ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
Full analysis:	https://app.any.run/tasks/cfabeeac-484e-4001-90fd-1c021774e295
Verdict:	Malicious activity
Analysis date:	March 18, 2022 at 21:26:40
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	⧉
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	42E52B8DAF63E6E26C3AA91E7E971492
SHA1:	98B3FB74B3E8B3F9B05A82473551C5A77B576D54
SHA256:	A294620543334A721A2AE8EAAF9680A0786F4B9A216D75B55CFD28F39E9430EA
SSDEEP:	192:76f0CW5P2Io4evFrDv2ZRJzCn7URRsjVJaZF:76fPWl24evFrT2ZR5Cn7UR0VJo

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

Internet Explorer 11.0.9600.19596 KB4534251
Adobe Acrobat Reader DC (20.013.20064)
Adobe Flash Player 32 ActiveX (32.0.0.453)
Adobe Flash Player 32 NPAPI (32.0.0.453)
Adobe Flash Player 32 PPAPI (32.0.0.453)
Adobe Refresh Manager (1.8.0)
CCleaner (5.74)
FileZilla Client 3.51.0 (3.51.0)
Google Chrome (86.0.4240.198)
Google Update Helper (1.3.36.31)
Java 8 Update 271 (8.0.2710.9)
Java Auto Updater (2.8.271.9)
Microsoft .NET Framework 4.5.2 (4.5.51209)
Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)

Hotfixes

Client LanguagePack Package
Client Refresh LanguagePack Package
CodecPack Basic Package
Foundation Package
IE Hyphenation Parent Package English
IE Spelling Parent Package English
IE Troubleshooters Package
InternetExplorer Optional Package
InternetExplorer Package TopLevel
KB2479943
KB2491683
KB2506212
KB2506928
KB2532531
KB2533552
KB2533623
KB2534111
KB2545698
KB2547666
KB2552343
KB2560656
KB2564958
KB2574819
KB2579686
KB2585542
KB2604115
KB2620704
KB2621440
KB2631813
KB2639308
KB2640148
KB2653956
KB2654428
KB2656356
KB2660075
KB2667402
KB2676562
KB2685811
KB2685813
KB2685939
KB2690533

Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972
Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461

Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102

Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Reads the computer name

a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 3532)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2636)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 3428)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 584)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2644)

Checks supported languages

a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 3532)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 584)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 3428)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2636)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2644)

Executed via COM

DllHost.exe (PID: 3148)

Modifies files in Chrome extension folder

chrome.exe (PID: 3868)

INFO

Manual execution by user

a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 584)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2644)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 2636)
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe (PID: 3428)
chrome.exe (PID: 3868)

Checks supported languages

DllHost.exe (PID: 3148)
chrome.exe (PID: 3868)
chrome.exe (PID: 3460)
chrome.exe (PID: 3944)
chrome.exe (PID: 3720)
chrome.exe (PID: 2416)
chrome.exe (PID: 1716)
chrome.exe (PID: 2980)
chrome.exe (PID: 2316)
chrome.exe (PID: 900)
chrome.exe (PID: 2752)
chrome.exe (PID: 120)
chrome.exe (PID: 3008)
chrome.exe (PID: 3128)
chrome.exe (PID: 1164)

Reads the computer name

DllHost.exe (PID: 3148)
chrome.exe (PID: 3868)
chrome.exe (PID: 3944)
chrome.exe (PID: 2980)
chrome.exe (PID: 2416)
chrome.exe (PID: 3008)

Application launched itself
chrome.exe (PID: 3868)

Reads settings of System Certificates
chrome.exe (PID: 3944)

Reads the hosts file
chrome.exe (PID: 3868)
chrome.exe (PID: 3944)

Static information

TRiD

.dll	Win32 Dynamic Link Library (generic) (43.5)
.exe	Win32 Executable (generic) (29.8)
.exe	Generic Win/DOS Executable (13.2)
.exe	DOS Executable Generic (13.2)

EXIF

EXE

Subsystem:	Windows GUI
SubsystemVersion:	5.1
ImageVersion:	0
OSVersion:	5.1
EntryPoint:	0x1000
UninitializedDataSize:	0
InitializedDataSize:	1024
CodeSize:	7168
LinkerVersion:	10
PEType:	PE32
TimeStamp:	2022:03:14 08:19:36+01:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	14-Mar-2022 07:19:36

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x000000C8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	14-Mar-2022 07:19:36
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE

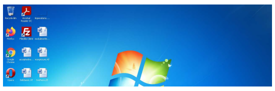
Sections

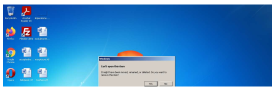
Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x00001B4A	0x00001C00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	5.64424
.rdata	0x00003000	0x0000006A	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	0.988058
.reloc	0x00004000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.0815394

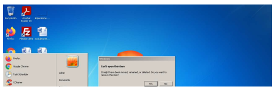
Imports

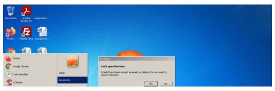
NETAPI32.dll

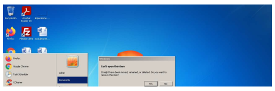
Video and screenshots

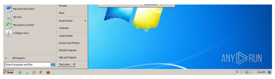
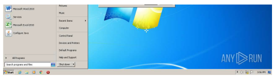
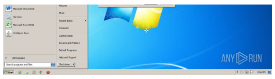
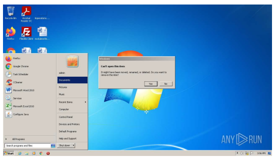
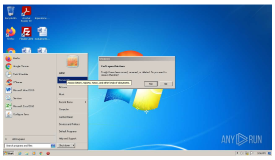
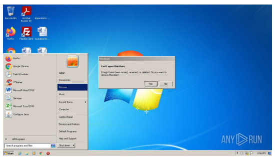
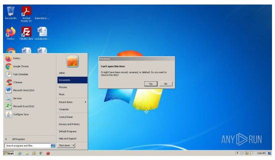
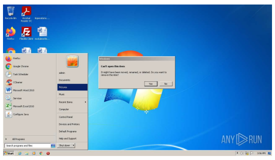
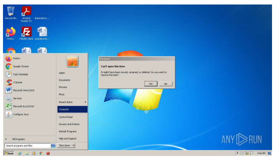
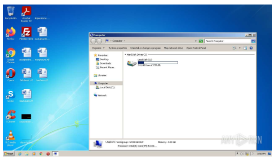
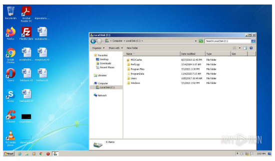
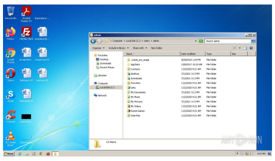
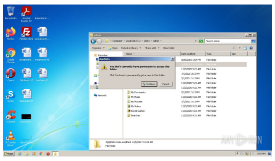
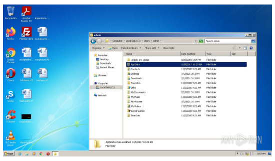
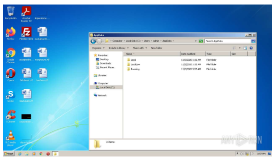
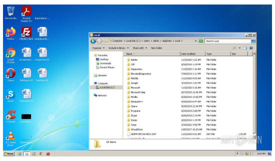
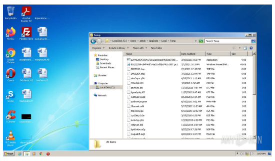
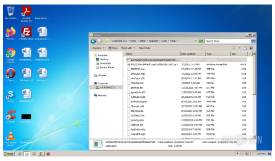
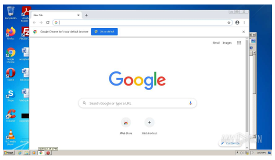
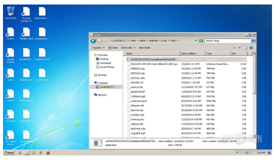








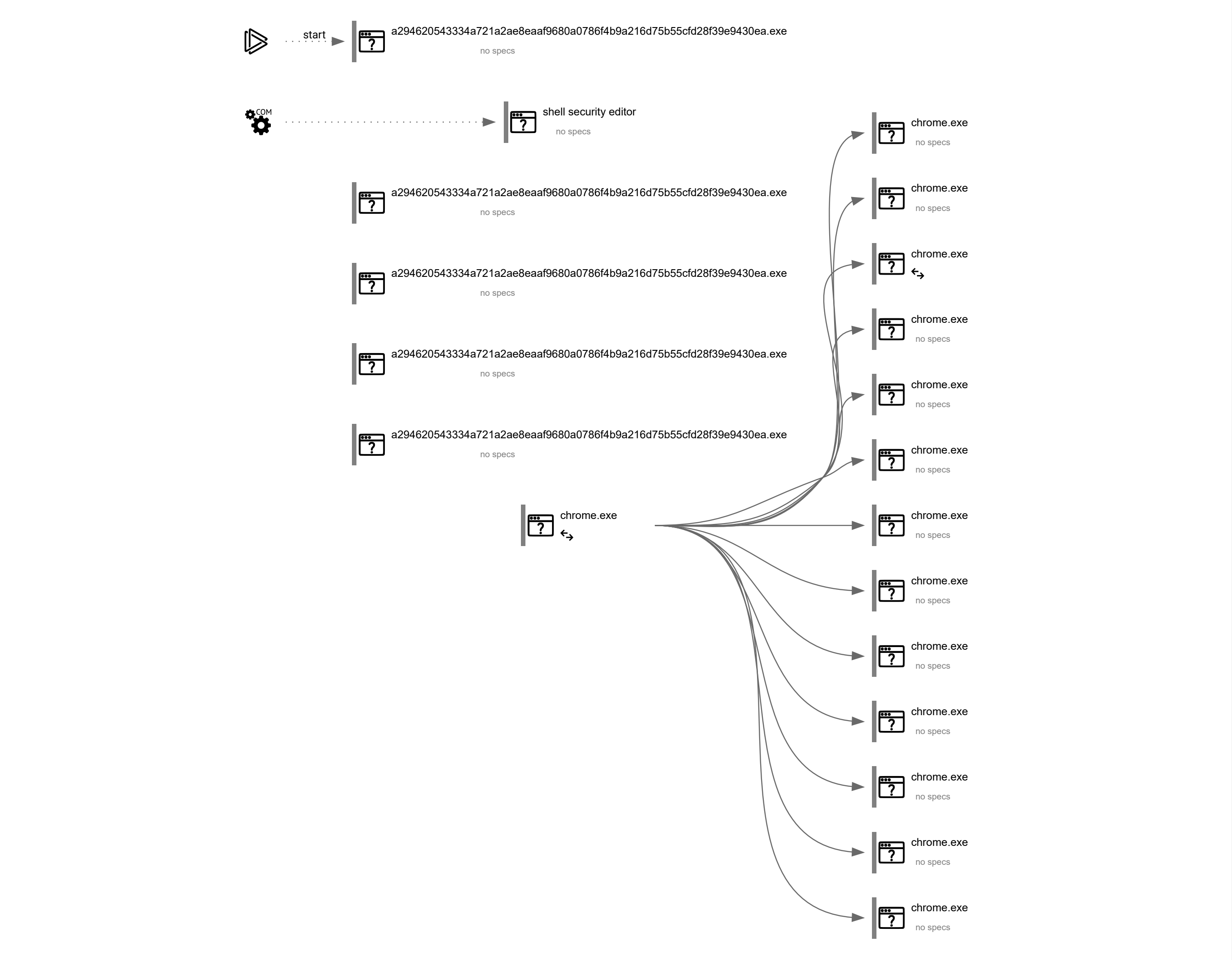


Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
59	20	0	0

Behavior graph


start
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
no specs
COM
shell security editor
no specs
chrome.exe
no specs
chrome.exe
no specs
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
no specs
chrome.exe
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
no specs
chrome.exe
no specs
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
no specs
chrome.exe
no specs
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe
no specs
chrome.exe
no specs
chrome.exe
chrome.exe
no specs
chrome.exe
no specs
chrome.exe
no specs
chrome.exe
no specs
chrome.exe
no specs
chrome.exe
no specs
chrome.exe
no specs

Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
3532	"C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe"	C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe	—	Explorer.EXE
Information User: admin Integrity Level: MEDIUM				
3148	C:\Windows\system32\DllHost.exe /Processid:{4D111E08-CBF7-4F12-A926-2C7920AF52FC}	C:\Windows\system32\DllHost.exe	—	svchost.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	COM Surrogate
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

584	"C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe"	C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe	—	Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM

2636	"C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe"	C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe	—	Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM

2644	"C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe"	C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe	—	Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM

3428	"C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe"	C:\Users\admin\AppData\Local\Temp\a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea.exe	—	Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM

3868	"C:\Program Files\Google\Chrome\Application\chrome.exe"	C:\Program Files\Google\Chrome\Application\chrome.exe	⇆	Explorer.EXE

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	3221225547	**Version:**	86.0.4240.198

3460	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win32 --annotation=prod=Chrome --annotation=ver=86.0.4240.198 --initial-client-data=0xc8,0xcc,0xd0,0x9c,0xd4,0x6bd2d988,0x6bd2d998,0x6bd2d9a4	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

3008	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --gpu-preferences=MAAAAAAAAADgAAAwAAAAAAAAAAAAAAAAAABgAAAAAAAQAAAAAAAAAAAAAAAAAAAKAAAAAQAAAAgAAAAAAAAACgAAAAAAAAAMAAAAAAAAAA4AAAAAAAAABAAAAAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAABAAAABQAAABAAAAAAAAAAAQAAAAYAAAA= --mojo-platform-channel-handle=1048 /prefetch:2	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

3944	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=network --mojo-platform-channel-handle=1344 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	⇆	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

900	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

--renderer-client-id=6 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1960 /prefetch:1

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

1716 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --instant-process --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1968 /prefetch:1 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

3128 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --extension-process --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=4 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2300 /prefetch:1 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

2980 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --gpu-preferences=MAAAAAAAAADgAAAwAAAAAAAAAAAAAAAAAABgAAAAAAAQAAAAAAAAAAAAAAAAAAAAKAAAAAQAAAAgAAAAAAAAACgAAAAAAAAAMAAAAAAAAAAAA4AAAAAAAAAABAAAAAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAAAAABAAAABQAAABAAAAAAAAAAAQAAAAYAAAA= --use-gl=swiftshader-webgl --mojo-platform-channel-handle=1100 /prefetch:2 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

2752 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=2940 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

3720 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=2948 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

2416 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=3224 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

2316 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=3304 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

120	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=3204 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

1164	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1064,12233388988462466603,18149781038876488604,131072 --enable-features=PasswordImport --disable-gpu-compositing --lang=en-US --extension-process --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=13 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3200 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	86.0.4240.198

Registry activity

Total events	Read events	Write events	Delete events
10 210	10 149	60	1

Modification events

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	failed_count
Value:	0		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	2		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:			

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:	01000000		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	1		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	dr
Value:	1		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome
Operation:	write	**Name:**	UsageStatsInSample
Value:	0		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
Operation:	write	**Name:**	usagestats
Value:	0		

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	metricsid
Value:			

(PID) Process:	(3868) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	metricsid_installdate
Value:	0		

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_enableddate
Value: 0

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13292092654911289

(PID) Process: (3944) chrome.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2416) chrome.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 1

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: delete key **Name:** (default)
Value:

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** ahfgeienlihckogmohjhadlkjgocpleb
Value: 15B1C3FE35F29528448F36A72A4DFBC58A8083C7190559D25865779166D220A2

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** apdfllckaahabafndbhieahigkjlhalf
Value: 911FE281CB88E8A6F8160E6417E4D83AF994824282798F4E7C2B33539ADC400A

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** blpcfgokakmgnkcojhhkbfbldkacnbeo
Value: 62C1A8BE68517759276CD5C4651DDE462F78AD56FF85C2E9473CB6BAC4BE2502

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** gfdkimpbcpahaombhbimeihdjnejgicl
Value: D6B079666F209503A09486C70AC09307652A0F7F783166A999B27C99D0DA79E2

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** kmendfapggjehodndflmmgagdbamhnfd
Value: E2FAFB5D51EEBE04A784740B11C6BA5B456D2A9E82CD008676C2D9453EFDE151

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** mfehgcgbbipciphmccgaenjidiccnmng
Value: 63355C14E8C7DF9A075F2EDDEA6F2807DC8166B83F96F4C975B9B6554C6324D7

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** mhjfbmdgcfjbbpaeojofohoefgiehjai
Value: 0E265BFED6F1C7D5F0A9BD790C50BB30E78E959631D51EEBB8BB0DE73E65763C

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** neajdppkdcdipfabeoofebfddakdcjhd
Value: 04A45240BDA55E8777FA04357712CA6DD942253A21323E4C7D3CCF769B34BFED

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** nkeimhogjdpnpccoofpliimaahmaaome
Value: 66D2E99AA8898940E49FE7278CF49621C6A74B34CB7C6DDC7F2A9F5AB065D54D

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** nmmhkkegccagdldgiimedpiccmgmieda
Value: 41926B40FCCC9FCFB72069FD2021D8E95037E332BE35B95DE0F694FF540D51AE

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** pjkljhegncpnkpknbcohdijeoejaedia
Value: 8F2892D07F5A7E08016D511C2CE6340132FC564675968393126070DFB7534F0B

(PID) Process: (3868) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Chrome\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** pkedcjkdefgpdelpbcmbmeomcjbeemfm
Value: 075D52643A72C98410EF2C6F5A06A10F9ADC44D50DDFF2CC2FFE32C81B77E67E

Files activity

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	125	99	9

Dropped files

PID	Process	Filename	Type
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-6234ABEE-F1C.pma **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\8a774720-55fa-4f5b-a7dd-3ada80789d7b.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old~RF138cd2.TMP **MD5:** 81F483F77EE490F35306A4F94DB2286B **SHA256:** 82434CE3C9D13F509EBEEBE3A7A1A1DE9AB4557629D9FC855761E0CFA45E8BCE	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** 5BD3C311F2136A7A88D3E197E55CF902 **SHA256:** FA331915E1797E59979A3E4BCC2BD0D3DEAA039B94D4DB992BE251FD02A224B9	text
3460	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma **MD5:** 03C4F648043A88675A920425D824E1B3 **SHA256:** F91DBB7C64B4582F529C968C480D2DCE1C8727390482F31E4355A27BB3D9B450	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat **MD5:** 9C016064A1F864C8140915D77CF3389A **SHA256:** 0E7265D4A8C16223538EDD8CD620B8820611C74538E420A88E333BE7F62AC787	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** 7721CDA9F5B73CE8A135471EB53B4E0E **SHA256:** DD730C576766A46FFC84E682123248ECE1FF1887EC0ACAB22A5CE93A450F4500	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old **MD5:** 8FF312A95D60ED89857FEB720D80D4E1 **SHA256:** 946A57FAFDD28C3164D5AB8AB4971B21BD5EC5BFFF7554DBF832CB58CC37700B	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF138ca3.TMP **MD5:** 936EB7280DA791E6DD28EF3A9B46D39C **SHA256:** CBAF2AFD831B32F6D1C12337EE5D2F090D6AE1F4DCB40B08BEF49BF52AD9721F	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Version **MD5:** 00046F773EFDD3C8F8F6D0F87A2B93DC **SHA256:** 593EDE11D17AF7F016828068BCA2E93CF240417563FB06DC8A579110AEF81731	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF138cb3.TMP **MD5:** 64AD8ED3E666540337BA541C549F72F7 **SHA256:** BECBDB08B5B37D203A85F2E974407334053BB1D2270F0B3C9A4DB963896F2206	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF138d7e.TMP **MD5:** B628564B8042F6E2CC2F53710AAECDC0 **SHA256:** 1D3B022BDEE9F48D79E3EC1E93F519036003642D3D72D10B05CFD47F43EFBF13	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old~RF138d7e.TMP **MD5:** 109A25C32EE1132ECD6D9F3ED9ADF01A **SHA256:** DA6028DB9485C65E683643658326F02B1D0A1566DE14914EF28E5248EB94F0DD	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old **MD5:** EF1D5606A483BB6C72C81A3F649BEB18 **SHA256:** BA083E7585ADA9936944FE56BC0141A544F18A01C3424E5C9F02375B34FE3D45	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old **MD5:** 995C92837E4775CAFFE387D51ADBA520 **SHA256:** 51247C3464FD988B72670002D01A57FBFF1348704D325DC8FF8817ED2459D0D9	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	vxd
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	vxd
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	vxd
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	vxd
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\index **MD5:** 192DEC91856E6735A1840FCD52AAE412 **SHA256:** 84097D40090156703AA1ABF3BC8E50BE1D6D460F252C331CA582E4E67A7C6B0A	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\92e8db6b-6f7c-47c4-9a7e-bb1fb0618c67.tmp **MD5:** 234EB77DCF95DB860753816910220743 **SHA256:** F2D20160C629C0C8D91C211DD4CFB1C671439249CA56A1C92B3FF11C9BA71547	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RF1398c8.TMP **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old **MD5:** 65437A648AB4EED358D296AE5DB81808 **SHA256:** C6AB5DB9378697E010D932185EE531F0755B570333766D18061755AE794CF0EE	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000001 **MD5:** 22B4EDAEC3A626EC661176B076112373 **SHA256:** 91FB3DE4447D630452F32D035EB25B626F0B42C5AE525812098114A2D0F3CCBB	binary

3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences **MD5:** 234EB77DCF95DB860753816910220743 **SHA256:** F2D20160C629C0C8D91C211DD4CFB1C671439249CA56A1C92B3FF11C9BA71547	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old~RF139619.TMP **MD5:** B973CC8BF1E257F9D170AAB59E6BFF06 **SHA256:** E24E8FE6AA3B1AFC2639480FA25247157E6B9AB54B98D0BAE221C2CD81C6F312	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old~RF138fa1.TMP **MD5:** D0BA19096D6C8F8DE58312E8D938E893 **SHA256:** AADE90A7B0984F3C719D528E4E6FAE3854E28B30363BDD4DF65037E69784A078	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF138e59.TMP **MD5:** 8304B8F42465198890090F52D3F80A4C **SHA256:** 80C32AC2585E7E81200104B1630F19560A156C4ABF51B5888B0FBF07323FAB34	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF139a6e.TMP **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old **MD5:** 5202CA4D6AF0C37DAEC0D528CC7F2986 **SHA256:** 8F5B8FF94B14C36EA0CBE8FA0A4D165A632B45F834BBB7239E1A6CF6685F256C	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1 **MD5:** 31C8C67916A1702C81696616CE7B0AC5 **SHA256:** 0264388DCA7D2423EC8E618C208D13422095742465376055FBC3A7B3F7223044	binary
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000002 **MD5:** FD380F307128BD80ACB3BAF69C14DD29 **SHA256:** 957D496AAF177D4AB51AA8101444ED854717CE1636BE015D4735CEFE9185DEF4	compressed
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF13935a.TMP **MD5:** D097F8EB2230B3F32C41C5D75790508C **SHA256:** ADDF87D20CD455CFB4AACB6B76719629C0277A4CF70B496343047BB73ABBAEF5	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000003 **MD5:** 70AE354CE421C724F886E84C9E5BDBE6 **SHA256:** 3FBA20649C9805C920ACACF297D0E2863EFF51C3992925374D634C94781119AD	compressed
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2c0a182ba780eff_0 **MD5:** 398011B4683413DC93093F11E2763CCC **SHA256:** 38C18852B580778937AAC0E8EAFE5A997348BACF372976C0C29AC1ADB248E5FF	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d3930873ee9f7f3_0 **MD5:** 33497858041F7CB78E18394F93F9DEBB **SHA256:** 5D29D96C0CD2B62FCD86DA9413E7C6FE697EF231BF864F9B9B6537D45BA2E124	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF139ba7.TMP **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RF139ca1.TMP **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Browser **MD5:** DE9EF0C5BCC012A3A1131988DEE272D8 **SHA256:** 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000060.dbtmp **MD5:** B0AC49FE387A1BED707F5AFF6F5F0412 **SHA256:** 9F9119402BB9B1D4F0BE1B26A43CB8233020C3FA7E6A1920D49284FFC6B543A4	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT~RF13980d.TMP **MD5:** E07C42D7821C8F460A8FC0C66BA65220 **SHA256:** 83CB24EE8B10CE9367F2788B95F21213C9C3AC7E50F068AC02439CCBB6EB7664	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old **MD5:** C960873C82FE2F69D8D319C001702441 **SHA256:** F88954FF7E77321B897574FC15B66CFEA0FA15A1099FC9AA8FC5835C5929921B	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old~RF1398c8.TMP **MD5:** 4F7AAE850B0F55DDC8CAB17285E0D8E9 **SHA256:** D05F4DAF70FACA1E9BCC1E2B14AC972D76623A5A4CD287CE8187A80CCAB0AF30	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT **MD5:** B0AC49FE387A1BED707F5AFF6F5F0412 **SHA256:** 9F9119402BB9B1D4F0BE1B26A43CB8233020C3FA7E6A1920D49284FFC6B543A4	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old **MD5:** 6A39437279C0A015F6913A843A96C74B **SHA256:** E2DC12D58075F50E95F0F98CF06D667B77385D18C87BE66F03CB59C6322C2373	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary

3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old~RF139d3d.TMP **MD5:** E33F74D1E35FB99C1644C43F3ED0AFD7	**SHA256:** 069104171E482C24B0D33CB121437599564A519005E2C3212A34773065BBD71D	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** E6A3408AA37852852A8028197A697BD3	**SHA256:** C214EC5EE62ABE38C1AA154F98C59988B6535B8D1512B28FB1ECFF978CDF4BC7	text
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\bg\messages.json **MD5:** D7A97183BCBD5FB677AA84D464F0C564	**SHA256:** 76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old **MD5:** 127179B7B6612EC3F7521B44F1CCD969	**SHA256:** 4281117BB71D1C8D5571E7DB5E8493E4DD3F9E60670678AB8CBC6C685EE443BA	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_url_fetcher_3868_1522501945\1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx **MD5:** 541F52E24FE1EF9F8E12377A6CCAE0C0	**SHA256:** 81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82	crx
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\ca\messages.json **MD5:** 58BA5F65ED971591D1F9D81848EE31D0	**SHA256:** CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old~RF139d3d.TMP **MD5:** 65F7BEE92771101B63D90E31DB82105A	**SHA256:** A0B0D20056D7798BA6CF228F8BC1D7B7FC894DDB01343158368F80ADA145E622	text
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\da\messages.json **MD5:** 31264DDBF251A95DE82D0A67FA47DB3A	**SHA256:** EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\cs\messages.json **MD5:** 43161EFFA28A0DBFC67B8F7DBE1B5184	**SHA256:** 3A04421DF5218E8ABD3B0E2AFE11E8338D7BDCBCD1ADB122416944B102BC9696	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\en_GB\messages.json **MD5:** DBEDF86FA9AFB3A23DBB126674F166D2	**SHA256:** C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\el\messages.json **MD5:** 3026E922B17DBEE2674FDAEE960DF584	**SHA256:** 876845B5A061FAB3CF2A1466E01015DC40DF8449F1CB4205F575CEBED8717BAD	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\en\messages.json **MD5:** DBEDF86FA9AFB3A23DBB126674F166D2	**SHA256:** C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\hr\messages.json **MD5:** 9CF848209FF50DBF68F5292B3421831C	**SHA256:** EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\es\messages.json **MD5:** 3F4B0F56C2839839FC3E3270ED4CB7B6	**SHA256:** 1912EA5E0A62BBC669DC14AB5A5BD5514B0502C483EE1F27C3F8834384187079	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\fr\messages.json **MD5:** 1E32A78526E3AC8108E73D384F17450B	**SHA256:** 80F6EE69F1E022812BCCC1DE1CDC53772CDF90F4E93224161B23FA607D45136A	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\hi\messages.json **MD5:** B739E3B798D3EEB8AFB3E368455A8E97	**SHA256:** BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\fi\messages.json **MD5:** E5BBE7DBBE75F45BDCD49DB8C797106E	**SHA256:** BFFB2248B4C66306133FA6ECBB1541F44B3BE22CC8D9A338D690E0B1D0C85532	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\et\messages.json **MD5:** 0293A7BAE6EEE62C4067A80E262D6A2D	**SHA256:** D06F20D4D68D1DBB89EF7D8E405D9499CB2EB2560217CD5B4A51AB1DD50CAB44	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\de\messages.json **MD5:** 7639B300B40DDAF95318D2177D3265F9	**SHA256:** 356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\fil\messages.json **MD5:** 658DAD2AF2DC3AC1567D84E8B95F68B0	**SHA256:** 978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\es_419\messages.json **MD5:** 1FD5DAF46C4D7C4F571C263EC37B943B	**SHA256:** BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\id\messages.json		binary

		MD5: 9008516AA1D8F8C2B8ECE70B7E4963AD **SHA256:** 89CAB0AF2B53C6ABEB93C8C628DDCBDD286A7A2672FE03440411BB654E3A0675	
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\hu\messages.json **MD5:** 4AD92AFDE3408FBBE43B0C3C71677650 **SHA256:** 61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\it\messages.json **MD5:** BB9C32BA62DDA02F9471C64B5F9CF916 **SHA256:** 43A0B113D3773BA78F82BB9E42DDC46F6892D0FBBB351F94A7C105E4A146E9C1	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\pt_BR\messages.json **MD5:** 1F4BC8A5EFD59D61127ABEECD4B6CAE3 **SHA256:** E1950CBBF056F068EA56160DDB318F3E6232BFBBE096D221C7CA6FCAACE2A8B9	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\pt_PT\messages.json **MD5:** D80ECE7E4B3741CD9CD29B89D006B864 **SHA256:** C8FF9ACAEA1D3B6F8483339CB40F66BC563CCA8DD87F2337F813C492B20F451B	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\lv\messages.json **MD5:** 1D21ED2D46338636E24401F6E56E326F **SHA256:** 434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\ja\messages.json **MD5:** 96C8CBD161D3CE9CB1A46CB2CD0C6583 **SHA256:** 81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\ro\messages.json **MD5:** D63E66B94A4EA2085D80E76209582FB1 **SHA256:** 91A5AAD210C3E0241106E8821B3897EDEFEC9D85033C94DB2324FF3A5FDE5AC7	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\ru\messages.json **MD5:** 22F9E62ABAD82C2190A839851245A495 **SHA256:** 9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\nl\messages.json **MD5:** E7F74DCE7B6411E4E0D95E9252CF74FA **SHA256:** 3564AEF46C01602B19CC29FD8A79676C543427EDE98206D0C91B33AF0CCF3977	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\sl\messages.json **MD5:** F45DE58765A37FD095319D7DEB0F2FB6 **SHA256:** 8366774AA582035BC7D949F4E28FAEC371C305D01404DF56FFF5A78B4F6ECDB7	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\sk\messages.json **MD5:** 4BBAA10FD00AADBBA3EF6E805E8E1A62 **SHA256:** 906C4F7FDDE15DE4C841E7910BBF14D9175E894BCB244B56E8447A5ADFA5B7AB	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\pl\messages.json **MD5:** E16649D87E4CA6462192CF78EBE543EC **SHA256:** EB435F7460A63576CA1ECB51948E7A3AD5168D2F175AE2B5836D469672923D84	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\lt\messages.json **MD5:** 41F2D63952202E528DBBB683B480F99C **SHA256:** FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\sr\messages.json **MD5:** 92C1FAC62EB7F92EC3794D4A141BEF32 **SHA256:** 9DF154C93B02695AF1CC39F085D9D178EC6AF131A62C2AFC65F125F8F9A5B7AC	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\sv\messages.json **MD5:** 6E1BE9CEE29818E54E3D1C7D483DD6F7 **SHA256:** E348583D8C53F4A5DEC4551DA93785C17108466E427E06F84708AA383EA0E326	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\ko\messages.json **MD5:** 3CAF23A8EA2332D78B725B6C99EC3202 **SHA256:** BFE72BBC492B9018A599CB6575366696E431E6A38400E4B2ED06EAE3340D3AE5	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\nb\messages.json **MD5:** 8F0168B9A546D5A99FD8A262C975C80E **SHA256:** F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\th\messages.json **MD5:** 283D5177FB2FC7082967988E2683EC7C **SHA256:** E8D5820BDE31B66A7641068FDEDD1A5F20C1A783460B98887A670F38422099CF	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\zh_CN\messages.json **MD5:** 393680A09DEE0CB9046A62BDC0750B74 **SHA256:** D5FB52C2897FD5C294784DB63C933AC77C609D10AC91431CCB295D87452CBEE6	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\css\craw_window.css **MD5:** 67BF9AABE17541852F9DDFF8245096CD **SHA256:** 10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC	text
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\topbar_floating_button_hover.png **MD5:** 7CB6B9DC1A30F63B8BD976924B75AD96 **SHA256:** 721B7AAA9A42A54A349881615A12E3A26983ACA48E173FD2F66E66AA0D725735	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\craw_window.js **MD5:** 1709B6F00A136241185161AA3DF46A06 **SHA256:** 5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8	text
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_metadata\verified_contents.json **MD5:** 0834821960CB5C6E9D477AEF649CB2E4 **SHA256:** 52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69	ini
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\topbar_floating_button_maximize.png **MD5:** 232CE72808B60CBE0F4FA788A76523DF **SHA256:** AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\craw_background.js **MD5:** 6EEBED29E6A6301E92A9B8B347807F5F **SHA256:** 04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697	text
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\topbar_floating_button_pressed.png **MD5:** E0862317407F2D54C85E12945799413B **SHA256:** 5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\flapper.gif **MD5:** 398ABB308EEBC355DA70BCE907B22E29 **SHA256:** 2B73533F47A99FFEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\zh_TW\messages.json **MD5:** CD30D132A7213FC1B7E03C6D0A49CCF7 **SHA256:** 5717F13D10E63255947F750C79CBB6BD04A6D97A08261E8D5764AF5EB0561A28	binary

2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\icon_16.png **MD5:** 344554D96E418120BD80EF5DE5194697	**SHA256:** 0A4BD08DB6422F8E7A8A218EF39C1B99A5A675F12697F26BE88F9AFC2E1F9378	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\tr\messages.json **MD5:** 1BF2AA4BB904B406C9C2B7DF769BB540	**SHA256:** 0F2E8285BA3E2BDBA6B16435FB941B07159AACFAC80196AD5941B79AB52B712A	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\icon_128.png **MD5:** 30899B6C4E4A757B8EC6DD2208ACDFB4	**SHA256:** 4F17EFBD974A41D88CB36567AAB6BF4586579E78780F00B1826676819E14BFF4	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\html\craw_window.html **MD5:** 34A839BC40DEBC746BBD181D9EF9310C	**SHA256:** BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D	html
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\topbar_floating_button.png **MD5:** 8803665A6328D23CC1014A7B0E9BE295	**SHA256:** D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C	image
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\manifest.json **MD5:** 6CA25F3EF585B63F01BCDF8635120704	**SHA256:** 49D9DE983F7436BA786E6E04A5A20C10F41687AE06B266B1B6553F696719563D	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\vi\messages.json **MD5:** 7D52E9357AB847B4CC8DBC8CC4DA93F5	**SHA256:** 313F71F3FFDCEFC76FC746FF2029FBF8FBE38BD83DCF952FC3DDCD8AA96D5CFB	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257_locales\uk\messages.json **MD5:** FD1C9890679036E1AD914218753B1E8E	**SHA256:** 39D19CC3387FFCE13A8F11DAD72E2FCBB7CD1A4367EC699AD7C40D6F52ECE717	binary
2316	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\images\topbar_floating_button_close.png **MD5:** 0599DFD9107C7647F27E69331B0A7D75	**SHA256:** 131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937	image
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\3868_207315257\manifest.fingerprint **MD5:** FD2735A192CC8F477E246787039A0128	**SHA256:** 8D5308C605A6D16C18F8C4170B30177992669477707383F53C9FD6FB0E5A5BE7	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log **MD5:** 51A2CBB807F5085530DEC18E45CB8569	**SHA256:** 1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG **MD5:** B1DF9E2B1A92BFFF6B31E7D9FCF93C82	**SHA256:** 49A758A5EDFAD8020706C7A5B8D8292B3AC41EB14775ACFB746764F4C6BBD72A	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\es_419\messages.json **MD5:** 6B2583D8D1C147E36A69A88009CBEBC7	**SHA256:** 6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\et\messages.json **MD5:** CFF6CB76EC724B17C1BC920726CB35A7	**SHA256:** C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\cs\messages.json **MD5:** 76DEC64ED1556180B452A13C83171883	**SHA256:** 32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\en\messages.json **MD5:** 91F5BC87FD478A007EC68C4E8ADF11AC	**SHA256:** 92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\es\messages.json **MD5:** 82719BD3999AD66193A9B0BB525F97CD	**SHA256:** 4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\en_GB\messages.json **MD5:** 91F5BC87FD478A007EC68C4E8ADF11AC	**SHA256:** 92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\bg\messages.json **MD5:** 6F8E288A9AD5B1ED8633B430E2B4D4CA	**SHA256:** A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\fil\messages.json **MD5:** 57AF5B654270A945BDA8053A83353A06	**SHA256:** EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL\images\icon_128.png **MD5:** 4DBC9F9E6F5A08D299BAC9E54DF07694	**SHA256:** 91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E	image
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\0bd11f59-4829-4691-a33e-07aec14afb6b.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D	**SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL\images\icon_16.png **MD5:** FB9C46EA81AD3E456D90D58697C12C06	**SHA256:** 016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8	image
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\ca\messages.json **MD5:** 1FDAFC926391BD580B655FBAF46ED260	**SHA256:** C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\da\messages.json **MD5:** 238B97A36E411E42FF37CEFAF2927ED1	**SHA256:** 4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\fi\messages.json **MD5:** 3A01FEE829445C482D1721FF63153D16	**SHA256:** 0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\de\messages.json **MD5:** 6B3E916E8C1991AA0453CBA00FEDCAAA	**SHA256:** A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\fr\messages.json **MD5:** 8D11C90F44A6585B57B933AB38D1FFF8	**SHA256:** 599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\el\messages.json		binary

			MD5: 05C437A322C1148B5F78B2F341339147	**SHA256:** A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070	
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\hr\messages.json	**MD5:** 8185D0490C86363602A137F9A261CC50	**SHA256:** A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\hu\messages.json	**MD5:** 85609CF8623582A8376C206556ED2131	**SHA256:** 32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\pt_BR\messages.json	**MD5:** 86A2B91FA18B867209024C522ED665D5	**SHA256:** 6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\ja\messages.json	**MD5:** 9B3A5D473C3F2BBFAEECE94A07A940B8	**SHA256:** 706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\nb\messages.json	**MD5:** 93C459A23BC6953FF744C35920CD2AF9	**SHA256:** 2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\nl\messages.json	**MD5:** 7A8F9D0249C680F64DEC7650A432BD57	**SHA256:** 92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\hi\messages.json	**MD5:** E376D757C8FD66AC70A7D2D49760B94E	**SHA256:** 8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\pt_PT\messages.json	**MD5:** 750A4800EDB93FBE56495963F9FB3B94	**SHA256:** C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\ko\messages.json	**MD5:** 9F6B4D82A70C74CA751E2EAE70FAB5CF	**SHA256:** D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\lv\messages.json	**MD5:** C5CE2C51391EAFD3DA9E4C71549A3C28	**SHA256:** 1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\pl\messages.json	**MD5:** 0E6194126AFCCD1E3098D276A7400175	**SHA256:** E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\it\messages.json	**MD5:** A328EEF5E841E0C72D3CD7366899C5C8	**SHA256:** CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\ro\messages.json	**MD5:** 98D43E4B1054A65DF3FA3CC40AB6FB6D	**SHA256:** 113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\id\messages.json	**MD5:** EAB2B946D1232AB98137E760954003AA	**SHA256:** C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\lt\messages.json	**MD5:** 4CA644F875606986A9898D04BDAE3EA5	**SHA256:** 7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\ru\messages.json	**MD5:** DB2EDF1465946C06BD95C71A1E13AE64	**SHA256:** FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\th\messages.json	**MD5:** 83E2D1E97791A4B2C5C69926EFB629C9	**SHA256:** 2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\sr\messages.json	**MD5:** D485DF17F085B6A37125694F85646FD0	**SHA256:** 7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old	**MD5:** 23FE827C759C66B4BF79534F0382B7F5	**SHA256:** 8AEB5A8D1604E253BD3545D587604ED5D1899950C7FD82C4B809A9D04D296F2C	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\vi\messages.json	**MD5:** 7EBB677FEAD8557D3676505225A7249A	**SHA256:** 051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\uk\messages.json	**MD5:** AB0B56120E6B38C42CC3612BE948EF50	**SHA256:** 68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\sk\messages.json	**MD5:** 8DF215D1EFBDABB175CCDD68ED8DCB0A	**SHA256:** 7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old	**MD5:** CB7250236EB5BEED080D36E442095200	**SHA256:** 717EB0AC0830309A339AC7C7DBD3260B435DB0C870E38BDD11336787791087D4	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Code Cache\wasm\index-dir\temp-index	**MD5:** BF8675476C927350111A10C1F2379702	**SHA256:** EA2CF435DAFFFDAE92BEF441B2F1B3DED8A33D31180A54A64A5C911FCD681071	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Code Cache\wasm\index	**MD5:** 54CB446F628B2EA4A5BCE5769910512E	**SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\sv\messages.json	**MD5:** D372B8204EB743E16F45C7CBD3CAAF37	**SHA256:** B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\tr\messages.json	**MD5:** 2CEAE0567B6BB1D240BBAD690A98CA3B	**SHA256:** A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\zh_CN\messages.json			binary

				MD5: BB73BF561BB79F89D9BF7C67C5AE5C65	**SHA256:** D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Code Cache\wasm\index-dir\the-real-index	binary	**MD5:** BF8675476C927350111A10C1F2379702	**SHA256:** EA2CF435DAFFFDAE92BEF441B2F1B3DED8A33D31180A54A64A5C911FCD681071
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\sl\messages.json	binary	**MD5:** 3943FA2A647AECEDFD685408B27139EE	**SHA256:** 18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old~RF13a200.TMP	text	**MD5:** 6FE92100838F65D6CB564D68D48C0659	**SHA256:** 469B11DE5E2A5742926B6E04D22E03BAC570E0D365EAFFB09300D93A0F0E2834
3868	chrome.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3868_568463570\CRX_INSTALL_locales\zh_TW\messages.json	binary	**MD5:** 5FF50C673CC0C661D615F0CFD0E6DCA0	**SHA256:** C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\MANIFEST-000001	binary	**MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	binary	**MD5:** 90F880064A42B29CCFF51FE5425BF1A3	**SHA256:** 965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico	image	**MD5:** 6C53108C981C84582B760DAD57E31D37	**SHA256:** AC7BFF1AE4531A65D6CAFBEA3B3B1189AF82E98E1BB535494B66C404DAC89F52
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\ef1fa932-c212-4c7a-895a-2e105e046c90.tmp	image	**MD5:** 6C53108C981C84582B760DAD57E31D37	**SHA256:** AC7BFF1AE4531A65D6CAFBEA3B3B1189AF82E98E1BB535494B66C404DAC89F52
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\CURRENT	text	**MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\000001.dbtmp	text	**MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	text	**MD5:** 1F12A768BF443D9F54F9099162B26C24	**SHA256:** AB528197F2EFD9D361C4F43B6782F2EC08D5FCE008C05BB6F2FD8B0A08F47A25
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\MANIFEST-000001	binary	**MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF13a2bb.TMP	text	**MD5:** 736F7579F0521DAF5695CD8A3B3CDA6A	**SHA256:** 10A24B1012BEF30456C31ABB66DF14CE66BAAA78C450A87E3E647A9E44E31E8E
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13292092654692164	binary	**MD5:** BDAD6E55EAB9D62B6FB3137C02675131	**SHA256:** 9349757E9E06AE6DC1107EBBC03DB910BA20DC2E2040A511CB64FEE746FBE5FE
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State	text	**MD5:** 904833CC0700A9C766FB3D60CAA27CE1	**SHA256:** B84BF2F985C89174AF9B4E0E23A24BD009FE199610922602D4CBA4F168F5113F
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000001.dbtmp	text	**MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	text	**MD5:** 57BE1D3E99A867A7BF4363C0C8CAD0DC	**SHA256:** E837748C274C512673BF955593A3A058C00B4E3C913A443B5D41C7AE63908AB4
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	text	**MD5:** 0C1617783481B9E51CC7070C9AADF7FA	**SHA256:** CD9E300C347C65FA18D1922059A7E6E6CB90FEED16530C934133B77EAF4DE711
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	text	**MD5:** 3C56FDFD05B0FD000E29948E405FA702	**SHA256:** 2E7DDB66FE3D7FD4ED94A2D7026DA4C5D5B74165A66376E61468540339988D1C
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\CURRENT	text	**MD5:** 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000003.log	binary	**MD5:** 0407B455F23E3655661BA46A574CFCA4	**SHA256:** AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	text	**MD5:** 58FDA100CA5911922D20B75B3C9E5B39	**SHA256:** 2F9B1B10F5B7C53C967EA59D8BFC767F2E6705A9460C2B571473E1776093EB71
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000003.log	binary	**MD5:** 0407B455F23E3655661BA46A574CFCA4	**SHA256:** AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\a8c7d469-08a4-4754-8fec-84c7f5ec2ad8.tmp	text	**MD5:** 904833CC0700A9C766FB3D60CAA27CE1	**SHA256:** B84BF2F985C89174AF9B4E0E23A24BD009FE199610922602D4CBA4F168F5113F
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	binary	**MD5:** BD801702CED176F23BA015B6CC8E6DA4	**SHA256:** 102EAE254047DB640C2C5106BEC330C3304106B6DF9F4518C80D849D9A721199
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	text	**MD5:** E83D837F58A820D952D9D522D44B7F2C	**SHA256:** 8CF4BAFD13BEEED6DC6955C5F425272585C09F6D6B4B6C9D0D62A6D8D10D79D9
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	bc		

		MD5: 36AE1954407F66426D7A59FBED3BFF78 **SHA256:** 526EE965C4B5F54395D0E0DC0171D3BB7711BEBB2CFC8FB560A679625A0E67B8	
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000008.log **MD5:** 9686F5BDA57B4399F789F261B9734D4D **SHA256:** 00184F1857E18A970D0B791DF50954C2678C34D0F51E70D75E89B822DEFFC279	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13292092654771164 **MD5:** 0686D6159557E1162D04C44240103333 **SHA256:** 3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000003.log **MD5:** 0407B455F23E3655661BA46A574CFCA4 **SHA256:** AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG **MD5:** 00478610EAF8ED91378E9A16372CA950 **SHA256:** 22546660DC6EEA743F51D5A831E863F044E3FCED7C7490A09497D06D2DC4D48C	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG **MD5:** 116D6A8CCB388C964555BA1A76F3F0BD **SHA256:** C86C0CA06A7540DD4707DF4C89E8F7B52D1295825251EA48688528F6174D4119	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG **MD5:** 6735BC97B42A96C83798A77BE590DA77 **SHA256:** 9A02DDB856ED7434A5204C6C32FF309401A60DADE8A4B2C204CAEEA49B69B1DF	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG **MD5:** 17116DC77A2E72FBA9903C26E913796C **SHA256:** 3F28E1509AB9E6AB413222906F6E57E8351A18854197D2A347A53FC91235592A	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG **MD5:** 2445114F09568F99217C08F2297BD8C3 **SHA256:** E0DB91A7C32916375E63BB772B35D81E33C48863B0136387BC130A0BE325F14D	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG **MD5:** D23F4A45571E5957A686B01633770C6A **SHA256:** 0B559248E84DB4F6B8EAC8E6E8F5D57D57A9D5E8CE353ACB34AAF3BE42166AAE	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000060 **MD5:** 5702F00F119BB0DCCCB7C1ECB800663E **SHA256:** 5705A2EB7712163A2602AB9ABAA9CE6174CC687890D2DC62738FAEF1B70BF5C1	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\000003.log **MD5:** AF1D95E1F9EB485393273B25446E1AE5 **SHA256:** 48D535BB330519C00D150578734C6CECB056C4B5CDD2A45C70590BC896D27D9F	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log **MD5:** 9F7EADC15E13D0608B4E4D590499AE2E **SHA256:** 5C3A5B578AB9FE853EAD7040BC161929EA4F6902073BA2B8BB84487622B98923	bc
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG **MD5:** 54C4DE9674E08B351C0590BCE1E1663C **SHA256:** 7E501A3AF0CF6A00FA92621D72036A7CD85A2F9A292D2A93FCBD42A6EA14C918	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG **MD5:** 435206198DF4A52752F51299DDA66253 **SHA256:** 93D9710F1E69A39DCCCCD1F58DA7F7186FDF1AD78288FC4543383FDF2A95C83F	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000003.log **MD5:** 849FE4D16141183CFF89B64F91DFE852 **SHA256:** 33875972F4BB2B793BA28878084F027CC4ABA416BE2D4D791E64F129AF6E2AB0	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG **MD5:** 6F1D06B038AF2428C3446CE4F4781BF6 **SHA256:** C83F539CC0514454FDC2FB93384D1171707877B39BF770AA70F03CED71311913	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log **MD5:** 6340A67001EEC7E9085E77B313707DF9 **SHA256:** 8F6FA11DED3DCD00867B3ACCFC809F3C875693CCDB99E03C7458D125103EB75C	binary
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal **MD5:** — **SHA256:** —	—
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal **MD5:** — **SHA256:** —	—
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG **MD5:** A3DC79D85382C6F51288E8FA95F8037C **SHA256:** B26103B75524143C675430482C6CE849CE8531165FDCD7FEF7D5DC2A890D7D5A	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG **MD5:** A568BEF9C96C0F40A15DCB92FAEA3C03 **SHA256:** 0E6FF6CC9F2704BAC013AC8558ECEDCF8C28FF2F33AB902E3DBA01D6C52BBAE6	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG **MD5:** 94C6F4ED296326D1ADDFE70504583BA0 **SHA256:** 4632A75CBE11242E5AAF9F209961A3281EEA452A42C9925F8990A91DCBCB71A5	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\4a9a8314-dccf-4697-a880-21c3ecfd0f90.tmp **MD5:** 9EBE73E92B06D03E2756CCDFD0B8055A **SHA256:** 7A05958990911A968D137D000AF91B95829BAC99BE1780BB2F7A8208B5E6C93B	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log **MD5:** FBE7019C87A334DDDEF9CBABC58DDD36 **SHA256:** 933AFC1FD66370964663FBB5972CD71D64DC9A4315B57DC8C6011DD232D511DC	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index **MD5:** F691572258E2AB530415A13D714CBADA **SHA256:** 4B44E948C3A24669E372F59A8D82706BE16EC649D2F9B3D98C994AD0F54A4EDC	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index~RF13a2cb.TMP **MD5:** 6FDF73939B99AFAF0DC885DC84462478 **SHA256:** CC37EFCEC0293964EF7D1D6EF310DD08EE07A6C784902B1EBCB52A50DC7F73C6	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences **MD5:** 9EBE73E92B06D03E2756CCDFD0B8055A **SHA256:** 7A05958990911A968D137D000AF91B95829BAC99BE1780BB2F7A8208B5E6C93B	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences~RF13a2db.TMP	text

		MD5: 33538D5FFA7F34D464A51D2E2A4DD017 **SHA256:** 6E4944C2C41916BDEFCD76273F04D2874F3E10CEF29EA13A7071C4B6028C358A	
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\eb4b3a80-9475-4dfb-a5fc-83cb8873d122.tmp **MD5:** 5E5D73BAB2D5820115FA780C7BEDCC60 **SHA256:** 19EF22F0DF6EE496EAF55616BC9262A0283524F6C7842DAC08CD58646717F50C	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF13a2db.TMP **MD5:** 234EB77DCF95DB860753816910220743 **SHA256:** F2D20160C629C0C8D91C211DD4CFB1C671439249CA56A1C92B3FF11C9BA71547	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\775e43e7-2d83-4964-a65d-e33e45d0ab87.tmp **MD5:** 904833CC0700A9C766FB3D60CAA27CE1 **SHA256:** B84BF2F985C89174AF9B4E0E23A24BD009FE199610922602D4CBA4F168F5113F	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index **MD5:** F691572258E2AB530415A13D714CBADA **SHA256:** 4B44E948C3A24669E372F59A8D82706BE16EC649D2F9B3D98C994AD0F54A4EDC	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF13a2db.TMP **MD5:** 904833CC0700A9C766FB3D60CAA27CE1 **SHA256:** B84BF2F985C89174AF9B4E0E23A24BD009FE199610922602D4CBA4F168F5113F	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cookies **MD5:** 1180432906293772C725603F07E500ED **SHA256:** 4ED70F74089DF558C3708B8FEFB740846664ACEEEA3863E957F3D03594B06A76	sqlite
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL **MD5:** 8BEB65A3FD3EE6D4B26CF6510E5AEB7C **SHA256:** EF2723FF13A492640B7EEA205AB7CAE827204CE1FE2FF3E5C8F6349EF59F0F36	sqlite
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache **MD5:** A9851AA4C3C8AF2D1BD8834201B2BA51 **SHA256:** E708BE5E34097C8B4B6ECB50EAD7705843D0DC4B0779B95EF57073D80F36C191	binary
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\5b2a2139-4bac-4bbf-8d92-a47879e50bde.tmp **MD5:** 18BF20C018B56BE7E13250820D2E8467 **SHA256:** 29EF8DE7E5436796CCAB044959EB9C91E867A9E4CE2C1DCEEAA3E6D880B18263	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State **MD5:** 18BF20C018B56BE7E13250820D2E8467 **SHA256:** 29EF8DE7E5436796CCAB044959EB9C91E867A9E4CE2C1DCEEAA3E6D880B18263	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State~RF13a319.TMP **MD5:** 754EAF5A9250886BB4DEC99EA2E40877 **SHA256:** FFE04E366CAC48D4D156535496BF4887B4B492E1C32D7592E8F82F4E94133BA3	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity **MD5:** 4D7FC1C472CCC1E1261BA19EEC71E31A **SHA256:** 49454DE6E0AC7FC5059ACB7D852ADC74E93FADE6E836144E891B877837C1C89C	text
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\ed5b14a8-1452-4c35-8808-f0734c1e10c1.tmp **MD5:** 4D7FC1C472CCC1E1261BA19EEC71E31A **SHA256:** 49454DE6E0AC7FC5059ACB7D852ADC74E93FADE6E836144E891B877837C1C89C	text
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5 **MD5:** 61B979ECA159ECAC9C7F8F1D6FD43E9D **SHA256:** AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\GrShaderCache\GPUCache\data_1 **MD5:** 82327EC486C5E696E90E3A47BEF8B025 **SHA256:** DC09F80EF19281BD3F1CABB885A764E7F52DD3DE3AE91EE52F4C11F75E1F3F23	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1 **MD5:** 5183A1AD5E94DFD0F9C57B2FF86B0565 **SHA256:** 9893D3B8F8CF18E04AEADFEC8F03B8F4BD8ECBD4EDE77169826600BF5C75094B	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\chrome_shutdown_ms.txt **MD5:** B746ED21800797C9E7BA5ECC8A5E169B **SHA256:** D474BEB049B53A2B285DF17F5B7F306ABC37FD1020CBFA6911D779376D17BBC9	binary
3868	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1 **MD5:** F50F89A0A91564D0B8A211F8921AA7DE **SHA256:** B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC	binary
3944	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity~RF13a348.TMP **MD5:** E0DF05B63EFBA1543AA0CF2C7FC08A18 **SHA256:** B71EF58C9F3E489CE79E9CF2D46EC010AD46E032CD91BE2CEDB5F074C82064A9	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
3	16	12	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3944	chrome.exe	GET	403	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx	US	text	37 b	whitelisted
3944	chrome.exe	GET	302	142.250.184.206:80	http://redirector.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx	US	html	592 b	whitelisted
3944	chrome.exe	GET	200	173.194.183.70:80	http://r1---sn-aigl6ned.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx?cms_redirect=yes&mh=e_&mip=185.192.69.77&mm=28&mn=sn-aigl6ned&ms=nvh&mt=1647618743&mv=m&mvi=1&pl=25&rmhost=r4---sn-aigl6ned.gvt1.com&shardbypass=sd&smhost=r5---sn-aigl6nsr.gvt1.com	US	crx	242 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3944	chrome.exe	142.250.181.228:443	www.google.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.185.67:443	clientservices.googleapis.com	Google Inc.	US	whitelisted
3944	chrome.exe	172.217.16.142:443	clients2.google.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.185.195:443	fonts.gstatic.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.184.206:443	apis.google.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.181.227:443	update.googleapis.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.186.35:443	www.gstatic.com	Google Inc.	US	whitelisted
3944	chrome.exe	216.58.212.170:443	fonts.googleapis.com	Google Inc.	US	whitelisted
3944	chrome.exe	172.217.23.109:443	accounts.google.com	Google Inc.	US	suspicious
3944	chrome.exe	34.104.35.123:80	edgedl.me.gvt1.com	—	US	whitelisted
3944	chrome.exe	173.194.183.70:80	r1---sn-aigl6ned.gvt1.com	Google Inc.	US	whitelisted
3944	chrome.exe	142.250.184.206:80	apis.google.com	Google Inc.	US	whitelisted

DNS requests

Domain	IP	Reputation
clientservices.googleapis.com	142.250.185.67	whitelisted
accounts.google.com	172.217.23.109	shared
clients2.google.com	172.217.16.142	whitelisted
www.google.com	142.250.181.228	whitelisted
fonts.googleapis.com	216.58.212.170	whitelisted
www.gstatic.com	142.250.186.35	whitelisted
apis.google.com	142.250.184.206	whitelisted
fonts.gstatic.com	142.250.185.195	whitelisted
update.googleapis.com	142.250.181.227	whitelisted
edgedl.me.gvt1.com	34.104.35.123	whitelisted
redirector.gvt1.com	142.250.184.206	whitelisted
r1---sn-aigl6ned.gvt1.com	173.194.183.70	whitelisted

Threats

No threats detected

Debug output strings

No debug info

Interactive malware hunting service ANY.RUN