



ID: 404279
Sample Name: test.html
Cookbook: default.jbs
Time: 21:30:16
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report test.html 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 42
General 42
File Icon 42
Network Behavior 42
Network Port Distribution 42
TCP Packets 43
UDP Packets 44
DNS Queries 47
DNS Answers 47
HTTPS Packets 47
Code Manipulations 47
Statistics 47
Behavior 47
System Behavior 48

Copyright Joe Security LLC 2021

Analysis Process: chrome.exe PID: 1364 Parent PID: 4232 48
General 48
File Activities 48
Registry Activities 48
Analysis Process: chrome.exe PID: 6160 Parent PID: 1364 48
General 48
File Activities 49
Disassembly 49

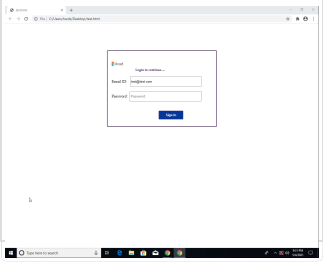
Analysis Report test.html

Overview

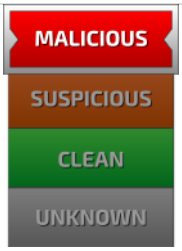
General Information

Sample Name:	test.html
Analysis ID:	404279
MD5:	0d80b3a43db9ad..
SHA1:	2d5984c3f0f7727..
SHA256:	edd93d70b8455e..
Infos:	

Most interesting Screenshot:



Detection



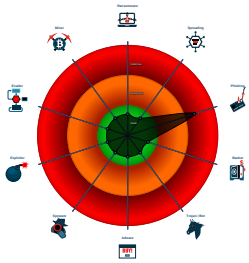
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- No HTML title found
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 1364 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\test.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6160 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1628,16747573067059828566,6713175093340114276,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

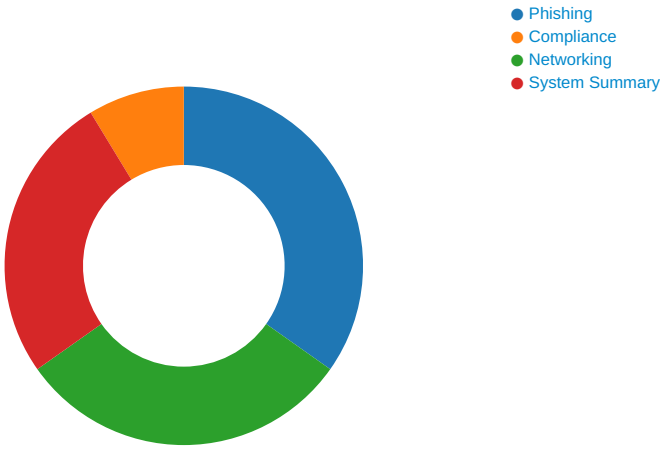
Initial Sample

Source	Rule	Description	Author	Strings
test.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

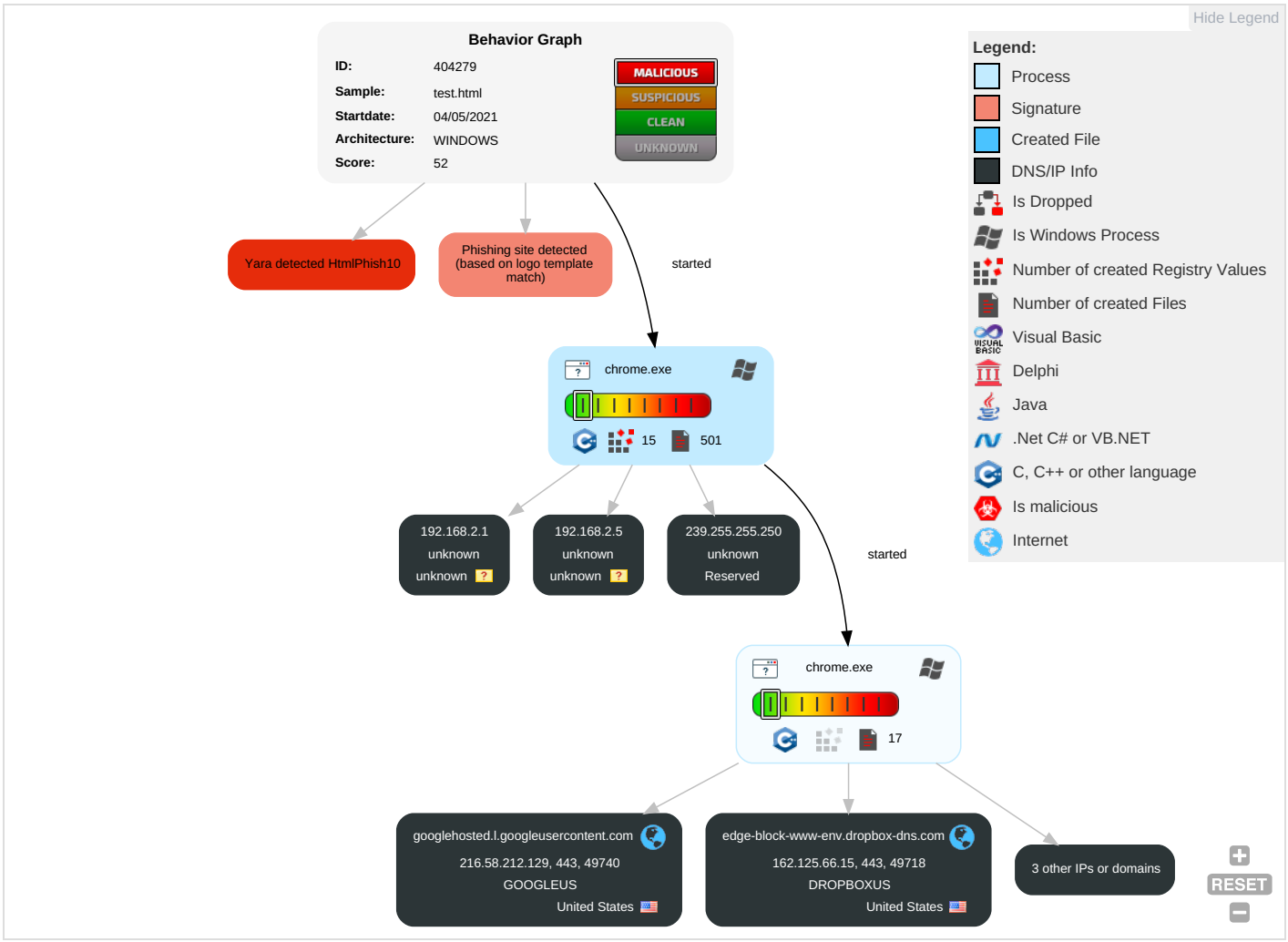
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

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 1	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

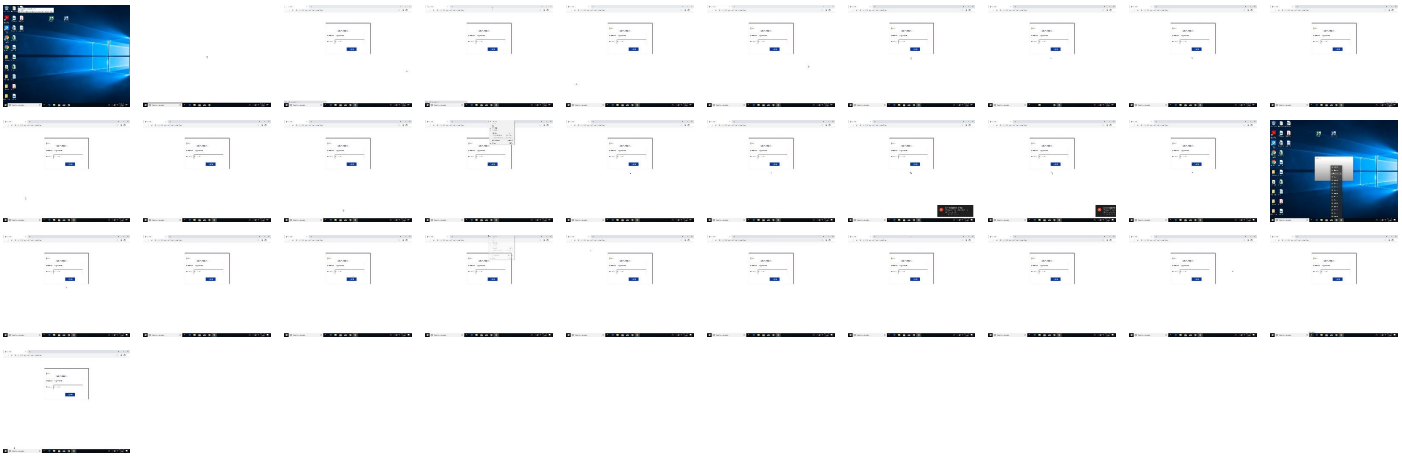
Behavior Graph

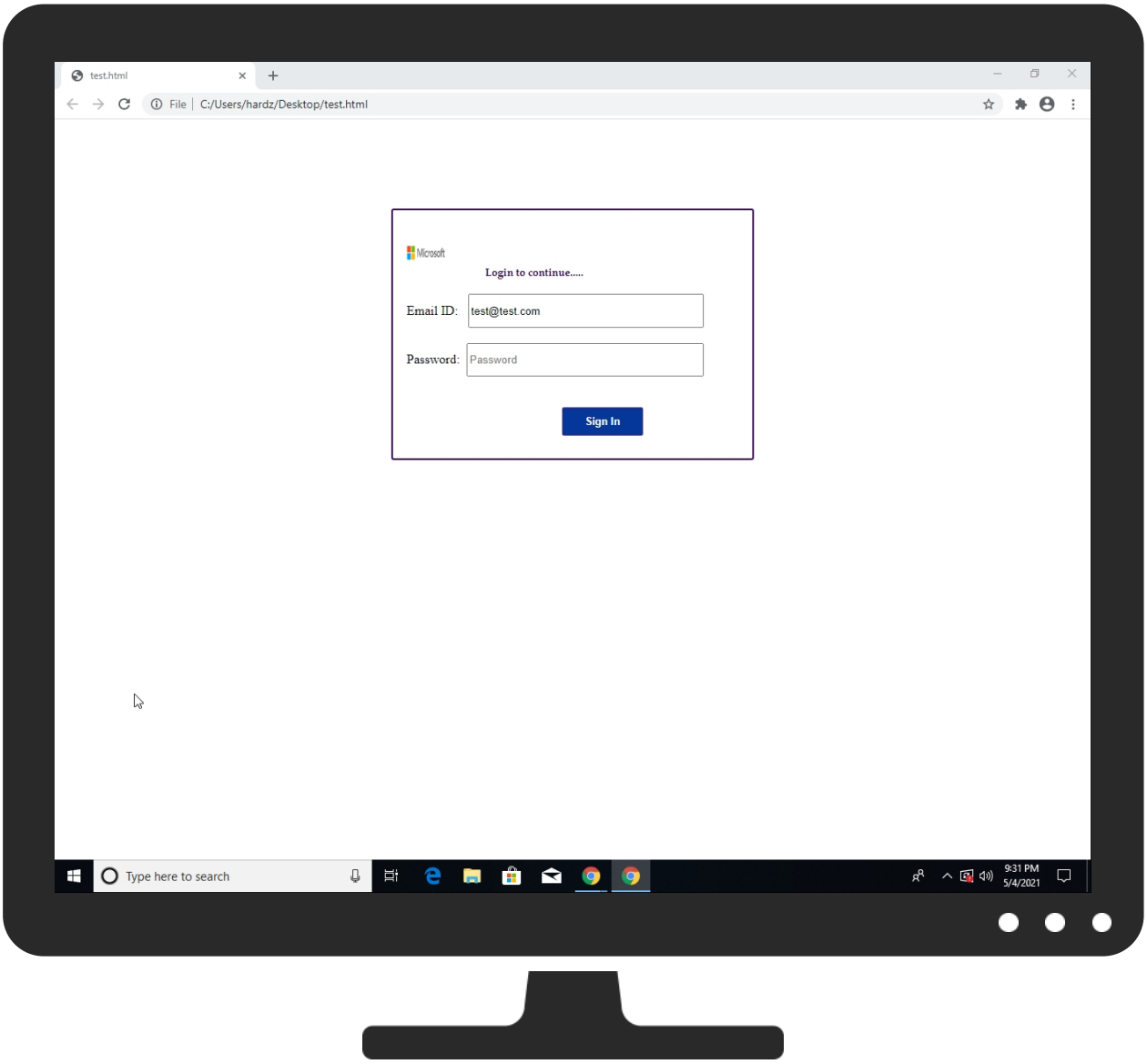


Screenshots

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
edge-block-www-env.dropbox-dns.com	0%	Virustotal		Browse

URLs

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

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://ppdt.trisakti.ac.id/wp-content/time/5/login.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
edge-block-www-env.dropbox-dns.com	162.125.66.15	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
dl.dropboxusercontent.com	unknown	unknown	false		high

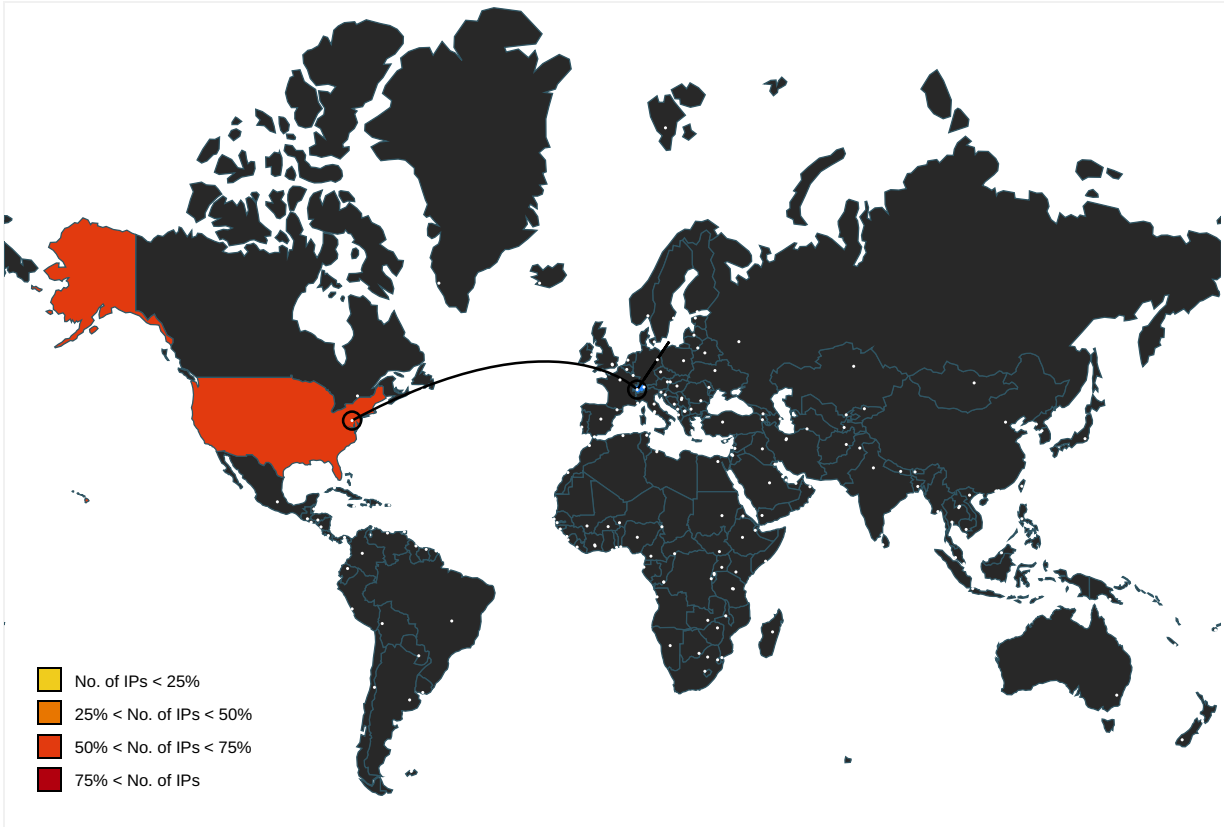
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/test.html	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	3399a358-8acf-4c6e-9fb6-1f82a1649030.tmp.1.dr, 9b3bf54c-5910-42a0-910b-7d92f48775c5.tmp.1.dr, 4a03e2b9-b11d-4d5c-be43-d5c958236abb.tmp.1.dr, 518a2c58-4a3d-4ff1-b9bc-f50618352008.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	3399a358-8acf-4c6e-9fb6-1f82a1649030.tmp.1.dr, 9b3bf54c-5910-42a0-910b-7d92f48775c5.tmp.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://ppdt.trisakti.ac.id/wp-content/time/5/login.php	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dl.dropboxusercontent.com	9b3bf54c-5910-42a0-910b-7d92f48775c5.tmp.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
162.125.66.15	edge-block-www-env.dropbox-dns.com	United States		19679	DROPBOXUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404279
Start date:	04.05.2021
Start time:	21:30:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test.html
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
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:	mal52.phis.winHTML@43/239@2/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html

Copyright Joe Security LLC 2021

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.193.48, 23.54.113.53, 104.42.151.234, 142.250.184.195, 142.250.185.206, 216.58.212.173, 216.58.212.142, 142.250.186.46, 95.168.222.146, 95.168.222.141, 34.104.35.123, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 23.57.80.111, 20.82.210.154, 93.184.221.240, 172.217.23.99, 142.250.185.67, 92.122.213.247, 92.122.213.194, 95.168.222.80, 20.54.26.129, 52.155.217.156, 20.190.160.2, 20.190.160.69, 20.190.160.73, 20.190.160.67, 20.190.160.136, 20.190.160.6, 20.190.160.75, 20.190.160.71, 51.124.78.146, 40.127.240.158, 51.104.136.2, 216.58.212.131, 95.168.222.18, 20.50.102.62 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, login.live.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, r5.sn-n02xgoxufvg3-2gbl.gvt1.com, au-bg-shim.trafficmanager.net, r7---sn-n02xgoxufvg3-2gbz.gvt1.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, www.tm.lg.prod.aadmsa.trafficmanager.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, encrypted-tbn0.gstatic.com, r7.sn-n02xgoxufvg3-2gbz.gvt1.com, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, r5---sn-n02xgoxufvg3-2gbl.gvt1.com, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, skypedataprdcolwus16.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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	
	referenceMemMem.hta	Get hash	malicious	Browse	
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	
	Tree Top.html	Get hash	malicious	Browse	
	ATT51630.htm	Get hash	malicious	Browse	
	message for dtriscritti@discountwaste.com.html	Get hash	malicious	Browse	
	efax637637637.htm	Get hash	malicious	Browse	
	afafd.htm	Get hash	malicious	Browse	
	efax663663663.htm	Get hash	malicious	Browse	
	FedEx Shipment Address Update Form2021.html	Get hash	malicious	Browse	
	jdCsAaeOMw3AekTOgSZ92vgpOBC5TwWgMkt.html	Get hash	malicious	Browse	
	Cws-Pay Application.html	Get hash	malicious	Browse	
	.htm	Get hash	malicious	Browse	
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	
	efax702702702.htm	Get hash	malicious	Browse	
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	
	Purchase Payment PPY029618.htm	Get hash	malicious	Browse	
162.125.66.15	ausgangsrechnung@condor.com_ProjectDocument.HTML	Get hash	malicious	Browse	
	rklein@vertexeng.com_80280265Application.HTML	Get hash	malicious	Browse	
	AWB783079370872.docm	Get hash	malicious	Browse	
	y0CRLCaQxA.exe	Get hash	malicious	Browse	
	Roomimglist Para Reserva.vbs	Get hash	malicious	Browse	
	http://https://uc7b53be34470077fa5a225e12df.dl.dropboxusercontent.com/cd/0/get/BFOurBML9LTrYESsgZVnt-7s_XcT1zeXR_UKUe727s4pkHr9HASCTbLCGqW4UetiP2mCY9lexFN5bUjD5CxShlCu3wHWVLxNCOSCmgAvE_LtlaQljaEAJPiqPF2MmSeHZlw/file?dl=1	Get hash	malicious	Browse	
	yorkcountygov.comPaymentCopy.htm	Get hash	malicious	Browse	
	http://https://ucf2e159dcdc627dd91c5955a5b2.dl.dropboxusercontent.com/cd/0/get/BFIJR_DLx5TrpQ0LUrIdtB-TiMb8hXWBtyaxeUO96o9pDO2kuhn8C1M100sfcNRduSe85JbdWYokMfX07myXHHCiJews_d8d9AU4Vbqsj4mNqfzUgaLCJ-Q80my2kOBIkNQ/file?dl=1	Get hash	malicious	Browse	
	digiturk.com.trPaymentCopy.htm	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.27966.31021.exe	Get hash	malicious	Browse	
	cxu46fus4k.exe	Get hash	malicious	Browse	
	LISTE DES TRANSACTIONS PAS CARTES.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.4c7063ec0fb39986.exe	Get hash	malicious	Browse	
	http://https://dynalist.io/d/JKioi6pWCqgcfJR0dl7PFAgg	Get hash	malicious	Browse	
	Damage.exe	Get hash	malicious	Browse	
	http://https://www.dropbox.com/s/cb2ge9mcx8ysgqh/Notification__VS61XA.doc?dl=1	Get hash	malicious	Browse	
	http://https://www.dropbox.com/s/id8j4kg05zg4ug0/Notice%20DJ0XBTM.doc?dl=1	Get hash	malicious	Browse	
	http://https://www.dropbox.com/s/5vgml9mqmjffp3n/Note%207V1N0UE.doc?dl=1	Get hash	malicious	Browse	
	http://https://serxcome.us-south.cf.appdomain.cloud/redirectfile/?email=fuck@fuck.com	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.dropbox.com/s/uakhik6hva7eazm/Copy_LAA8D4K.doc?dl=1	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
edge-block-www-env.dropbox-dns.com	ausgangsrechnung@condor.com_ProjectDocument.HTML	Get hash	malicious	Browse	• 162.125.66.15
	x6I8ze0ztQ.exe	Get hash	malicious	Browse	• 162.125.69.15
	rklein@vertexeng.com_80280265Application.HTML	Get hash	malicious	Browse	• 162.125.66.15
	AWB783079370872.docm	Get hash	malicious	Browse	• 162.125.66.15
	y0CRLCaQxA.exe	Get hash	malicious	Browse	• 162.125.66.15
	Roomimglist Para Reserva.vbs	Get hash	malicious	Browse	• 162.125.66.15
	http://https://www.dropbox.com/s/1jk3ia2o2kx0p1n/Invitation_2036.doc?dl=1	Get hash	malicious	Browse	• 162.125.67.15
	http://https://uc7b53be34470077fa5a225e12df.dl.dropboxusercontent.com/cd/0/get/BFOurBML9LTrYESsgZVnt-7s_XcT1zeXR_UKUe727s4pkHr9HASCTbLCGqW4UetiP2mCY9lexFN5bUjD5CxShlCu3wHWVLxNCOSCmgAvE_LtlaQIjaEAJPiqPF2MmSeHZlw/file?dl=1	Get hash	malicious	Browse	• 162.125.66.15
	yorkcountygov.comPaymentCopy.htm	Get hash	malicious	Browse	• 162.125.66.15
	http://https://ucf2e159dcdc627dd91c5955a5b2.dl.dropboxusercontent.com/cd/0/get/BFIJR_DLx5TrpQ0LUrIdtB-TiMb8hXWBtyaxeUO96o9pDO2kuhn8C1M100sfcNRduSe85JbdWYokMfX07myXHHCiJews_d8d9AU4Vbqsj4mNqfzUgaLCJ-Q80my2kOBIkNQ/file?dl=1	Get hash	malicious	Browse	• 162.125.66.15
	digiturk.com.trPaymentCopy.htm	Get hash	malicious	Browse	• 162.125.66.15
	SecuriteInfo.com.Trojan.DownLoader36.27966.31021.exe	Get hash	malicious	Browse	• 162.125.66.15
	cxu46fus4k.exe	Get hash	malicious	Browse	• 162.125.66.15
	LISTE DES TRANSACTIONS PAS CARTES.xls	Get hash	malicious	Browse	• 162.125.66.15
	SecuriteInfo.com.Generic.mg.4c7063ec0fb39986.exe	Get hash	malicious	Browse	• 162.125.66.15
	http://https://dynalist.io/d/JKioi6pWCqgcfJR0dl7PFAgg	Get hash	malicious	Browse	• 162.125.66.15
	Damage.exe	Get hash	malicious	Browse	• 162.125.66.15
	http://https://www.dropbox.com/s/cb2ge9mcx8ysgqh/Notification__VS61XA.doc?dl=1	Get hash	malicious	Browse	• 162.125.66.15
	http://https://www.dropbox.com/s/id8j4kg05zg4ug0/Notice%20DJ0XBTM.doc?dl=1	Get hash	malicious	Browse	• 162.125.66.15
	http://https://www.dropbox.com/s/5vgml9mqmjffp3n/Note%207V1N0UE.doc?dl=1	Get hash	malicious	Browse	• 162.125.66.15

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DROPBOXUS	ausgangsrechnung@condor.com_ProjectDocument.HTML	Get hash	malicious	Browse	• 162.125.66.15
	bootlocker.exe	Get hash	malicious	Browse	• 162.125.66.18
	VESSELS DETAILS.exe	Get hash	malicious	Browse	• 162.125.66.18
	x6I8ze0ztQ.exe	Get hash	malicious	Browse	• 162.125.69.15
	gv9rD9vqPS.exe	Get hash	malicious	Browse	• 162.125.69.18
	Balance payment..exe	Get hash	malicious	Browse	• 162.125.66.18
	unk.dll	Get hash	malicious	Browse	• 162.125.66.14
	rklein@vertexeng.com_80280265Application.HTML	Get hash	malicious	Browse	• 162.125.66.15
	L2NVQjRX9s.exe	Get hash	malicious	Browse	• 162.125.66.18
	a.exe	Get hash	malicious	Browse	• 162.125.66.18
	AWB783079370872.docm	Get hash	malicious	Browse	• 162.125.66.15
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 162.125.66.18
	y0CRLCaQxA.exe	Get hash	malicious	Browse	• 162.125.66.15
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 162.125.66.18
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 162.125.66.18
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 162.125.66.18
	prints-eduardo-bolsonaro.docm	Get hash	malicious	Browse	• 162.125.66.18
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 162.125.66.18
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 162.125.66.18
	prints carlos bolsonaro.docm	Get hash	malicious	Browse	• 162.125.66.18

Copyright Joe Security LLC 2021

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	• 162.125.66.15
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	• 162.125.66.15
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 162.125.66.15
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 162.125.66.15
	Tree Top.html	Get hash	malicious	Browse	• 162.125.66.15
	efax637637637.htm	Get hash	malicious	Browse	• 162.125.66.15
	afafd.htm	Get hash	malicious	Browse	• 162.125.66.15
	FedEx Shipment Address Update Form2021.html	Get hash	malicious	Browse	• 162.125.66.15
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 162.125.66.15
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	• 162.125.66.15
	Monday, April 19th, 2021, 20210419034211.37352E088CBDC09B@classactsautobody.com.htm	Get hash	malicious	Browse	• 162.125.66.15
	042021.htm	Get hash	malicious	Browse	• 162.125.66.15
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 162.125.66.15
	042021.htm	Get hash	malicious	Browse	• 162.125.66.15
	042021.htm	Get hash	malicious	Browse	• 162.125.66.15
	AttachementHtm.html	Get hash	malicious	Browse	• 162.125.66.15
	1-page-fax-from-+33822822.htm	Get hash	malicious	Browse	• 162.125.66.15
	#U266b VM-Tunes-Playback.html	Get hash	malicious	Browse	• 162.125.66.15
	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	• 162.125.66.15
	Monday, April 19th, 2021, 20210419111136.68B7C9F20FAF4F3F@classactsautobody.com.htm	Get hash	malicious	Browse	• 162.125.66.15

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
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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\03e3f0ac-678f-41e6-b7e6-4286bbedaec3.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):	159928
Entropy (8bit):	6.050876497601597
Encrypted:	false
SSDEEP:	3072:LMtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:QEr/NOX3aqfIlUOoSiuRU
MD5:	9A1E63269A5CEBBD71C9F112A93566E4

C:\Users\user\AppData\Local\Google\Chrome\User Data\03e3f0ac-678f-41e6-b7e6-4286bbedaec3.tmp	
SHA1:	6305BB14A32C4E31D22B95B4B2D0E3501067C593
SHA-256:	A5AD5BBB939F07E1851BBD87E3509CEE4B6D7F8AFE4FB8C3E9267E1EE2123CD2
SHA-512:	44798EF3C3ADB20BE94552D585B2C022234CB4F00573F5D600D73D87495A96E3446502D75E63DE30DE85D42BE50E59873375A098EE3559380B5C964421582AB5
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\15c62da8-9c54-476f-b833-9a3d95bef786.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.748556024810905
Encrypted:	false
SSDEEP:	384:nHdySsPZYMb21NKr/v+G3tGkZH0tGRYrzQSUxb5lIQbrD6xmvUzgq2WVOgEmNQS/:PmRxCEF9Qef8u0s/DWmKs2WBL
MD5:	4BB4A1B85D00742D58934905D3FA11C1
SHA1:	A6355E3D9278B1855ABC50C4B24CFB7F8B36B4F9
SHA-256:	E59FF1504F8CF195B712FB313A7441887A5A18723896A4C1D34551F0E022BA74
SHA-512:	D45DFC8C9F92D5DD41A6180B86D2F90AD70BEB1D0A4DDF8C2B22DA2A9EEE9EFFAABA81FB1CB5B856B79E52592398D36CC08AE1E068B8C402062AEA5378A0C64
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.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\15ea6b3b-6aea-4dc6-865d-924d08d3cd9e.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):	160387
Entropy (8bit):	6.052053525945578
Encrypted:	false
SSDEEP:	3072:tgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:+Er/NOX3aqfIlUOoSiuRU
MD5:	18125822E5CD511EAB8452579C312014
SHA1:	934D838238790A1223B02DB3C544414330DC8A5C
SHA-256:	F426CFA9A2A78B4F10088C909B0B7B5EC529BC33C46473DCF1456C2C9069ED15
SHA-512:	20224BFC7F1DD740786BE320F4A4205CF27B5F26F3716D596D3B44391E759A10D5D0EE73705AEE2002371A856AC97B929F95C758505C825B101A58232641628F
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a8415c5-a15d-4a64-8bbf-c861c8796020.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):	168319
Entropy (8bit):	6.080796808508154
Encrypted:	false
SSDEEP:	3072:v5OtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:BOEr/NOX3aqfIlUOoSiuRU
MD5:	C14341FA7A6F7CA7BB83F4996745F0BD
SHA1:	3DE700A7937F258E7228ACEC04680235C77EC5FE

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a8415c5-a15d-4a64-8bbf-c861c8796020.tmp	
SHA-256:	DD4BEAF8B664A54D993F161C4E380FDE8A5EE00D9CAF442CE411379ACB7F11A2
SHA-512:	6CEAFFF531281F891336D1F522DE6E94936649B3D1AB696011F09BBA1596446AC8C38D18C7E02DC0AC6DEAECC02A18FFC919654A3E20E580B6599D362CDB4F5
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2e90929d-608b-4b96-b226-4681592ce83e.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):	168319
Entropy (8bit):	6.080797160198648
Encrypted:	false
SSDEEP:	3072:vkHtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:8HEr/NOX3aqfIlUOoSiuRU
MD5:	CEDD3A1B5380161FD23D15812B1D54FD
SHA1:	B2AC4778FCB6D79406E8863545C4CA814A0E58F6
SHA-256:	631DCDDB13312AB0154F4B4860FC5656111EB5AC7EA5F32E54B01CECF90C3119
SHA-512:	93BEFC629BC55EA21888DEE0075EAACE814232A4B48AB7EAFABD11EA649203DA0D53076078597FA62A994A9E1560F633DBCF22DE8C8D9E0FBB4C4D2008BD3BE1
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\411771f4-5312-4119-95b7-72435cb96760.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):	168319
Entropy (8bit):	6.080795871570151
Encrypted:	false
SSDEEP:	3072:/d3tkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:F3Er/NOX3aqfIlUOoSiuRU
MD5:	C4029D260470D0DF08780244B33055C7
SHA1:	5780A8777291B17A00CA7253878236DB3BC36EFE
SHA-256:	43CB5EC64736AB32F08BB797C83E668746F9A43740190DC8D3CEC0C8C23D9E12
SHA-512:	97901B3849716F067902E962E9E55AB804F823D42EC7CCA3EA5DCF7660D70C9E18283CEE4FCA78E9264053FC3CCC4CFFE3C11F99EEEF7721359C77BB0456AAC
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\46468361-b37a-474e-9fe2-5faa8ac62fc4.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):	160291
Entropy (8bit):	6.051788542129696
Encrypted:	false
SSDEEP:	3072:IgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:1Er/NOX3aqfIlUOoSiuRU
MD5:	C6730B78925CACED3EA20539CF4F3E3C

C:\Users\user\AppData\Local\Google\Chrome\User Data\46468361-b37a-474e-9fe2-5faa8ac62fc4.tmp	
SHA1:	DD0E1670DB9FBE853AA7137BA2A3951576CABF88
SHA-256:	9DEA4D7F86CA9739218D2AB183ACD48F6F1036F71D390759C216BFD25D307DC9
SHA-512:	E06CDC19797863293062822304 36E0B1759C34F6F4FF177CB01680052252832CA8D17BF36A5DE1EC7A5DA0B27DFE9B80102CEBE2E2163B36B898526D7396B547
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fb3beb8-5e78-4533-b147-ebbdc046d54f.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):	160115
Entropy (8bit):	6.0513644151293144
Encrypted:	false
SSDEEP:	3072:FMtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:aEr/NOX3aqfIlUOoSiuRU
MD5:	9985942F1C1C3BEBF9ED33153FC4CAE5
SHA1:	B7FB4D1E93F6BC32B46A18BA1C631383C66746E5
SHA-256:	D5C583A0CAB9D67F8DF4239A33617FEB9118BE5780DB212FE4D7425B9139CF2D
SHA-512:	B91BCBD05814BF8680A48AFFCE8E971E77C97419706D5E45D45A042C63B351A0AEB4E6DF197ACC57ED9105FBF5148D16A9C9F165013F14A790380DCAFDE909I 8
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\75ad8aae-acd5-4459-aec0-87b4c2a7fdfc.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):	160291
Entropy (8bit):	6.051788542129696
Encrypted:	false
SSDEEP:	3072:IgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:1Er/NOX3aqfIlUOoSiuRU
MD5:	C6730B78925CACED3EA20539CF4F3E3C
SHA1:	DD0E1670DB9FBE853AA7137BA2A3951576CABF88
SHA-256:	9DEA4D7F86CA9739218D2AB183ACD48F6F1036F71D390759C216BFD25D307DC9
SHA-512:	E06CDC19797863293062822304 36E0B1759C34F6F4FF177CB01680052252832CA8D17BF36A5DE1EC7A5DA0B27DFE9B80102CEBE2E2163B36B898526D7396B547
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b4ca80e-6693-4acf-b5b1-c61fe3a08493.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):	160199
Entropy (8bit):	6.051524084052077
Encrypted:	false
SSDEEP:	3072:FgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:2Er/NOX3aqfIlUOoSiuRU
MD5:	636CD7AE83B5A637B902E41B047D805A
SHA1:	A3057C0705126FFAB38DE8561D846CCC0095E714

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b4ca80e-6693-4acf-b5b1-c61fe3a08493.tmp	
SHA-256:	83EB70D3C5529B4FB73CC74B46BC797EC8FAF7F3DDCDEF2FC06F9F4E0F84DB60
SHA-512:	CA70B2D6E0F798D7B3A582CC7FA280B8AB68B58E7E830A33B837B8C6318BBD2B885673E1C158051F801B9148E7507E47AE322D53F9C234D550D73EF756048712
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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:+ftlE1G1mkftlE1G1mkftlE1n
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\3399a358-8acf-4c6e-9fb6-1f82a1649030.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\4a6eaa8f-527f-4485-80cc-d5f177cd3658.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):	22596
Entropy (8bit):	5.535364056195194
Encrypted:	false
SSDEEP:	384:x5ItZLlBfXY1kXqKf/pUZNCgVLH2HfDnrUHHGCnTkublIx4N:ILllY1kXqKf/pUZNCgVLH2HfDrUnGCn3
MD5:	1679A0FAEC881D7987D961ECC73ED066
SHA1:	75233575300B637D7B1A974516D5903455FBE0C4
SHA-256:	2DAE384124FE25EDFE4F71855DAEC298287AFA830AEADBEDB31A94FB1668E5FC
SHA-512:	083041240248E0D632A336A48174B51B5A5A654A4B72B486970C11AB20025A46645093E8B0123295CE1F464D02EA0BA60FD648DA991464BC67751E74386FF2A0
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4a6eaa8f-527f-4485-80cc-d5f177cd3658.tmp	
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":"13264662668603199","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\5e1b4f6a-7d95-404f-96d4-0657a755a05a.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):	1206
Entropy (8bit):	5.569225512504242
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUe5+Uykq/HeUeXby2qUeXvt7wU29RUenHQ:YI6UUhVseKUeQU3qPeUer2UeftwU2TUD
MD5:	B818E8356F59CCA95544DE47B6086C4A
SHA1:	6873752F889FADED0ECC2333D410E7933BA0A604
SHA-256:	14ED0231742FCE814F5D2BDB283529B602970748A5559800018538E305E44A01
SHA-512:	9B48B2F6E53514440129003C8A73E2A9D01BE22B78A5AC982B26415339183394E13E3A0C303036824AACECD89ED5AF9B8662B708DE19D83C91245AFDE250984E
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":1651725074.408553,"host":"0FudNMFWX4RXqKtsolVS54GZEeKUrlKPufmSVP5lWp0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620189074.408559},{"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":1651725073.689182,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\667ba670-5e5b-40cd-a053-56eac611171e.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):	5390
Entropy (8bit):	5.18317557349519
Encrypted:	false
SSDEEP:	96:n99858f8q9d4+cVyWok0JCKL8klAbOTQVuwn:n9zf8eRce4KP
MD5:	C58EA92FA132187CDB0F7540AD29B524
SHA1:	9A83984398F4E10BE5D58894D04390892FEDB0C1
SHA-256:	AD48AF219DC26B8E24C55621CF140724D67F302A1D54B828F716EDED851AC513
SHA-512:	A13CCB2EF7C74C9EB58BD9EE882D55E37B8D49E3C2535C8399C047EA32DC726723B89C913D218DFF4146D1DF2A827040D43B527D8A89C433FE5344D802B688
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662669051718","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\77457dea-f617-435f-94a3-70974dbd0666.tmp	
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":"13264662668603199","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\7de5a6c6-e871-4297-8f73-a3a96e71637c.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):	5364
Entropy (8bit):	5.1802350515763615
Encrypted:	false
SSDEEP:	96:n998o8f8q9d4+cVyWok0JCKL8VbOTQVuwn:n9Af8eRce4K6
MD5:	0F73806E5426013EA1D1DCE554234453
SHA1:	D3929CAA03DA7A77B3A6E9D3886ADDBE82C58069
SHA-256:	DEA91BCB30FBF4AA2237678BF461F9583F6362B0D8490A855A6C5EFBCC054F5C
SHA-512:	338439F116D81FAA17D1CBAA97AA8B8282963723293CA547B61B8C714238EB697FE61F20756FAA1FE62B8C9586493C44648B255711DBFD39A9D53C74B1C0FA97
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662669051718","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.223068713335133
Encrypted:	false
SSDEEP:	6:m6aC+q2PWXp+N23iKKdK9RXXTZIFUtpN+WZmwPN+tVkwOWXp+N23iKKdK9RXX5LJ:daTva5Kk7XT2FUtpNT/PNo5f5Kk7XVJ
MD5:	232BCEDFBAB3540CFFC9AFDCD2AFDEBA
SHA1:	58AD8826BE01DE1E2DEC6C87BE35A8A8EAEEA79B
SHA-256:	8C1E4041CF4CDC817745718025FEE5D4BA46342431A89852E414D3EC6F3F8FD9
SHA-512:	F2030C99C3D4FE010F79DB0DAF90696A81ABABBD8010B5BF239FC5BF7BCE52013A850C1D00C6A85168B45BF802EFA374385EDD02D8FEA9CE87397F2546C1FDF9
Malicious:	false
Preview:	2021/05/04-21:31:20.847 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-21:31:20.852 12b8 Recovering log #3.2021/05/04-21:31:20.853 12b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.206852497703405
Encrypted:	false
SSDEEP:	6:m6wN+q2PWXp+N23iKKdKyDZIFUtpNENXZmwPNMFMVkwOWXp+N23iKKdKyJLJ:d7va5Kk02FUtpN8/PNd5f5KkWJ
MD5:	2E798AEC93687390DEB86CD3FA1CF7DC
SHA1:	04E10785BD8EE83397E5C2E798C47AB2E64E68FD
SHA-256:	514178A6E35AFC1E8BA11AA756EE058FF6794EFB3F41078E2BCB2A768DC9F468
SHA-512:	F95A7797AF23587CB2061DE76D758780F84881202043FF03CC450147D4D57AFADFAB78419365C5F880C5B07B25419FD27C21756F30043E553120ED1130BC35E0
Malicious:	false
Preview:	2021/05/04-21:31:20.824 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-21:31:20.826 12b8 Recovering log #3.2021/05/04-21:31:20.827 12b8 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):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	0.9689540679823638
Encrypted:	false
SSDEEP:	24:UCcLgAZOZD/L/qLbJLbXaFpEO5bNmISHn06UwV8:p8NOZL/q5LLOpEO5J/Kn7U68
MD5:	738BF5D235C02D32BBD331B7D85F8692
SHA1:	54C2C9BF0496C0D98BA28A34A3BFC4B391148388
SHA-256:	2FE591EE2BB461117646552ACE12B2E491094C7EEB07F97AB7D0AFA1698EBFCC
SHA-512:	27572EEF6F5A7DE68B4DB1794AA8466CF6726D8A189534A6034FBE7E704003D83E7B2C31A0455512D0E50BA9A0DD32ADF5ECD91A0E5365CF3A0A16C0DF4BBBE7

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2063
Entropy (8bit):	3.200187468908073
Encrypted:	false
SSDEEP:	24:34SplrlAlTjR0CQZ5aTjR0ql5TjR0wp1mZeT8ZLkFx432TjR0olr:34mxGjmCQZ5EjmeNjmUIZeAkFxpjm4r
MD5:	2581500F39C7F0079B3CCF470A97566B
SHA1:	BA2673AD79DE8CF1AF33E521A49F70AA903590F8
SHA-256:	DBFD259DA8925AFEC53A251A9206EFFBDCC1204F7E745DF2F70CD1805AA2E870
SHA-512:	2A6C591B4730FC9A8E7E31C0DE84150C065FD18E899572DC2A47B79129DD893F88F3CF6BCD20E70B80DB7352185BE2C83F49B5131EBDB1F2BBD0441AA485376F
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...c849f154_9135_4e0a_a8a7_28729d11ee29.....o..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....Q..L.....(...file:///C:/Users/user/Desktop/test.html..... .....h.....`.....H.....I.....X...(...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.t.e.s.t...h.t.m.l..... .....8.....0.....8..... .....(...file:///C:/Users/user/Desktop/test.html.....# /..... .....1.,.....(...file:///C:/Users/user/Desktop/tes

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):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....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):	317
Entropy (8bit):	5.186648225568624
Encrypted:	false
SSDEEP:	6:mbYOq2PWXp+N23iKKdK8aPrqIFUtp8lUvJZmwP8PGAkwOWXp+N23iKKdK8amLJ:Sva5KkL3FUtprh/PlA5f5KkQJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
MD5:	8661D00124F69AB253EFD04426735A15
SHA1:	51478A46C448B8E1CC8EFF096BCC904B9B652AC4
SHA-256:	0F129B0F2020B5D2A868759539641019CCF644E80F05D95C53E5E52708C6D5E9
SHA-512:	6644924B776831E5C3DA2673DECC656FDE0E8BA7F5B0E14C8762249379BF513C3EFC3DC1430A401D909387166EAEC0D37CAA75B30BE64B76C24C2F6A8FA215 9
Malicious:	false
Preview:	2021/05/04-21:31:09.043 c10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-21 :31:09.045 c10 Recovering log #3.2021/05/04-21:31:09.046 c10 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
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.....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):	317
Entropy (8bit):	5.163692417667105
Encrypted:	false
SSDEEP:	6:mse4q2PWXp+N23iKKdK8NIFUtpeZmwPSkwOWXp+N23iKKdK8+eLJ:39va5KkpFUtpe/PS5f5KkqJ
MD5:	9B331705AC1964ABB5E3D842D0A8F1AB
SHA1:	9A7ACC7756AA65BD573D6F5583E500422C96BBA6
SHA-256:	217EEAD428E7ACC900EE136BD0A9A19F6D4AC73F22A5CA68311BBAE5CBEC73E0
SHA-512:	42586A7FD910F0C7045838990D4A5DE67F3B56C74133BA0FA17E5BD407A494413F4D0B90E387538275315C12B05701B185352A5AADA4C1CAFFA78B0FAE10396D
Malicious:	false
Preview:	2021/05/04-21:31:11.227 c10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-21 :31:11.229 c10 Recovering log #3.2021/05/04-21:31:11.229 c10 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\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:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	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=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
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=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.276844165562338
Encrypted:	false
SSDEEP:	6:m6Mq2PWXp+N23iKKdK25+Xqx8chI+IFUtpN+CXZmwPN+jkwOWXp+N23iKKdK25+M:dMva5KkTXfchI3FUtpNN/PN65f5KkTXc
MD5:	9D5FBF6D7311CF415251B664193F9811
SHA1:	0558459A14B409FA3E4AAE5DBC04A41062CFA19D
SHA-256:	B9D03B0655C425D72AF020DAAD0DA90F148DE912106380906E6A7852C815CBA2
SHA-512:	E9EC8BDB23E15FCCDB6CE14ED50896299DB401FC64D9700B84B3AF3F334FEDB54BB80BA8F071EC4CC797161ABAC06427D172F6F15D3C1C242253A1A4AFC659C
Malicious:	false
Preview:	2021/05/04-21:31:20.846 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-21:31:20.851 864 Recovering log #3.2021/05/04-21:31:20.852 864 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):	5.221474311743616
Encrypted:	false
SSDEEP:	6:m6KFRMq2PWXp+N23iKKdK25+XuoIFUtpNBZmwPNbkwOWXp+N23iKKdK25+XuxWLJ:dKFRMva5KkTXYFUtpNB/PNb5f5KkTXHJ
MD5:	153076E814184F9DC9CF3A7D7521CE87
SHA1:	FECB03E6818D5391E837F37B3B66FC0C3818DC45
SHA-256:	7DE9AA4DD1071640196C669617CB88F14F986B819DADD0ED7B32224E3B1B8D7B
SHA-512:	6A3DF8DA803A1385947C18944B36EC79EB0DC9BCCF0788E0ACF0C48AA8A94D9A7D30A9816E0AF8E7BEBB14EC710AEFB37EF56C96BF7B39074B38ACD4A57CAB37
Malicious:	false
Preview:	2021/05/04-21:31:20.821 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-21:31:20.824 864 Recovering log #3.2021/05/04-21:31:20.824 864 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):	5.24473077861097
Encrypted:	false
SSDEEP:	6:m64+q2PWXp+N23iKKdKWT5g1IdqIFUtpNqR9ZmwPNqRPkwOWXp+N23iKKdKWT5gZ:d4+va5Kkg5gSRFUtpNU/PNU5f5Kkg5gZ
MD5:	72EFB9C770908849A07328291752EA86
SHA1:	DC07D613A336E47B886717D222DCCFB622A3A263
SHA-256:	394E92C4D962E443D7C8A5C2DE99D5CFC05B39F7C3BBFBEE23203DE6DAD850CE
SHA-512:	3C848E02368474C870AE63A160492D185CBDCF2D27592D644E0DB968FABE4006B69875228E48E2D662677F0A37648678570FF4ECD32B840470D5BB7D33BF370D
Malicious:	false
Preview:	2021/05/04-21:31:20.522 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-21:31:20.524 864 Recovering log #3.2021/05/04-21:31:20.524 864 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):	592
Entropy (8bit):	0.4536056456034717
Encrypted:	false
SSDEEP:	3:8Efl3/sEZlP/:8qsc
MD5:	350A7A396F64EF907D1C55827C752EF7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
SHA1:	807EFDBC425D22D423D622E170743C11FC0316CB
SHA-256:	536E86750BC5F004137BE7E9D032E8F2C6E8450E111A23CA975625503404F6EC
SHA-512:	994E1E864EAFF087B75A8151AD13EF806AC72754D5BA9D08F77C3F2AEA0C8B4EC951EAF504065465DDE85AF5B6E02EC22344A898293724F33FA4936185919355
Malicious:	false
Preview:	.'..(.....]:.# /.....'..(..... .....]:.# /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09828657325561362
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvRGxIbjF1K+LAW5Re/kHOo/lCxthiZOCGCxC+/er61KJjF1K+Li:TL+A/zo4BRjRbNuQECGI/gJBRjR0
MD5:	FB290F62585F3B2189308E2C9A2DCAD3
SHA1:	DF73A8CDE6D1FC6FC0FCC7DB6E0443DB72C0A10A
SHA-256:	781CE2DA888243A6332AAE7A9DBFEEEEE462A085C4AF955A891FBE97DADDA1DB
SHA-512:	A0F9236EDAEC051B81B53BCBD27175E3B0E995BEFD0D0423AFA114A854011CE24A99DDB27ECFDE3ADEF95EAA73A189E227746A5A7CA3A0F44F0627CBD256C 737
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):	472
Entropy (8bit):	5.059004690876651
Encrypted:	false
SSDEEP:	12:b3Et2unRKdN1eU7sASBLVEMBk778B/xgskJnDBRjRqivJkWh:TGh6NT7CBLVE2Y78BJgskpDTjRTRkWh
MD5:	970A64C62DB0FB85E4306A0C3C1076BF
SHA1:	BC060AD118425859D7800E7DDB9BADD13CEDC103
SHA-256:	F61945EB0B116C5E7A575BBF145020A5D5CDC3BC49EBD688E5D19F935804BBFF
SHA-512:	3E7825D71A5681AEFAEFEE3625A28BFD0FE3A5F6D7D7230062D5ADF373A6FD95C53C558A6161BAD6830807DA83ECE140D6819B2306A064098F483E541152742E
Malicious:	false
Preview:	....."....c..desktop..file..user..html..test..users*J.....c.....desktop.....file.....user.....html.....test.....users..2.....a.....c.....d.....e.....f.....h.....i.....k..... .l.....m.....o.....p.....r.....s.....t.....u.....z...:A.....BP...L..... .....*(file:///C:/Users/user/Desktop/test.html2.:.....J .....$

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):	0.11676020902229291
Encrypted:	false
SSDEEP:	6:sqra0v8yuy0xng9bNFlWCj/l/CH/l3ll4/fMt76Y4QZVRtRex99pG/WqR4EZY4QW:RG/nqLBj/FCHt3ll4nMWQA9LuBQZ8fOA
MD5:	4C933AA10E044294A5A54E1D0673D166
SHA1:	8F7527ECD97E995D54BEFDBA4500FDE878E42AF4
SHA-256:	5B548D04C9B087346398C3EE2CE105F432F4FCBE02BF00EA71394DEB6D24F237
SHA-512:	C50085232F99C9BB9992D847F434C9BF95189793BDB75DF16AE57B418B829F9169D9A815F1ACB82D114D4B843C51BEB90AC321AF804428D87AB2C4AF5B5004F9
Malicious:	false
Preview:	.....'E..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.471956695102484
Encrypted:	false
SSDEEP:	48:dQGrB/JL/Da78Mt8dbwKabbQSefgGezNrS0U9RdiN9OB/3:Jba78MGdbwKabbQ5fgGehrS0k
MD5:	7D74917D744B3F5132E4F2F02BF8B447
SHA1:	08F9A25FF62FBBAAA2ABA87CCB62F523116A923B
SHA-256:	CCC6F35B997789B54A9FCCD3F49BCCC7010C915E88EC01378C7316C03DBFC4F8
SHA-512:	42CFDA3E6E6DBB603195F9A1BD3894123CE255E2C680A27EA06BF546682BA3D68E3F27236D62F6766A3A7E1AB4CA76738B238421132F78FCF60F05407CC8E70D
Malicious:	false
Preview:	.R.....*.....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..198210000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-04 21:31:23.49][INFO][mr.Init] MR instance ID: b2b34738-fde3-452e-b3d4-d59f06001a2b\n","[2021-05-04 21:31:23.49][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-04 21:31:23.49][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-04 21:31:23.49][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-04 21:31:23.49][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-04 21:31:23.50][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-04 21:31:23.50][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):	329
Entropy (8bit):	5.228858818107558
Encrypted:	false
SSDEEP:	6:mc6EOq2PWXp+N23iKKdK8a2jMGIFUtpvN3JZmwPvCPkwOWXp+N23iKKdK8a2jMmd:4va5Kk8EFUtpdJ/Pm5f5Kk8bJ
MD5:	A47E207E193FA82BB6FF08D625CB582D
SHA1:	2B8B0EFA7E4F823E00C28F0B172F740102A6DB47
SHA-256:	1ED71FB1272AAB64C215E87F50D1760ECF7884026ECB8AA03CB824FCF7BE1681
SHA-512:	10C32FA580DC9A6F2B7E40B182B337DC430FB53D74D3863ABD4CBA5F772EFAE464CC8F834F22CA80C5B66EA5B260ACF577000CAA153E048946EE33A8862629C
Malicious:	false
Preview:	2021/05/04-21:31:08.686 c54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:31:08.688 c54 Recovering log #3.2021/05/04-21:31:08.689 c54 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
Size (bytes):	334
Entropy (8bit):	5.215557186569935
Encrypted:	false
SSDEEP:	6:mbBl+q2PWXp+N23iKKdKgXz4rRIFUtp8kFVZmwP8kF5VkwOWXp+N23iKKdKgXz4n:qI+va5KkgXiuFUtpv/PvV5f5KkgX2J
MD5:	AA2B1A82170B6D228AC2AEABBFE39285
SHA1:	153F9C927B5A4EE502BA8E4C4A129573416F87D6
SHA-256:	6F3F730D838802868CC3D57A4C7E25FFC2E59CB65A8B3CF147EE39DEC8452335
SHA-512:	B0283BDCF2EC17714428B836555C3E8AC783489CBD5C834439CA86307B17FCD897F27DCD895FD03383C9BBD20F020A1E16DFD570B63FB07C777C7AF0693FBCA
Malicious:	false
Preview:	2021/05/04-21:31:09.087 182c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/04-21:31:09.090 182c Recovering log #3.2021/05/04-21:31:09.090 182c 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\Reporting and NEL	
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):	20480
Entropy (8bit):	1.0109084309301315
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAor:wIElwQF8mpcSJ2YL1
MD5:	26A286003B7C5225EA04C77A840A4FF1
SHA1:	6A0B44AFD8FECB3DC21A49921CE3B6019D23CC6A
SHA-256:	CC9A564D51BBF768459D0F241F1DE069BC922A5C2E21D6B9B282B098098539EE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA-512:	EA8A3412C69148D7676EE1B4C3DB87D1CC7D55F823D0C64222CCD28B2AF6B685DE7F8C7172AF933D5FC012DA11CE09315D34EBFFDA715DEA3EF1EA630A0821E
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8268285005338883
Encrypted:	false
SSDEEP:	48:EUqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU86:EUhIElwQF8mpcSl
MD5:	3D02046D840CA97453B3867D453EC3AF
SHA1:	B3F8E96364621A896EFBB08774070FB63BC772A1
SHA-256:	45BE7E4B649740EAF90B7FDF69DD79ECF6E0AC1149EC708A4A1F1E9E198722A6
SHA-512:	84D5F162C2BFAD363763CE369A89006265F254CD712DBB83DD069930F2EC625A7674A5C439D942036CBE44E1944485814B97C7FDE8F2A291EA1F1AF0963C5858
Malicious:	false
Preview:	.....}..... ....

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):	317
Entropy (8bit):	5.178583012296958
Encrypted:	false
SSDEEP:	6:mc5q2PWXp+N23iKKdKrQMxIFUtpvThZmwPv48AkwOWXp+N23iKKdKrQMFLJ:xva5KkCFUtpbh/PQ8A5f5KktJ
MD5:	FC902B83F7ED740F6E1A72E7D3A3C1E9
SHA1:	5B3644C651C587A6D36CA0CD2A52D9F45A9B64AD
SHA-256:	36299534B1E36D285D845171EE4035FEC2360AB123A04C07DECB7EA81015DA3E
SHA-512:	CD7E9D0CE152EDBC7E0EED2B33A789E5017DD0FFFBFC14F0E4CE663193EA8F01ACDAB010658AF71DC36622493EB20298DB7C96B155F166A2CF8388989D61D71
Malicious:	false
Preview:	2021/05/04-21:31:08.874 c10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-21:31:08.879 c10 Recovering log #3.2021/05/04-21:31:08.881 c10 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):	345

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Entropy (8bit):	5.187971504234301
Encrypted:	false
SSDEEP:	6:mcURa3+q2PWXp+N23iKKdK7Uh2ghZIFUtpvU4JZmwPvU49VkwOWXp+N23iKKdK7w:cRHva5KklhHh2FUtps4J/Ps4D5f5KkIT
MD5:	32A39E77AAD7E62E380D46F2AA045537
SHA1:	74683E5EA96FFF63F6314007156B25077CBC8B2A
SHA-256:	CF7A47F6FA43AF48A0F8564E4E0C4A080FAA3BAAF12E2591FD5F574AD34CB7D0
SHA-512:	2BBC55F505CB5ACBCFAE8F044AD1C6BE156FABE225FC0973560357F64CDE81A80170AC433B03CCA7BE6673E37C5C6FC9636352F112904354B4B809593F41C26
Malicious:	false
Preview:	2021/05/04-21:31:08.583 738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/05/04-21:31:08.585 738 Recovering log #3.2021/05/04-21:31:08.585 738 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\518a2c58-4a3d-4ff1-b9bc-f50618352008.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):	427
Entropy (8bit):	5.236704652241289
Encrypted:	false
SSDEEP:	6:mbK2q2PWXp+N23iKKdKusNpV/2jMGIFUtp8xvJZmwP8E9kwOWXp+N23iKKdKusNA:Z2va5KkFFUtpc/P95f5KkOJ
MD5:	1D5149C019684D5B8BD2DB1721BC03DB
SHA1:	58949E54F0B1F5AD1B01808FD14D90029EBA51F0
SHA-256:	B09D572A6D25A4A89BF98B036E4919205A7BF3B746E853E0EA561B60CE59C756
SHA-512:	A02D34308CC22DA25284B0381123BF8F3CFEB9D4DCBF927E53AFF85F30474AC6429048E64459364963D461D72B0A8169980CD1C0B65A2B616536DADA653D56A
Malicious:	false
Preview:	2021/05/04-21:31:09.016 c10 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:31:09.017 c10 Recovering log #3.2021/05/04-21:31:09.018 c10 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):	5.298856982282514
Encrypted:	false
SSDEEP:	6:mb6SQL+q2PWXp+N23iKKdKusNpqz4rRIFUtp8rG1ZmwP8BUQQLVkwOWXp+N23iKV:nOva5KkmiuFUtpf1/Pao5f5Kkm2J
MD5:	36447D4BAE1687FE140F3AF9380944AB
SHA1:	4BBE4944FB192B1CA02DF6008AB1DC066B057065
SHA-256:	37ADAED8EF824F05AD7E2D5455D7DFC6E27649E5C7E620E2F3ED7524883A8C4E
SHA-512:	EDE6CFE956437C1EA1E851CF13992E7818FF5C328C8EDE3E2C8CF8D32815EFFB03ABAADE327258CA4DFE16865EBDB3B2D51269DFF49C87DD95AD74280C3E9E3E
Malicious:	false
Preview:	2021/05/04-21:31:09.083 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/04-21:31:09.085 1838 Recovering log #3.2021/05/04-21:31:09.087 1838 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):	5.295113157460598
Encrypted:	false
SSDEEP:	6:m8KRyQL+q2PWXp+N23iKKdKusNpZQMxIFUtpLKTyG1ZmwPLNSaSQLVkwOWXp+N2R:ORuva5KkMFUtpeh1/PRSW5f5KkTJ
MD5:	FA4F05CD21252E84535AAEFECD7AAA94
SHA1:	9DB2D1D725785809CE63EC42A0543B349E9F7F3A
SHA-256:	CBDDCC8821345C96354CF64F26DBA461A310A910E95D0F68866310D834FCC2CD
SHA-512:	2BF43156570CC60365157D014A49CBF7C432C2D27DACE79DDAE3D830CB175B9EED6DB1140DD52D191D0A2C21534D38C2D5CDBFD6D9F348EFAF19CE94690CBE
Malicious:	false
Preview:	2021/05/04-21:31:26.094 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/04-21:31:26.096 1838 Recovering log #3.2021/05/04-21:31:26.141 1838 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\4a03e2b9-b11d-4d5c-be43-d5c958236abb.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\4a03e2b9-b11d-4d5c-be43-d5c958236abb.tmp	
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):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
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):	5.207922408142917
Encrypted:	false
SSDEEP:	12:daOva5KkkGHArBFUtpND/POu5f5KkkGHAryJ:wMa5KkkGgPg1f5KkkGga
MD5:	FBA1CED366D3F1C6EDE2C8B6C4B7E4C0
SHA1:	F7617066C7444E9E656C08312AD278E132A1B39F
SHA-256:	3F6D40C906CB5B5816F6FE82AC2E15677696CCE04B542A7D948E4504604BB75C
SHA-512:	A71527391A1DB9D6F58E7ED6217BED5B6C8304B70E2B881868DAD5FDFCDDC6E4999EB42132A47ADFB14577B17207BC4D4F470A9AB808853100DCD12AB2E0CEE
Malicious:	false
Preview:	2021/05/04-21:31:20.996 1828 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:31:20.999 1828 Recovering log #3.2021/05/04-21:31:21.002 1828 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.220754916780426
Encrypted:	false
SSDEEP:	12:d3va5KkkGHArqiuFUtpO/m1/POe5f5KkkGHArq2J:ta5KkkGgCgLf5KkkGg7
MD5:	A1BEB9982F5E3FCB2D745FC23B2EE031
SHA1:	2C7A2D429090FB53D9459EC980E720BD10E4628B
SHA-256:	3738643356FA896C73AEA1AFC405D0722B85044D164A9AA46216292B45F816C1
SHA-512:	ED4507031DBD66E3E8659F30EA42AD1DA5451F8C2EE956EE1E0D76F67E49FC4D36668C7D4EEF07738A74EAB83E41C485AD18C91DB22B6A8584418F9EE0F5384
Malicious:	false
Preview:	2021/05/04-21:31:20.997 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/04-21:31:21.001 1838 Recovering log #3.2021/05/04-21:31:21.003 1838 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):	38
Entropy (8bit):	1.9837406708828553

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Preview:	..&f.....&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):	5.221894877268496
Encrypted:	false
SSDEEP:	12:eva5KkkGHArAFUtpmH11/PMW5f5KkkGHArfJ:8a5KkkGgkggVf5KkkGgV
MD5:	B8C684EB2CCA235C65FEA098099691A9
SHA1:	7754C33CA7F5E02F8326264273EC6C362D0AC1E8
SHA-256:	BAAC59E14327C7883F163A1D22B2000F2D6798C84BDCF1B255A22EB78AC38B53
SHA-512:	33EF4AB1355DDC6EDBDC4C22481537944D5D4ED8193B8872DD3AC1D8C9E59F6C8EAB690931B7F4A65BC793C147121A64776AB37A298945C7CA93652EE4864F4
Malicious:	false
Preview:	2021/05/04-21:31:36.254 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/04-21:31:36.255 1838 Recovering log #3.2021/05/04-21:31:36.256 1838 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
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):	321
Entropy (8bit):	5.284461797011497
Encrypted:	false
SSDEEP:	6:mcEL+q2PWXp+N23iKKdKpIFUtpvs1ZmwPvSn1jLVkwOWXp+N23iKKdKa/WLJ:s+va5KkmFUtpk1/PqVV5f5KkaUJ
MD5:	4F49D29A323665488A0B99655897E0A0
SHA1:	5624C7F47A7F90C10D3AF1F295FBA202DD826F20
SHA-256:	0CA89D27BA8C2E2446146021167DD29660B2C8D9FB48941EB7F8BBAA6B6A28E9
SHA-512:	1B722FEC999EF12CCA5063A3C42F348A104C043CEEECBF0AB3AFD527642A2C9149E136842E198639EAAF72A345DA829F0E7527214D0A4DD73BCBCB4BA7E4D716
Malicious:	false
Preview:	2021/05/04-21:31:08.627 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/04-21:31:08.629 87c Recovering log #3.2021/05/04-21:31:08.630 87c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.344441535686488
Encrypted:	false
SSDEEP:	6:m5QL+q2PWXp+N23iKKdKks8Y5JKKhdIFUtppG1ZmwP4tQLVkwOWXp+N23iKKdKk0:ava5KkkOrsFUtpo1/PH5f5KkkOrzJ
MD5:	3BC6076F25E843ECB361D973C2BBE08C
SHA1:	2A1481C581DD386D605CB8BD65D11498C441FEA9
SHA-256:	3215F4097A7FE11BD308DA1B0447554519DDDF66E67A300579069AB3FACA106B
SHA-512:	9966D19165BD319E9E931366450DAF898D7328565ABAC19C7C0A3393981A916CD01B541D3C9A6B408D199F5E4A563A8D3F0307999EB20AF68BCD4610A2FF6BE5
Malicious:	false
Preview:	2021/05/04-21:31:23.515 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/04-21:31:23.516 1838 Recovering log #3.2021/05/04-21:31:23.517 1838 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
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:RqtgpbRqtU
MD5:	0BF970555075737D7D1447361E955CFB
SHA1:	0B9E921C5184E42C7B796F355BC55199B6697EFC
SHA-256:	71BB3B2F34AF995FBCA439C06268E65DA091FD8E60AFC63A8C09FA6AEAFF248D
SHA-512:	CC97C42A83CA8221AE6F8649A462849602D13A1E039407DBF157CBB19A73AB98B4CAB0E272D7472FA6D71D27A91C52EED9EDC3395DD7A1FAC883AE875B0B8097
Malicious:	false
Preview:	.....O.z.L.e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\b8a7d7e2-ac3f-493f-b508-d32cf340b57c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\b8a7d7e2-ac3f-493f-b508-d32cf340b57c.tmp	
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a283b9b7-c2a5-4aa9-8459-d6eac9cb2407.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):	24055
Entropy (8bit):	5.533065529028472
Encrypted:	false
SSDEEP:	384:x5ItZLlBfXY1kXqKf/pUZNCgVLH2HfDnrUmHG7HGcnTkublnx4W:ILllY1kXqKf/pUZNCgVLH2HfDrUGGLGk
MD5:	0C2A4B683F472BDEA0493EFD616ACE4D
SHA1:	C05F8E5B68801161C4C6351BF79F9D7D3DEF7641
SHA-256:	7FDEA706BD14B58864DA5F9F3F7EFD60D3299A9D8D92C33A58910740DA828B62
SHA-512:	60CF51E6531EEF56A1A359108AE4435AF98ADD5DB42D0506C878C49CA349001D3340D517CC10BFF7DE0D1ADDF482155DF66E4F6B2DB7EC70075C65DB5BB57(2
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":"13264662668603199","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\bff6522a-e2f2-4259-9ed9-806b2b8b0716.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):	4767
Entropy (8bit):	4.949943179300019
Encrypted:	false
SSDEEP:	48:YcfUkPklwHj/HcBqA8QqTlYqlQuoTw0wvAH3CH3G/s8C1Nfct/9BhUJo3KhmeSnz:n998oXfpcVyWok0JCKL8VbOTQVuwn
MD5:	E3EB39FA1FEBC7C868980954D2324A6D
SHA1:	0D203F72C1B1012317039A51C84CF0DAE694CB4A
SHA-256:	2D73D9D2DD2054218EE6B64701FADB38109A29C2A99E701D1851689AD0AFACAB
SHA-512:	58D2C73B78B82CD17F285AAAAB0F9B507137E0FB77B4BF3320FCBEB4150B505CD38FAFDA8D053F7D84F3508116765771F417858B1993BD699A188BCCE863976
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264662669051718","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.430720615038
Encrypted:	false
SSDEEP:	3:tUKDRIXUrdoEyZmwv39RIXUrdq2SV8s9RIXUrdKSWGv:m6uZmwPN9SVvNKStv
MD5:	938D040037B58E9930B2D701244A13E8
SHA1:	1D51C14E8DD4A915D5606653AF9168F2BE7E6A83
SHA-256:	D107A297696038A893A1AE6B5D0BB397D9CEA0CAC0C3F8B4353B0BF45F1D680B
SHA-512:	3FE2F8FA5674D85D27D05E33C3FA7E73827C68A86A5453A987904577D8ECAA9324E4F28E7E83FE40869797AC3F2A3E38AE7EB31E783A7FAA5975477C499406DA
Malicious:	false
Preview:	2021/05/04-21:31:20.302 864 Recovering log #3.2021/05/04-21:31:20.362 864 Delete type=0 #3.2021/05/04-21:31:20.363 864 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:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dee6b745-5d69-4ba4-804b-cbb639091c60.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):	22595
Entropy (8bit):	5.535560842075149
Encrypted:	false
SSDEEP:	384:x5ItZLlBfXY1kXqKf/pUZNCgVLH2HfDnrUHHGbnTkublMax43:ILllY1kXqKf/pUZNCgVLH2HfDrUnGbni
MD5:	6BB022C44273BFDC4B11A0CA913A4213
SHA1:	985EF2813BF9F25A0B74D25A9496431C9CADFCB4
SHA-256:	8312A11D56302F8DDF844D2BCB845FA263720B314135257C10ECF0884064933E
SHA-512:	76CDB12CD521EE040C9D5147BC35FECCDE8B3FE26C1E8A8E93F50A617A9DF2FDF8F9ACB0BA4D1F8243082421CBD933FE41EC8EBB75691C2FEEE711D75D4B 1AF
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13264662668603199","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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):	5.210418356619529
Encrypted:	false
SSDEEP:	6:m68itQL+q2PWXp+N23iKKdKfrzAdIFUtpN8CYG1ZmwPN8UQLVkwOWXp+N23iKKdn:d8eva5Kk9FUtpN8Cr1/PN8v5f5Kk2J
MD5:	A78F12A4C85DF41FF674F66DC250CA46
SHA1:	BC59A599B4F9B43F708C887CFB26FD8D0169BC15
SHA-256:	4079C60A97AB1D99041410BC562B83547E7E0904D2AEB213970498FFD2FD7C4F
SHA-512:	860902D0D4769356CAA4E916F64562A53EB160C7944BA731434FC3160A4DCD63AD293D69C23E8289607874790C19D440042FA9057699913027A4990F995D869A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/05/04-21:31:20.872 1838 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/05/04-21:31:20.873 1838 Recovering log #3.2021/05/04-21:31:20.874 1838 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.4536056456034717
Encrypted:	false
SSDEEP:	3:8EflJES+//sEZlxES+//:8z7Xs97X
MD5:	A729B7563D426F7F60392522EAE98C3C
SHA1:	82658CFE667748330B4017F69E672E6494497283
SHA-256:	5A5636C8CDD9C786AE2C5A7775BAB9D8E8C33AB8A3C94F6A39D9BF0054F76D84
SHA-512:	57098296A418B729C26BDABAF2443C69BC16E4A0E4DAA71EA7C6F4911B73D0A41C4D7CE8382F708AA75E0F922A1CB56EB4C91EA84486397BC16EC34B47C3CA 04
Malicious:	false
Preview:	.'..(.....5.# /.....'..(.....5.# /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.22.0\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.22.0\Indexing in Progress	
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir1364_1575087964\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208920
Entropy (8bit):	4.964307261909652
Encrypted:	false
SSDEEP:	3072:gzChBJeloN++/mYWcT8WSkb1RqmYb8zpoPo/smfgbpxT0C0oUBXrvzpnuidAut:5clEHRAqggCylW1
MD5:	A96F63877D2B8648563905C60513B9F0
SHA1:	EE63F5F68E176DCEA8416C9877F09533C4E5498E
SHA-256:	B5A3D515B1673D134B197878D681C0CC8290BC476EB69D69EF27FF9669EC2E80
SHA-512:	C137035D92E4161FF55AF447D61F7F61E9FB8812EF0D32649011A6D7A07AEBA317B4197CF0205B37B755FACF7A1ABCA586507A1B825BC2FD4194E8306DB4E008
Malicious:	false
Preview:	.....$...,.....C.....p.....P.....,.....geips..... n.....lgoog.....R.....ozama.....onwod.....h...(.....g.bat... ....<...@.....uotpo.....X.....ennab.....nozam.....e..l....E.....-.....l...P.....,.....\|.....h...p...H...,.....\...X...T...P.....H .....@...<...8.....d...,...(...$... .....,.....`...D.....|...x...t.....l...h...d...`.....X.....P...L...\...D. ..@...<...8...0...0..... .....`.....0.....h.....H...,.....x.....p...l...h...d...`...\...X...T...P...L...H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\a78e6f03-24c4-4552-be76-48281d91d4df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7489200208885074
Encrypted:	false
SSDEEP:	384:BHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvbpzgq2WVOgF:t6mRxCE89Qef8u0s/DWmKs2WBJ
MD5:	ABA8C108ED3459E556FE087A4A4998B6
SHA1:	70917A83147F261CA831FBBB77EA02C444EBEC53
SHA-256:	DF6B40775F62FCE5DC245DAB2586A4F32C72222B86DFF59AF6845B0009B430A9
SHA-512:	D6E8FD3A67060D855AFAD81F4B69EA3DE8E137123DA1C95D903A664AA59C57A0B684FF1A9F1037AB031B1ADB037078E35108505A2EC7E781575B197FF7D2500
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.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\ab232c17-64ff-407d-a513-bbc60f1d2427.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):	160387
Entropy (8bit):	6.052053525945578
Encrypted:	false
SSDEEP:	3072:tgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:+Er/NOX3aqfIlUOoSiuRU
MD5:	18125822E5CD511EAB8452579C312014
SHA1:	934D838238790A1223B02DB3C544414330DC8A5C
SHA-256:	F426CFA9A2A78B4F10088C909B0B7B5EC529BC33C46473DCF1456C2C9069ED15
SHA-512:	20224BFC7F1DD740786BE320F4A4205CF27B5F26F3716D596D3B44391E759A10D5D0EE73705AEE2002371A856AC97B929F95C758505C825B101A58232641628F
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\aefbdda7-d59b-4199-b750-2b6d25f835c5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\aefbdda7-d59b-4199-b750-2b6d25f835c5.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	160473
Entropy (8bit):	6.052211194684695
Encrypted:	false
SSDEEP:	3072:tjtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:hEr/NOX3aqfIlUOoSiuRU
MD5:	72C1A4D97DBCA08F9527BE4997A4756C
SHA1:	2DFC4B798605218C1E3F8DEA1929595B276BEB75
SHA-256:	BA3CA92AACB1EC014B37F0B4AC3DEA5641698B140E0D7565622125FA9BFA5679
SHA-512:	FA0BD40B8DA109CAE0C9E8ED13F10D9340024F14EE607F625E480AF0650C01B9295C546DFCE1850008CE6742E9B3FEDB400FBB76E3C5C0CB3E5CC405F88A56B2
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\bb55688a-c4e9-4793-9e23-4e31b49695af.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):	160199
Entropy (8bit):	6.051524084052077
Encrypted:	false
SSDEEP:	3072:FgtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:2Er/NOX3aqfIlUOoSiuRU
MD5:	636CD7AE83B5A637B902E41B047D805A
SHA1:	A3057C0705126FFAB38DE8561D846CCC0095E714
SHA-256:	83EB70D3C5529B4FB73CC74B46BC797EC8FAF7F3DDCDEF2FC06F9F4E0F84DB60
SHA-512:	CA70B2D6E0F798D7B3A582CC7FA280B8AB68B58E7E830A33B837B8C6318BBD2B885673E1C158051F801B9148E7507E47AE322D53F9C234D550D73EF756048712
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\bc823faf-2221-46af-ada5-00508410a0c9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7489562423803466
Encrypted:	false
SSDEEP:	384:RHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvUzgq2WVOgE2:d6mRxCEF9Qef8u0s/DWmKs2WBR
MD5:	9D9EE2D847A0307EF735D63C40FB9D46
SHA1:	214019E8B1E69BA7215D57653AB56BE06231536D
SHA-256:	776F91663D6E6249B662647D60A1996A21CCFC68BDF3F12A9219F686CD0912D0
SHA-512:	E48DDAB8AC51B0000BBF241D47BE2060D9952BF5B5E6E9D4B6C430934E7ACDEC8B391F14155221B8E91D8ABC1EF06F448E24512D2470915C7AFE435318B63C3
Malicious:	false
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....98.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\d854af62-2091-452e-974e-9e20cd323a15.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):	159928
Entropy (8bit):	6.050876497601597

C:\Users\user\AppData\Local\Google\Chrome\User Data\d854af62-2091-452e-974e-9e20cd323a15.tmp	
Encrypted:	false
SSDEEP:	3072:LMtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:QEr/NOX3aqfIlUOoSiuRU
MD5:	9A1E63269A5CEBBD71C9F112A93566E4
SHA1:	6305BB14A32C4E31D22B95B4B2D0E3501067C593
SHA-256:	A5AD5BBB939F07E1851BBD87E3509CEE4B6D7F8AFE4FB8C3E9267E1EE2123CD2
SHA-512:	44798EF3C3ADB20BE94552D585B2C022234CB4F00573F5D600D73D87495A96E3446502D75E63DE30DE85D42BE50E59873375A098EE3559380B5C964421582AB5
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\f0061e94-74a2-423f-bbb7-e3323322c992.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):	160473
Entropy (8bit):	6.052211194684695
Encrypted:	false
SSDEEP:	3072:tjtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:hEr/NOX3aqfIlUOoSiuRU
MD5:	72C1A4D97DBCA08F9527BE4997A4756C
SHA1:	2DFC4B798605218C1E3F8DEA1929595B276BEB75
SHA-256:	BA3CA92AACB1EC014B37F0B4AC3DEA5641698B140E0D7565622125FA9BFA5679
SHA-512:	FA0BD40B8DA109CAE0C9E8ED13F10D9340024F14EE607F625E480AF0650C01B9295C546DFCE1850008CE6742E9B3FEDB400FBB76E3C5C0CB3E5CC405F88A56B2
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ffbff902-081f-4a6a-ac72-354a3364ac8c.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):	159842
Entropy (8bit):	6.050703975119525
Encrypted:	false
SSDEEP:	3072:jtkHD12oBp3YPi1OXZFcbXafIB0u1GOJmA3iuRU:jEr/NOX3aqfIlUOoSiuRU
MD5:	0CA9812A143F855228BCCDF65454A4B0
SHA1:	FD5748D8EF60B0CD38E3D87A9338E710C55D32A1
SHA-256:	071040A397125249BE1D070B20037A693A9D43C8CE3C4C7DB23947CE462701C0
SHA-512:	40FFE50293E5664DD657AAAFCDFE2FB3168DEC10B477198137D773D16FA2735EAB1A98CE956E7AE2C1121DC1B1CD4D3FAEF81D9C6F750F4A9261F416346D328
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":1.620189071968968e+12,"network":1.620156673e+12,"ticks":101987015.0,"uncertainty":4805323.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016581700"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\1364_1177258535\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):	3.8930693175496365
Encrypted:	false
SSDEEP:	3:SUnVaQhScJ1ZQAQcISUaHt/QdTgdL:SUV4cJ1ZVQcISUu/gcL
MD5:	F59ECC2CE0B171DEF3F23762AB413CC0

C:\Users\user\AppData\Local\Temp\1364_1177258535\manifest.fingerprint	
SHA1:	9A6FC649656C9E109C29092B826BF95A786B7171
SHA-256:	AD708E42FDCD11998DDBBBA651EBE1F7B520168A2DD8EACE1DDE49AAB954FF32
SHA-512:	60CA66134171A1F990762561EDA12D6BB1693D699D2FEF2B0C705C7A9B26105E19BCE341914AB07E63CEAACEC6E2B5ABF5BC1BAE75837DD40C66B650BB3F3E2C
Malicious:	false
Preview:	1.1f2c1b01f5f8279f0b0acd2ee595877a0e3011fb0b50aa49a3873836cdb008c9

C:\Users\user\AppData\Local\Temp\1364_1295231640\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):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B56D
Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\1364_1493249959\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):	3.872935977280404
Encrypted:	false
SSDEEP:	3:S0bEVMqCVQD5mhG8d6+qGn:SGlQUhG8Im
MD5:	A43371DACA3F176ED5A048BC5E2899B1
SHA1:	32FC0A9ECB568BDF3CE13F9EA17E827A900EDB42
SHA-256:	736DB43A7CCB37136CAEFF0B80670BD76BFE528203856CB19CB6C3D161B48F9C
SHA-512:	8754C5D823A9EED2749852B37084F5ED14176B6CB74D946CA3F152DD91F2C03CC4457F1CA0219D883522C7213C4CD04FCD2E33BBB31C7F7EBD6968CEE35AF91
Malicious:	false
Preview:	1.a8a79d350c2a5e3bc36226633a8e0bed0dfab184e77f38fc8f0820ebacf8eafc

C:\Users\user\AppData\Local\Temp\1364_1543410132\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):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\1364_2104900616\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):	3.8661423255272727
Encrypted:	false
SSDEEP:	3:SS2BBS0XnGJHXhcWeVxObhNIL:SSmBSmnGJHdMsI
MD5:	8067D1C22DD706E20C3B1B1C6A64B0B8

C:\Users\user\AppData\Local\Temp\1364_2104900616\manifest.fingerprint	
SHA1:	2BDA3268F06E453ADAB2EDFB9F0585BB306122B4
SHA-256:	1AA6AF004762782DD8FA229C950C90946FA71145F3F12C6CE078F85FD2E7EFF6
SHA-512:	27E66AF3F49C5E6F7C5D3153CDCED0A63B1ADCEAC06AF5660354B1C71C05780A0D2D0364A852A5DEF9B2D917740C0C66A53BDF59DD1C0B2B9538AFC6BDA9 B2
Malicious:	false
Preview:	1.749cadd76db233b1ee2c3051cb01c2d2393e2d293df1042f7f00343bf458f6bf

C:\Users\user\AppData\Local\Temp\1364_2128964736\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):	3.89429824295036
Encrypted:	false
SSDEEP:	3:SRwGXyUtz24TSXhV6DDt5WBG9EBn:SGGXyA5kDoDt5WwaBn
MD5:	7FB6C0307DFC7235990A87216D6EFE79
SHA1:	9C86024DE6EE647227E73C5905468DB9C31D8447
SHA-256:	F01B98701AE70087F82AAC256AB3ECFB736F4865B7DF915051C7D5B1C51BA78E
SHA-512:	AC7106F2503DB666C4B3A382587C9DAE424CC5692D75E555D1F6BC0E4F4B3A360B82C1C356D06E4F607EA40206699191F5F206979E67B9614F1DE2073D5B0E40
Malicious:	false
Preview:	1.4dcc255c0d82123c9c4251bb453165672ea0458f0379f3a7a534dc2a666d7c6d

C:\Users\user\AppData\Local\Temp\1364_311365399\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):	3.9038730072798953
Encrypted:	false
SSDEEP:	3:SbE71mckqWGMdKHSDX5QCdM:Semn5xvM
MD5:	0E19773D8AE759FFA0271FDB6E99998D
SHA1:	91D4B7813D8056F43A02A6CCCA86CA751949AC68
SHA-256:	5581125D97967B76F685C2149D3E1F68AABC3E533357A710A71E11395B77DCF8
SHA-512:	313ACBD2ABE980AF30AF98FB3D4C09CC07394A035D893F8BFA616DD17829BFF663AAF4419AFA79918D322838440482A0D533CE84411F680FDE6766B84CBEC3D
Malicious:	false
Preview:	1.cacf8de20a51296cf5c0975b99bfbc8e21dec29872fb7f1ca6a88432a6db68f5

C:\Users\user\AppData\Local\Temp\1598f9c3-7357-47dd-9fa3-a498be3fc401.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\1e40bdb3-90f8-4609-b269-58206566e4ad.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

C:\Users\user\AppData\Local\Temp\1e40bdb3-90f8-4609-b269-58206566e4ad.tmp	
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\221935d5-357b-48c1-9171-812e9e248ec7.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\3e73ca80-00c5-4bc3-9e4f-9bfa18ec9c10.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	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...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\8745ee7f-ca99-4ee4-a6a8-1fe6a73c2a41.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\957d89ea-283c-4003-ad2f-a6b7b92fdf8d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\957d89ea-283c-4003-ad2f-a6b7b92fdf8d.tmp	
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	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...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.721743409135556
TrID:	
File name:	test.html
File size:	3804
MD5:	0d80b3a43db9adf29fe973890a099230
SHA1:	2d5984c3f0f77273bc7c896a0be318000a790e06
SHA256:	edd93d70b8455e9ac5462e8488ce717c7baea2960c6bfece09b7b5855b267ae5
SHA512:	1cba3687fb3df63770630ce2e78795a4a18e958d83fba2e1dad9753083033513551160 58b930a08936effcca23b3e1ecc589ad0f4f6eb374e8dd1786d0f6be90
SSDEEP:	96:REaKX0rxXqfARGRqIdQ3OuoTbbdddddQmAZPmEaFWRijsjl6r+dTd6CxddddSdy:REaKqxXeSkqIdQPoLAPmEakwjwl0hKOW
File Content Preview:	<HTML><HEAD>..<BODY text=black vLink=blue aLink=blue link=blue background=https://dl.dropboxusercontent.com/s/kegpfj8ltyjjh24/00

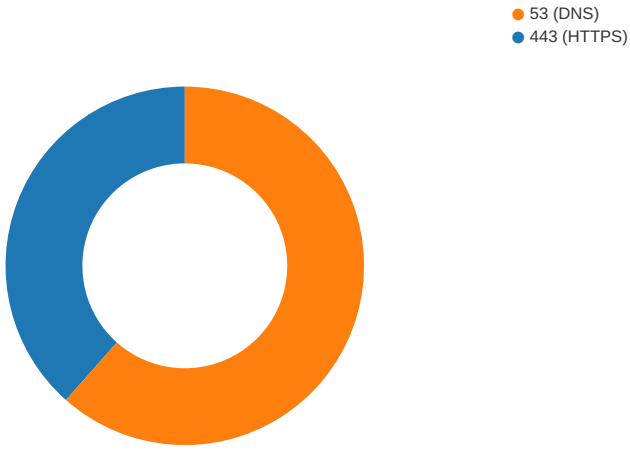
File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

Total Packets: 117



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:31:13.242908001 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.283674002 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.283747911 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.284122944 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.324613094 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.326141119 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.326251984 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.326277018 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.326302052 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.423311949 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.646224022 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.653721094 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.654769897 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.688112020 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.688258886 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.688420057 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.694294930 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.694360971 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.694422960 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.694549084 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:13.728986025 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:13.776447058 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:14.434364080 CEST	443	49718	162.125.66.15	192.168.2.3
May 4, 2021 21:31:14.533716917 CEST	49718	443	192.168.2.3	162.125.66.15
May 4, 2021 21:31:20.515403032 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.556054115 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.556207895 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.556596041 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.597218037 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604736090 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604772091 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604796886 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604820013 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604835033 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.604845047 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604863882 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.604865074 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.604902029 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.627722025 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.627890110 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.628035069 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.668703079 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.668955088 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.668979883 CEST	49740	443	192.168.2.3	216.58.212.129

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:31:20.671344995 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.671375990 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.671437979 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.671462059 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.672712088 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.672744989 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.672796965 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.672818899 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.675555944 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.675585985 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.675642967 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.675663948 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.678411961 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.678438902 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.678492069 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.678515911 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.681261063 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.681294918 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.681339979 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.681363106 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.684175968 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.684205055 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.684259892 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.684283972 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.687022924 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.687048912 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.687103987 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.687127113 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.709600925 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.709640026 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.709733963 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.712107897 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.712143898 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.712239981 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.713815928 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.713848114 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.713917017 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.716717958 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.716753960 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.716836929 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.719532013 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.719563007 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.719640017 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.722445011 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.722479105 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.722556114 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.725295067 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.725326061 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.725404978 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.728108883 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.728138924 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.728208065 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.730988979 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.731020927 CEST	443	49740	216.58.212.129	192.168.2.3
May 4, 2021 21:31:20.731096983 CEST	49740	443	192.168.2.3	216.58.212.129
May 4, 2021 21:31:20.733786106 CEST	443	49740	216.58.212.129	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:31:01.876580954 CEST	51281	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:01.925213099 CEST	53	51281	8.8.8.8	192.168.2.3
May 4, 2021 21:31:02.666968107 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:02.717161894 CEST	53	49199	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:31:03.810715914 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:03.859483957 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 21:31:04.289700985 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:04.351452112 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:31:04.959203959 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:05.007961035 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 21:31:06.124047041 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:06.172646999 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 21:31:07.111855984 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:07.161488056 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 21:31:08.289643049 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:08.343251944 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 21:31:11.221234083 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:11.269926071 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 21:31:12.053652048 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:12.114181995 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 21:31:12.948057890 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:12.996725082 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.156373024 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.163664103 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.166074991 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.172125101 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.178762913 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.199301958 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.208146095 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.217549086 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.234276056 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.237246037 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.238224030 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.266357899 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.741081953 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:13.806297064 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 21:31:13.946532965 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:14.008666992 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 21:31:14.967133045 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:15.015921116 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 21:31:15.869213104 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:15.920013905 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:31:17.081713915 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:17.130340099 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 21:31:20.263642073 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:20.315210104 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 21:31:20.448879004 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:20.514200926 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 21:31:21.288999081 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:21.353879929 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 21:31:22.576968908 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:22.638094902 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:31:28.335658073 CEST	61946	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:28.393551111 CEST	53	61946	8.8.8.8	192.168.2.3
May 4, 2021 21:31:29.284343958 CEST	64910	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:29.341562033 CEST	53	64910	8.8.8.8	192.168.2.3
May 4, 2021 21:31:30.439621925 CEST	52123	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:30.488363981 CEST	53	52123	8.8.8.8	192.168.2.3
May 4, 2021 21:31:33.918288946 CEST	56130	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:33.981005907 CEST	53	56130	8.8.8.8	192.168.2.3
May 4, 2021 21:31:34.052241087 CEST	56338	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:34.101037025 CEST	53	56338	8.8.8.8	192.168.2.3
May 4, 2021 21:31:35.296056986 CEST	59420	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:35.346163034 CEST	53	59420	8.8.8.8	192.168.2.3
May 4, 2021 21:31:48.476492882 CEST	58784	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:48.525176048 CEST	53	58784	8.8.8.8	192.168.2.3
May 4, 2021 21:31:55.523838043 CEST	63978	53	192.168.2.3	8.8.8.8
May 4, 2021 21:31:55.580960989 CEST	53	63978	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:32:09.104996920 CEST	62938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:09.162009954 CEST	53	62938	8.8.8.8	192.168.2.3
May 4, 2021 21:32:09.774445057 CEST	56803	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:09.853010893 CEST	53	56803	8.8.8.8	192.168.2.3
May 4, 2021 21:32:10.029920101 CEST	57145	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:10.091953039 CEST	53	57145	8.8.8.8	192.168.2.3
May 4, 2021 21:32:10.151515961 CEST	55359	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:10.208436966 CEST	53	55359	8.8.8.8	192.168.2.3
May 4, 2021 21:32:21.609605074 CEST	58306	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:21.668294907 CEST	53	58306	8.8.8.8	192.168.2.3
May 4, 2021 21:32:51.107208967 CEST	64124	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:51.166763067 CEST	53	64124	8.8.8.8	192.168.2.3
May 4, 2021 21:32:52.890180111 CEST	49361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:52.938837051 CEST	53	49361	8.8.8.8	192.168.2.3
May 4, 2021 21:32:59.592417955 CEST	63150	53	192.168.2.3	8.8.8.8
May 4, 2021 21:32:59.650298119 CEST	53	63150	8.8.8.8	192.168.2.3
May 4, 2021 21:33:00.485061884 CEST	53279	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:00.547405958 CEST	53	53279	8.8.8.8	192.168.2.3
May 4, 2021 21:33:07.625998020 CEST	56881	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:07.691529989 CEST	53	56881	8.8.8.8	192.168.2.3
May 4, 2021 21:33:07.821106911 CEST	53642	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:07.881432056 CEST	53	53642	8.8.8.8	192.168.2.3
May 4, 2021 21:33:08.049726963 CEST	55667	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:08.117106915 CEST	53	55667	8.8.8.8	192.168.2.3
May 4, 2021 21:33:18.126023054 CEST	54833	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:18.202529907 CEST	53	54833	8.8.8.8	192.168.2.3
May 4, 2021 21:33:32.551460028 CEST	62476	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:32.602210999 CEST	53	62476	8.8.8.8	192.168.2.3
May 4, 2021 21:33:35.618284941 CEST	49705	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:35.686999083 CEST	53	49705	8.8.8.8	192.168.2.3
May 4, 2021 21:33:54.814011097 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:54.968372107 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 21:33:55.548418045 CEST	61633	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:55.676798105 CEST	53	61633	8.8.8.8	192.168.2.3
May 4, 2021 21:33:56.303064108 CEST	55949	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:56.360555887 CEST	53	55949	8.8.8.8	192.168.2.3
May 4, 2021 21:33:56.853671074 CEST	57601	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:56.910931110 CEST	53	57601	8.8.8.8	192.168.2.3
May 4, 2021 21:33:57.489049911 CEST	49342	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:57.548988104 CEST	53	49342	8.8.8.8	192.168.2.3
May 4, 2021 21:33:58.504998922 CEST	56253	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:58.554064035 CEST	53	56253	8.8.8.8	192.168.2.3
May 4, 2021 21:33:59.291910887 CEST	49667	53	192.168.2.3	8.8.8.8
May 4, 2021 21:33:59.354084015 CEST	53	49667	8.8.8.8	192.168.2.3
May 4, 2021 21:34:00.120939016 CEST	55439	53	192.168.2.3	8.8.8.8
May 4, 2021 21:34:00.177953959 CEST	53	55439	8.8.8.8	192.168.2.3
May 4, 2021 21:34:01.033034086 CEST	57069	53	192.168.2.3	8.8.8.8
May 4, 2021 21:34:01.084623098 CEST	53	57069	8.8.8.8	192.168.2.3
May 4, 2021 21:34:01.599133015 CEST	57659	53	192.168.2.3	8.8.8.8
May 4, 2021 21:34:01.648022890 CEST	53	57659	8.8.8.8	192.168.2.3
May 4, 2021 21:34:12.263885975 CEST	54717	53	192.168.2.3	8.8.8.8
May 4, 2021 21:34:12.323267937 CEST	53	54717	8.8.8.8	192.168.2.3
May 4, 2021 21:34:58.163832903 CEST	63975	53	192.168.2.3	8.8.8.8
May 4, 2021 21:34:58.223764896 CEST	53	63975	8.8.8.8	192.168.2.3
May 4, 2021 21:35:05.545073986 CEST	56639	53	192.168.2.3	8.8.8.8
May 4, 2021 21:35:05.615334988 CEST	53	56639	8.8.8.8	192.168.2.3
May 4, 2021 21:35:55.643764973 CEST	56546	53	192.168.2.3	8.8.8.8
May 4, 2021 21:35:55.704031944 CEST	53	56546	8.8.8.8	192.168.2.3
May 4, 2021 21:35:56.268413067 CEST	62152	53	192.168.2.3	8.8.8.8
May 4, 2021 21:35:56.328387022 CEST	53	62152	8.8.8.8	192.168.2.3
May 4, 2021 21:36:00.367847919 CEST	53470	53	192.168.2.3	8.8.8.8
May 4, 2021 21:36:00.439852953 CEST	53	53470	8.8.8.8	192.168.2.3
May 4, 2021 21:36:02.203162909 CEST	56446	53	192.168.2.3	8.8.8.8
May 4, 2021 21:36:02.279720068 CEST	53	56446	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:36:55.577301025 CEST	59631	53	192.168.2.3	8.8.8.8
May 4, 2021 21:36:55.635873079 CEST	53	59631	8.8.8.8	192.168.2.3
May 4, 2021 21:36:59.549320936 CEST	55515	53	192.168.2.3	8.8.8.8
May 4, 2021 21:36:59.607582092 CEST	53	55515	8.8.8.8	192.168.2.3
May 4, 2021 21:38:53.742898941 CEST	64547	53	192.168.2.3	8.8.8.8
May 4, 2021 21:38:53.822531939 CEST	53	64547	8.8.8.8	192.168.2.3
May 4, 2021 21:38:53.971136093 CEST	51759	53	192.168.2.3	8.8.8.8
May 4, 2021 21:38:54.029278994 CEST	53	51759	8.8.8.8	192.168.2.3
May 4, 2021 21:39:06.310743093 CEST	59207	53	192.168.2.3	8.8.8.8
May 4, 2021 21:39:06.359432936 CEST	53	59207	8.8.8.8	192.168.2.3
May 4, 2021 21:39:09.731457949 CEST	54269	53	192.168.2.3	8.8.8.8
May 4, 2021 21:39:09.780673027 CEST	53	54269	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:31:13.178762913 CEST	192.168.2.3	8.8.8.8	0x52c1	Standard query (0)	dl.dropbox usercontent.com	A (IP address)	IN (0x0001)
May 4, 2021 21:31:20.448879004 CEST	192.168.2.3	8.8.8.8	0x42d8	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:31:13.238224030 CEST	8.8.8.8	192.168.2.3	0x52c1	No error (0)	dl.dropbox usercontent.com	edge-block-www-env.dropbox-dns.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:31:13.238224030 CEST	8.8.8.8	192.168.2.3	0x52c1	No error (0)	edge-block-www-env.dropbox-dns.com		162.125.66.15	A (IP address)	IN (0x0001)
May 4, 2021 21:31:20.514200926 CEST	8.8.8.8	192.168.2.3	0x42d8	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuserc ontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:31:20.514200926 CEST	8.8.8.8	192.168.2.3	0x42d8	No error (0)	googlehost ed.l.googl euserconte nt.com		216.58.212.129	A (IP address)	IN (0x0001)
May 4, 2021 21:35:55.704031944 CEST	8.8.8.8	192.168.2.3	0x1b75	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	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
May 4, 2021 21:31:13.326277018 CEST	162.125.66.15	443	192.168.2.3	49718	CN=*.dl.dropboxusercontent.com, O="Dropbox, Inc", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 19 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Tue Feb 15 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1364 Parent PID: 4232

General

Start time:	21:31:07
Start date:	04/05/2021
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\test.html'
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: 6160 Parent PID: 1364

General

Start time:	21:31:09
Start date:	04/05/2021
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=1628,16747573067059828566,6713175093340114276,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /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

Disassembly