EFC4611D153EB36AE44587C74D2E8521C688BDE1A7FF33730F09EA09F7
SHA-512:	DD7ACB6090A32D2DDEE85BFF9585B1485D754A3B967A8F96F76B575C03C5FE68C6F6EFB905E85B3599A22282024B1CB4538D60E0770741E0FBB3276C92C9AAA9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\cc6ed88d-4e6f-4685-8dcb-66c4f43266fb.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.615000399263621e+12,"network":1.614968002e+12,"ticks":96297023.0,"uncertainty":4474638.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510163185 93"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\5138917a-43e1-4f45-a435-634e6faec0f8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\6396_1243133164\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6396_291140863\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9477608398895883
Encrypted:	false
SSDEEP:	3:SdUoLS6MTYUAZdXtbJXBVGHIVWfE:S/7MTYUATPv8c
MD5:	AFFD907C7BB49B4A7449E67EE49D99C7
SHA1:	3DAEC57822D8C39E0BDE14BCD19B906CED0F55ED
SHA-256:	D5CDD87B76D7E6C3DC16374D41B8350519BE46B978EAC80AB70E6386F6E702FB
SHA-512:	488D45EA5C58C2F27360E86CC50F487AE81F6E5C8D58D82C0155346297AAA542018BBCCAD138972D173E3E822F06D62A95EFDE2426D8823AC1C987214D67D01
Malicious:	false
Preview:	1.869f6197c3fdd474910319ff37ee13b73f8fb8ceeaaa62517e2d056b6a03ff54

C:\Users\user\AppData\Local\Temp\701b3d3c-ac60-49c1-ac8c-fc4cc3e28ae3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false

C:\Users\user\AppData\Local\Temp\701b3d3c-ac60-49c1-ac8c-fc4cc3e28ae3.tmp	
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\8e406ee2-b81a-441a-ad84-e5fd93f2e5ec.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\dd07e072-61ae-4833-8361-b4e47274e595.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\5138917a-43e1-4f45-a435-634e6faec0f8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": ".... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874943 76": {.. "message": "... ...".. },.. "18027627465894571 77": {.. "message": "...".. },.. "18503975003120203 88": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .. ..".. },.. "14284488690781267 31": {.. "message": "..... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".... .. ..".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\bn\messages.json	
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\da\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768460319075": {.. "message": "..... ......".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\fi\messages.json	
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050321
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C000
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "1636686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\gu\messages.json	
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6396_716159316\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

Static File Info

General

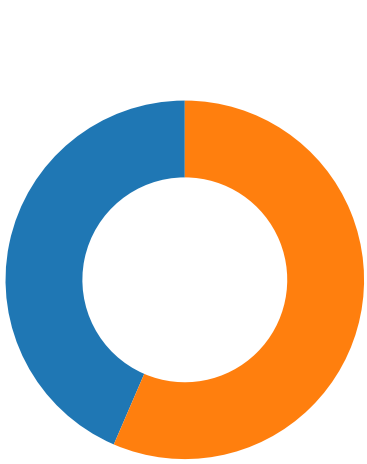
File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	2.756293097868353
TrID:	
File name:	%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm
File size:	328595
MD5:	55e8459fd775c236c493f21f36a6ba45
SHA1:	e7a99dbb4450838203dba66b03ec60c78dac50f7
SHA256:	bd841306b786d46ef57695e1f458a58140684626d444baf3c783ae439fa11ead
SHA512:	446289d40185b8b44cc35060fbdb91076f2eec79ae59e4cb6855703a0f170a50512ade51135b44e93c64231732990b7df10fce2463c8001de3114b49431473a0
SSDEEP:	768:NwdZZZZZZZZZlZZZZMZZZZZZZGZZZZZZXZZZZZTZZZZZZZZM:z
File Content Preview:	<script language="javascript">document.write(unescape('%3c%73%63%72%69%70%74%20%74%79%70%65%3d%22%74%65%78%74%2f%6a%61%76%61%73%63%72%69%70%74%22%3e%77%69%6e%64%6f%77%2e%6c%6f%63%61%74%69%6f%6e%2e%68%72%65%66%20%3d%22%68%74%74%70%73%3a%2f%5c%63%6f%6e%76%6

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:13:20.050326109 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.051218033 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.204104900 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.247812033 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.247919083 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.248171091 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.251118898 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.251297951 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.251451969 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.402506113 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.402622938 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.402827978 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.444677114 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.448682070 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.448709965 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.448725939 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.448802948 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.451967955 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.454479933 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.454500914 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.454519987 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.454586983 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.459465981 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.460299015 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.460488081 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.601149082 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.608053923 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.608102083 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.608156919 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.608242989 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.609138966 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.658245087 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.658431053 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.662445068 CET	443	49702	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.680155993 CET	443	49704	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.680232048 CET	49704	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.738610983 CET	49702	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:20.752188921 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.790577888 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.790697098 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.790869951 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.809287071 CET	443	49705	52.52.65.159	192.168.2.3
Mar 5, 2021 19:13:20.829281092 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.830892086 CET	443	49709	13.224.193.100	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:13:20.830931902 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.830979109 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.830998898 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.831021070 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.831091881 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.833899975 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.862629890 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.862848043 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:20.901073933 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.901335001 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:20.938559055 CET	49705	443	192.168.2.3	52.52.65.159
Mar 5, 2021 19:13:21.197525024 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.222240925 CET	443	49709	13.224.193.100	192.168.2.3
Mar 5, 2021 19:13:21.238615036 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.238725901 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.238944054 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.279815912 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.293800116 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.293878078 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.293920994 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.293957949 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.293973923 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.294053078 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.317542076 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.317930937 CET	49712	443	192.168.2.3	34.192.142.116
Mar 5, 2021 19:13:21.318036079 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.318175077 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.333698988 CET	49709	443	192.168.2.3	13.224.193.100
Mar 5, 2021 19:13:21.358902931 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.358958006 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.359143019 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.359412909 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.361093044 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.361138105 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.361177921 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.361212969 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.361241102 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.361267090 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.361277103 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.363970995 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.364015102 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.364255905 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.366832972 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.366875887 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.367100954 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.367130995 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.369698048 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.369749069 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.369868994 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.372570992 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.372613907 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.372710943 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.372760057 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.372766972 CET	49711	443	192.168.2.3	172.217.23.65
Mar 5, 2021 19:13:21.400221109 CET	443	49711	172.217.23.65	192.168.2.3
Mar 5, 2021 19:13:21.400289059 CET	443	49711	172.217.23.65	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:13:12.599786997 CET	60985	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:12.662192106 CET	53	60985	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:19.524736881 CET	49199	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:19.570976973 CET	53	49199	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:13:19.943344116 CET	50620	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:19.951874971 CET	64938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:19.957520962 CET	60152	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:19.960988998 CET	57544	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:20.008238077 CET	53	50620	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.014240026 CET	53	64938	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.025167942 CET	53	60152	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.025475025 CET	53	57544	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.463124990 CET	55984	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:20.526802063 CET	53	55984	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.607342958 CET	64185	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:20.672125101 CET	53	64185	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:20.691198111 CET	65110	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:20.750678062 CET	53	65110	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:21.125036001 CET	63492	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:21.192137957 CET	53	63492	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:21.237257004 CET	60831	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:21.294528961 CET	53	60831	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:21.339507103 CET	60100	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:21.386145115 CET	53	60100	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:21.763987064 CET	53195	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:21.804445028 CET	50141	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:21.819698095 CET	53	53195	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:21.869693995 CET	53	50141	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:22.418437004 CET	53023	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:22.505538940 CET	53	53023	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:22.870651007 CET	49563	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:22.925499916 CET	53	49563	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:24.946330070 CET	58823	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:24.993437052 CET	53	58823	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:25.508160114 CET	57568	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:25.508470058 CET	50540	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:25.564165115 CET	53	57568	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:25.584894896 CET	53	50540	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:26.101116896 CET	54366	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:26.161035061 CET	53	54366	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:26.255023003 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:26.309900045 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:28.204590082 CET	50713	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:28.265979052 CET	53	50713	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:34.277122974 CET	58987	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:34.341429949 CET	53	58987	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:36.888046026 CET	56579	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:36.934123039 CET	53	56579	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:37.898989916 CET	60633	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:37.945148945 CET	53	60633	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:39.033338070 CET	61292	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:39.081312895 CET	53	61292	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:40.177530050 CET	63619	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:40.223366022 CET	53	63619	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:41.284542084 CET	64938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:41.330492020 CET	53	64938	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:42.485922098 CET	61946	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:42.536499023 CET	53	61946	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:43.613200903 CET	64910	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:43.662237883 CET	53	64910	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:44.643400908 CET	52123	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:44.701627970 CET	53	52123	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:45.592459917 CET	56130	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:45.638818979 CET	53	56130	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:46.643893003 CET	56338	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:46.690130949 CET	53	56338	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:46.774548054 CET	59420	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:46.825663090 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:13:47.800748110 CET	58784	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:47.867449999 CET	53	58784	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:48.307235003 CET	63978	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:48.355911016 CET	53	63978	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:50.991533995 CET	62938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:51.037548065 CET	53	62938	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:53.098820925 CET	55708	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:53.146023035 CET	53	55708	8.8.8.8	192.168.2.3
Mar 5, 2021 19:13:54.345457077 CET	56803	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:13:54.395909071 CET	53	56803	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:05.262149096 CET	57145	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:05.309350014 CET	53	57145	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:17.808473110 CET	55359	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:17.873482943 CET	53	55359	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:18.386493921 CET	64124	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:18.448467970 CET	53	64124	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:18.591772079 CET	49361	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:18.649178028 CET	53	49361	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:18.794866085 CET	63150	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:18.854758024 CET	53	63150	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:18.860059977 CET	53279	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:18.914292097 CET	53	53279	8.8.8.8	192.168.2.3
Mar 5, 2021 19:14:46.986268997 CET	56881	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:14:47.035491943 CET	53	56881	8.8.8.8	192.168.2.3
Mar 5, 2021 19:15:00.753496885 CET	53642	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:15:00.810172081 CET	53	53642	8.8.8.8	192.168.2.3
Mar 5, 2021 19:15:19.555224895 CET	55667	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:15:19.620781898 CET	53	55667	8.8.8.8	192.168.2.3
Mar 5, 2021 19:15:31.917598963 CET	54833	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:15:31.985110044 CET	53	54833	8.8.8.8	192.168.2.3
Mar 5, 2021 19:15:32.125103951 CET	62476	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:15:32.188484907 CET	53	62476	8.8.8.8	192.168.2.3
Mar 5, 2021 19:15:35.959738970 CET	49705	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:15:36.014353991 CET	53	49705	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:03.739640951 CET	61477	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:03.825334072 CET	53	61477	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:04.256525040 CET	61633	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:04.323256969 CET	53	61633	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:04.734966040 CET	55949	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:04.794807911 CET	53	55949	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:05.235258102 CET	57601	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:05.303911924 CET	53	57601	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:05.737080097 CET	49342	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:05.793139935 CET	53	49342	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:06.224581003 CET	56253	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:06.282572031 CET	53	56253	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:06.860610962 CET	49667	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:06.915761948 CET	53	49667	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:07.562882900 CET	55439	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:07.620811939 CET	53	55439	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:08.388473988 CET	57069	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:08.446378946 CET	53	57069	8.8.8.8	192.168.2.3
Mar 5, 2021 19:16:08.837384939 CET	57659	53	192.168.2.3	8.8.8.8
Mar 5, 2021 19:16:08.917018890 CET	53	57659	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 19:13:19.957520962 CET	192.168.2.3	8.8.8.8	0x890a	Standard query (0)	convoy.app	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.691198111 CET	192.168.2.3	8.8.8.8	0x5497	Standard query (0)	cnvy.app.link	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.125036001 CET	192.168.2.3	8.8.8.8	0x1e89	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 19:13:21.237257004 CET	192.168.2.3	8.8.8.8	0x7153	Standard query (0)	t.dripemail2.com	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:22.418437004 CET	192.168.2.3	8.8.8.8	0x84fd	Standard query (0)	sharepoint uploadsfus 5.z13.web. core.windows.net	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:25.508160114 CET	192.168.2.3	8.8.8.8	0x7eb1	Standard query (0)	oomslalase rvice.com	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:28.204590082 CET	192.168.2.3	8.8.8.8	0x4db9	Standard query (0)	aadcdn.msa uthimages.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		52.52.65.159	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		52.53.99.37	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		50.18.137.36	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		52.8.107.16	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		13.57.151.101	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		50.18.199.4	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		52.53.67.13	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.025167942 CET	8.8.8.8	192.168.2.3	0x890a	No error (0)	convoy.app		52.52.224.167	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.750678062 CET	8.8.8.8	192.168.2.3	0x5497	No error (0)	cnvy.app.link		13.224.193.100	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.750678062 CET	8.8.8.8	192.168.2.3	0x5497	No error (0)	cnvy.app.link		13.224.193.44	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.750678062 CET	8.8.8.8	192.168.2.3	0x5497	No error (0)	cnvy.app.link		13.224.193.82	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:20.750678062 CET	8.8.8.8	192.168.2.3	0x5497	No error (0)	cnvy.app.link		13.224.193.104	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.192137957 CET	8.8.8.8	192.168.2.3	0x1e89	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuse rcontent.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 19:13:21.192137957 CET	8.8.8.8	192.168.2.3	0x1e89	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.23.65	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.294528961 CET	8.8.8.8	192.168.2.3	0x7153	No error (0)	t.dripemail2.com		34.192.142.116	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.294528961 CET	8.8.8.8	192.168.2.3	0x7153	No error (0)	t.dripemail2.com		3.92.124.243	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.294528961 CET	8.8.8.8	192.168.2.3	0x7153	No error (0)	t.dripemail2.com		54.205.203.21	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.294528961 CET	8.8.8.8	192.168.2.3	0x7153	No error (0)	t.dripemail2.com		184.73.223.134	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:21.294528961 CET	8.8.8.8	192.168.2.3	0x7153	No error (0)	t.dripemail2.com		18.232.43.29	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:22.505538940 CET	8.8.8.8	192.168.2.3	0x84fd	No error (0)	sharepoint uploadsfus 5.z13.web. core.windo ws.net	web.blz22prdstr18a.store. core.windows.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 19:13:22.505538940 CET	8.8.8.8	192.168.2.3	0x84fd	No error (0)	web.blz22prdstr18a.store.core.windows.net		20.60.7.97	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:25.564165115 CET	8.8.8.8	192.168.2.3	0x7eb1	No error (0)	oomslalaservice.com		104.219.248.112	A (IP address)	IN (0x0001)
Mar 5, 2021 19:13:28.265979052 CET	8.8.8.8	192.168.2.3	0x4db9	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 19:13:28.265979052 CET	8.8.8.8	192.168.2.3	0x4db9	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)

HTTPS Packets

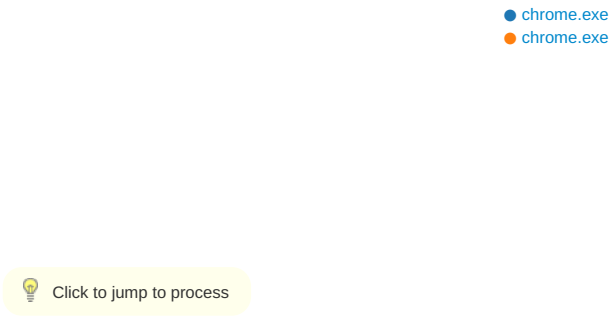
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 19:13:20.448709965 CET	52.52.65.159	443	192.168.2.3	49704	CN=convoy.app CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 30 13:31:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 30 14:31:07 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 19:13:20.454500914 CET	52.52.65.159	443	192.168.2.3	49702	CN=convoy.app CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 30 13:31:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 30 14:31:07 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 19:13:20.608102083 CET	52.52.65.159	443	192.168.2.3	49705	CN=convoy.app CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 30 13:31:07 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 30 14:31:07 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 19:13:21.568145037 CET	34.192.142.116	443	192.168.2.3	49712	CN=dripemail2.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Feb 07 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Mar 09 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6396 Parent PID: 996

General

Start time:	19:13:15
Start date:	05/03/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6580 Parent PID: 6396

General

Start time:	19:13:16
Start date:	05/03/2021
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=1520,6376799053035196430,7750294235629446408,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly