Summary

File Name: AutoKey.exe.malware

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

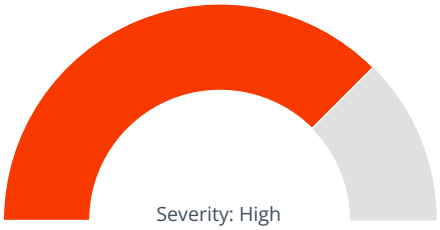
SHA1: 83555e4d225b6c2f74ea4661cefd9f9e9b22970d

MD5: 4a537d90e7f0ffb3a331c6d885e54a79

MALWARE

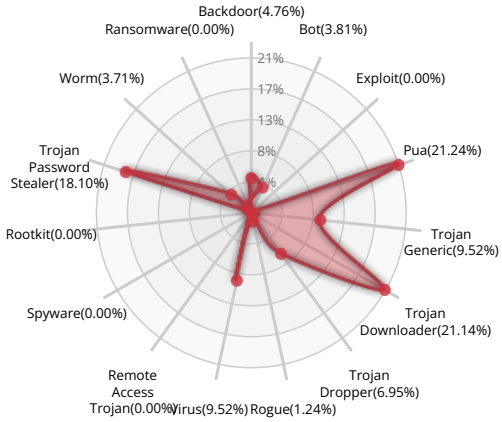
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

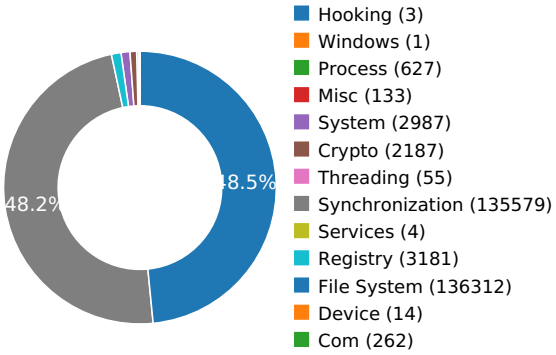


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

STATIC ANOMALY

Anomalous binary characteristics — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task by a long amount of time. — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

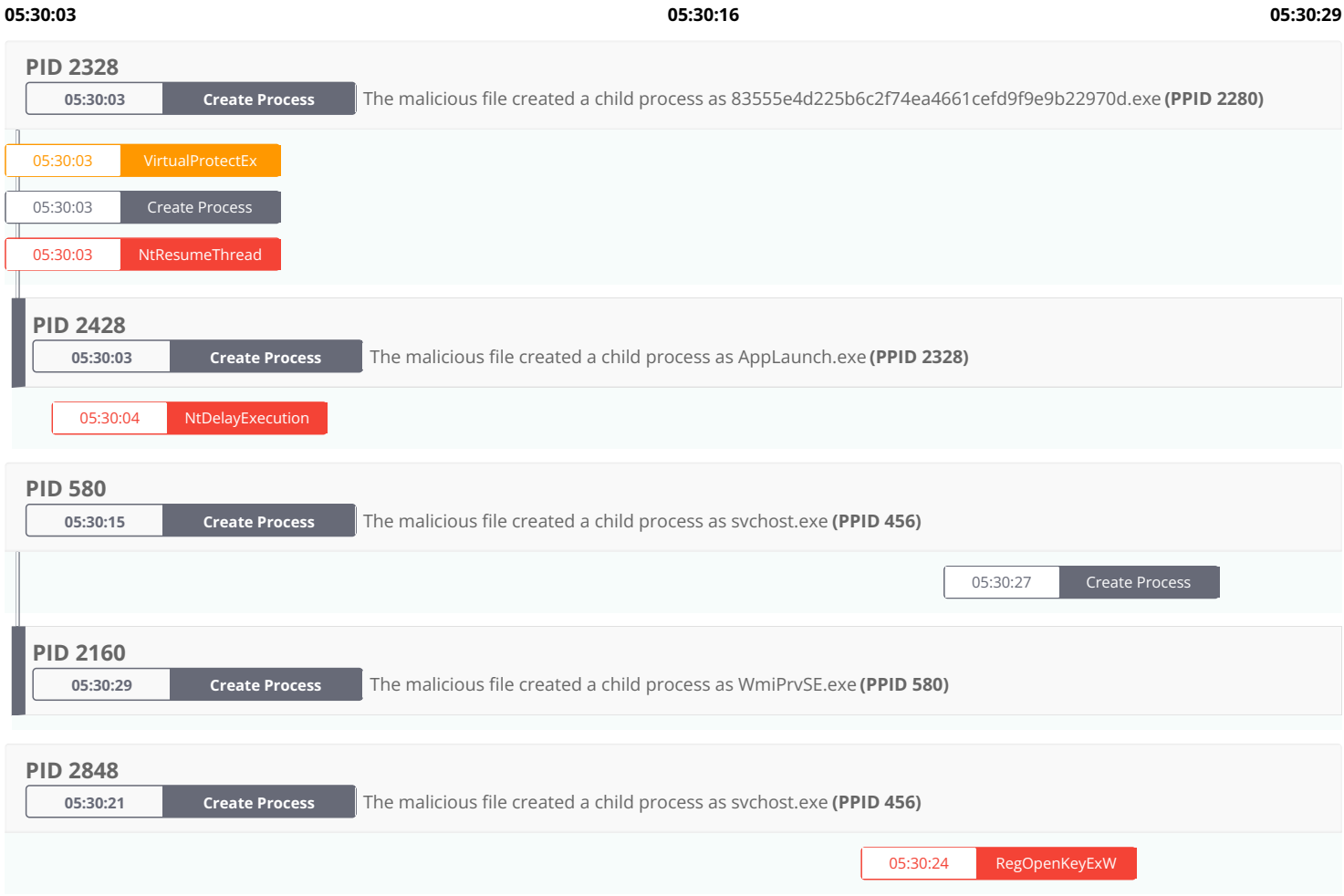
Attempts to block SafeBoot use by removing registry keys — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

Executed a process and injected code into it, probably while unpacking — Show sources

Behavior Graph



Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSVCR120_CLR0400.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoree.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.localgac
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib*
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
C:\Windows
C:\Windows\Microsoft.NET
C:\Windows\Microsoft.NET\Framework
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ole32.dll
\Device\KsecDD
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config
C:\Windows\assembly\NativeImages_v4.0.30319_32\Name*
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.INI
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\Microsoft.Net\assembly\GAC_32\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\469570308309641656 44b52b0696c5d9\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\469570308309641656 44b52b0696c5d9\System.Configuration.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Security.dll
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core*

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll.aux

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Numerics\v4.0_4.0.0.0__b77a5c561934e089\System.Numerics.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml*

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll.aux

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Data.SqlXml\v4.0_4.0.0.0__b77a5c561934e089\System.Data.SqlXml.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\ntdll.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\System.Management\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Management.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar-SA

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar-SA

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg-BG

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg-BG

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca-ES

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca-ES

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-Hans

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-Hans

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-CN

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-CN

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs-CZ

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs-CZ

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\da

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\da

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\da-DK
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\da-DK
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\de
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\de
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\de-DE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\de-DE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\el
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\el
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\el-GR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\el-GR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\es
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\es
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\es-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\es-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fi
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fi
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fi-FI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fi-FI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fr
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fr
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fr-FR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fr-FR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\he
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\he
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\he-IL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\he-IL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\hu
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\hu
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\hu-HU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\hu-HU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\is
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\is
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\is-IS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\is-IS
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\it
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\it
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\it-IT
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\it-IT
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ja
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ja
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ja-JP
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ja-JP
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ko
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ko
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ko-KR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ko-KR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\nl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\nl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\nl-NL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\nl-NL

MODIFIED FILES

\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx

kernel32.dll.AreFileApisANSI
kernel32.dll.FlsFree
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
api-ms-win-core-synch-l1-2-0.dll.SleepConditionVariableCS

api-ms-win-core-synch-l1-2-0.dll.WakeAllConditionVariable
kernel32.dll.FreeConsole
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCIDToLocaleName
kernel32.dll.LocaleNameToLCID
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.GetLogicalProcessorInformation
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback
mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
shlwapi.dll.UrlIsW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
clr.dll.SetRuntimeInfo
clr.dll._CorExeMain
mscoree.dll.CreateConfigStream
mscoreei.dll.CreateConfigStream
kernel32.dll.GetNumaHighestNodeNumber
kernel32.dll.GetSystemWindowsDirectoryW
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken

advapi32.dll.GetTokenInformation

advapi32.dll.InitializeAcl

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ar-SA

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ar-SA

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\bg-BG

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\bg-BG

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ca-ES

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ca-ES

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-Hans

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-Hans

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\zh-CN

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\zh-CN

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\cs-CZ

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\cs-CZ

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\da

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\da

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\da-DK

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\da-DK

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\de

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\de

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\de-DE

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\de-DE
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\el
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\el
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\el-GR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\el-GR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\es
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\es
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\es-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\es-ES
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fi
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fi
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fi-FI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fi-FI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fr
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fr
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\fr-FR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\fr-FR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\he
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\he
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\he-IL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\he-IL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\hu
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\hu
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\hu-HU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\hu-HU
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\is
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\is
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\is-IS
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\is-IS
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\it
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\it
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\it-IT
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\it-IT

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ja
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ja
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ja-JP
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ja-JP
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ko
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ko
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\ko-KR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\ko-KR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\nl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\nl

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
\Device\KsecDD
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\4695703083096416564b52b0696c5d9\System.Configuration.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\4695703083096416564b52b0696c5d9\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll

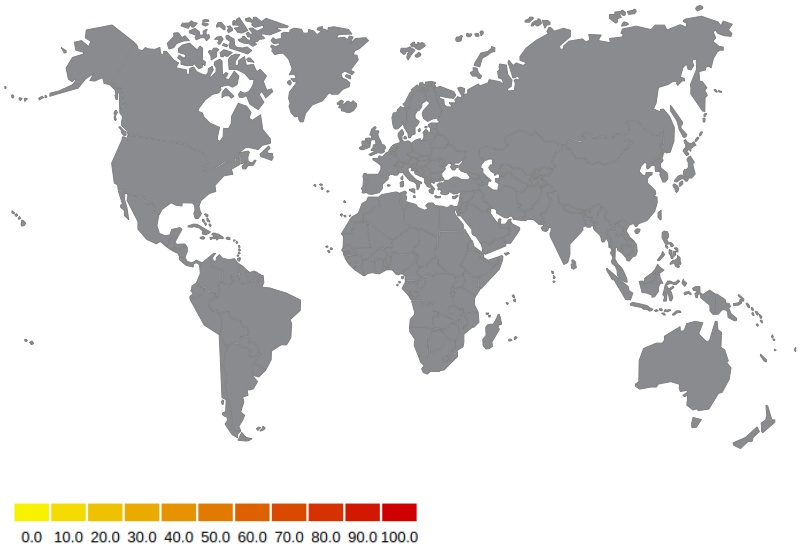
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\wminet_utils.dll
C:\Windows\sysnative\wbem\WmiPrvSE.exe
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Windows\Branding\Basebrd\basebrd.dll
C:
C:\Windows\sysnative\tzres.dll

MODIFIED REGISTRY KEYS

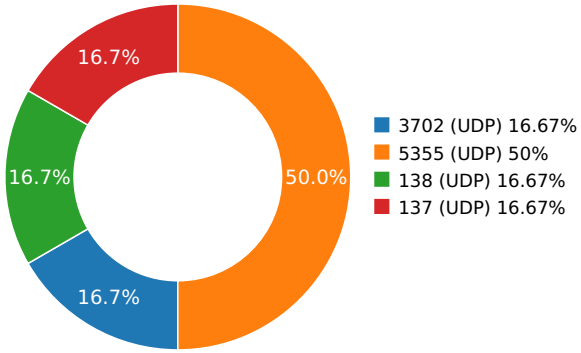
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.72628879547	Sandbox	224.0.0.252	5355
6.72740888596	Sandbox	224.0.0.252	5355
6.73358392715	Sandbox	239.255.255.250	3702
6.76173090935	Sandbox	192.168.56.255	137
9.32039999962	Sandbox	224.0.0.252	5355
12.7615308762	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	AutoKey.exe.malware
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	83555e4d225b6c2f74ea4661cefd9f9e9b22970d
MD5:	4a537d90e7f0ffb3a331c6d885e54a79
First Seen Date:	2023-06-24 09:17:50.840095 (4 days ago)
Number Of Clients Seen:	2
Last Analysis Date:	2023-06-24 14:05:21.486252 (3 days ago)
Human Expert Analysis Date:	2023-06-25 14:57:44.878255 (2 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	11
Trid	[]
Compilation Time Stamp	0x6495A4FB [Fri Jun 23 13:58:19 2023 UTC]
Entry Point	0x44b1ef (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1174968
Ssdeep	
Sha256	b8e5c688ae452cb32081a9d049f7c7a7532f330df35e87d72ab8ac96f9153feb
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.textbss	0x1000	0x49532	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.text	0x4b000	0xa7839	0xa7a00	5.73813197992	75ee95bc69ffe22444dd20598f40f9aa
.rdata	0xf3000	0x1afa2	0x1b000	4.09784659054	72d7ffb41a60905d8d5edbfae53f83c8
.data	0x10e000	0x4da0	0x3000	3.71813935214	dc954b9395bf37b8ffe8055a0d232ab7
.idata	0x113000	0x1474	0x1600	4.62231358499	be4093ec2ff9940650a1b931f9166787
.bss	0x115000	0x3ef6d	0x3f000	6.12213633467	f0a9cca51fa2463ee02b56a33afb694c
.xsbss	0x154000	0x116	0x200	0.0	bf619eac0cdf3f68d496ea9344137e8b
.tls	0x155000	0x309	0x400	0.0111738187212	c573bd7cea296a9c5d230ca6b5aee1a6
.00cfg	0x156000	0x10e	0x200	0.110557131259	3d41ec9475fa1e437dc48bd5b0376e2b
.reloc	0x157000	0x5f81	0x6000	5.97136918245	235bd02debd0b91decf65e56aedc3df4
.rsrc	0x15d000	0x50e	0x600	4.72602877122	1cfcfeee338e96cbf0438e87eb7a60f0

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 1429592, u'sha256': u'a43ab388e18d22dc45574c702b2e9ca1a873f3be65e81869f2902892c37b4695', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1206}

CERTIFICATE VALIDATION

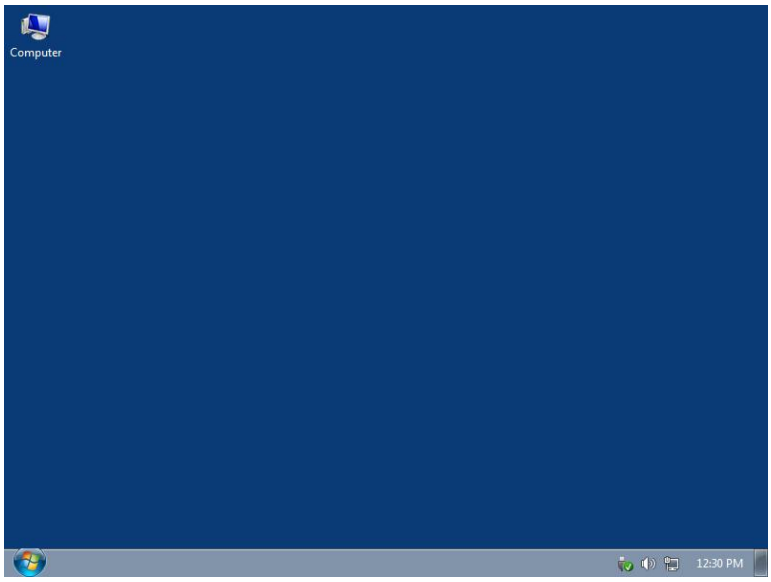
- SignatureOrFileCorrupt ✖

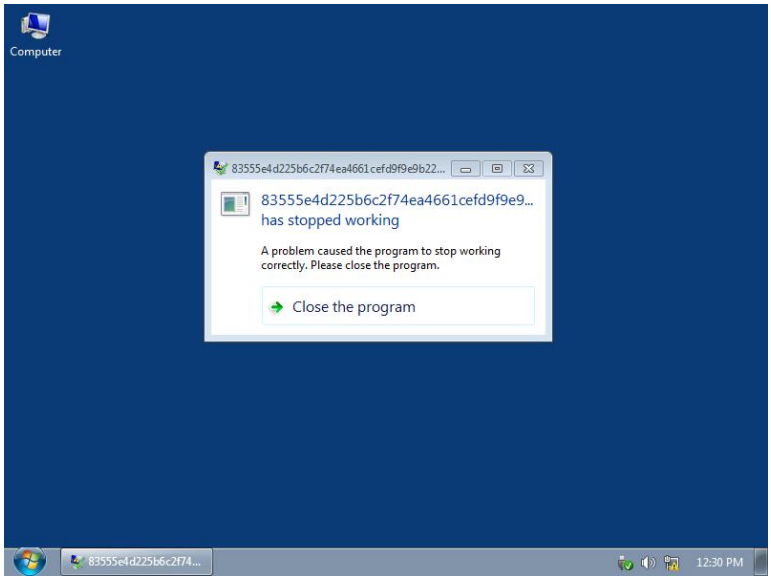
[+] USERTrust RSA Certification Authority	
Status	NoError ✔
Start Date	2010-02-01 02:00:00
End Date	2038-01-19 01:59:59
Sha256	3a3e24f6878c37f2ae39a7669f2ad8e309b4994e08b96a1753af478d256eebb6
Serial	01FD6D30FCA3CA51A81BBC640E35032D
Subject Key Identifier	53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb
Issuer Name	USERTrust RSA Certification Authority
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

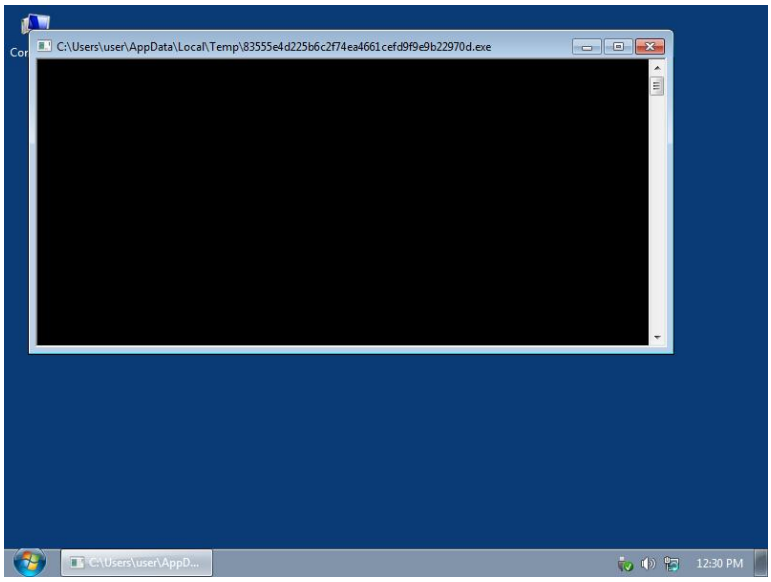
[+] Sectigo RSA Code Signing CA 2	
Status	NoError ✔
Start Date	2021-05-25 03:00:00
End Date	2036-05-25 02:59:59
Sha256	863f38cee7b30b1338e15dcf842004c480ed7eb698f823c25e490d3421cb2dba
Serial	009E02B0E94ACEB2109CA1E9836BE0C2DB
Subject Key Identifier	24 65 93 98 08 01 e8 4e d4 d6 4c ea 64 55 e1 c0 fa fb cf b3
Issuer Name	USERTrust RSA Certification Authority
Issuer Key Identifier	53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb
Crl link	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] Malwarebytes Inc.	
Status	NoError ✔
Start Date	2022-03-23 02:00:00
End Date	2025-03-17 01:59:59
Sha256	307ff4cf12f2f8401dd3fe7957cf9d380a30c1c03512abb34370d8b99999bd75
Serial	00A657F778B31AE523D667131718D16EB2
Subject Key Identifier	bc 87 36 a5 d4 ac e2 96 55 e8 57 e8 b4 fd f0 a8 f6 8a cc 62
Issuer Name	Sectigo RSA Code Signing CA 2
Issuer Key Identifier	24 65 93 98 08 01 e8 4e d4 d6 4c ea 64 55 e1 c0 fa fb cf b3
Crl link	http://crl.sectigo.com/SectigoRSACodeSigningCA2.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

SCREENSHOTS

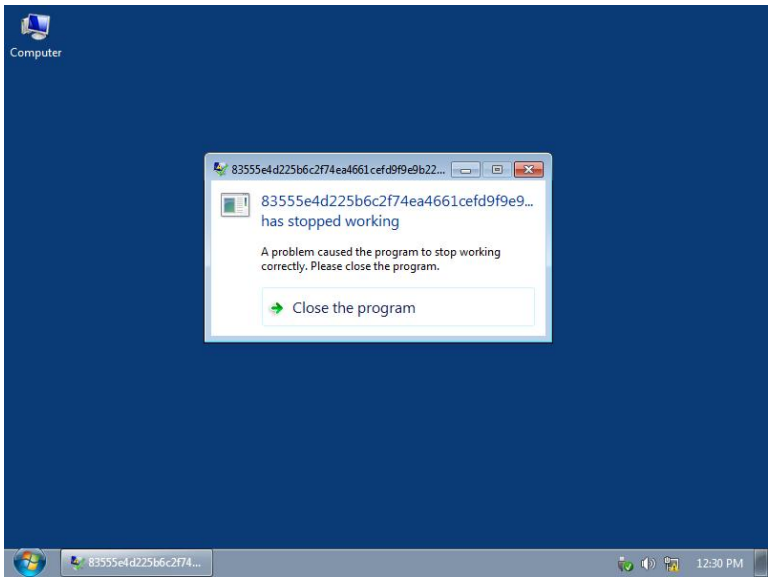





C:\Users\user\AppData\Local\Temp\83555e4d225b6c2f74ea4661cefd9f9e9b22970d.exe
12:30 PM


Computer
12:30 PM


Computer
12:30 PM


Computer
83555e4d225b6c2f74ea4661cefd9f9e9b22...
83555e4d225b6c2f74ea4661cefd9f9e9...
has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
83555e4d225b6c2f74...
12:30 PM