VALKYRIE COMODO

Summary

File Name: ccsetup533.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

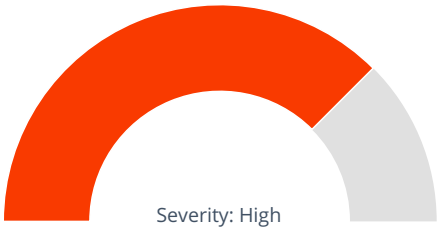
SHA1: c705c0b0210ebda6a3301c6ca9c6091b2ee11d5b

MD5: 75735db7291a19329190757437bdb847

MALWARE

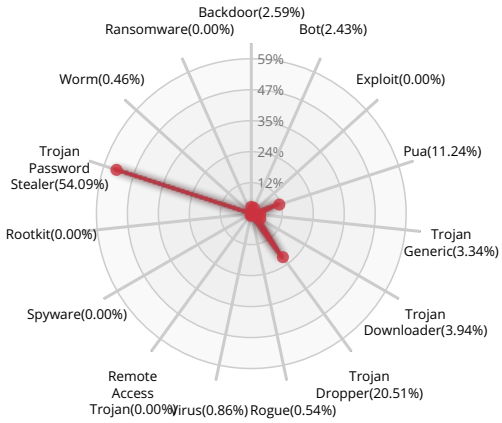
Valkyrie Final Verdict

DETECTION SECTION

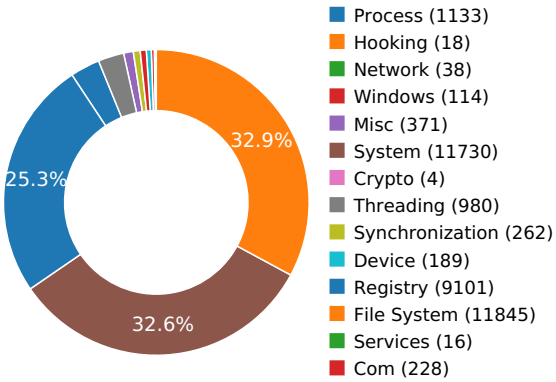


Verdict: Malware

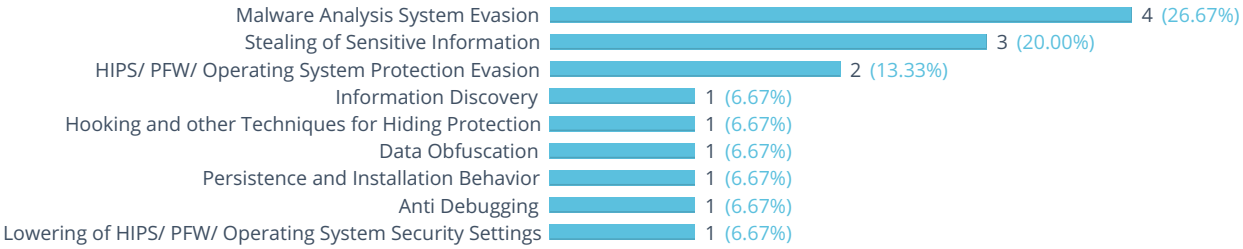
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory	Show sources
Attempts to identify installed AV products by registry key	Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources
Harvests credentials from local FTP client softwares	Show sources
Harvests information related to installed mail clients	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources

ANTI DEBUGGING

Checks for the presence of known windows from debuggers and forensic tools	Show sources

MALWARE ANALYSIS SYSTEM EVASION

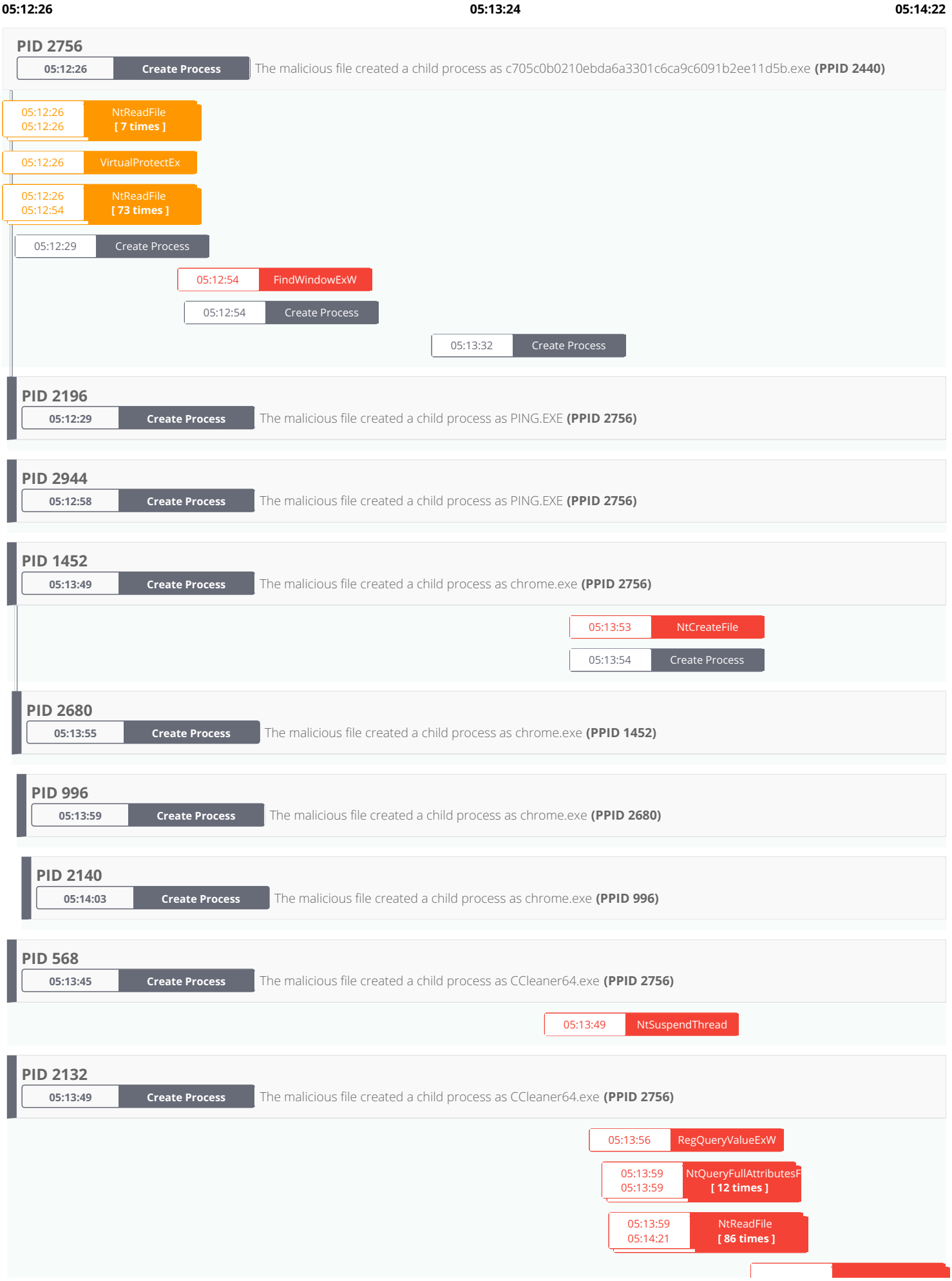
Tries to suspend Cuckoo threads to prevent logging of malicious activity	Show sources
Checks the CPU name from registry, possibly for anti-virtualization	Show sources
Detects VirtualBox through the presence of a file	Show sources
Creates a hidden or system file	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

VALKYRIE COMODO

Behavior Graph



05:14:22 05:14:22	NtQueryAttributesFile **[8 times]**
05:14:22 05:14:22	RegOpenKeyExW **[2 times]**
05:14:22 05:14:22	NtQueryAttributesFile **[4 times]**
05:14:22 05:14:22	RegOpenKeyExW **[4 times]**
05:14:22 05:14:22	NtReadFile **[3 times]**
05:14:22 05:14:22	NtQueryAttributesFile **[2 times]**

PID 1840

05:14:03	Create Process	The malicious file created a child process as CCleaner64.exe **(PPID 2132)**

05:14:08	RegSetValueExW

PID 872

05:14:02	Create Process	The malicious file created a child process as svchost.exe **(PPID 460)**

PID 584

05:14:12	Create Process	The malicious file created a child process as svchost.exe **(PPID 460)**

PID 2516

05:14:17	Create Process	The malicious file created a child process as svchost.exe **(PPID 460)**

05:14:19	RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsaA916.tmp
C:\Users\user\AppData\Local\Temp\c705c0b0210ebda6a3301c6ca9c6091b2ee11d5b.exe
C:\Users\user\AppData\Local\Temp\nsqA9C3.tmp
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\UserInfo.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.DLL
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.DLL.3.Manifest
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcapi_dll.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcapi_dll.DLL
C:\Users\user\AppData\Local\Temp\WINMM.dll
C:\Windows\System32\winmm.dll
C:\
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1025.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1026.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1027.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1028.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1029.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1030.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1031.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1032.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1033.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1034.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1035.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1036.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1037.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1038.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1040.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1041.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1042.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1043.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1044.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1045.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1046.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1048.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1049.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1050.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1051.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1053.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1054.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1055.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1057.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1058.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1060.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1061.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1062.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1066.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1102.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2052.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2070.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_3098.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\combo-offer.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\syschk.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsExec.dll
\Device\NamedPipe\
\Device\NamedPipe
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\pfUI.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\PF_logo.png
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\CC_logo_72x66.png

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UserInfo.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Google Toolbar\test
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}\pv
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\lastrun
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\nsExec.dll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\nsDialogs.dll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\th-TH
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\th-TH
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\id-ID
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\id-ID
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\be-BY
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\be-BY
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\sl-SI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\sl-SI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\lv-LV
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\lv-LV
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\az-Latn-AZ

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\az-Latn-AZ
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ka-GE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ka-GE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\hi-IN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\hi-IN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\kk-KZ
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\kk-KZ
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\tk-TM
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\tk-TM
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\tt-RU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\tt-RU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\mr-IN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\mr-IN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\mn-MN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\mn-MN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings\Anchor Color
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings\Anchor Color Visited
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{EAB22AC0-30C1-11CF-A7EB-0000C05BAE0B}\1.1\0\win32\(Default)

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsqA9C3.tmp
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcapi_dll.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1025.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1026.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1027.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1028.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1029.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1030.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1031.html
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1032.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1033.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1034.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1035.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1036.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1037.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1038.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1040.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1041.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1042.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1043.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1044.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1045.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1046.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1048.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1049.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1050.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1051.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1053.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1054.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1055.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1057.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1058.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1060.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1061.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1062.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1066.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1102.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2052.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2070.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_3098.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\combo-offer.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\syschk.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsExec.dll

\Device\NamedPipe
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\pfUI.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\PF_logo.png
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\CC_logo_72x66.png
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\PF_computer.png
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\Montserrat-Regular.otf
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1031.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1041.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1049.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1053.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1042.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1044.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1040.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-2070.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1043.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1036.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1034.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1045.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1028.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1030.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1035.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1046.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1038.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1029.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-2052.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1027.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1037.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1032.dll

RESOLVED APIS

version.dll.GetFileVersionInfoW
shfolder.dll.SHGetFolderPathW
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware

setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
kernel32.dll.GetUserDefaultUILanguage
system.dll.Alloc
system.dll.Call
kernel32.dll.GetVersionExW
system.dll.Free
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
userinfo.dll.GetAccountType
advapi32.dll.CheckTokenMembership
kernel32.dll.GetCurrentProcess
kernel32.dll.IsWow64Process
kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree

kernel32.dll.InitializeCriticalSectionAndSpinCount
gtapi_signed.dll.ToolbarCompatibilityCheck
kernel32.dll.QueryActCtxW
kernel32.dll.GetModuleHandleExW
kernel32.dll.CreateActCtxW
kernel32.dll.ActivateActCtx
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.DeactivateActCtx
kernel32.dll.VerifyVersionInfoA
kernel32.dll.VerSetConditionMask
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.IsValidSid
advapi32.dll.GetSidIdentifierAuthority
advapi32.dll.GetSidSubAuthorityCount
advapi32.dll.GetSidSubAuthority
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx

kernel32.dll.GetDateFormatEx

kernel32.dll.GetLocaleInfoEx

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsaA916.tmp

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal

C:\Users\user\AppData\Local\Temp\CheckUpdate.log

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ButtonEvent.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcapi_dll.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\combo-offer.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1025.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1026.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1027.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1028.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1029.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1030.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1031.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1032.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1033.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1034.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1035.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1036.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1037.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1038.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1040.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1041.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1042.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1043.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1044.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1045.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1046.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1048.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1049.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1050.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1051.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1053.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1054.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1055.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1057.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1058.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1060.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1061.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1062.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1066.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1102.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2052.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_2070.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_3098.html

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\inetc.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\modern-header.bmp

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\modern-wizard.bmp

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsDialogs.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsExec.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsProcess.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\pfWWW.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\syschk.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\p\

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\System.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\pfUI.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\CC_logo_72x66.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1025.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1026.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1027.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1028.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1029.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1030.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1031.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1032.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1034.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1035.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1036.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\lang-1037.dll

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Google Toolbar\test
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFavoritesInitialSelection
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFeedsInitialSelection
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}\FirstNotDefault\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_CURRENT_USER\Software\Piriform\CCleaner\AutoICS
HKEY_CURRENT_USER\Software\Piriform\CCleaner\AutoUpdateNotificationExpiryTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\CCleanerSkipUAC.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\CCleanerSkipUAC.job.fp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\CCleaner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\c705c0b0210ebda6a3301c6ca9c6091b2ee11d5b.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UserInfo.dll
HKEY_LOCAL_MACHINE\SOFTWARE\CCleaner
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_CURRENT_USER\Software\Piriform\CCleaner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_CLASSES_ROOT\CLSID\{2318C2B1-4965-11d4-9B18-009027A5CD4F}\InprocServer32
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\URLAssociations\http\UserChoice
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice\Progid
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Google\Google Toolbar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Google Toolbar\test
HKEY_LOCAL_MACHINE\Software\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}\pv
HKEY_CURRENT_USER\Software\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\lastrun

HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463C-AFF1-A69D9E530F96}\reactivation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\nsExec.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots

EXECUTED COMMANDS

ping -n 1 -w 1000 www.piriform.com
ping -n 1 -w 5000 www.piriform.com
C:\Program Files\CCleaner\CCleaner64.exe /createSkipUAC
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --new-window "http://www.google.com" "http://www.piriform.com/go/app_releasenotes?p=1&v=5.33.6162&l=1033&b=1&a=0"
C:\Program Files\CCleaner\CCleaner64.exe
C:\Program Files\CCleaner\CCleaner64.exe /monitor

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\nsaA916.tmp
C:\Users\user\AppData\Local\Temp\c705c0b0210ebda6a3301c6ca9c6091b2ee11d5b.exe
C:\Users\user\AppData\Local\Temp\nsqA9C3.tmp
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\System.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.DLL
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gtapi_signed.DLL.3.Manifest
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcapi_dll.DLL
C:\Windows\System32\winmm.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsExec.dll
\Device\NamedPipe\
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\pfUI.dll
C:\Windows\System32\msimg32.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Windows\System32\wtsapi32.dll
C:\Windows\System32\netapi32.dll
C:\Windows\System32\netutils.dll

C:\Windows\System32\srvcli.dll

C:\Windows\System32\esent.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsDialogs.dll

C:\Windows\System32\UXTHEME.DLL.Config

C:\Windows\System32\uxtheme.dll

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\CC_logo_72x66.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\PF_logo.png

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ui\res\PF_computer.png

C:\Windows\SysWOW64\ieframe.dll

C:\

C:\Users\desktop.ini

C:\Users

C:\Users\user

C:\Users\user\AppData

C:\Users\user\AppData\Local

C:\Users\user\AppData\Local\Temp

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo

C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\g\gcombo\ComboOffer_1033.html

C:\Windows\WindowsShell.manifest

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\Users\user\AppData\Local\Microsoft

C:\Users\user\AppData\Local\Microsoft\Windows

C:\Users\user\AppData\Local\Microsoft\Windows\History\desktop.ini

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012017091920170920\index.dat

C:\Windows\System32\shell32.dll

C:\Users\user\AppData\Roaming

C:\Users\user\AppData\Roaming\Microsoft\desktop.ini

C:\Users\user\AppData\Roaming\Microsoft

C:\Users\user\AppData\Roaming\Microsoft\Windows

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\desktop.ini

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@c1.microsoft[2].txt

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@microsoft[2].txt
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\SiteSecurityServiceState.txt
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Origin Bound Certs
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\modern-header.bmp
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\ButtonEvent.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\nsProcess.dll
C:\Users\user\AppData\Local\Temp\nsgA9D4.tmp\inetc.dll
C:\Program Files\desktop.ini
C:\Program Files
C:\Program Files\CCleaner
\??\PIPE\srvsvc
C:\Program Files\CCleaner\CCleaner64.exe

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\WininetStartupMutex
Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\!IETld!Mutex
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
!SHMSFTHISTORY!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012017091920170920!

IESQMMUTEX_0_208
Piriform_CCleaner_PreventSecondInstance
Piriform_CCleaner_Monitoring
Local\ChromeProcessSingletonStartup!
{A946A6A9-917E-4949-B9BC-6BADA8C7FD63}
Piriform_CCleaner_SystemTrayIconActive
Local\c:!users!user!appdata!local!microsoft!internet explorer!domstore!
Piriform_CCleaner_Checking_for_Updates
Piriform_CCleaner_SystemTraySingleIcon
Piriform_CCleaner_SystemTrayMonitorIconActive

MODIFIED REGISTRY KEYS

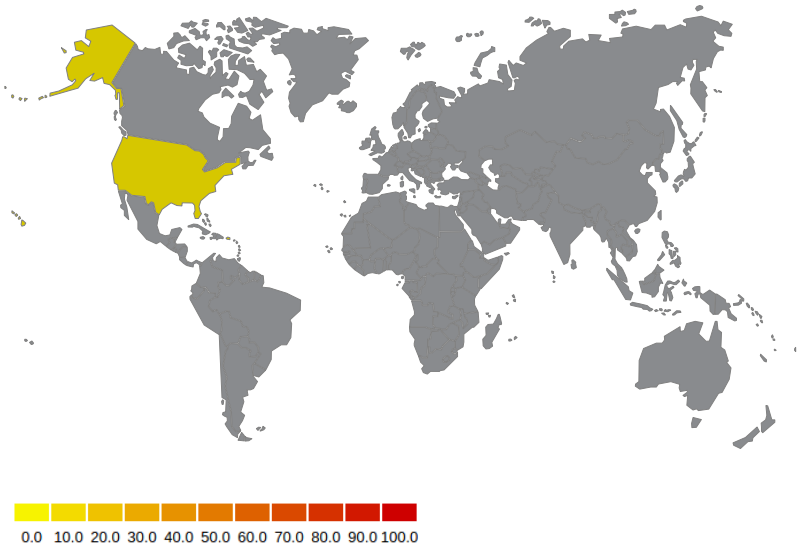
HKEY_LOCAL_MACHINE\SOFTWARE\Google\Google Toolbar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Google Toolbar\test
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091920170920\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\reactivationbrand
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463C-AFF1-A69D9E530F96}\reactivation
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\reactivation\PRFK
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\experiment_labels
HKEY_LOCAL_MACHINE\Software\Piriform
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\CR
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\Shell\Run CCleaner\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\Run CCleaner\command\(Default)
HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\Shell\Open CCleaner...\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\Open CCleaner...\command\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\CCleaner
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\CCleaner\UpdateCheck
HKEY_CLASSES_ROOT\cclaunch
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cclaunch\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cclaunch\URL Protocol
HKEY_CLASSES_ROOT\cclaunch\shell
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cclaunch\shell\(Default)
HKEY_CLASSES_ROOT\cclaunch\shell\open
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cclaunch\shell\open\(Default)
HKEY_CLASSES_ROOT\cclaunch\shell\open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\cclaunch\shell\open\command\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\ccleaner.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ccleaner.exe\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ccleaner.exe\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\CCleaner\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\Publisher
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\VersionMajor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\VersionMinor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\DisplayIcon
HKEY_USERS\.DEFAULT\Software\Piriform\CCleaner
HKEY_USERS\.DEFAULT\SOFTWARE\Piriform\CCleaner\AutoICS

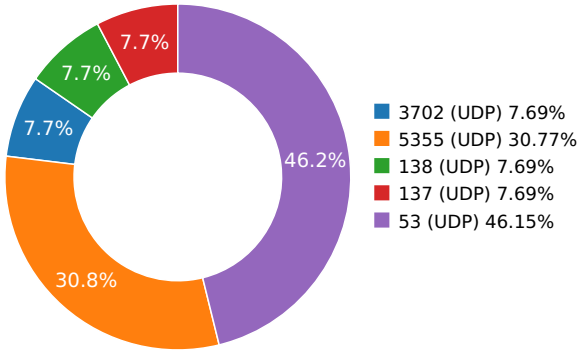
HKEY_USERS\.DEFAULT\SOFTWARE\Piriform\CCleaner\Brandover
HKEY_USERS\S-1-5-19\Software\Piriform\CCleaner
HKEY_USERS\S-1-5-19\Software\Piriform\CCleaner\AutoICS
HKEY_USERS\S-1-5-19\Software\Piriform\CCleaner\Brandover
HKEY_USERS\S-1-5-20\Software\Piriform\CCleaner
HKEY_USERS\S-1-5-20\Software\Piriform\CCleaner\AutoICS
HKEY_USERS\S-1-5-20\Software\Piriform\CCleaner\Brandover
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Piriform\CCleaner
HKEY_CURRENT_USER\Software\Piriform\CCleaner\AutoICS
HKEY_CURRENT_USER\Software\Piriform\CCleaner\Brandover
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000_Classes\Software\Piriform\CCleaner
HKEY_CURRENT_USER\Software\Classes\Software\Piriform\CCleaner\AutoICS
HKEY_CURRENT_USER\Software\Classes\Software\Piriform\CCleaner\Brandover
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter
HKEY_CURRENT_USER\Software\Piriform\CCleaner\Language
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice\Progid
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\https\UserChoice\Progid
HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\ftp\UserChoice\Progid
HKEY_CURRENT_USER\Software\Piriform\CCleaner\SkipUAC

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
	8.8.8.8	United States	15169	Level 3 Communications, Inc.	Malware Process

DNS QUERIES

Request	Type
www.piriform.com	A
service.piriform.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.098072052	Sandbox	192.168.56.255	137
3.14180088043	Sandbox	224.0.0.252	5355
3.23581790924	Sandbox	224.0.0.252	5355
3.55709004402	Sandbox	239.255.255.250	3702
5.79790592194	Sandbox	224.0.0.252	5355
9.10434103012	Sandbox	8.8.4.4	53
9.14076185226	Sandbox	192.168.56.255	138
10.0941770077	Sandbox	8.8.8.8	53
35.26668787	Sandbox	8.8.8.8	53
36.2662580013	Sandbox	8.8.4.4	53
48.2365448475	Sandbox	224.0.0.252	5355
51.0632059574	Sandbox	8.8.8.8	53
52.0624418259	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1053.Dll **C:\Program Files\CCleaner\Lang\Lang-1053.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 65b248990f62cc6e0e882b18e228c6ef **SHA-1 :** fd44d7a596be9eccd4454310c6f5917042b9c3e3 **SHA-256 :** a028ba45cae285d9986d691127264c9da9d42b7 **SHA-512 :** 21251cafd95e39740b4929e442a2574aa7841a8f **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\PfUI.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4ddbdbdee17ae06e6f364d04657d13ae **SHA-1 :** 756715393b0e2b39bafdcd0b18aa7e332b4d5da2 **SHA-256 :** c3155e622ae00b54530bd6331dae1a9ba8c74c2 **SHA-512 :** 4dd01041c5c884eac4ff377479c1eb67c3e337721 **Size :** 4290.776 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\DOMStore\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** c22b8c552eca3bf070ef39c852b22de2 **SHA-1 :** 8968f0159ca6bb477c3b5f3af317f413cacf16cf **SHA-256 :** 83e7d51429e7158afbc903b0f28dd92d903cc088 **SHA-512 :** e8db06d900dbd4458b9723f1f4007ba3e17569b **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-5146.Dll **C:\Program Files\CCleaner\Lang\Lang-5146.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 58b319f5c1a42a42bae726c7aa20a5a5 **SHA-1 :** 79ce4bf5c912ded03a8377055d37debc6451081c **SHA-256 :** 08d92ac098bb5fbfb57180efcf5d91629c1ebf1e4 **SHA-512 :** 5b4097d7625cbbca032355e564ad8d0b75c8fcab **Size :** 69.632 Kilobytes.
C:\Program Files\CCleaner\Uninst.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive **MD5 :** 7c0bfadecfaa9aec0b031acd37df565b **SHA-1 :** 962690835e34eea62ca20142a59080d47ce28744 **SHA-256 :** f72b769b0c22f06a30167b6e21f40394b13a4c21 **SHA-512 :** b41f0582ecc92fd443b04635192eb059429d3637 **Size :** 173.248 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1054.Dll **C:\Program Files\CCleaner\Lang\Lang-1054.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** a18e68d89fa38f2b7032a96b74371def **SHA-1 :** 5ac6ec5a2cbe29bbdde9777ef3302e2d04bc0849 **SHA-256 :** 7a37da5ab1f6ee2ecfc946685d941a772454d9dd **SHA-512 :** 4511e7d35eaeeacb543ea5286fe3c6109a1508f0 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1037.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 9b97c8eb5df75c96f82a4630935040cc **SHA-1 :** 060835151173922245f46eb468a420a038670820 **SHA-256 :** 603adca2b2a4bb0767f059f2c8f94be036432bba **SHA-512 :** a5921fb5d7a0612b30b547d1881332da84cbeca **Size :** 3.913 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\History-Journal	**Type :** data **MD5 :** e15f91dd47e3055bf3504a832b3019c0 **SHA-1 :** 916070b09be5d0a5289345072a3aacabe99a2413 **SHA-256 :** 169ef6cdbe3e872a0699c10dd06ea5153ebaae4 **SHA-512 :** ce730b7666ef13c401dddd42276bd55540e3f693 **Size :** 16.928 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-9999.Dll **C:\Program Files\CCleaner\Lang\Lang-9999.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 1c6e6e4fc015ed32adcf3b8e7bfd1445 **SHA-1 :** 41b1e086e75e8d146f1301666dcd6d5cdb6d1031 **SHA-256 :** 5fdb4787500a326a32f2caa11b531d4293eb5ac7 **SHA-512 :** 3e45a8ed4ec4d4aac83a84566637aebe25c1d5e **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1044.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 093491b47301f76406c7096b8f157a03 **SHA-1 :** da6263d151fb53dd72541189da05c872f7d21f0d **SHA-256 :** f7fa13c6e54151a47e2e9b7a0e55f2b6e681dff10 **SHA-512 :** 7d5e77ffbe5ab0135ae439089149974fbc4e68c8 **Size :** 3.565 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1030.Dll **C:\Program Files\CCleaner\Lang\Lang-1030.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 254ccbc4dc7ae8ce3d751488c4829626 **SHA-1 :** 252a48d1e78a5f30be20e3d8c4aef7c1a1f6b26c **SHA-256 :** c88337db83407111b557345025d40982dbd96ac **SHA-512 :** f40e0df98b6fce15d1bf199c157a2942c0121a278 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1061.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 5bb71b08068e1e8620c871694658d78d **SHA-1 :** d8dff54c9f88cea987f6cb8d801682bac7ad75a2 **SHA-256 :** 290872a2c9aae57d8fbeea08722c23c159ff4df23 **SHA-512 :** 4957e6c8d985d2ac794b723729acedeb9c74743e **Size :** 3.535 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1063.Dll **C:\Program Files\CCleaner\Lang\Lang-1063.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3d778114d82b6b882fd495a4ccbca48a **SHA-1 :** fa229648eca2d54badb34e10c504410a0f2edb39 **SHA-256 :** 8e1f1089d88310cd3cdbf330abb1bb2277750d85 **SHA-512 :** ed0c463b249c114ab52bf8806629483a06991697 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1049.Dll **C:\Program Files\CCleaner\Lang\Lang-1049.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3418790957866823b5a78137db567462 **SHA-1 :** f7bbb291c5bf619efac9a12a40688f0b09fa2379 **SHA-256 :** 2f7696bb424aaf786ac5c9f2a135c26b8732cb9c7 **SHA-512 :** 0af41736a60ab17bf1cba8f2440d37d4058883ce **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1061.Dll **C:\Program Files\CCleaner\Lang\Lang-1061.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 53d32f02d04870e6db8c5b747cf0db79 **SHA-1 :** ae713bf8427bf1ec726dbc8d405143024bd07f2e **SHA-256 :** d5e13dae2b778e28c8bbba4eaef121eee83af6fd **SHA-512 :** 371d0981dc17f2d720658638e1e4e5011217091 **Size :** 65.536 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1055.Dll **C:\Program Files\CCleaner\Lang\Lang-1055.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 6634dfbd79e2ae4e9bf72668a15bf51c **SHA-1 :** b819168f919389e8db8a337d28a43e2983841f00 **SHA-256 :** d140fbd06e4998fb9ba0410c7d6f83b96c75fe3a4 **SHA-512 :** 6a7aba5d71765f1b7cbafd4b224c7f78b182f83c0 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1090.Dll **C:\Program Files\CCleaner\Lang\Lang-1090.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0abb0d6662dac3c96a058e38b54d2459 **SHA-1 :** ce663b6b2c6cf680f2b6784d2a0772d518977942 **SHA-256 :** b3f5e080fc0291b3e449717dd4c844ff9351fdfc05 **SHA-512 :** 90f81407917eedcbffad57fd385d3466825e78317 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1036.Dll **C:\Program Files\CCleaner\Lang\Lang-1036.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** dc24ea22ec737465e1296d973dc0a14d **SHA-1 :** d765208bfb3d3227c29f195d8a318aed5256af04 **SHA-256 :** 7fa7f1763ce891623f4f50911358e678ad6398f9b **SHA-512 :** 9f26ce3142a56cc2653bdf8ec8a02c3b4026aa16e **Size :** 77.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1026.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 31f4afa1e87f0243c43b0203b89d50b1 **SHA-1 :** dba384c943d572d39ecebe68e9598945549d571d **SHA-256 :** 34c5182d004df6016042423e040a79f597e9286f5 **SHA-512 :** 7ba8fb63df10b23e6506cb315f683b3fed5ffe1c97 **Size :** 4.076 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1030.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 74fb5c6592947c542fd036fe1d332aaf **SHA-1 :** 04a952c3c06619bca16b95a3f6c48073a740a745 **SHA-256 :** 63b9e98cbd2ca35590318a0307145a5bc541cac4 **SHA-512 :** 0afc46d4596945ecc5c80517d7cc34879a4ae2f10 **Size :** 3.497 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1051.Dll **C:\Program Files\CCleaner\Lang\Lang-1051.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 49ac4341539f3b700662d9d3a1f27a4d **SHA-1 :** fab52e2ee601f1d26909c7a5a7b0e2874a2e7faa **SHA-256 :** 5fc4896cb9d609d3435dfae9c8956a8cb9873046 **SHA-512 :** e5dfd78feabf99b3f8924090bc4233e5e43571cf7 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1092.Dll **C:\Program Files\CCleaner\Lang\Lang-1092.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 04951dbd3a4e1ea91744846a24d5d2f9 **SHA-1 :** 52ba9b5e61e44907d5cc81ee418568e98320316f **SHA-256 :** 3e86155d01f7ef0f29b1d5b787b5734fb6b7fcd14 **SHA-512 :** 659a422989d994e21a80a58d00f6f2687b90a48c **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1067.Dll **C:\Program Files\CCleaner\Lang\Lang-1067.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f266769ff2a2fe94e2ac2db65fc9bae2 **SHA-1 :** b293723fecc4d8bce6c84f28927e590c8b425b61 **SHA-256 :** 8e65a8c1a0c51003cb00d8eb43141a9343367636 **SHA-512 :** e224be5be9a45d42ec2824fab35d56a7984f746f **Size :** 65.536 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1032.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** b304784ff5cb5f21c84838fab5fc9dcd **SHA-1 :** 778f642b31b4efda2dc3524f3b6a5a7aa2b92d8a **SHA-256 :** e0f89a65f2dc26b278b4daf1f3e75ac2de25c4985 **SHA-512 :** 9c4c29cf3cd08820a11112024714d8301a2750fff **Size :** 4.316 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_3098.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** f0489537926326c7ef808f091263a555 **SHA-1 :** 066b3f333ac39cb73a4cf890d81da784167f4cd0 **SHA-256 :** 74e374ec1dc8c5066ed296a725d8e864f0247508 **SHA-512 :** 112a6958a9c7409fd99c1e422070cbd8db39848a **Size :** 3.964 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcapi_dll.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** 2973af8515effd0a3bfc7a43b03b3fcc **SHA-1 :** 4209cded0caac7c5cb07bcb29f1ee0dc5ac211ee **SHA-256 :** d0e4581210a22135ce5deb47d9df4d636a94b38 **SHA-512 :** b6f9653142ec00b2e0a5045f0f2c7ba5dbbda8ef3 **Size :** 356.864 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1048.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** ee3a80443b9ab94bed34e19e00fac5fb **SHA-1 :** e2b8b22525b154f46d47ee5267865171744ae0ea **SHA-256 :** 962cf551ae22e36c973f63b20064f51201306ee7e **SHA-512 :** 60ae3fd1f75efeb1849d3f9d0d44e95f3c461bcff0 **Size :** 3.65 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-2074.Dll **C:\Program Files\CCleaner\Lang\Lang-2074.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 967af0cb69ef80ee6d008a19e4bbadb2 **SHA-1 :** a2edd7a75f2eb14780e42985b9a52d25924b4ee1 **SHA-256 :** 73b6bf073ff71a39eb2eac13b39a43eaf6132493C **SHA-512 :** 0533f2b5dba523bce5bafc3a1720ff160dee67ef2 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1028.Dll **C:\Program Files\CCleaner\Lang\Lang-1028.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 831d8b77d3f41ef2c91a34aa0f1661d7 **SHA-1 :** c088d7885617a210ead27d74aa77f6fbb944f925 **SHA-256 :** a866c050a754b54f2ddd79cba5a8ee29f8c5d4ce **SHA-512 :** 2d3ddaeef1658d0eb94896a7eb3955e9d4767d0 **Size :** 30.72 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\NsExec.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 5ed60250f74fa36a5a247a715bcd026e **SHA-1 :** ff5f3ad0b32ede49a28e744664d086f6fe9e46b0 **SHA-256 :** ea8026766adc2d7cc26e2206cfdf5f0865b1426bf **SHA-512 :** 2dd77324c1e0fea801a5cac1fe1d67349a5a93d4 **Size :** 6.144 Kilobytes.
C:\Program Files\CCleaner\CCleaner.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** ef694b89ad7addb9a16bb6f26f1efaf7 **SHA-1 :** 8983a49172af96178458266f93d65fa193eaaef2 **SHA-256 :** 6f7840c77f99049d788155c1351e1560b62b8ad1 **SHA-512 :** 73b55632babc25a1194cf2df91a0480f35960a407 **Size :** 7680.216 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cookies.Sqlite-Shm **C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Webappsstore.Sqlite-Shm**	**Type :** FoxPro FPT, blocks size 0, next free block index 417475840 **MD5 :** b7c14ec6110fa820ca6b65f5aec85911 **SHA-1 :** 608eeb7488042453c9ca40f7e1398fc1a270f3f4 **SHA-256 :** fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e **SHA-512 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be5 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1034.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** e9ffd57dcdb8c4e634dca2fbf9e19e70 **SHA-1 :** d60cd9d7979a38b6ff1ddab6e6948c20ab0073df **SHA-256 :** 70ad2c871e0a5a842a3089c62cb80f9ddcd7fa99 **SHA-512 :** 094d5972af48615b5fa626b13da953097ab975cc **Size :** 3.627 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1050.Dll **C:\Program Files\CCleaner\Lang\Lang-1050.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 25d02a650974602ae899a286fd3010ff **SHA-1 :** c8f0eaee66c6af3e37d4856096c1ab52da4bc544 **SHA-256 :** d577f0e29008d134a634ded275c62788019b213 **SHA-512 :** cffef5c0b0d6b083578fc61d0a719d00215ef6341 **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** fd1614579c8755d8bdb5055289d261a1 **SHA-1 :** 3e936c4b2d5e2ea66d9532f3e5052023ca59a4b3 **SHA-256 :** cb2cbecf9c90df628f07b0a674f5f2a908bab6d57 **SHA-512 :** a4ac5413c3276fb7cd107afaf6950acbc500047d2 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1053.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** f759f1c938fdb5804373af120f1ca381 **SHA-1 :** 6c949a51e24fe578176240f8f9bb5f7e6b3a84fc **SHA-256 :** 0ecf9bf50a55fc59c663ce930f7a193f71af63b83cl **SHA-512 :** 18e27592a545d9598a34522dfdb16b64c8dd56f5 **Size :** 3.576 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1052.Dll **C:\Program Files\CCleaner\Lang\Lang-1052.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 737fb8d3cb70c1760240fcc67a71c039 **SHA-1 :** 386fa01151fdb6cbeea21e3cf34e55d1d09b4f89 **SHA-256 :** fc0f13114224d4d9847ab46128f46266f27cae566 **SHA-512 :** c8db66ceb0d8ed77b546d40a39dfcf6d2c5ef309 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1066.Dll **C:\Program Files\CCleaner\Lang\Lang-1066.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** eaee95f0fafade1998b58f0dc0ab104d **SHA-1 :** 73cca86fcd6cf6cdf84d28b333755c88a64feb2c **SHA-256 :** 077af41d91c4a40f539efdd3fa9c77331c95e17a4 **SHA-512 :** 44f28f2fea86b216e4811991eba0ea079a0486a9 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1058.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 4caa371c8d0133269c1f3f380a5f81c5 **SHA-1 :** a80c038f5efd286d46ba2d8e0df4a3d82bfcb99d **SHA-256 :** 403a3488d651cc942bb25ad0765f7ce99ddd165 **SHA-512 :** 9dc2fde7138b0c2907057bce2e27b1ada7774dfe **Size :** 4.093 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1031.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 7bfef739a458a6c54378fc4eeab2e30d **SHA-1 :** 72e99c54550f198c860dd51cebb43ff9dfb1eac8 **SHA-256 :** 4786ecf1484b6d5463d31b57ea4b6314906c2f81 **SHA-512 :** 7701cebb1a9a12d5785ad2e1c163a0af4620eafd **Size :** 3.627 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gtapi_signed.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 61bc40d1fad9e0faa9a07219b90ba0e4 **SHA-1 :** 5b5c3badedba915707000d2047eaf13f27b8925e **SHA-256 :** 89e157a4f61d7d18180cb7f901c0095da3b7a5cc **SHA-512 :** fa341aa975c471082b4b6c380f794d1e9ab39393 **Size :** 73.344 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1081.Dll **C:\Program Files\CCleaner\Lang\Lang-1081.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fea24b52d1dcfe767567dd70da9a1d8f **SHA-1 :** c82f8d9d165e3818c4287ca641378a81373be77f **SHA-256 :** 09bd2e1529566593b74b9cba66adac2c9666dd7 **SHA-512 :** 83e1cd8a301341fdd00dbf2137490ea7d92fb915 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1044.Dll **C:\Program Files\CCleaner\Lang\Lang-1044.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bc4117cd4ad49e5f40a8064b46ab77c2 **SHA-1 :** dc0c3e4bb5c3b8eca496966831439a98e47e2e45 **SHA-256 :** e73d9c7e9ffd766665989345a21c008b6d8b0c81 **SHA-512 :** 751d34377aa877f3b03eccd7e68b954d118e3db **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1037.Dll **C:\Program Files\CCleaner\Lang\Lang-1037.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 9a6c720d5fd333cd8cd6d131c593d2d8 **SHA-1 :** bafb9145523e9c4389a136150911dfbc5b5556a1 **SHA-256 :** 7ac52cf9aec4b4c4dbea477f2f7c6a72de4364f67 **SHA-512 :** 04d8938ed261cd4584c13add63ecf45bbfad85b7 **Size :** 57.344 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1043.Dll **C:\Program Files\CCleaner\Lang\Lang-1043.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 41b2fc0ab96ea1e5217d4ab3f0c5daee **SHA-1 :** d49cd3987bc0939b37cd7ff1aac852fb3f361f2d **SHA-256 :** 85501cff1e3c341eca21d9061616bac999074ae8f **SHA-512 :** a8688dbf076b3af85def1874f3de1d379d8124b3 **Size :** 77.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1035.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 9cb61e718d2c7b5e4be6d44f871ef640 **SHA-1 :** e334aa060977432aaa6143e4705e4d7de05c61f7 **SHA-256 :** 2940229bc3044b84fa8f613a071afeead25bda3fc **SHA-512 :** 88632894ec6f861c551f9a36069fe138fa09e32dc **Size :** 3.539 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\P\Syschk.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f46bc8015929e17a2b1aff097d7df0e4 **SHA-1 :** 6c30de3e6a004021e231aaa62a2c5cedec72bc6d **SHA-256 :** 26602d21203cf28b0c840a57bee8f1ff52ff885223 **SHA-512 :** ddee56e56a60db139029bc6a43e281d0eaeb842 **Size :** 259.584 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1057.Html	**Type :** HTML document, ASCII text **MD5 :** a09f1a093f506cd6fdc8a9fe032ad3aa **SHA-1 :** 20be56bce7fab1767e85733c25545109cf37623a **SHA-256 :** 448a73054b3789c87d81f28c48452e563a55c5a7 **SHA-512 :** b4879bed756e354ac77fc20afd363c4eb130d6b1 **Size :** 3.577 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\CC_logo_72x66.Png	**Type :** PNG image data, 72 x 66, 8-bit/color RGBA, non-interlaced **MD5 :** a736159759a56c29575e49cb2a51f2b3 **SHA-1 :** b1594bbca4358886d25c3a1bc662d87c913318cb **SHA-256 :** 58e75de1789c90333daaf93176194d2a3d64f2ee **SHA-512 :** 4da523a36375b37fa7bc4b4ccf7c93e1df7b2da1 **Size :** 7.486 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\PF_computer.Png	**Type :** PNG image data, 679 x 176, 8-bit/color RGB, non-interlaced **MD5 :** 7f4f45c9393a0664d9d0725a2ff42c6b **SHA-1 :** b7b30eb534e6dc69e8e293443c157134569e8ce7 **SHA-256 :** dbd8b6fdb66604a0a5e8efe269fbfa598e4a94dc **SHA-512 :** 0c27f9ce615cbff3e17fd772ce3929ab4419d7432 **Size :** 89.461 Kilobytes.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner\CCleaner.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Thu Aug 3 06:42:22 2017, mtime=Mon Sep 18 23:13:37 2017, atime=Thu Aug 3 06:42:22 2017, length=9832152, window=hide **MD5 :** e98a3d2a6e7d92e810f8d1118cddab97 **SHA-1 :** 4f34d93a5b953f2ef9c3015fc877e1016fabb462 **SHA-256 :** b2d96681d32401db284f1a215be126ccc885f23b **SHA-512 :** 9491f13d9946eaf3bfb453ba544e76352e9977b9 **Size :** 0.84 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1102.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 408e99583ec9ea84da8f3221704783d4 **SHA-1 :** 3303736e91748e9cbcce0be1ab6af3679432f383 **SHA-256 :** 5eeb90b4d8de8077b683cbcfce04fe0b8b3b4e4a **SHA-512 :** c730717e0023af5b1005cdf09cb3ce6a2c9e94e47 **Size :** 4.577 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1028.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 3c9d9a1818bede3e8e7fa99685d503df **SHA-1 :** 0db677e7ce9707e89c865a89cc6ab60e04af0119 **SHA-256 :** 5cdeaa26f12096e1aecda8acc42516341599ae41 **SHA-512 :** 9b9c06ef13ba802e0850fd98ff025479bd955c93 **Size :** 3.499 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1025.Dll **C:\Program Files\CCleaner\Lang\Lang-1025.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ed2e3096c08eff07c6268ed8453c2f54 **SHA-1 :** f0372e41bbba0d78d351fc31766e049ba10543a6 **SHA-256 :** ec86e2acc6094fc4cf022dab73c5564bd40927b5a **SHA-512 :** 62434ba49954d7bae5ef9c70addd53a72f170cee **Size :** 61.44 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1155.Dll **C:\Program Files\CCleaner\Lang\Lang-1155.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ae54548d6d57f68117d06e0791a11440 **SHA-1 :** f885b2f04ffa510f941e21f8a72dd594918655ab **SHA-256 :** 2cbb57386f6317dc73ff6ddc5fad018ae7d54c4d1 **SHA-512 :** 15c2a870d4ad9b8b719179890fe8aad2f8fad1bc **Size :** 77.824 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1038.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 7f6619f86770ae2dd1d8184e8cd95757 **SHA-1 :** 707a77f2305b8afbdfdf36f71f2e14ba54734952 **SHA-256 :** 98975ea1660fd6c28ba74f5ed6b1491294abbe13 **SHA-512 :** d69219de0addd5204690a52b61a7564c35a5436 **Size :** 3.723 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\NsDialogs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 2aba8f16eca82517460013a3de7cbf67 **SHA-1 :** 3812192fa7b873f426c4b0d0d822b3c9d51aa164 **SHA-256 :** 60b85fad2477b8c0138067be3697290b280b933 **SHA-512 :** 4e059f70ef420c22d69199557ff3eab9e51fcefc75 **Size :** 9.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_2052.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 25643d0be6a54fa5a5d618646befcf52 **SHA-1 :** ea049d1885806d7437aaa060b5ce3ca6ad08066c **SHA-256 :** fe956cacb752e088c07e33e431af2e97f53b2fe4f2 **SHA-512 :** ff93dff816fdbc180487dcec9285887185f37316bc **Size :** 3.562 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1046.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 84cae6e1687c91bfe077906276e73061 **SHA-1 :** 64b916e1589cc2dd27e4f4b0c4bdd9f10819a555 **SHA-256 :** cda034b22769116d9be7b7f6451590107dd2135 **SHA-512 :** 05cc748022a9d13c29b5770c7b8b4381d35af7a5 **Size :** 3.651 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\PfWWW.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 1bf8a77ace38e746320dc8d67b2e7236 **SHA-1 :** 6d5a74ab5ebd39fc3a450818a06d9406efe6e40e **SHA-256 :** 43ddba137b3a980f427524577dc1af481193163c **SHA-512 :** 54a6e07797a53cf9a6806daf068a20601e01a5c3 **Size :** 151.552 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1102.Dll **C:\Program Files\CCleaner\Lang\Lang-1102.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8d31d0e71747be5f49d10300b1e7bafc **SHA-1 :** 777b6050044f92e4d71e21ef0242bf25144d830f **SHA-256 :** b6fae8a401ac4c1efc133e0ff4a53d9265675ef229 **SHA-512 :** dbebe7c2a8baa29700e83c3edef5ae62859979a6 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1035.Dll **C:\Program Files\CCleaner\Lang\Lang-1035.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bdd6db6cc4785885b0559a85258fad11 **SHA-1 :** 43d8965daf67d4caf6f0d495a5b35e00f2bb45ea **SHA-256 :** 7c98a502f929fe63bad311f406ac53295d14234fb **SHA-512 :** e6091d9ff105cce7692d5bac84efc345f7f9ded9d **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1038.Dll **C:\Program Files\CCleaner\Lang\Lang-1038.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c283a666a3aa6a8d963f6767d997ab69 **SHA-1 :** 6340849b4e91628fd7d93d9086c6154ec5f8c4d4 **SHA-256 :** 4caacfa6a9e0017b0c7eabce58cb260afb9a36d23 **SHA-512 :** 5f2d1904c6e763ce9fc296fca18b30cf93319c7442 **Size :** 73.728 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Modern-Wizard.Bmp	**Type :** PC bitmap, Windows 3.x format, 164 x 314 x 8 **MD5 :** bf670074262a7e29da8c0ff2d94c1438 **SHA-1 :** 5d608a1cb519e5751a4736a6b8e9f3e80477f3e3 **SHA-256 :** 1ea1d0a8b0302840b2ba4743fdef788c93517ac0 **SHA-512 :** 6c974589ba1e2939e86216078b5ec8bf750346fa **Size :** 9.884 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1110.Dll **C:\Program Files\CCleaner\Lang\Lang-1110.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e22b072af725fe36e1f961e7495ea984 **SHA-1 :** 3a83ec1ad98869461bbf75927dbe72c4c5338dea **SHA-256 :** 56f8bdb7d3757d8066523bfcfaca93bc7b1fe28ce **SHA-512 :** a421d093699ca123a51b643f5e5b44654414920 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1027.Dll **C:\Program Files\CCleaner\Lang\Lang-1027.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** a6f6a8c0b24aac99e6a737ff47477bd5 **SHA-1 :** 0c98c0a68c7b22c70dca026d281f9911f5a961ab **SHA-256 :** b0fd62b34e7c7742a2561ce6a8f16adb98270fdc **SHA-512 :** f86511b4c8265add84dad600df453b915f35bcdc **Size :** 77.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1068.Dll **C:\Program Files\CCleaner\Lang\Lang-1068.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e0d813d78690c02b4bfc99d29110ff9d **SHA-1 :** f8631b3d53cf7f32ca5db613fd8944be79fc4cba **SHA-256 :** 0ddcf0d8c628b60cbf27a13935ccaad61c46411e **SHA-512 :** 9c1661eb2e87c6133757b21e1a9ff1eed41a62c3 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\Combo-Offer.Png	**Type :** PNG image data, 200 x 66, 8-bit/color RGBA, non-interlaced **MD5 :** 871bcef4f97837998a926cabc8bca29b **SHA-1 :** f76911bb5d09aa625b3b873a13afb5ae14639bcf **SHA-256 :** 916d3f364d397a36d2fa72cc259d6f14aeabf47a0 **SHA-512 :** c285513e50cd97eea85bc725da2ca6154e33cdeb **Size :** 8.14 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012017091920170920\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 9e9929949d9e1a812f9bdeb88a77a68a **SHA-1 :** 9fa03e76a745205adb770cbeab134a389da50abf **SHA-256 :** 3620f58988bde16ec811fb12d1d9d36f6be4a0cd **SHA-512 :** 7d860b7607fdc503d2e7a4212c9718cfc439994b **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1057.Dll **C:\Program Files\CCleaner\Lang\Lang-1057.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** de68ff550656aa56a731fb39cd46c4cc **SHA-1 :** 61e3f0bf8cb3595a05e33a1940a17f0ffb00dc2f **SHA-256 :** b80e4bd9991f418cf7f6dba0b93d79997940134a **SHA-512 :** 008ef3eafdeb4724e9ca39ee73dd10789fb94b31 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1029.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** d4a26ee683f64d4192888e427503dba2 **SHA-1 :** ccac5f52ea4708ba1452411ebfa4a5b4c522edd0 **SHA-256 :** 55b1d3aef2c70664efd560b22bdaffc4a4be25d2 **SHA-512 :** feb287ae2c812a074f3405204f162cce18da2441c **Size :** 3.641 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\P\PfWWW.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** cb1d8d51abc47fcf036a8aac36c5f4aa **SHA-1 :** b96e5093b2983cf1392927756a141c9d015bbe70 **SHA-256 :** 903ebbd07a9d551e41ba8cf581069e5e1c70894c **SHA-512 :** 4314a62d302e871372d68dd8d3f0c8f18f7fce5e4 **Size :** 154.624 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1046.Dll **C:\Program Files\CCleaner\Lang\Lang-1046.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0ae60b8c1e93b82811885b95f0fa3471 **SHA-1 :** 124f68d9fae3328cede871fe26f4d0747ea9b33f **SHA-256 :** 9f50fcaef72196ed3f9f2b765fcf24e45a7edbb611 **SHA-512 :** 1f3f1dd4d9ebd5b69f221629aab2f69f6d72e6a06 **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1104.Dll **C:\Program Files\CCleaner\Lang\Lang-1104.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 54f79a3fba1fe3b6dff9be7e88b06bd0 **SHA-1 :** 23b159b746a4fa0f9dfe304fa0389be06721d123 **SHA-256 :** e99e51f3387f22d1005414454ec97052912213be **SHA-512 :** 0bccef019e1b2328369e5b1c7c763e55ce1b8c0a2 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1062.Dll **C:\Program Files\CCleaner\Lang\Lang-1062.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0143db4621c5f331fcd6fa22766666c8 **SHA-1 :** e6b84d9e4a33c80d7039eaf62b92a3e89ba1b966 **SHA-256 :** 1e78121abdb6071fc695241f090b40af8967efdbe **SHA-512 :** 1b43982f6f19399512490090cc64b389b387e0b8 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-2052.Dll **C:\Program Files\CCleaner\Lang\Lang-2052.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fc61fac4c0b168198ba4641b40858483 **SHA-1 :** 10ebed72f76789088c9e6fe7993ba3d3625a11e1 **SHA-256 :** c538a71294f694d5a35340ea2a425892d8124e01 **SHA-512 :** f736687dbd06ad846c81a1a742e095d6342a5f40 **Size :** 28.672 Kilobytes.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner\CCleaner Homepage.Url	**Type :** MS Windows 95 Internet shortcut text (URL=< >), **MD5 :** 20aac90eefd7fcf37027fde1fcf35214 **SHA-1 :** 5161cc36b8e0fbe826ef12f536308cc26e5727b6 **SHA-256 :** b6a13260e3576b5163fd56e0be2b03a89155534 **SHA-512 :** 15624c1f35906e22203108345df6ddf0b1dfc2205 **Size :** 0.082 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1036.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** c69da1c2761d758f92603d59f4addb28 **SHA-1 :** b9fb06bdc3466127c419af13be2141b750bd8c2b **SHA-256 :** 4bd2dfb0d9d60f7b83942d8f43a45597bbbba427 **SHA-512 :** ce7f6edadcd1109377596fb177d92930c06afceb7 **Size :** 3.641 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-2070.Dll **C:\Program Files\CCleaner\Lang\Lang-2070.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3e83253c7d8b1e6da76183ee996fc8f5 **SHA-1 :** 2217bcabf6aff0ee8a9813c32ca88d72663f4e4f **SHA-256 :** 6d1dfabc3a2d9e68d74691fcc4d3205e62ff85878 **SHA-512 :** 6d55d20116c2c4aadbdc1972f7b48c934a6e8f6b **Size :** 73.728 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1027.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** d23b9d2a41fb327025c45b392b8415a5 **SHA-1 :** 8ac0e6f20608ef80e3a67cf6e7a93a6aa9d9d7fa **SHA-256 :** 36b5327492d4a1097a87c6f52ea89d90ab52457 **SHA-512 :** fd7af60a9946ab1acfbc5747da571e04807c4fcf3c **Size :** 3.618 Kilobytes.
C:\Windows\Temp\Fwtsqmfile00.Sqm	**Type :** data **MD5 :** 82030d9e541fbfffde1f2674d845d7cd **SHA-1 :** 0ceff0268020b9a5b57251cd59610bc0bcff9245 **SHA-256 :** e1d397bf8c5be20b6d5bc0f28543aca05ca7e4d7 **SHA-512 :** 7d291e263119a0f31dd0edd39fc1a63114b56d36 **Size :** 0.14 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1062.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 0fe72bb267b87d193215956c5767dbad **SHA-1 :** 88e5327b0f3b29171a7f2498e1508df33f8ec57e **SHA-256 :** c0651bc6dd49dbb2be17f3a05c612c2b3e439315 **SHA-512 :** dad380d3f89ad2a9e05e51e68aed1acede71e5f2 **Size :** 3.644 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1066.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 29740736d078df955876f38f203ac4a2 **SHA-1 :** 5de03f66b185df11b135bb40018014dcf5531fc8 **SHA-256 :** 8232fff956ef50fdeaae5408c2b382be41388b060 **SHA-512 :** a490fa188056477872cabdb599ca57947c2a45b8 **Size :** 3.863 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1026.Dll **C:\Program Files\CCleaner\Lang\Lang-1026.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8eb1ac41288ce6347b300421423bc13a **SHA-1 :** 5c8b7cf64073f56157c971bc3876710459cea2ce **SHA-256 :** 6b1fd0de2665dd1d221e48c4dcf2cc6f354065ab **SHA-512 :** 0e46721738eb68e106fe8e0670597637ebdc4d8 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1040.Dll **C:\Program Files\CCleaner\Lang\Lang-1040.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** dc499ed28db352435ed3aa0063f246fe **SHA-1 :** b9a93860a9224e2efaf81a288cfe054875709cc9 **SHA-256 :** 37de186e146a30f85366536eeb374f9a9478e61d **SHA-512 :** de8b985b2c677c655b1d216ab525ad225c3f6b8 **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Shortcuts-Journal	**Type :** empty **MD5 :** d41d8cd98f00b204e9800998ecf8427e **SHA-1 :** da39a3ee5e6b4b0d3255bfef95601890afd80709 **SHA-256 :** e3b0c44298fc1c149afbf4c8996fb92427ae41e46 **SHA-512 :** cf83e1357eefb8bdf1542850d66d8007d620e405 **Size :** 0.0 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1049.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 5b4539f0342db6bc9eed915792721efe **SHA-1 :** f9cee2ae5dd909739b11d327a05193011d5a9a06 **SHA-256 :** cb1ff172361043a67da9d800c7d88a4fb2204648 **SHA-512 :** 1afca3646b70c41806d047045974bb8d792154a **Size :** 3.881 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1045.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 8248a0baf076898bac32a55df9f18e5f **SHA-1 :** 36565cd47d70ccbb6efe1c3c3cc374ea41d7ed87 **SHA-256 :** 4bdbb7946335b4c8bc9d2943e224753303ed2af **SHA-512 :** c62f1744d8f09b4e1d74c970d39f938a0066954b **Size :** 3.629 Kilobytes.
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Data_reduction_proxy_leveldb\LOG	**Type :** ASCII text **MD5 :** ccda99ee1f6d8f9d8a05611645ec7924 **SHA-1 :** 5d40b2609d8ed2e0256a0ba2ad2b99313099525f **SHA-256 :** ab13d65c48ea2f60b80dd71955b8dbeb0769cb6 **SHA-512 :** 4ba6054ff2cae815e78a1b4bab212f1455b1a0a3 **Size :** 0.344 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1087.Dll **C:\Program Files\CCleaner\Lang\Lang-1087.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fce4ef1c9c358f99604f5ad996d0891e **SHA-1 :** 3fafab09bce106777f4bd1740c1954717ca4d90c **SHA-256 :** 96dfe6a5445ff38337f9c232f63b78e4a5a104310 **SHA-512 :** e7f8298d93ceaa5a2ee3e45fe0a02993208de8fb4 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1041.Dll **C:\Program Files\CCleaner\Lang\Lang-1041.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 89d83b55dd5931ebbca0c0e264b1e5ac **SHA-1 :** 27ec938f047036f70824fbb5ecff42c2b2435b76 **SHA-256 :** 5f8d561ca8e53e67a811f8465404badf6c198bfe1 **SHA-512 :** c52cf409c517b6c222ada2be8ec54658db6b9bc0 **Size :** 36.864 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1065.Dll **C:\Program Files\CCleaner\Lang\Lang-1065.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4b36442eb1d4cebe59b3c0c01ae9ac14 **SHA-1 :** efc58f442dd0cec7a363979eacb37fae771308b4 **SHA-256 :** 6c4da54cec15f7260e65b1553427785c31f79662 **SHA-512 :** 3515cdd0d99a369b398f338cfb954c058ec87820 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1079.Dll **C:\Program Files\CCleaner\Lang\Lang-1079.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 982f93e94a690035488671979d9aa53f **SHA-1 :** 8947795a54cb051decdab53f35859075e8a35335 **SHA-256 :** 49ae86ded19076f97aaaf5c6829ec32e47d46c8c **SHA-512 :** ebb676d3da3e365ef6b9f1cfabdae6d337eddd71 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1025.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 3876777e8e7b73a9a1113402fe54aca9 **SHA-1 :** d5fc2d953530949ebd474925dcc2f737058d09e6 **SHA-256 :** 06ee0d941530d5bf86009e7df0d15dd5767be6d **SHA-512 :** 55ed0ceb960dfec3e77a583ff2db11f29b0c6b619 **Size :** 3.857 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Modern-Header.Bmp	**Type :** PC bitmap, Windows 3.x format, 150 x 57 x 8 **MD5 :** 6412e0b095da5095b321d376eb912ca5 **SHA-1 :** e93a95c724ba969c656f1cca47595a178176b238 **SHA-256 :** f2d07a76ad7d89e64ee261c81039205e44cd0f49 **SHA-512 :** f1a32da61b3d219d72256c2fcc5e01923052832b **Size :** 2.5 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1041.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 7ab9531bd9e2038be1a8497d49145424 **SHA-1 :** 94ded744b5b6dfaf5b55261dad39972bac9553aa **SHA-256 :** a513d80f8fc3ac157f70948ebbc134190bad6169c **SHA-512 :** 274f8af2429fccf81d44127127223413300310830 **Size :** 3.807 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 155e103bfb72c4e624763cfb13ae3e82 **SHA-1 :** 1f8d5c1a076835df926d7f9c48f46e48e907a267 **SHA-256 :** f82b64d2985428448588df8de52d2bf615242322 **SHA-512 :** ca1cf0b0dbf9cbda69c7f41e5267fd1924715ee03 **Size :** 180.224 Kilobytes.
C:\Users\Public\Desktop\CCleaner.Lnk	**Type :** MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Thu Aug 3 06:42:22 2017, mtime=Mon Sep 18 23:13:37 2017, atime=Thu Aug 3 06:42:22 2017, length=9832152, window=hide **MD5 :** 9db1a3aeef461378426ad3540cf4cecc **SHA-1 :** 287cf4ac2aa5b58ca072d3d21cb67c6c306c0bbd **SHA-256 :** e55a00834f40350dae81945b2fe4c05163452a50 **SHA-512 :** 46ea904e9cbaf720c62f201941b177e1ede218c8 **Size :** 0.822 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1040.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** d598bbd0693932b30f089181119861e0 **SHA-1 :** 6074954a161949958ad5d520f934f20efc3eb707 **SHA-256 :** da1198daa69c3803b0643d33024cb8a4b8a3b78 **SHA-512 :** 629d585b8bf10b4b532eaa5baf0b5b0054950afb **Size :** 3.578 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1033.Html	**Type :** HTML document, ASCII text **MD5 :** 016f10e3840423fd75a776923aa3e57d **SHA-1 :** 01ea9f2731917a6af28d62a94463ba87ede557a4 **SHA-256 :** c89b3683c75b641526524e2397d9beb24f5bbd0 **SHA-512 :** d469e9709590d01101f27a75bf597ed5f1d08a1c **Size :** 3.406 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1059.Dll **C:\Program Files\CCleaner\Lang\Lang-1059.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c95c9b9a7f79f0231c70783d87dff914 **SHA-1 :** c619f7c87406c8c6b4a4692416b9822df48da379 **SHA-256 :** e2f09d42fa6e003dab74120c62590bc66d564879 **SHA-512 :** 43d1b25113fefe885cccc5609ce6c870078196945 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\NsProcess.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f0438a894f3a7e01a4aae8d1b5dd0289 **SHA-1 :** b058e3fcfb7b550041da16bf10d8837024c38bf6 **SHA-256 :** 30c6c3dd3cc7fcea6e6081ce821adc7b2888542da **SHA-512 :** f91fcea19cbddf8086affcb63fe599dc2b36351fc8 **Size :** 4.608 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Inetc.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7760daf1b6a7f13f06b25b5a09137ca1 **SHA-1 :** cc5a98ea3aa582de5428c819731e1faeccfcf33a **SHA-256 :** 5233110ed8e95a4a1042f57d9b2dc72bc253e8cb **SHA-512 :** d038bea292ffa2f2f44c85305350645d504be5c45 **Size :** 24.064 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1051.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 1f073fe3d44e48fbcac1254a48964431 **SHA-1 :** ba715d4bdb2e63850744dc2fa8da1fbb34754db2 **SHA-256 :** b1f95781aa8d2d562682a043b1152c8894bdf98c **SHA-512 :** 3527886397235903d79257b79204fdcb0978d57 **Size :** 3.687 Kilobytes.
C:\Program Files\CCleaner\CCleaner64.Exe	**Type :** PE32+ executable (GUI) x86-64, for MS Windows **MD5 :** ab9f3741ce70ed9d7ebe94051d6a7778 **SHA-1 :** bc750e6f098d1e250ce074d0514431238fad1891 **SHA-256 :** 70dd6da9d21c00ea759880aae779920675227cc **SHA-512 :** ac711cc9642712fd4fcf92f863ce842033c081235c **Size :** 9832.152 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 41a3c964232edd2d7d5edea53e8245cd **SHA-1 :** 76d7e1fbf15cc3da4dd63a063d6ab2f0868a2206 **SHA-256 :** 8b65fec615c7b371c23f8f7f344b12dc5085e40a5 **SHA-512 :** fa16bd9d020602e3065afd5c0638bc37775b40eb **Size :** 11.264 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1031.Dll **C:\Program Files\CCleaner\Lang\Lang-1031.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e5aabfcd7ba3440baa0d99090c08ca68 **SHA-1 :** 19d72f1e110a4ea7d61d91a14d019755c0d9528e **SHA-256 :** 7ad48dd195defc9a01319c7bfbd9526a0045fbc7 **SHA-512 :** a8b0e937aba9aaaf92f288211a13af6d79d4e9ed **Size :** 69.632 Kilobytes.
C:\Windows\Sysnative\Tasks\CCleanerSkipUAC	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** c65ba3e46be77cb18b13074eb229e9a5 **SHA-1 :** e63e070749dd94fbce1f5dbb9a71537e118eadfb **SHA-256 :** f9e73addc0f8ef2dc75596e06c60f3247ded83a2b **SHA-512 :** 8f1324edc2e5dcd95c7accb12d6d315913054d57 **Size :** 2.78 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\UserInfo.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c1f778a6d65178d34bde4206161a98e0 **SHA-1 :** 29719fffef1ab6fe2df47e5ed258a5e3b3a11cfc **SHA-256 :** 9caf7a78f750713180cf64d18967a2b803b5580e **SHA-512 :** 9c3cf25cf43f85a5f9c9ed555f12f3626ef9daeeed **Size :** 4.096 Kilobytes.
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\BFF5.Tmp	**Type :** very short file (no magic) **MD5 :** 5058f1af8388633f609cadb75a75dc9d **SHA-1 :** 3a52ce780950d4d969792a2559cd519d7ee8c727 **SHA-256 :** cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21 **SHA-512 :** 0b61241d7c17bcbb1baee7094d14b7c451efecc7 **Size :** 0.001 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1060.Dll **C:\Program Files\CCleaner\Lang\Lang-1060.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 862d74044b0d62c44890b3129c0eafd0 **SHA-1 :** c9126e84d7fa6a10dd6d505a70cac4500576b797 **SHA-256 :** 8a2505af8be892be1fccd3c7afa9ddd20a6ee8641 **SHA-512 :** 0ce058b6b22e7f37b1441447593874fcc4bec2a3 **Size :** 69.632 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1058.Dll **C:\Program Files\CCleaner\Lang\Lang-1058.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 32249d8bc1ee8ad9a98453bd20009c99 **SHA-1 :** 380e3892caf091b6f6ef0d45b5a974e77934e0b7 **SHA-256 :** 363915b4e5d1139153144f25bfc6ebc3fe368871 **SHA-512 :** 9e0df1ac7932c92c295b11e6dee80a90c56b3749 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Montserrat-Regular.Otf	**Type :** OpenType font data **MD5 :** 27e50ffd6a14cbc8221c9dbd3b5208dc **SHA-1 :** 713c997ce002a4d8762c2dcc405213061233e4bc **SHA-256 :** 40fc1142200a5c1c18f80b6915257083c528c7f7f **SHA-512 :** 0a602f88cfba906b41719943465edb09917c447d **Size :** 45.36 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1071.Dll **C:\Program Files\CCleaner\Lang\Lang-1071.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fbf5ceb321d56a889a02b0cd34d378f9 **SHA-1 :** b18d928de0ed2a6fe61c22035055052f8cef930a **SHA-256 :** 3294ec720f6fc973677c53930f2e05eda2289ebf6 **SHA-512 :** 81a5d9e505599e92d7208e85a92bed67b9303ef **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\Ccc0fa1b9f86f7b3.CustomDestinations-Ms	**Type :** data **MD5 :** 054bc35e08870709e8e043c42e73bb6b **SHA-1 :** 178ec236cb049465da1fabed34d020db41c2141f **SHA-256 :** dd6d7797cb4cf0287050675f94322fd85e4d9b96 **SHA-512 :** 5c57ce18fd907a3e920f9d8ba3dd05de83079662 **Size :** 8.39 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad58 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1048.Dll **C:\Program Files\CCleaner\Lang\Lang-1048.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 50a63f115a8b53ef91ab44d9a309962f **SHA-1 :** 216ad3e3f5a9e78df5fe99582378c6256122966c **SHA-256 :** c385b9bb3caecc4d152b29cac4d398f3d2eecbb3 **SHA-512 :** 432f7b51c8f6815a3c22769862b20f48f044a8385 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Shortcuts	**Type :** SQLite 3.x database **MD5 :** a4ffc074e2440dd847dfddc661a05406 **SHA-1 :** 5805c333ea5257ececbea06d6133e1c95fc20268 **SHA-256 :** 926fffa70f6dd89c0c3d16b559df10ec3330c2c0f3 **SHA-512 :** 93e3291bf2797536772be385015ee7f34a48d57c **Size :** 20.48 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1042.Dll **C:\Program Files\CCleaner\Lang\Lang-1042.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bebb627cecdd0e47c9e8157448fa68b0 **SHA-1 :** f7acaf54df383f4f49d4e04c66e9fb34226195b8 **SHA-256 :** 2b3508bf0daf4b3aeef7bfbe7e7041f0ddb674547 **SHA-512 :** 9888ee8785d20414ab1b410b7e3e16d8cd029c4 **Size :** 38.4 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1029.Dll **C:\Program Files\CCleaner\Lang\Lang-1029.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f5f2fa1cffd7a8e759524c743d842dc6 **SHA-1 :** f6c0e485ef533e9040666935eef12b565099537c **SHA-256 :** 2d10962f1598724be6fc287efc7e8ad54b7e1c83c **SHA-512 :** 91f631fb7d9f165d6781d3f17aac50bf4f47e6f69f4 **Size :** 65.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1034.Dll **C:\Program Files\CCleaner\Lang\Lang-1034.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 38ef53518fa97e5e0480ad539568bf05 **SHA-1 :** dfa87e0444faba9b9dd109d1b2c4ec1558a4e3a5 **SHA-256 :** d702263c1b4d797f74629aae53182869e960f945 **SHA-512 :** be1d1f455fd3bd6739e18e9ac5f1ecc46cd164d98 **Size :** 77.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-3098.Dll **C:\Program Files\CCleaner\Lang\Lang-3098.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4e0e4673c4490ebd2fd132f5a6dd1b41 **SHA-1 :** 3288f14c2f76ac2440f32144cf81f8c7ccbaf829 **SHA-256 :** 868c9f1bc92bba232f3b4bea5f7faa9d1be9f8f73e **SHA-512 :** ee22b40b2d2b401c66d9acfac01c49c0d591b4a2 **Size :** 69.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1109.Dll **C:\Program Files\CCleaner\Lang\Lang-1109.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c3567d5e9defc5b0c359811a31a6bc13 **SHA-1 :** cf6c1604d5c6c0a64fb97806a1d589a0d41e953b **SHA-256 :** e30c0f44a4a5f5e4f04a4d64dc52f1a1597649d9e **SHA-512 :** 06ceb5ea823ca5752402e1a7a3d293907616f49b **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1055.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** b00bd0ae677db12d912f64e0e842df11 **SHA-1 :** 140abaf67fc7fda54dbd7227bf221e8eb55d8b0d **SHA-256 :** f8ca17cc913bbf7a7b4bb04643384d1cc488e5a93 **SHA-512 :** e89ec77310ce24ed4306529ac460909f84538757 **Size :** 3.715 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1045.Dll **C:\Program Files\CCleaner\Lang\Lang-1045.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0f00a00fc5a220b7ff6a11d9abc2f614 **SHA-1 :** f0c5f5276ff409ab90a6b85d165e2a2c93df6fb6 **SHA-256 :** 1d462bbe5772b00f0d3a835f46e3eb403aa49c63 **SHA-512 :** 74454f59b035708a733dc46c714e37a70b32acfd **Size :** 73.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_2070.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** b93114dd50be7b2a006d77fd4f8795e6 **SHA-1 :** f185121c6575706759dd56d0d7d7d0fb8b7ddf79 **SHA-256 :** fe9d93184f525275b7baca40f82dcc6205cb20258 **SHA-512 :** af36eb806b4f4556e3082d708bf4ee5b192f7a0d **Size :** 3.691 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1043.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 00ea5653c95ccac4a0c58e90a74302bf **SHA-1 :** c75eaa13203753c966c06d8ba72d4a07d2f8c716 **SHA-256 :** 56e4053e97d6c0f858de5250922c7db88b4646bb **SHA-512 :** b190c3f95391110f4755d8aad73276a87e6c2652 **Size :** 3.583 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\Lang-1032.Dll **C:\Program Files\CCleaner\Lang\Lang-1032.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 58a34b883be99759dcafd9461e9d66d0 **SHA-1 :** d27b43d8d8a895e8ebc304577c902e29fc4700d0 **SHA-256 :** 744cc6e9325ecb1d1cc16967aedd1c69c1ba3fc1 **SHA-512 :** 4834b0d10b05596f5d7c8b944bb03a28d2958c1 **Size :** 77.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1050.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 58bb2538d1f9a2cb0a441113a8469edf **SHA-1 :** d76ab709fbd113d5d0e024747f62950f743ac320 **SHA-256 :** ddbd7cc2c42edd53a027a85e0ec14c88c068dd3 **SHA-512 :** 0bf69da90028c49b8b5c85b697d70157039b325 **Size :** 3.612 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1054.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** a95bb0cee0f4afad6872783150704461 **SHA-1 :** c5b8a10579710a4847af873258fba5a6740f9b5b **SHA-256 :** 082d294077778b52adebf79c8606a0fdf844775c **SHA-512 :** 0929d27c158ff071859a66deef5c3351dee67d2d4 **Size :** 4.521 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1060.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** 8f6e01aa42b8381ece3290fbef846090 **SHA-1 :** 22756e5a8620102b7089bc09c1f0d4ce9d1143a2 **SHA-256 :** 27dcf2ccb6d1fe67fffc917c239d76908289ecdc93 **SHA-512 :** f54cf75ba9316ca1c4ad3ed159316b56102cd3f2c **Size :** 3.531 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\G\Gcombo\ComboOffer_1042.Html	**Type :** HTML document, UTF-8 Unicode text **MD5 :** aa6d057a4a77887d17643d19565e36cb **SHA-1 :** 9edaafcc3e1888971da1e31a406e183124b9a244 **SHA-256 :** 47e256c785a6d00bc22b5904c8d1d0823cf27fb2 **SHA-512 :** 7c1b23523098afd8a3c23c313b9dacff23bd1a147 **Size :** 3.69 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\ButtonEvent.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c24568a3b0d7c8d7761e684eb77252b5 **SHA-1 :** 66db7f147cbc2309d8d78fdce54660041acbc60d **SHA-256 :** e2da6d8b73b5954d58baa89a949aacece0527df **SHA-512 :** 5d43e4c838fd7f4c6a4ab6cc6d63e0f81d765d9ca **Size :** 5.12 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsgA9D4.Tmp\Ui\Res\PF_logo.Png	**Type :** PNG image data, 123 x 25, 8-bit/color RGB, non-interlaced **MD5 :** 079cca30760cca3c01863b6b96e87848 **SHA-1 :** 98c2ca01f248bc61817db7e5faea4a3d8310db50 **SHA-256 :** 8dd37d3721e25c32c5bf878b6dba9e61d04b7ce **SHA-512 :** 3e25c10e3a5830584c608b9178ab062e93e0e90 **Size :** 3.346 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	ccsetup533.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	c705c0b0210ebda6a3301c6ca9c6091b2ee11d5b
MD5:	75735db7291a19329190757437bdb847
First Seen Date:	2017-08-16 05:34:48.181869 (2 years ago)
Number Of Clients Seen:	21
Last Analysis Date:	2017-09-20 12:45:24.345822 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	5
Compilation Time Stamp	0x5682FC79 [Tue Dec 29 21:34:49 2015 UTC]
Entry Point	0x403a1c (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	9791816
Sha256	1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7250	0x7400	6.46491468355	2cf4cea611906abda27f6bec5b76ffbd
.rdata	0x9000	0x2b38	0x2c00	4.41938697887	5275f8cae603f81939930ac752de3d01
.data	0xc000	0x67edc	0x200	1.89688793125	3096d49b7b4c3de8338c4639cbb79a13
.ndata	0x74000	0x359000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x3cd000	0x8d3c	0x8e00	4.96141676167	ebe7c4587da7f94a51ca4527b4961e11

CERTIFICATE VALIDATION

- Success ✔

[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 00:00:00
End Date	2020-12-31 23:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

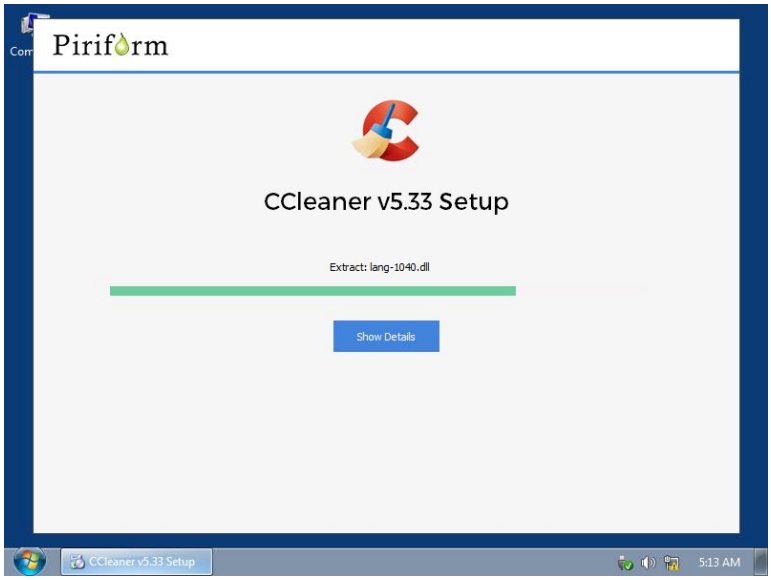
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

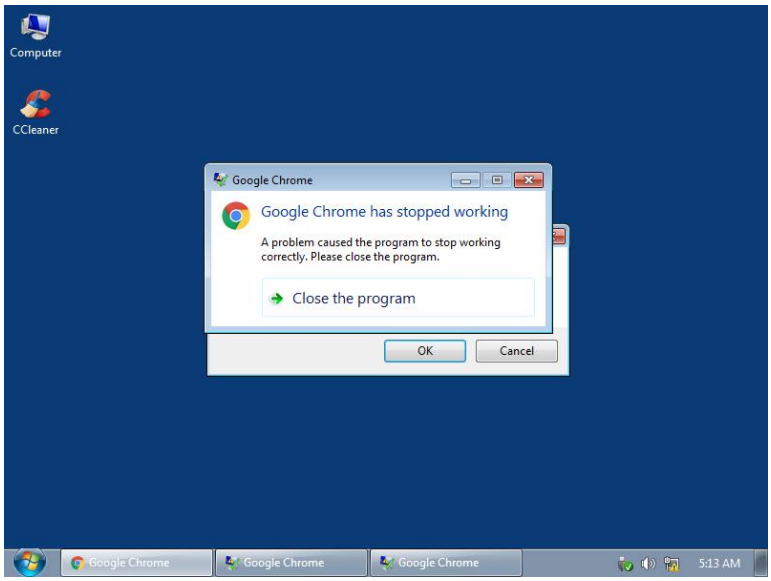
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00
End Date	2036-07-16 23:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

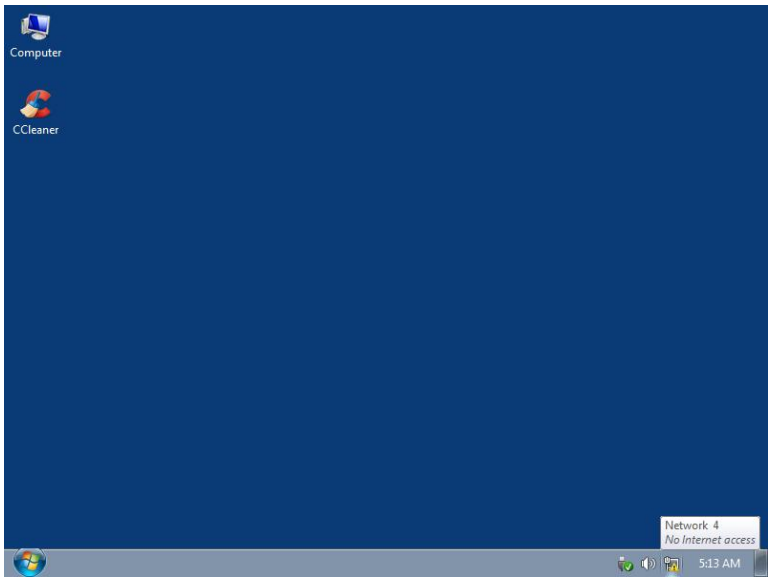
[+] Symantec Class 3 SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 00:00:00
End Date	2023-12-09 23:59:59
Sha256	0649cde463467e8e26bb6b7c23965e030248f95df21f6dcf28c51507fbb77c08
Serial	3D78D7F9764960B2617DF4F01ECA862A
Subject Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Crl link	http://s1.symcb.com/pca3-g5.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Client Authentication (1.3.6.1.5.5.7.3.2)"}

[+] Piriform Ltd	
Status	NoError ✔
Start Date	2015-08-12 00:00:00
End Date	2018-10-10 23:59:59
Sha256	8101958f74ecbef127b03ecb0fd6f24d5e709670eb5fa105d5334dc9c766a334
Serial	4B48B27C8224FE37B17A6A2ED7A81C9F
Subject Key Identifier	6e 5a fa 49 7f 13 a6 28 2b 16 22 c5 43 aa fb da b6 80 d6 4e
Issuer Name	Symantec Class 3 SHA256 Code Signing CA
Issuer Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Crl link	http://sv.symcb.com/sv.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

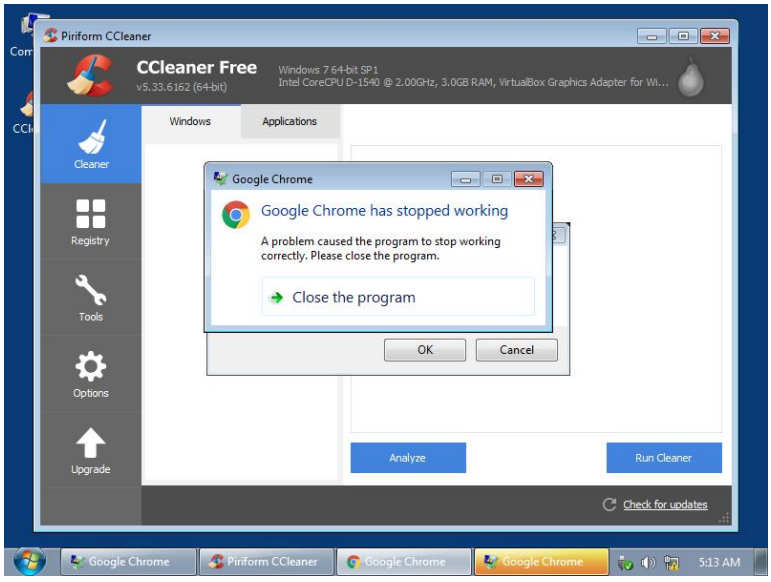
SCREENSHOTS

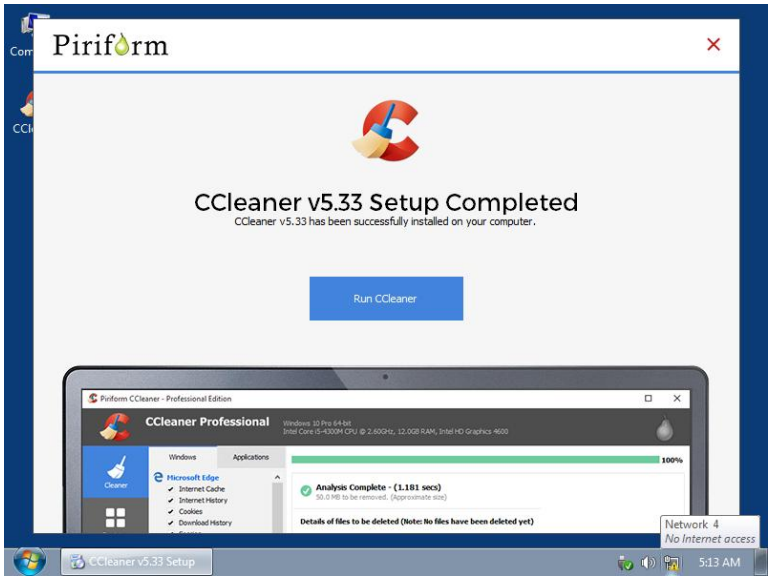

Piriform
CCleaner v5.33 Setup
Extract: lang-1040.dll
Show Details
CCleaner v5.33 Setup
5:13 AM

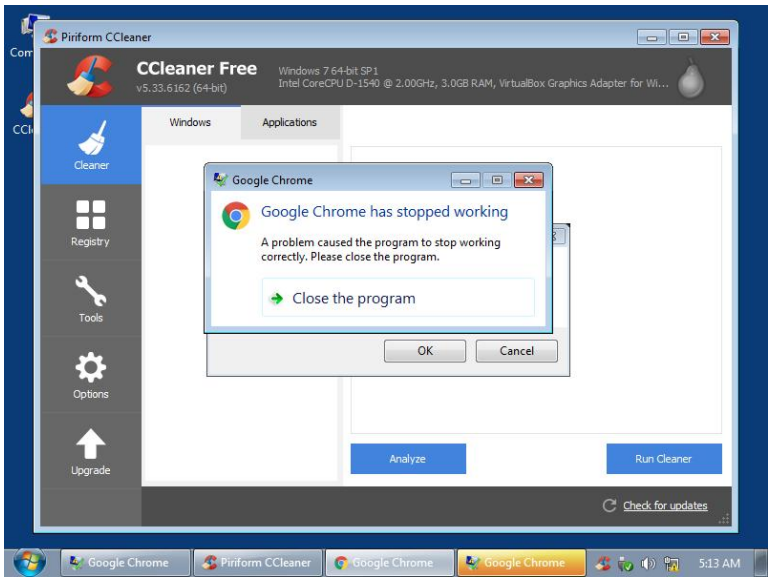

Computer
CCleaner
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
OK
Cancel
Google Chrome
Google Chrome
Google Chrome
5:13 AM

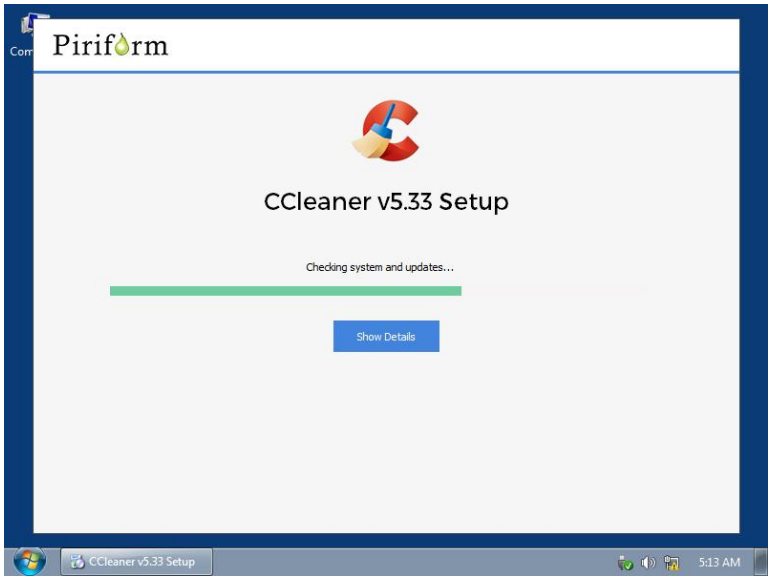

Computer
CCleaner
Network 4
No Internet access
5:13 AM


Computer
5:12 AM

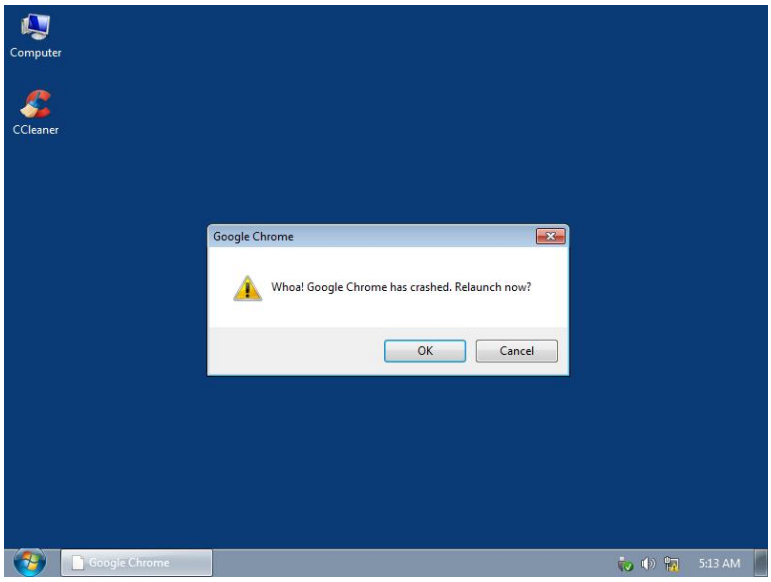

Piriform CCleaner
CCleaner Free
v5.33.6162 (64-bit)
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Windows
Applications
Cleaner
Registry
Tools
Options
Upgrade
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
OK
Cancel
Analyze
Run Cleaner
Check for updates
Google Chrome
Piriform CCleaner
Google Chrome
Google Chrome
5:13 AM

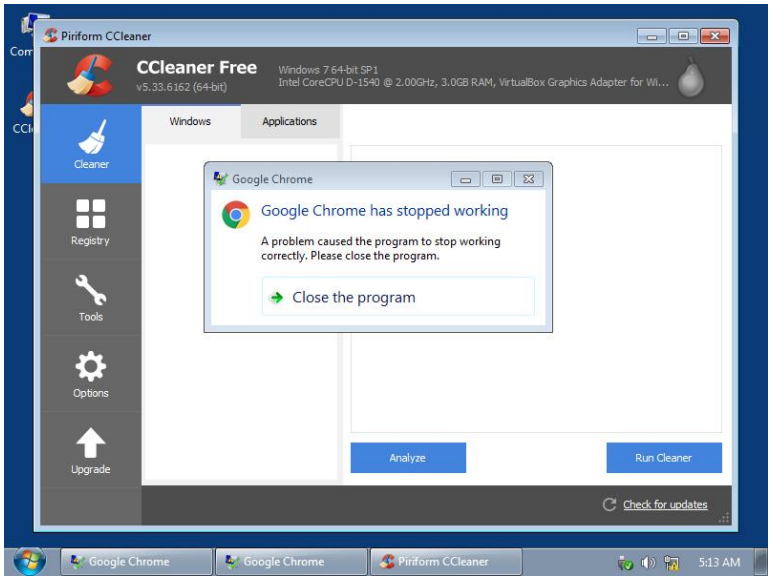

Piriform
CCleaner v5.33 Setup Completed
CCleaner v5.33 has been successfully installed on your computer.
Run CCleaner
CCleaner Professional
Analysis Complete - (1.181 secs)
Network 4
No Internet access
CCleaner v5.33 Setup
5:13 AM

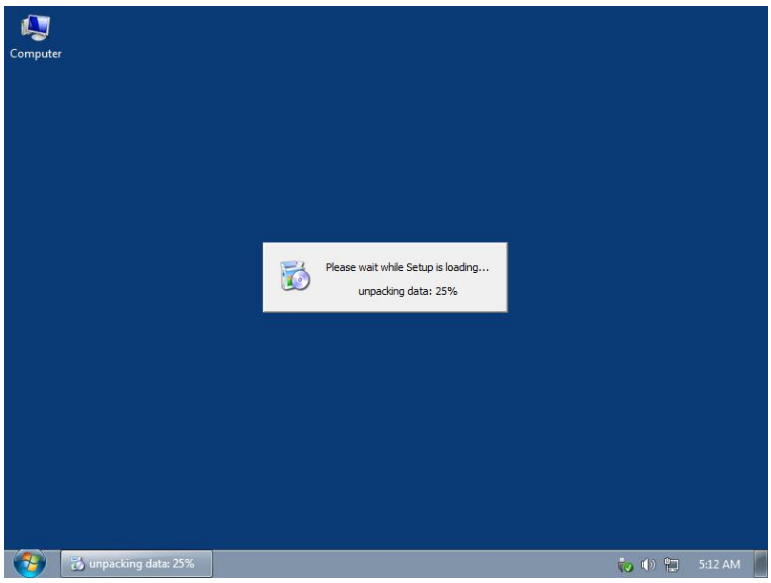

Piriform CCleaner
CCleaner Free
v5.33.6162 (64-bit)
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Windows
Applications
Cleaner
Registry
Tools
Options
Upgrade
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
OK
Cancel
Analyze
Run Cleaner
Check for updates
Google Chrome
Piriform CCleaner
Google Chrome
Google Chrome
5:13 AM

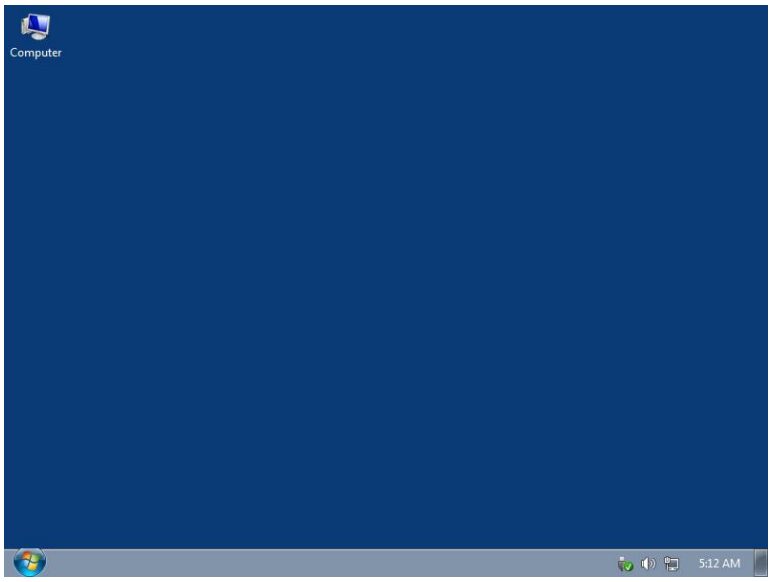

Piriform
CCleaner v5.33 Setup
Checking system and updates...
Show Details
CCleaner v5.33 Setup
5:13 AM

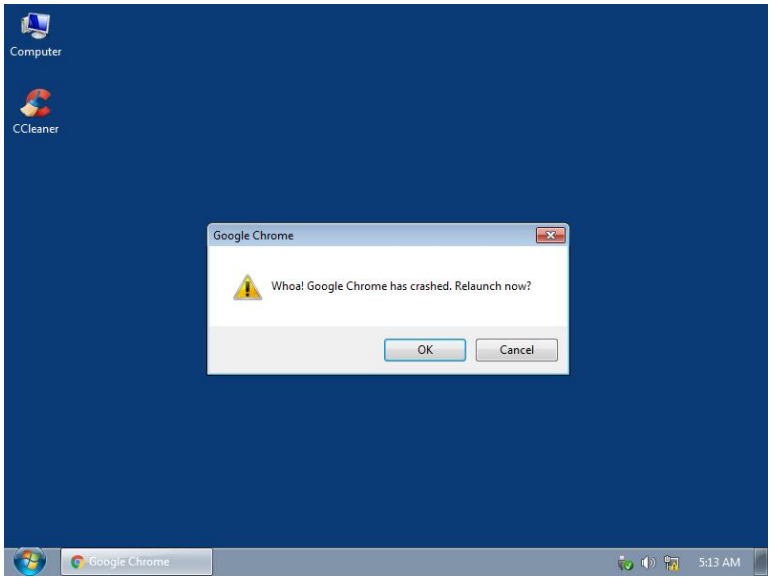

Computer
5:12 AM

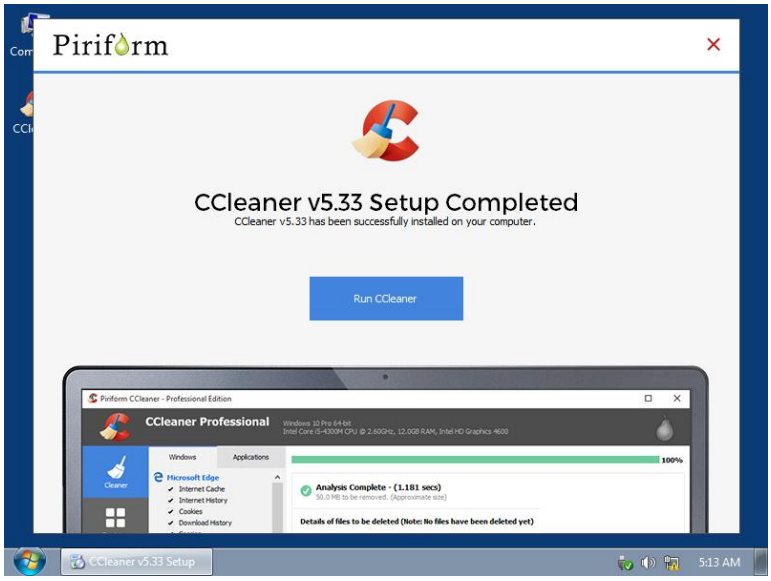

Computer
CCleaner
Google Chrome
Whoa! Google Chrome has crashed. Relaunch now?
OK
Cancel
Google Chrome
5:13 AM


Piriform CCleaner
CCleaner Free
v5.33.6162 (64-bit)
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Windows
Applications
Cleaner
Registry
Tools
Options
Upgrade
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Analyze
Run Cleaner
Check for updates
Google Chrome
Google Chrome
Piriform CCleaner
5:13 AM

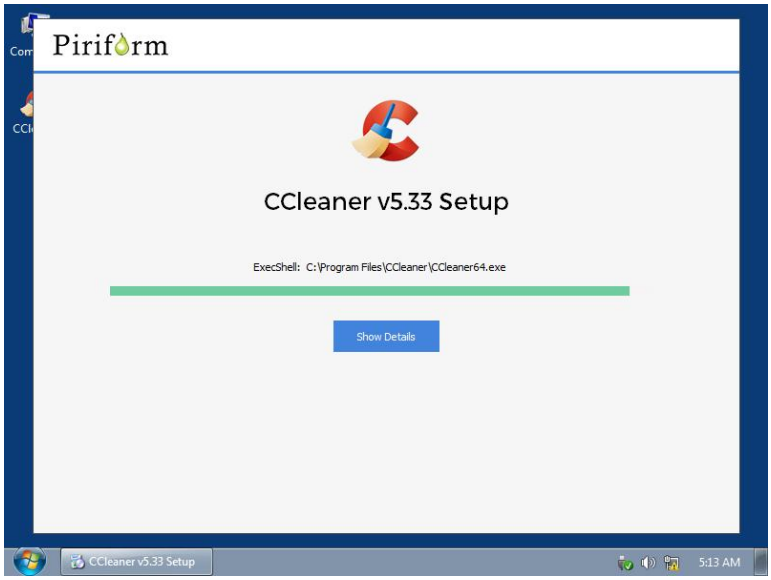

Computer
Please wait while Setup is loading...
unpacking data: 25%
unpacking data: 25%
5:12 AM

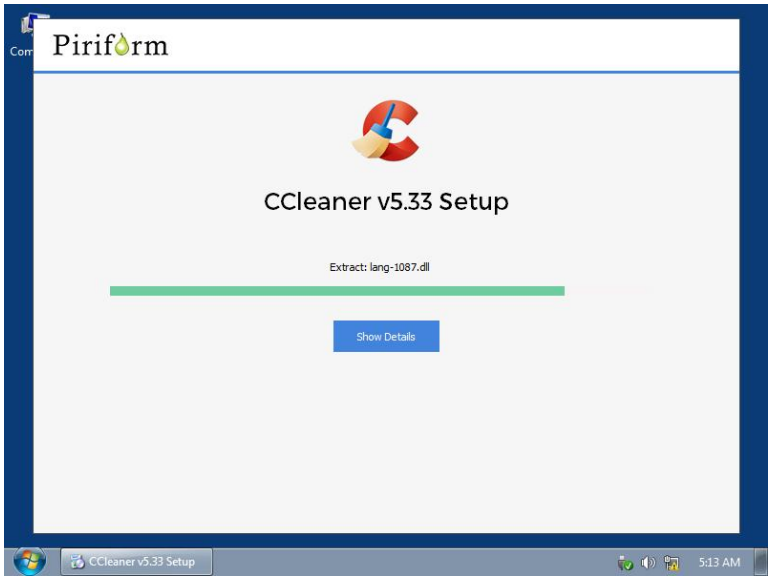

Computer
5:12 AM

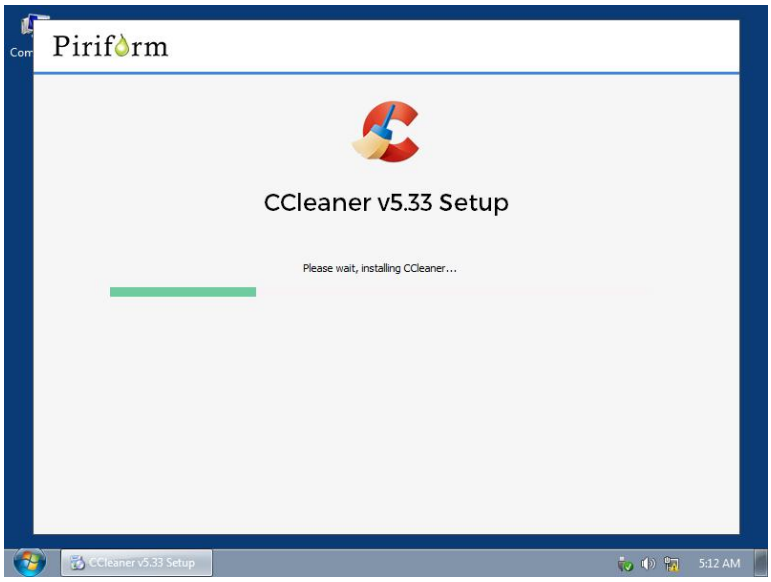

Computer
CCleaner
Google Chrome
Whoa! Google Chrome has crashed. Relaunch now?
OK
Cancel
Google Chrome
5:13 AM

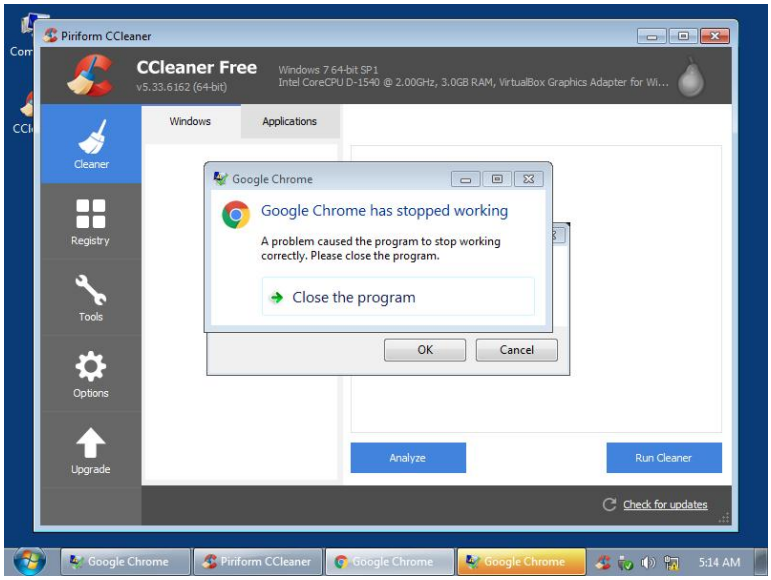

Piriform
CCleaner v5.33 Setup Completed
CCleaner v5.33 has been successfully installed on your computer.
Run CCleaner
CCleaner Professional
Analysis Complete - (1.181 secs)
Details of files to be deleted (Note: No files have been deleted yet)
CCleaner v5.33 Setup
5:13 AM

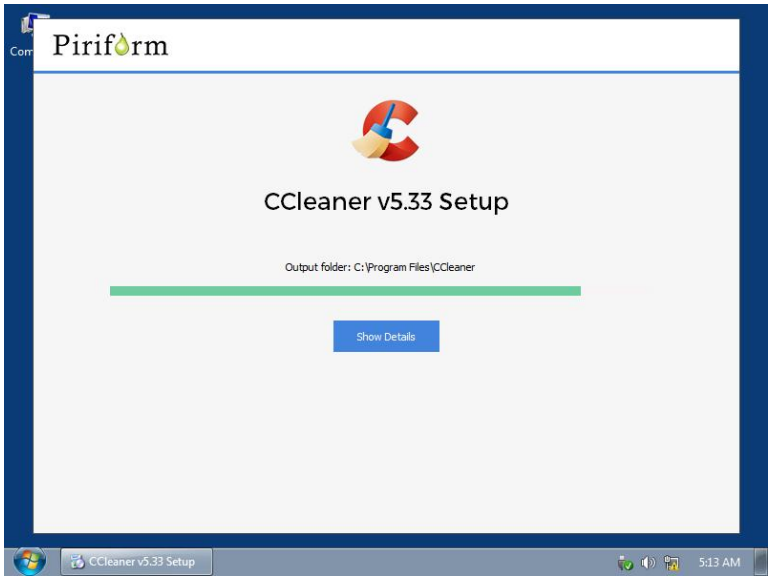

Computer
CCleaner
5:13 AM


Piriform
CCleaner v5.33 Setup
ExecShell: C:\Program Files\CCleaner\CCleaner64.exe
Show Details
CCleaner v5.33 Setup
5:13 AM

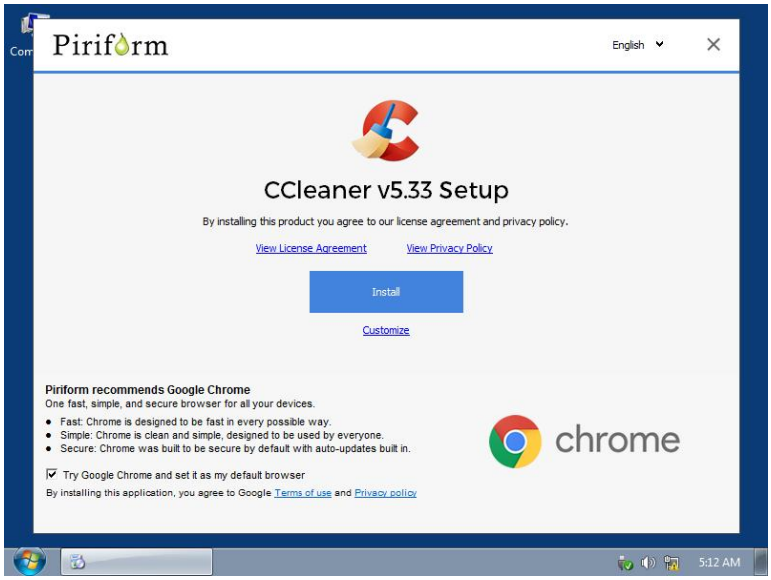

Piriform
CCleaner v5.33 Setup
Extract: lang-1087.dll
Show Details
CCleaner v5.33 Setup
5:13 AM

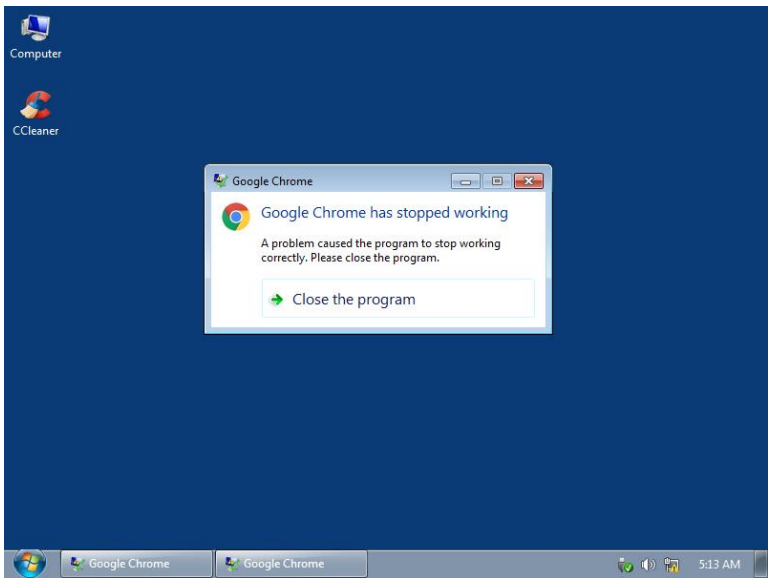

Piriform
CCleaner v5.33 Setup
Please wait, installing CCleaner...
CCleaner v5.33 Setup
5:12 AM


Piriform CCleaner
CCleaner Free
v5.33.6162 (64-bit)
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Windows
Applications
Cleaner
Registry
Tools
Options
Upgrade
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
OK
Cancel
Analyze
Run Cleaner
Check for updates
Google Chrome
Piriform CCleaner
Google Chrome
Google Chrome
5:14 AM


Piriform
CCleaner v5.33 Setup
Output folder: C:\Program Files\CCleaner
Show Details
CCleaner v5.33 Setup
5:13 AM


Computer
CCleaner
5:13 AM


Piriform
English
CCleaner v5.33 Setup
By installing this product you agree to our license agreement and privacy policy.
View License Agreement
View Privacy Policy
Install
Customize
Piriform recommends Google Chrome
One fast, simple, and secure browser for all your devices.
Fast: Chrome is designed to be fast in every possible way.
Simple: Chrome is clean and simple, designed to be used by everyone.
Secure: Chrome was built to be secure by default with auto-updates built in.
Try Google Chrome and set it as my default browser
By installing this application, you agree to Google Terms of use and Privacy policy
chrome
5:12 AM


Computer
CCleaner
Google Chrome
Google Chrome has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Google Chrome
Google Chrome
5:13 AM