Summary

File Name: LMAOBOXPREMIUM.exe

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

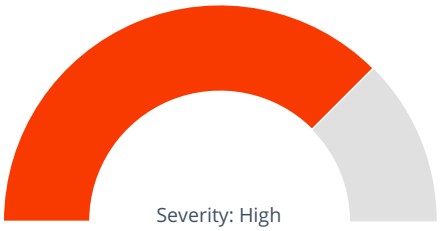
SHA1: 24b8d0208fdc46b720d6c07b71949f0ebe792442

MD5: deff401baf9df67d9731da2b98407f14

MALWARE

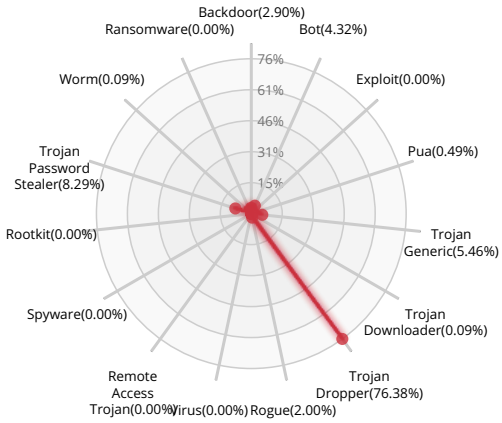
Valkyrie Final Verdict

DETECTION SECTION

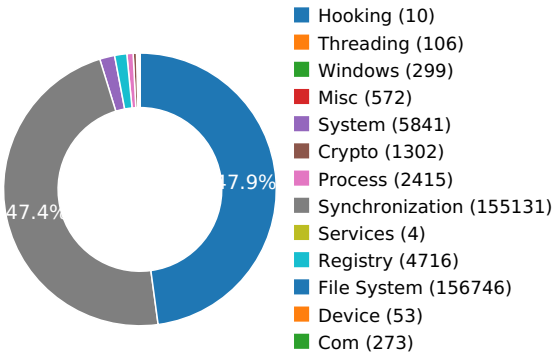


Verdict: Malware

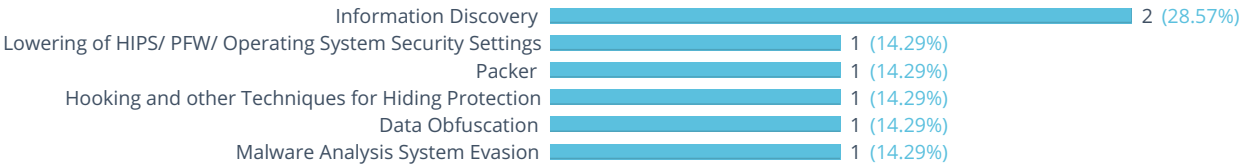
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

Attempts to remove evidence of file being downloaded from the Internet — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys

PACKER

The binary likely contains encrypted or compressed data. — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

DATA OBFUSCATION

Drops a binary and executes it — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

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:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe.config
C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe
C:\Users\user\AppData\Local\Temp\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:\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:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows

C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Windows\System32\l_intl.nls
C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.INI
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.INI
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a\System.Drawing.INI
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\uxtheme.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Globalization\en-us.nlp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Gdiplus.dll

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\ahronbd.ttf
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\ConfigMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\MVID

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\EvalationData

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\ILDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\NIDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a\MissingDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\475dce40\2d382ce6\85\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\475dce40\2d382ce6\85\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\475dce40\2d382ce6\85\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\475dce40\2d382ce6\85\SIG

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\475dce40\2d382ce6\85\LastModTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2dd6ac50\163e1f5e\80\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2dd6ac50\163e1f5e\80\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2dd6ac50\163e1f5e\80\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2dd6ac50\163e1f5e\80\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2dd6ac50\163e1f5e\80\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\41c04c7e\7f3b6ac4\78\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\41c04c7e\7f3b6ac4\78\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\41c04c7e\7f3b6ac4\78\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\41c04c7e\7f3b6ac4\78\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\41c04c7e\7f3b6ac4\78\LastModTime

MODIFIED FILES

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Users\user\AppData\Roaming\NvBackend.exe
C:\Users\user\AppData\Roaming\NvBackend.txt
C:\Users\user\Documents\New text document.txt
\??\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

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
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
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
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
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE
mscorwks.dll.IEE
mscoree.dll.GetStartupFlags
mscoreei.dll.GetStartupFlags
mscoree.dll.GetHostConfigurationFile
mscoreei.dll.GetHostConfigurationFile
mscoreei.dll.GetCORVersion
mscoree.dll.GetCORSystemDirectory
mscoreei.dll.GetCORSystemDirectory_RetAddr

mscoreei.dll.CreateConfigStream
ntdll.dll.RtlUnwind
kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation

DELETED FILES

C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe:Zone.Identifier
C:\Users\user\AppData\Roaming\NvBackend.exe:Zone.Identifier
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2476.28461125
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2476.28461125
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2476.28461125
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.1192.28463500
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.1192.28463500
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1192.28463500
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.1660.28463859
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.1660.28463859
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1660.28463859

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\2b50c649\383292fe

HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.2.0.System.Windows.Forms__b77a5c561934e089

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064\7a

EXECUTED COMMANDS

C:\Users\user\AppData\Roaming\NvBackend.exe

"C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe"

"C:\Users\user\AppData\Roaming\NvBackend.exe"

dw20.exe -x -s 660

C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe.config
C:\Users\user\AppData\Local\Temp\24b8d0208fdc46b720d6c07b71949f0ebe792442.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\System32\l_intl.nls
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf
C:\Windows\Fonts\segoeui.ttf
C:\Windows\Fonts\staticcache.dat
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
C:\Users\user\AppData\Roaming\NvBackend.exe
C:\Users\user\AppData\Roaming\NvBackend.txt
C:\Users\user\AppData\Roaming\NvBackend.exe.config
C:\Users\user\Documents\New text document.txt
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuratio#\f02737c83305687a68c088927a6c5a98\System.Configuration.Install.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
C:\Windows\Fonts\calibri.ttf
C:\Windows\Fonts\calibrib.ttf
C:\Windows\Fonts\calibrii.ttf
C:\Windows\Fonts\calibriz.ttf
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\6f3b99ed0b791ff4d8aa52f2f0cd0bcf\System.Management.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\wminet_utils.dll
C:\Windows\inf\oem16.PNF
\??\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\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\en-US\wer.dll.mui
C:\Windows\System32\en-US\werui.dll.mui
C:\Windows\System32\werui.dll
C:\Windows\System32\en-US\DUser.dll.mui
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\Comctl32.dll.mui

MUTEXES

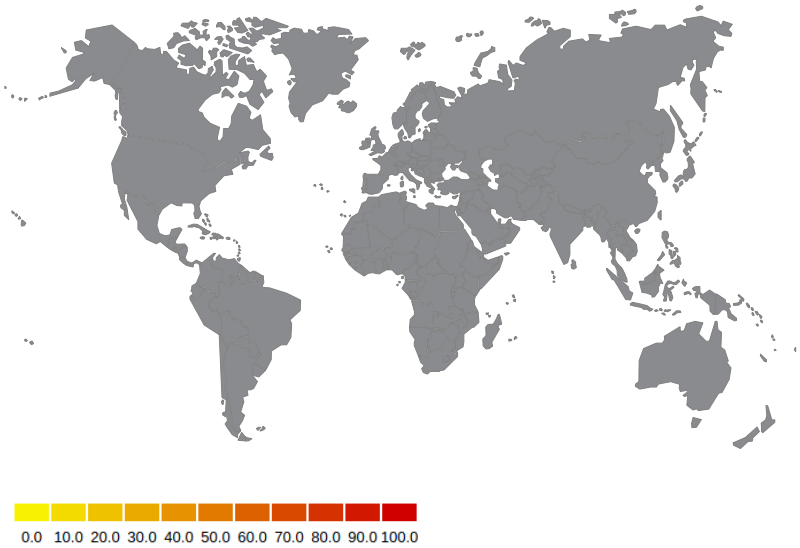
Global\CLR_CASOFF_MUTEX
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\cc8450d6-2e7a-11e7-9c49-080027cb305f

MODIFIED REGISTRY KEYS

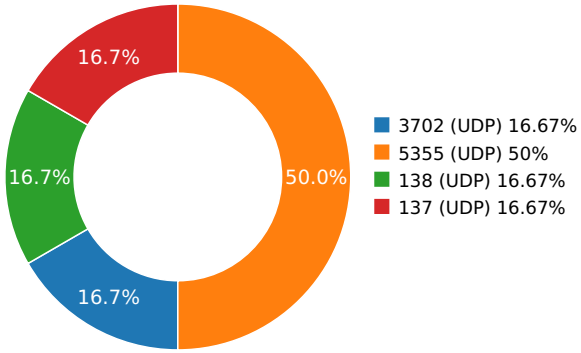
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting\Debug\UIHandles\FirstLevelConsentDialog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug\UIHandles\FirstLevelConsentDialog

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
3.08719205856	Sandbox	224.0.0.252	5355
3.11781096458	Sandbox	224.0.0.252	5355
3.13344097137	Sandbox	239.255.255.250	3702
3.16138911247	Sandbox	192.168.56.255	137
5.67790699005	Sandbox	224.0.0.252	5355
9.16004705429	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\Documents\New Text Document.Txt **C:\Users\User\AppData\Roaming\NvBackend.Txt**	**Type :** ASCII text, with no line terminators **MD5 :** 7f69fa7b32545f9de386d329fce62114 **SHA-1 :** 45e299958de955fe7cc08e238338009c87b08621 **SHA-256 :** 88ab3c4d7bedd6a5e591619e427e8f9499f06d7f **SHA-512 :** 2d5f1fe6483b6860e381d3ce9f8e908164d4b926 **Size :** 0.032 Kilobytes.
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c357 **Size :** 84.528 Kilobytes.
C:\Users\User\AppData\Roaming\NvBackend.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 1ae7999a166e4b293608096c09a2a57c **SHA-1 :** 090519c4582e129fd1694256adf7fa1c99c40a23 **SHA-256 :** c234524034ccf8a92ec2cac80c4f9c69d28b0fb02 **SHA-512 :** 1f6d79eeb271b89ba555559e301b477d59a5daa **Size :** 798.208 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	LMAOBOXPREMIUM.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	24b8d0208fdc46b720d6c07b71949f0ebe792442
MD5:	deff401baf9df67d9731da2b98407f14
First Seen Date:	2017-01-08 02:38:23.359716 (2 years ago)
Number Of Clients Seen:	10
Last Analysis Date:	2018-05-06 01:22:43.613000 (10 months 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
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[[63.1, u'Generic CIL Executable (.NET, Mono, etc.)'], [23.8, u'Win64 Executable (generic)'], [5.6, u'Win32 Dynamic Link Library (generic)'], [3.8, u'Win32 Executable (generic)'], [1.7, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x57A7E4E2 [Mon Aug 8 01:48:18 2016 UTC]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2013
Assembly Version	1.4.7.0
InternalName	LMAOBOXLOADER.exe
FileVersion	1.4.7.0
ProductName	LMAOBOX
ProductVersion	1.4.7.0
FileDescription	LMAOBOX
OriginalFilename	LMAOBOXLOADER.exe
Entry Point	0x56fc8e (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1510400
Ssdeep	24576:Q1ZVrIjC71MBkYlONBuSXSLB9oe4eDcRM9EsP3BxiD7zCsFg:AfrIjDBkYlKub5X9b3LiDLFg
Sha256	9d215a843b45bb39578efb5f3c883996c1f50023c59715cbc4aaa2a5114664e2
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/4/b/8/24b8d0208fdc46b720d6c07b71949f0ebe792442', u'EXE:OriginalFileName': u'LMAOBOXLOADER.exe', u'EXE:ProductName': u'LMAOBOX', u'EXE:InternalName': u'LMAOBOXLOADER.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:05:06 01:13:45+00:00', u'EXE:InitializedDataSize': 11264, u'File:FileModifyDate': u'2018:05:06 01:13:44+00:00', u'EXE:AssemblyVersion': u'1.4.7.0', u'EXE:FileVersionNumber': u'1.4.7.0', u'EXE:FileVersion': u'1.4.7.0', u'File:FileSize': u'1475 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.4.7.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'24b8d0208fdc46b720d6c07b71949f0ebe792442', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2016:08:08 01:48:18+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2013', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/4/b/8', u'EXE:FileDescription': u'LMAOBOX', u'EXE:EntryPoint': u'0x16fc8e', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 1498624, u'File:FileInodeChangeDate': u'2018:05:06 01:13:44+00:00', u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.4.7.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x16dc94	0x16de00	7.90773949414	c6c4e843d5d63f8c2e2816a4f25f2d2d
.rsrc	0x170000	0x2a00	0x2a00	4.55310250321	c7fe9b76fc09d491e93743463c951369
.reloc	0x174000	0xc	0x200	0.101910425663	56e61fed0172d26b89b7361d651ff5ed

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1507560, u'sha256': u'778c7b6a12c19c8ad37ed58f5b877050082fb62c27224c5b9ae6bc3312968116', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777215, next used block 16777215', u'size': 9640}

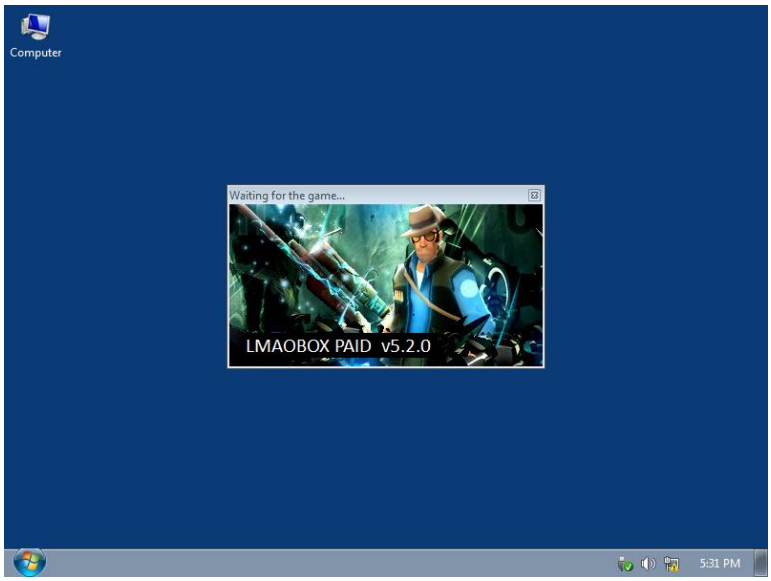
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1517200, u'sha256': u'51bbd5ae8d46e74b7424733b993e42552856bea79d1826b7f767cee02bd4c0f4', u'type': u'MS Windows icon resource - 1 icon, 48x48', u'size': 20}

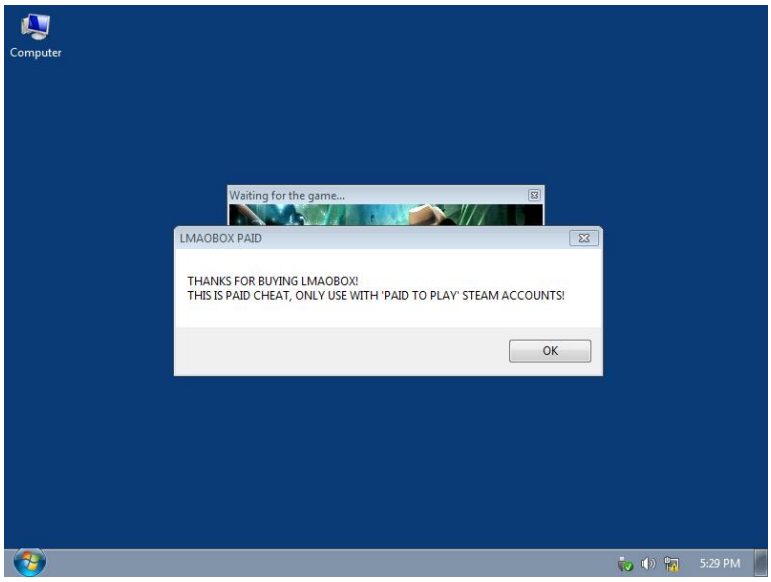
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 1517220, u'sha256': u'8b08fda41ca0402ae9de9783b580f5be8adc0ca1247b8a393b8c9e32138ce087', u'type': u'COM executable for DOS', u'size': 696}

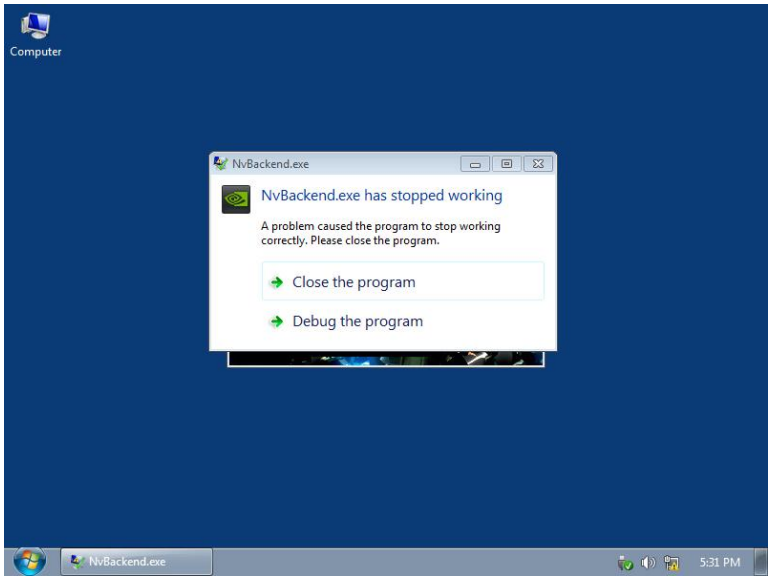
CERTIFICATE VALIDATION

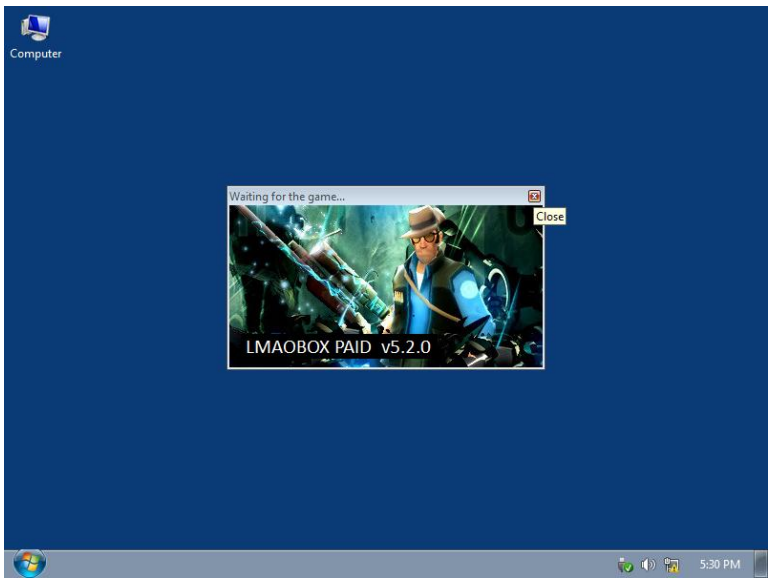
- Certificate Validation is not Applicable ?

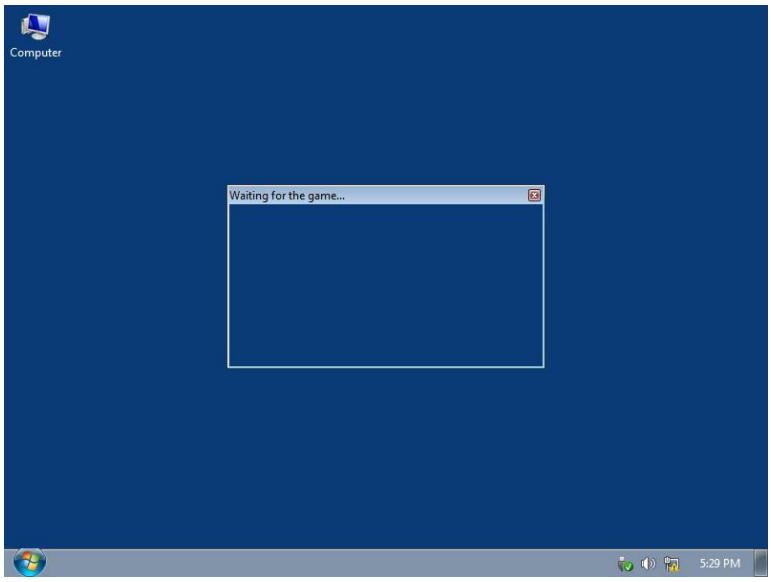
SCREENSHOTS



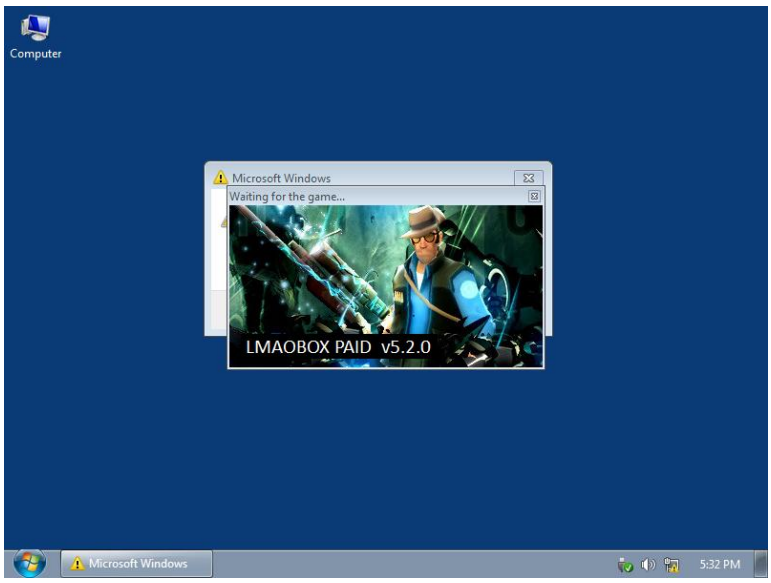

Computer
Waiting for the game...
LMAOBOX PAID
THANKS FOR BUYING LMAOBOX!
THIS IS PAID CHEAT, ONLY USE WITH 'PAID TO PLAY' STEAM ACCOUNTS!
OK
5:29 PM

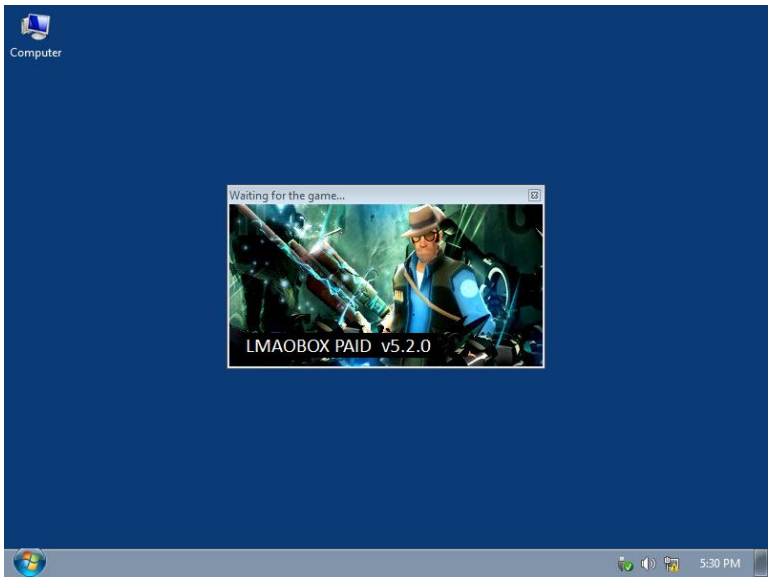

Computer
NvBackend.exe
NvBackend.exe has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Debug the program
NvBackend.exe
5:31 PM

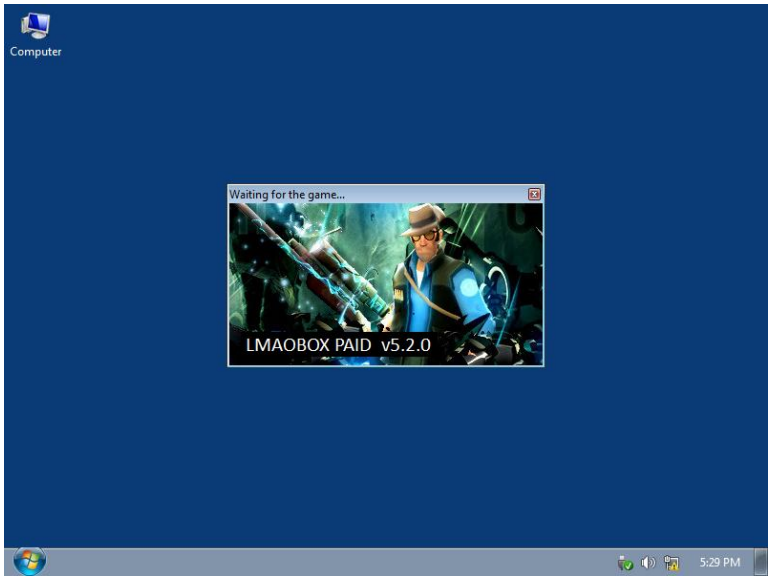

Computer
Waiting for the game...
Close
LMAOBOX PAID v5.2.0
5:30 PM


Computer
Waiting for the game...
5:29 PM


Computer
5:28 PM


Computer
Microsoft Windows
Waiting for the game...
LMAOBOX PAID v5.2.0
Microsoft Windows
5:32 PM


Computer
Waiting for the game...
LMAOBOX PAID v5.2.0
5:30 PM


Computer
Waiting for the game...
LMAOBOX PAID v5.2.0
5:29 PM