VALKYRIE COMODO

Summary

File Name: CCleaner.exe

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

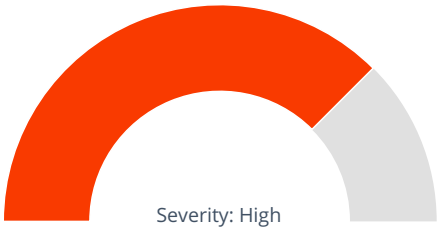
SHA1: 8983a49172af96178458266f93d65fa193eaaef2

MD5: ef694b89ad7addb9a16bb6f26f1efaf7

MALWARE

Valkyrie Final Verdict

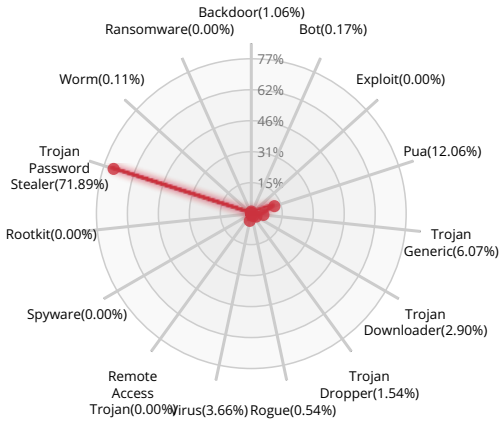
DETECTION SECTION



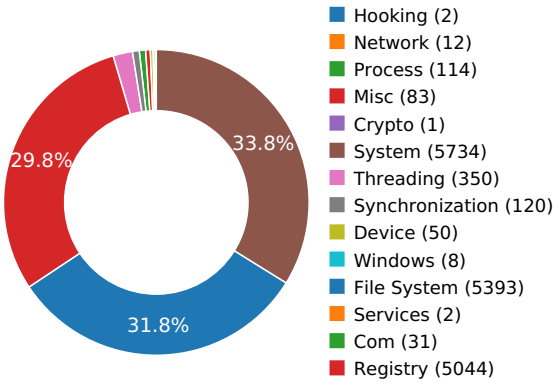
Severity: High

Verdict: Malware

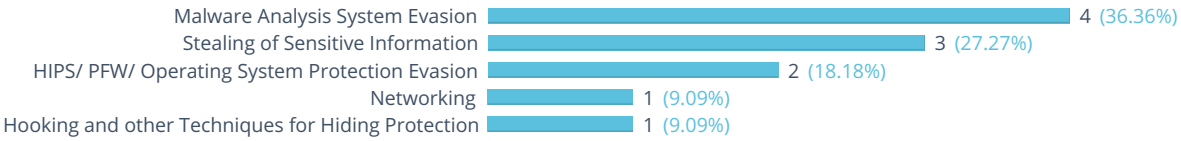
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

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

NETWORKING

Generates some ICMP traffic	

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

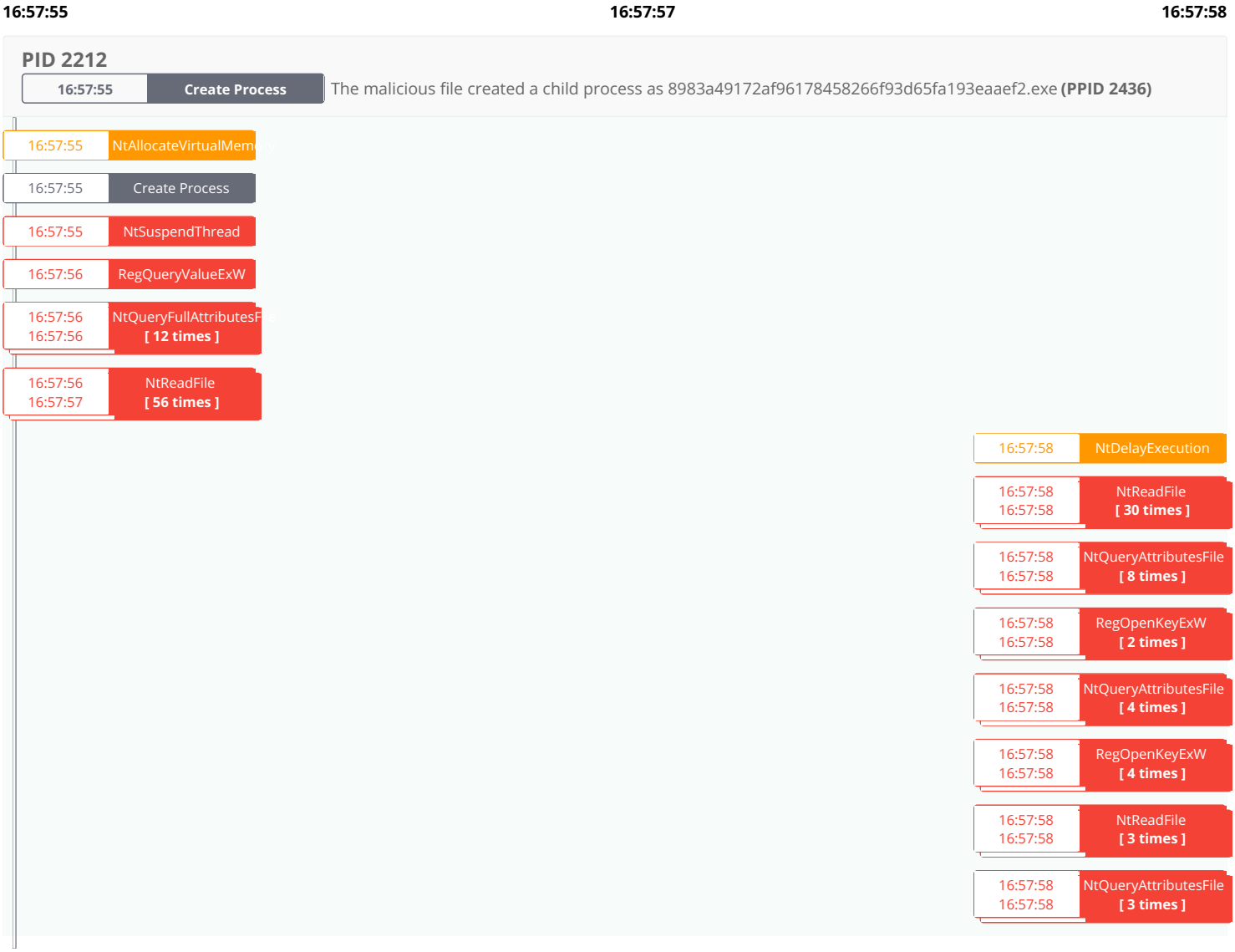
Creates RWX memory	Show sources

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

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\api-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-fibers-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\api-ms-win-core-localization-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\Scripts\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\sysinternals\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-localization-l1-2-1.DLL

C:\Users\user\AppData\Local\Temp\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Python27\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Python27\Scripts\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\tools\sysinternals\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\tools\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-sysinfo-l1-2-1.DLL
\??\Nsi
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\ccleaner_checkpoint.dat
C:\Users\user\AppData\Local\Temp\branding.dll
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\ccleaner.ini
C:\Users\user\AppData\Local\Temp\portable.dat
C:\Users\user\AppData\Local\Temp\8983a49172af96178458266f93d65fa193eaaef2.dat
C:\Users\user\AppData\Local\Temp\license.ini
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Windows\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-1.DLL

C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Python27\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\tools\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\ext-ms-win-kernel32-package-current-l1-1-0.DLL

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
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_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings\Anchor Color
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings\Anchor Color Visited
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\FontSubstitutes\Tahoma
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem\NtfsDisableLastAccessUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Piriform\CCleaner\WipeFreeSpaceDrives
HKEY_CURRENT_USER\Software\Piriform\CCleaner\WipeMFTFreeSpace
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\svcVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Start Menu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser

MODIFIED FILES

C:
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\Internet Explorer\DOMStore\index.dat
\??\PIPE\srvsvc

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\IWQKYCEEUGVHO1G0YNP6.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\c3f711b4f59871fb.customDestinations-ms
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\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite-wal
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite-shm
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\OfflineCache\index.sqlite
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\Google\Chrome\User Data\Default\databases\Databases.db

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.InitOnceExecuteOnce
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreW
kernel32.dll.CreateSemaphoreExW
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.CreateSymbolicLinkW
kernel32.dll.GetTickCount64
kernel32.dll.GetFileInformationByHandleEx
kernel32.dll.SetFileInformationByHandle
kernel32.dll.InitializeConditionVariable
kernel32.dll.WakeConditionVariable
kernel32.dll.WakeAllConditionVariable
kernel32.dll.SleepConditionVariableCS
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.TryAcquireSRWLockExclusive
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.SleepConditionVariableSRW
kernel32.dll.CreateThreadpoolWork
kernel32.dll.SubmitThreadpoolWork
kernel32.dll.CloseThreadpoolWork
kernel32.dll.CompareStringEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.CreateHardLinkW
kernel32.dll.IsWow64Process
user32.dll.EnableScrollBar
user32.dll.GetScrollInfo
user32.dll.GetScrollPos
user32.dll.GetScrollRange
user32.dll.SetScrollInfo
user32.dll.SetScrollPos
user32.dll.SetScrollRange
user32.dll.ShowScrollBar
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Thread32First
kernel32.dll.Thread32Next
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualAlloc
msvcrt.dll.memcpy
kernel32.dll.LocalFree

kernel32.dll.LocalAlloc
kernel32.dll.lstrcmpiA
kernel32.dll.OpenProcess
kernel32.dll.GetVersionExA
kernel32.dll.VirtualFree
kernel32.dll.GetLocalTime
kernel32.dll.Sleep
kernel32.dll.GetComputerNameExA
kernel32.dll.GetComputerNameA
kernel32.dll.ExitThread
kernel32.dll.GetFileAttributesA
kernel32.dll.GetProcAddress
kernel32.dll.GetTickCount
kernel32.dll.CreateThread
kernel32.dll.GetCurrentProcess
kernel32.dll.CloseHandle
advapi32.dll.LookupPrivilegeValueA
advapi32.dll.AdjustTokenPrivileges
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegCloseKey
advapi32.dll.OpenProcessToken

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\IWQKYCEEUGVHO1G0YNP6.temp
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\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite-wal

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Piriform\CCleaner\AutoICS
HKEY_CURRENT_USER\Software\Piriform\CCleaner\AutoUpdateNotificationExpiryTime

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

HKEY_CLASSES_ROOT\CLSID\{FAE3D380-FEA4-4623-8C75-C6B61110B681}\Instance
HKEY_CLASSES_ROOT\CLSID\{FAE3D380-FEA4-4623-8C75-C6B61110B681}\Instance\Disabled
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\CCleaner\Options
HKEY_CURRENT_USER\Software\Piriform\CCleaner
HKEY_LOCAL_MACHINE\Software\Piriform\CCleaner
HKEY_LOCAL_MACHINE\Hardware\Description\System\CentralProcessor
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
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\Tahoma
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Settings
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\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\8983a49172af96178458266f93d65fa193eaaef2.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\Windows NT\CurrentVersion\FontSubstitutes\Tahoma
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem\NtfsDisableLastAccessUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Piriform\CCleaner\WipeFreeSpaceDrives
HKEY_CURRENT_USER\Software\Piriform\CCleaner\WipeMFTFreeSpace
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer
HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Spartan_cw5n1h2txyewy
HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\svcVersion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\8983a49172af96178458266f93d65fa193eaaef2.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name

READ FILES

\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\ccleaner_checkpoint.dat
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\Fonts\staticcache.dat
C:
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
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\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini

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:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\index.dat
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\Microsoft\Windows\Recent\CustomDestinations\c3f711b4f59871fb.customDestinations-ms
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos\desktop.ini
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Music\desktop.ini
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Documents\desktop.ini
C:\Users\user\Links\desktop.ini
C:\Users\user\Saved Games\desktop.ini
\??\PIPE\srvsvc

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\IWQKYCEEUGVHO1G0YNP6.temp

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\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webappsstore.sqlite

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

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

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\OfflineCache\index.sqlite

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\Google\Chrome\User Data\Default\databases\Databases.db

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol

MUTEXES

Piriform_CCleaner_PreventSecondInstance

Piriform_CCleaner_SystemTrayIconActive

CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1

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!

Local\c:!users!user!appdata!local!microsoft!internet explorer!domstore!

IESQMMUTEX_0_208

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Piriform\CCleaner

HKEY_CURRENT_USER\Software\Piriform\CCleaner\WipeFreeSpaceDrives

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

HKEY_CURRENT_USER\Software\Piriform\CCleaner\CookiesToSave

HKEY_CURRENT_USER\Software\Piriform\CCleaner\RunICS

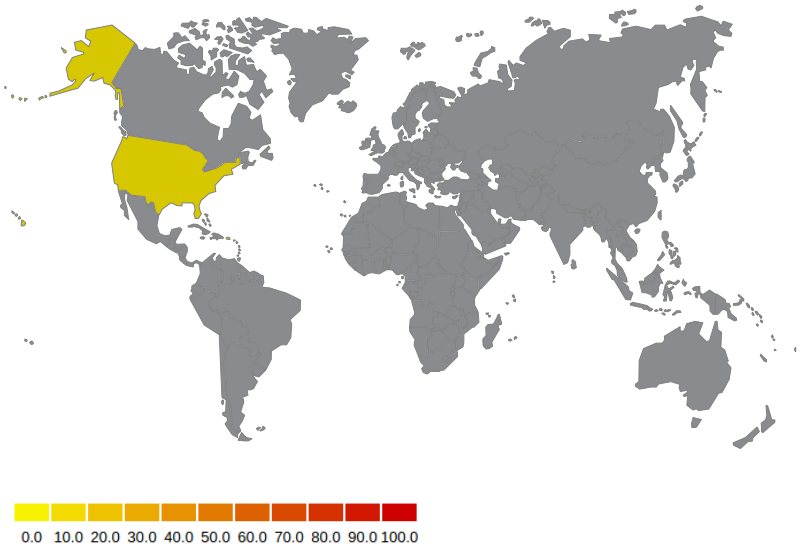
HKEY_CURRENT_USER\Software\Piriform\CCleaner\Monitoring

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-

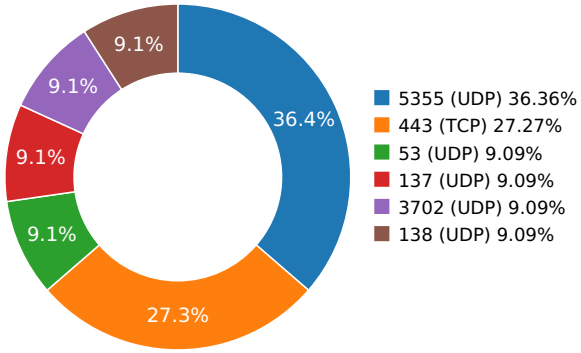
A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
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

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 Parent, LLC	Malware Process
www.piriform.com	151.101.0.64	United States	54113	Fastly	Malware Process

DNS QUERIES

Request	Type
www.piriform.com	A
Answers - 151.101.0.64 (A) - 151.101.192.64 (A) - 151.101.64.64 (A) - 151.101.128.64 (A) - f.global-ssl.fastly.net (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.2432219982	Sandbox	151.101.0.64	443
12.2664370537	Sandbox	151.101.0.64	443
12.2887969017	Sandbox	151.101.0.64	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.11384606361	Sandbox	192.168.56.255	137
3.20466685295	Sandbox	224.0.0.252	5355
3.20517086983	Sandbox	224.0.0.252	5355
3.34041786194	Sandbox	239.255.255.250	3702
5.76743388176	Sandbox	224.0.0.252	5355
9.15860390663	Sandbox	192.168.56.255	138
9.45129084587	Sandbox	224.0.0.252	5355
12.1844658852	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
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\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 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6c **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c8 **Size :** 49.152 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 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f08 **Size :** 180.224 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 :** 69a0d29dc846c82d785231dbf94e4c4b731ad588 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\C3f711b4f59871fb.CustomDestinations-Ms	**Type :** data **MD5 :** e6de5f297af0711d802d9e9760f69e55 **SHA-1 :** 78427832ad1c34be27df06a3235829b5500e308b **SHA-256 :** d7ba51323391a94aab00018eaa7d06e482554e8 **SHA-512 :** 4af903d6c33ef6e023185007a80545012596728a **Size :** 9.39 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	CCleaner.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	8983a49172af96178458266f93d65fa193eaaef2
MD5:	ef694b89ad7addb9a16bb6f26f1efaf7
First Seen Date:	2017-09-19 09:24:56.829124 (about a year ago)
Number Of Clients Seen:	29
Last Analysis Date:	2017-09-20 17:10:58.986305 (about a year ago)
Human Expert Analysis Date:	2019-02-14 10:43:13.376523 (7 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	7
Compilation Time Stamp	0x5982EBF9 [Thu Aug 3 09:25:13 2017 UTC]
Entry Point	0x4d4dfd (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	7680216
Sha256	6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x334d01	0x334e00	6.7324585276	649e07bff6f1f89a8323ee36d57fbd31
.rdata	0x336000	0xf7526	0xf7600	4.55320749929	973346732294411152b629f71ba63a47
.data	0x42e000	0x25f4cc	0x5a800	4.22713939648	9c11de22507d6d809474a8a146f71974
.gfids	0x68e000	0x11d4	0x1200	4.11345994361	aa68a98bfa861b9165237d1722e6efa3
.tls	0x690000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0x691000	0x288188	0x288200	6.8002574736	80bded09eb6c7ba616382c96b49f3bd1
.reloc	0x91a000	0x3f72c	0x3f800	6.53156734598	049bb8d50741d337fc497f27cedb5ee7

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

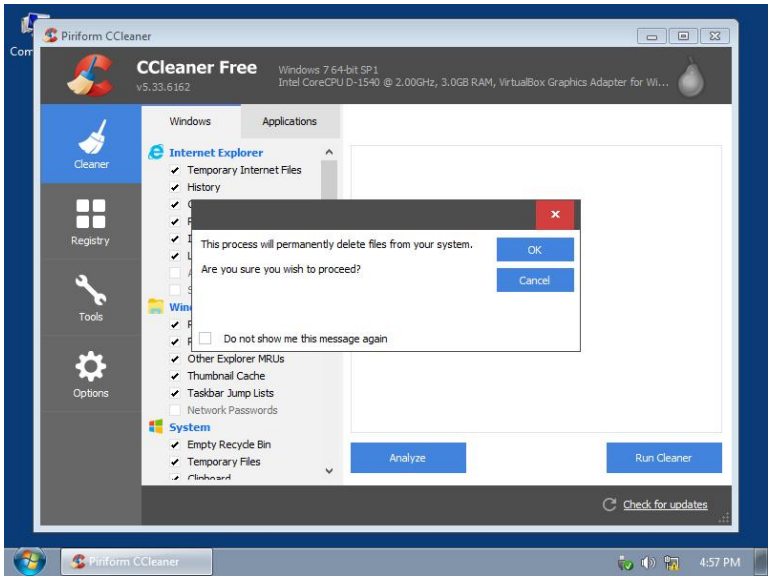
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db 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)"}

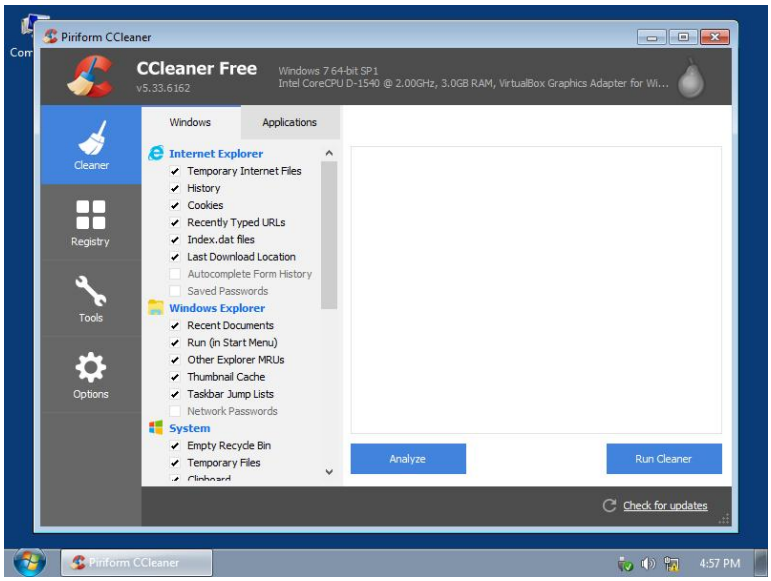
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00
End Date	2036-07-16 23:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb 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
CCleaner Free
v5.33.6162
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Cleaner
Registry
Tools
Options
Windows
Applications
Internet Explorer
Temporary Internet Files
History
This process will permanently delete files from your system.
Are you sure you wish to proceed?
OK
Cancel
Do not show me this message again
Other Explorer MRUs
Thumbnail Cache
Taskbar Jump Lists
Network Passwords
System
Empty Recycle Bin
Temporary Files
Analyze
Run Cleaner
Check for updates
4:57 PM


Piriform CCleaner
CCleaner Free
v5.33.6162
Windows 7 64-bit SP1
Intel CoreCPU D-1540 @ 2.00GHz, 3.0GB RAM, VirtualBox Graphics Adapter for Wi...
Cleaner
Registry
Tools
Options
Windows
Applications
Internet Explorer
Temporary Internet Files
History
Cookies
Recently Typed URLs
Index.dat files
Last Download Location
Autocomplete Form History
Saved Passwords
Windows Explorer
Recent Documents
Run (in Start Menu)
Other Explorer MRUs
Thumbnail Cache
Taskbar Jump Lists
Network Passwords
System
Empty Recycle Bin
Temporary Files
Analyze
Run Cleaner
Check for updates
4:57 PM


Computer
4:57 PM