Summary

File Name: AutoItObfuscator_1.bin

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

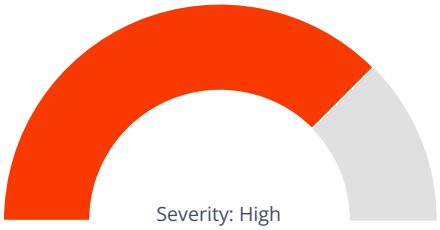
SHA1: 97cf21650dfc7e50972bf09a2760fe8b78d367b8

MD5: baf02b6b2480028d73775a43cbcec09b

MALWARE

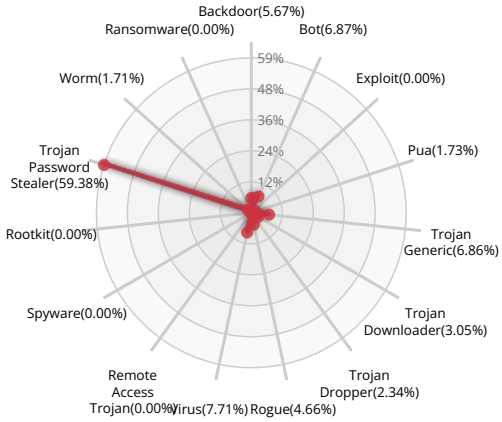
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

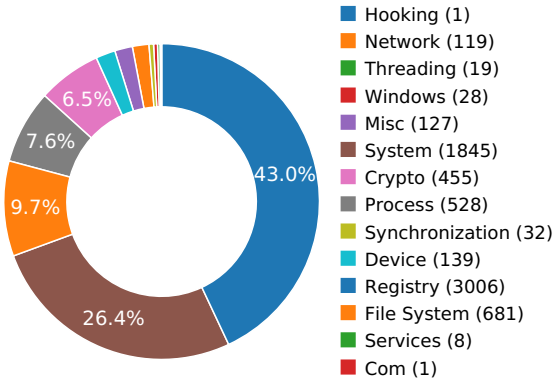


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

STATIC ANOMALY

Anomalous binary characteristics Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

Behavior Summary

ACCESSED FILES

C:\Windows\sysnative\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.exe.config
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\97cf21650dfc7e50972bf09a2760fe8b78d367b8.exe.Local\
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\GAC_64\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\Framework64\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.config
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.INI
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Users\user\AppData\Local\Temp\68161C21.dll
C:\Users\user\AppData\Local\Temp\68161C21\68161C21.dll
C:\Users\user\AppData\Local\Temp\68161C21.exe
C:\Users\user\AppData\Local\Temp\68161C21\68161C21.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\en-US\mscorrc.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\en-US\mscorrc.dll.DLL
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\en\mscorrc.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\en\mscorrc.dll.DLL
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Users\user\AppData\Local\Temp\shlwapi.dll

C:\Windows\Globalization\en-us.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\bcrypt.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\diasymreader.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.pdb
C:\Windows\symbols\dll\mscorlib.pdb
C:\Windows\dll\mscorlib.pdb

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\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\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
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\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\30bc7c4f\3f50fe4f\90\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\3f50fe4f\6f1da7aa\90\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Xml,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Configuration,2.0.0.0,,b03f5f7f11d50a3a,MSIL

MODIFIED FILES

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Local\Temp\CabDA52.tmp
C:\Users\user\AppData\Local\Temp\TarDA63.tmp

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
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.RtlVirtualUnwind
kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.InitializeAcl

DELETED FILES

C:\Users\user\AppData\Local\Temp\CabDA52.tmp

C:\Users\user\AppData\Local\Temp\TarDA63.tmp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\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\97cf21650dfc7e50972bf09a2760fe8b78d367b8.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\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\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\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_64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\2952fd23\7b476fde

HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\internal\jit\Perf

READ FILES

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.exe.config
C:\Users\user\AppData\Local\Temp\97cf21650dfc7e50972bf09a2760fe8b78d367b8.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\diasymreader.dll

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.pdb

C:\Windows\symbols\dll\mscorlib.pdb

C:\Windows\dll\mscorlib.pdb

C:\Windows\mscorlib.pdb

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\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\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\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\segoeuib.ttf

C:\Windows\Fonts\segoeuii.ttf

C:\Windows\Fonts\segoeuiz.ttf

C:\Windows\Fonts\staticcache.dat

C:\Windows\Fonts\cour.ttf

C:\Windows\Fonts\courbd.ttf

C:\Windows\Fonts\couri.ttf

C:\Windows\Fonts\courbi.ttf

C:\Windows\sysnative\ieframe.dll

C:\Windows\sysnative\en-US\KERNELBASE.dll.mui

C:\Windows\Fonts\ariblk.ttf

C:\Windows\sysnative\uxtheme.dll.Config

C:\Windows\sysnative\uxtheme.dll

C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.pdb

C:\Windows\symbols\dll\System.Windows.Forms.pdb

C:\Windows\dll\System.Windows.Forms.pdb

C:\Windows\System.Windows.Forms.pdb

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\091b931d0f6408001747dbbbb05dbe66\System.Configuration.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\ee795155543768ea67eecddc686a1e9e\System.Xml.ni.dll

C:\Windows\sysnative\tzres.dll
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D

MUTEXES

Global\CLR_CASOFF_MUTEX
Global\.net clr networking
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

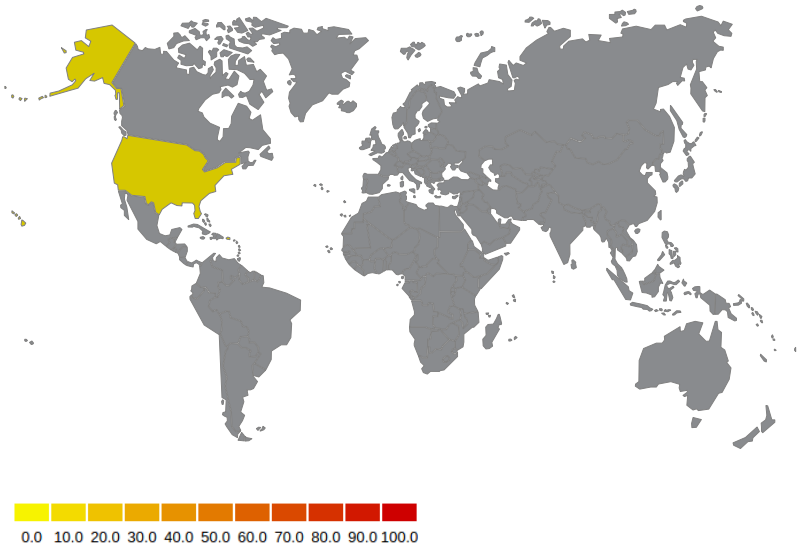
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\PELock\AutoItObfuscator
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\97cf21650dfc7e50972bf09a2760fe8b78d367b8_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042

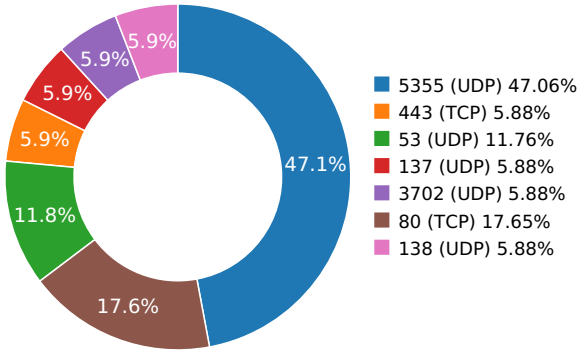
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\qagentrt.dll,-10
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-843
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-844

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
	13.107.4.50	United States	8068	Microsoft Corporation	OS Process
www.pelock.com	212.71.235.46	United Kingdom	63949	Linode, LLC	Malware Process
ctldl.windowsupdate.com	69.164.0.0	United States	22822	Limelight Networks, Inc.	OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	23.5516331196
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdb16b39901d45a5 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdb16b39901d45a5						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	28.9201290607
Path: /msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?50518b9ce1203a2e **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?50518b9ce1203a2e						

DNS QUERIES

Request	Type
www.pelock.com	A
Answers - 212.71.235.46 (A)	
ctldl.windowsupdate.com	A
Answers - wu-shim.trafficmanager.net (CNAME) - b1ns.au-msedge.net (CNAME) - b1ns.c-0001.c-msedge.net (CNAME) - c-0001.c-msedge.net (CNAME) - 13.107.4.50 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
17.6913230419	Sandbox	212.71.235.46	443
23.5516331196	Sandbox	13.107.4.50	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.48489308357	Sandbox	224.0.0.252	5355
6.49903607368	Sandbox	224.0.0.252	5355
6.50430011749	Sandbox	239.255.255.250	3702
6.54542517662	Sandbox	192.168.56.255	137
9.10903811455	Sandbox	224.0.0.252	5355
12.5912652016	Sandbox	192.168.56.255	138
14.6619901657	Sandbox	224.0.0.252	5355
17.3402671814	Sandbox	8.8.4.4	53
18.3899049759	Sandbox	224.0.0.252	5355
20.9790370464	Sandbox	224.0.0.252	5355
23.5294411182	Sandbox	8.8.4.4	53
23.8029370308	Sandbox	224.0.0.252	5355
26.3685460091	Sandbox	224.0.0.252	5355

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
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\Local\Temp\TarDA63.Tmp	**Type :** data **MD5 :** d99661d0893a52a0700b8ae68457351a **SHA-1 :** 01491fd23c4813a602d48988531ea4abbcdf7ed9 **SHA-256 :** bdd5111162a6fa25682e18fa74e37e676d49cafcb **SHA-512 :** 6f2291ca958cbf5423cbbe570fd871c4d379a435b **Size :** 161.595 Kilobytes.
C:\Users\User\AppData\Local\Temp\CabDA52.Tmp **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506**	**Type :** Microsoft Cabinet archive data, 61414 bytes, 1 file **MD5 :** acaeda60c79c6bcac925eeb3653f45e0 **SHA-1 :** 2aaae490bcdaccc6172240ff1697753b37ac5578 **SHA-256 :** 6b0ceccf0103afd89844761417c1d23acc41f8aeb **SHA-512 :** feaa6e7ed7dda1583739b3e531ab5c562a222ee6 **Size :** 61.414 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** c5f74d76e3b036ccd7fafc4d3aaa5b5a **SHA-1 :** c1f084ffeea20d92e955ca6f2358bbd46f766c8c **SHA-256 :** 6b63b215aedfb5146d864c3b5efb075afb791238 **SHA-512 :** 0c2f802d3fa6238319bdc2f0b58b06ce59483f091 **Size :** 0.328 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	AutoItObfuscator_1.bin
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	97cf21650dfc7e50972bf09a2760fe8b78d367b8
MD5:	baf02b6b2480028d73775a43cbcec09b
First Seen Date:	2022-01-10 18:33:30.697168 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2022-01-10 18:33:30.697168 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[64.5, u'Win32 Executable MS Visual C++ (generic)'], [13.6, u'Win32 Dynamic Link Library (generic)'], [9.3, u'Win32 Executable (generic)'], [4.2, u'Win16/32 Executable Delphi generic'], [4.1, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5CCAE30D [Thu May 2 12:31:09 2019 UTC]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 PELock LLC 2019
Assembly Version	1.4.0.0
InternalName	AutoItObfuscator.exe
FileVersion	1.4.0.0
CompanyName	PELock LLC
LegalTrademarks	
Comments	AutoIt Script Source Code Obfuscator
ProductName	AutoItObfuscator
ProductVersion	1.4.0.0
FileDescription	AutoIt Obfuscator
OriginalFilename	AutoItObfuscator.exe
Entry Point	0x61200a ()
Machine Type	Intel 386 or later - 32Bit
File Size	2152976
Ssdeep	49152:LVYdOvDfhl3eyBe2bnIVlFfvcaaJAsC9o7DI5P:JzdMytnIVl+i9lZ
Sha256	f9a46133ecb6a5bd6ec98679b107e08fddf892283791d2b25820e17569cdb44f
Exifinfo	[{u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/7/c/f/97cf21650dfc7e50972bf09a2760fe8b78d367b8', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2022:01:10 18:33:14+00:00', u'EXE:InitializedDataSize': 125952, u'File:FileModifyDate': u'2022:01:10 18:32:10+00:00', u'File:FileSize': u'2.1 MB', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'97cf21650dfc7e50972bf09a2760fe8b78d367b8', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2019:05:02 12:31:09+00:00', u'EXE:LinkerVersion': 48.0, u'ExifTool:ExifToolVersion': 10.1, u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/7/c/f', u'EXE:EntryPoint': u'0x21200a', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 2025984, u'File:FileInodeChangeDate': u'2022:01:10 18:32:49+00:00', u'EXE:Subsystem': u'Windows GUI'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
&9nFiL$	0x2000	0x5b8c	0x5c00	7.9934056437	89ee70d5b588ccc253e310e47c343181
.text	0x8000	0x1ee7c8	0x1ee800	7.80550774048	87ff8974e7b7f139373f4a68baf935cc
]Cp.	0x1f8000	0x18d28	0x18e00	3.65696540736	fde5df402326a97ef1c3c7cc3bc836cc
	0x212000	0x10	0x200	0.122275881259	349d3e73c04a41606f3a4d8bce9ad839
.reloc	0x214000	0xc	0x200	0.0980041756627	115bf8b5632f3b7040c06eeeac3de1c3

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2065312, u'sha256': u'1f079a97a4da276b97d2b90c7e7665d6f7ec6ec421b905db1b40c541090adddc', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 8509}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2073824, u'sha256': u'53992acc1311dd0c22a94d49f1eb47e983e3a439e86ccdad4c6dc23d77479b4d', u'type': u'data', u'size': 38056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2111880, u'sha256': u'243d39814fe7dd9bb7536f16bb537e14e362bdee5b90798ffd606f3090133a02', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0', u'size': 16936}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2128816, u'sha256': u'41e8d6f7ab97b671e9842b7efc23718d8a64d2952e80996fe621e3c6c1cdfaa7', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2138456, u'sha256': u'168699229603f03b6ce18f56075d226ceb4177e145e109d6d11e2bbd5dd2c794', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2142208, u'sha256': u'55794c29731f84e8d51e515a8bc3919707ae30c78de68f4c1b087e27bd1dc495', u'type': u'data', u'size': 6760}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2148968, u'sha256': u'8c83a2bb1fe26cfe07a453672d7f249f2cc9d5dd1f8bff4c59bd05f942d63279', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2153232, u'sha256': u'29863261ad073f9ba83d4038d90c640643f072ad7b11360824097dc5a84af1e9', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2155448, u'sha256': u'208840a89425ed1b19adc581f25aa7349de25d7fbc18b45e0ceb36e6fba4e19a', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2156192, u'sha256': u'3668d777b1042fe38177192ceda146388fa989fee95ef1d8140580c8826b82ff', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2158632, u'sha256': u'3a3ba11dbc1e615eb67fa1dcbc870aa360495948129b05fb5b585edca775e664', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2160352, u'sha256': u'ce379efc01fd9a3f397b3340bf7c1cc800ae88594a7c75ce52d414c6f96372b4', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2161480, u'sha256': u'efd0f88a155987af5ee32c27aa7a8f9f3435af2e94f3b8eca096dcd7e526222c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2162864, u'sha256': u'6796306cdde0644d2292f846729fbaec402a2f41b4331544c2d2c394287ff99c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 2163160, u'sha256': u'd243e9c27e56ccef0b5122ff9b3217b11196a4c77d86463bfa2f06c9cfbd014c', u'type': u'MS Windows icon resource - 14 icons, 256x256', u'size': 202}

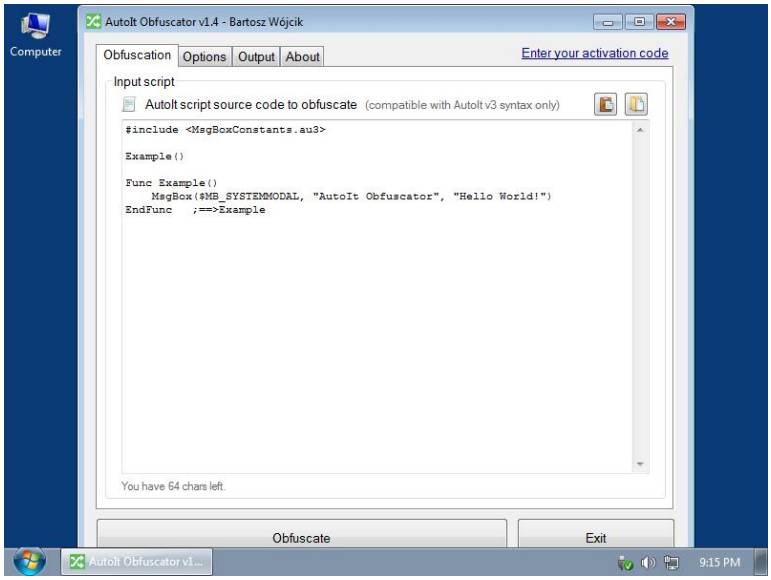
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 2163364, u'sha256': u'2ba2550148dc0edc5814e62efd4f6a000654a8aa7a81f0c42d3e9d1b15990387', u'type': u'data', u'size': 972}

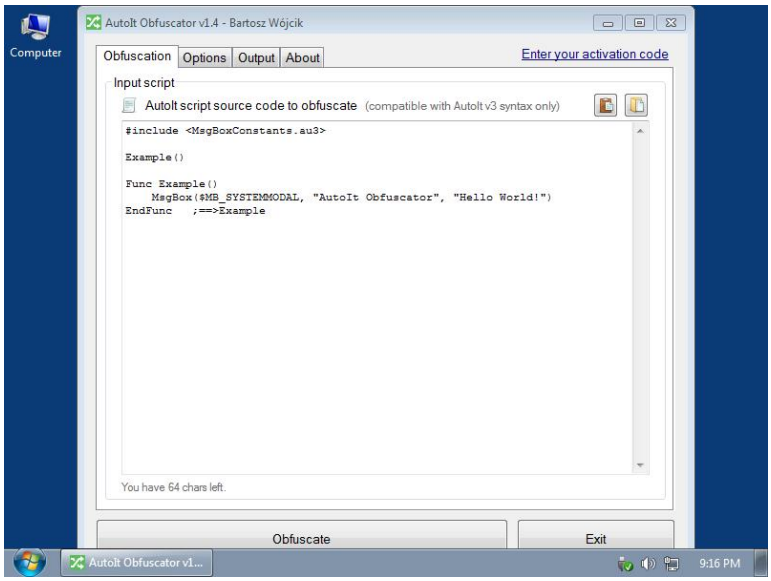
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 2164336, u'sha256': u'4e268cdc47c3d0f3911b8806de5252171afc95845394aba382bfd780d1705185', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 1714}

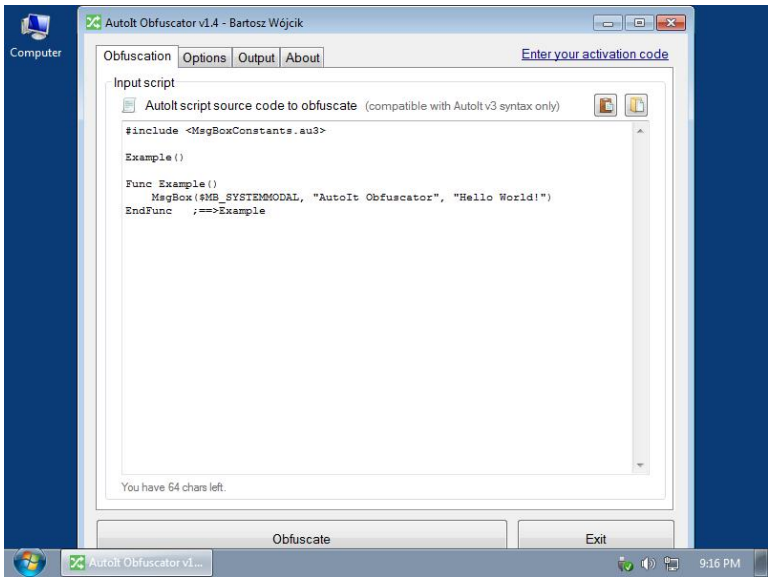
CERTIFICATE VALIDATION

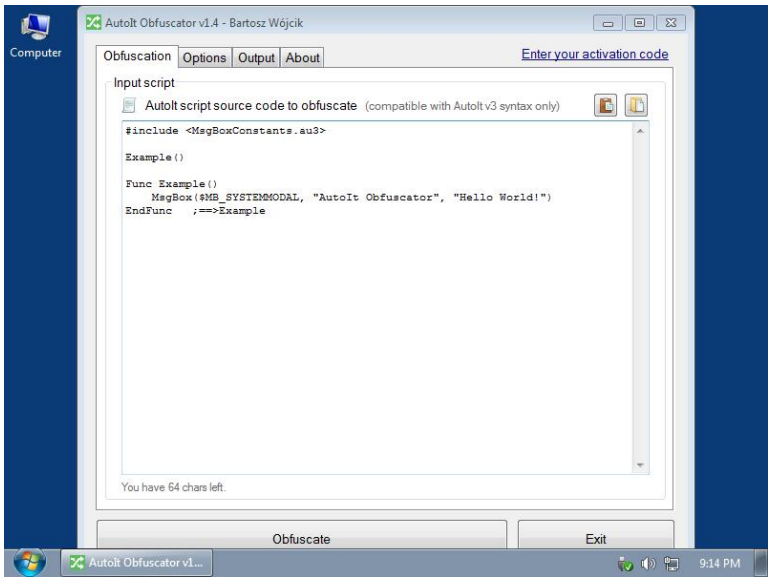
- Certificate Validation is not Applicable ?

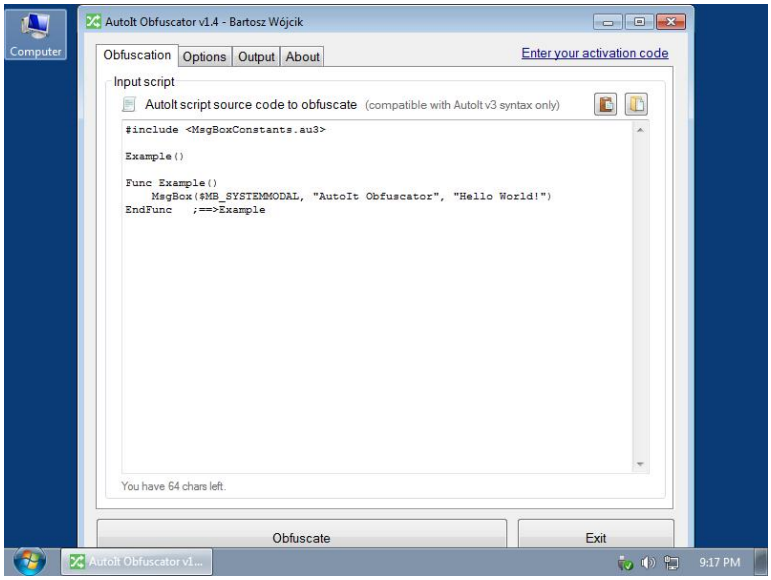
SCREENSHOTS

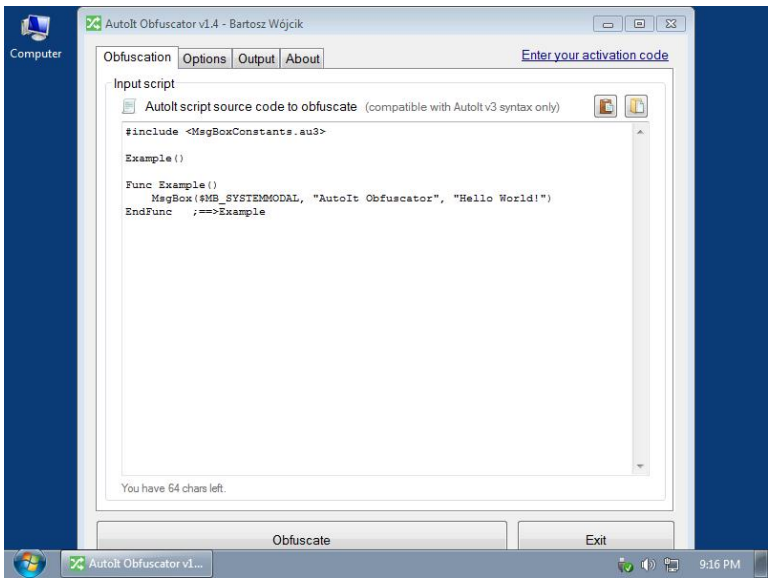

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:15 PM

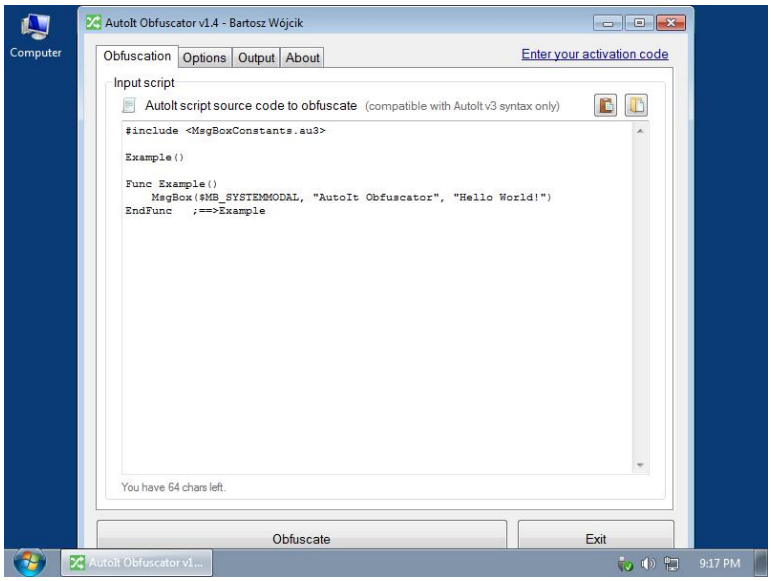

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

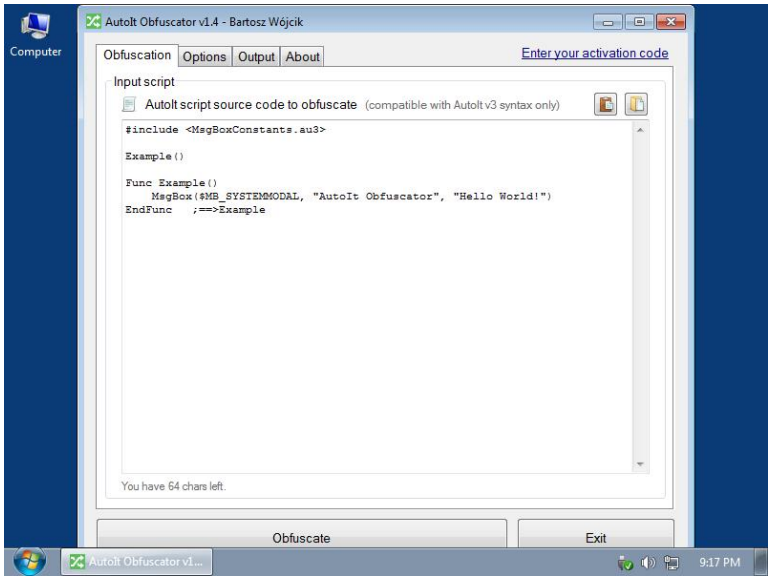

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

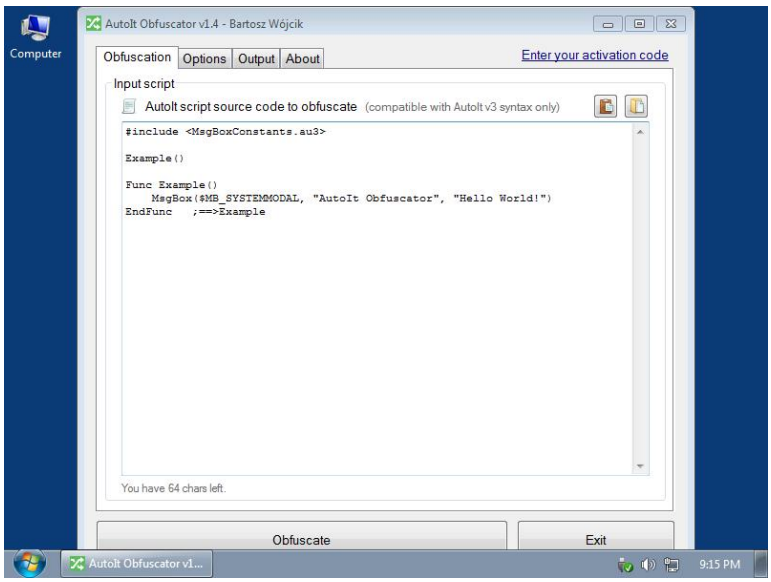

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
AutoIt Obfuscator v1...
9:14 PM

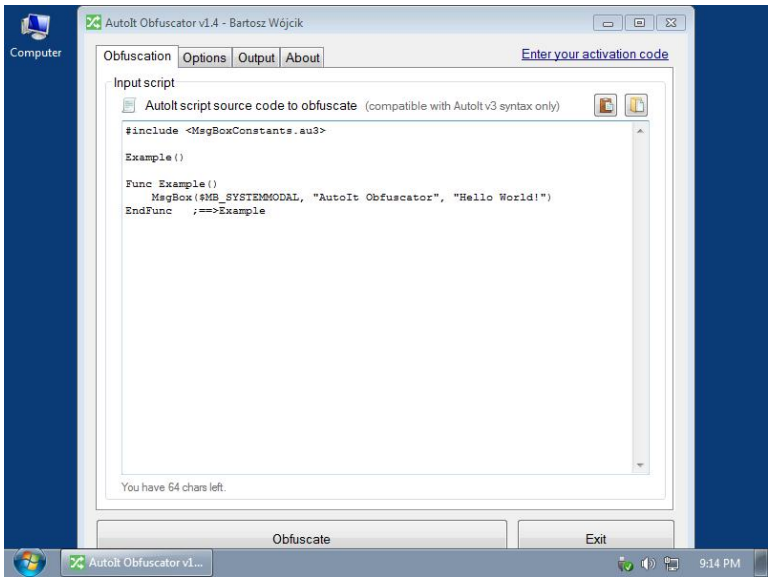

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
AutoIt Obfuscator v1...
9:17 PM

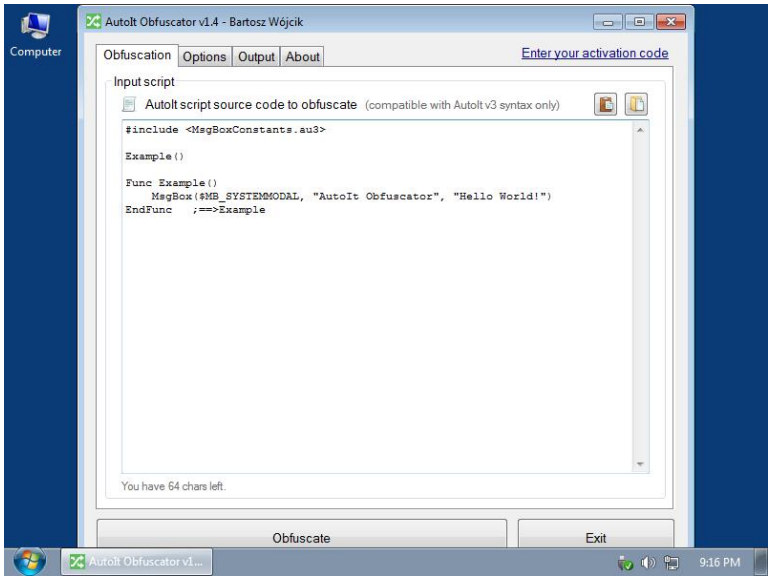

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
AutoIt Obfuscator v1...
9:16 PM

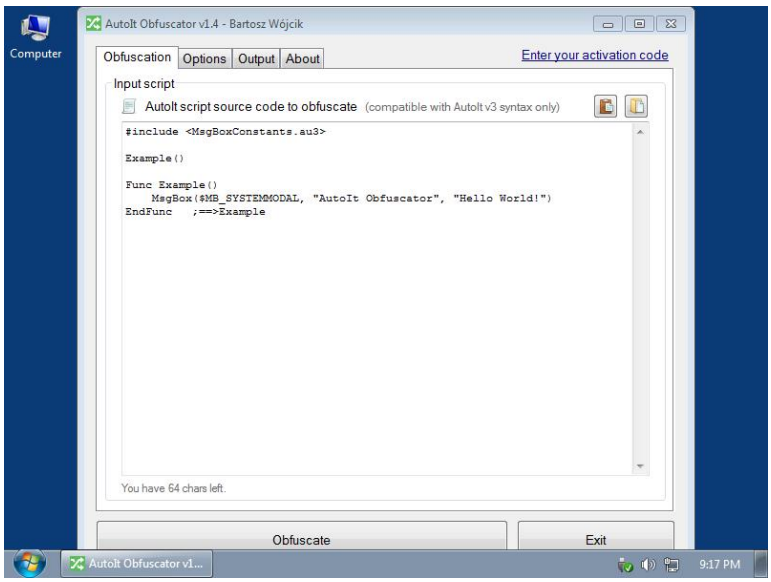

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
9:17 PM

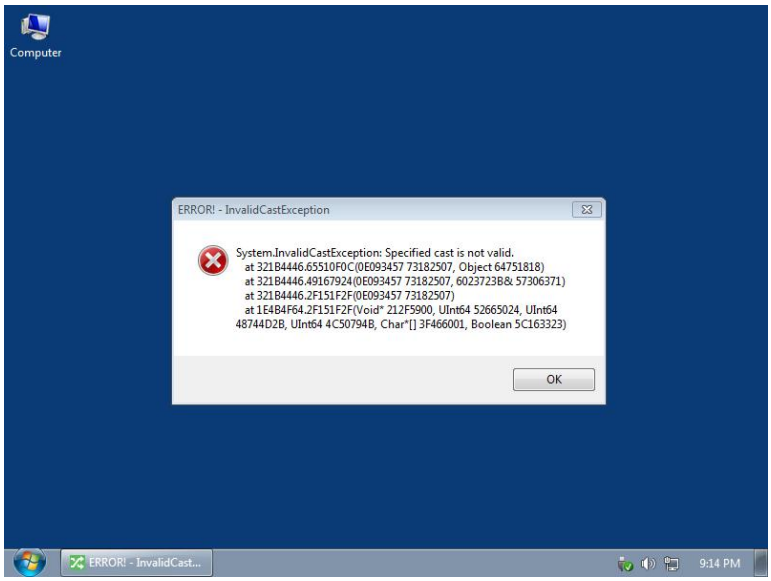

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
9:17 PM


AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Computer
9:15 PM

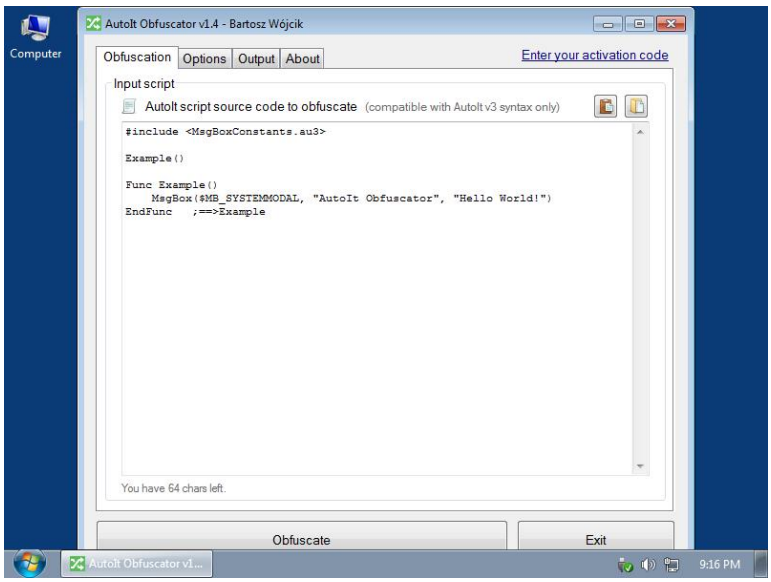

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:14 PM

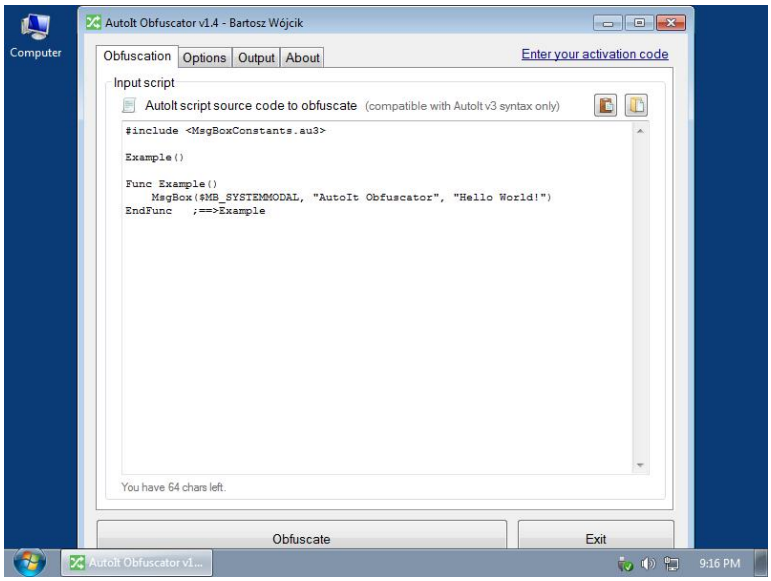

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

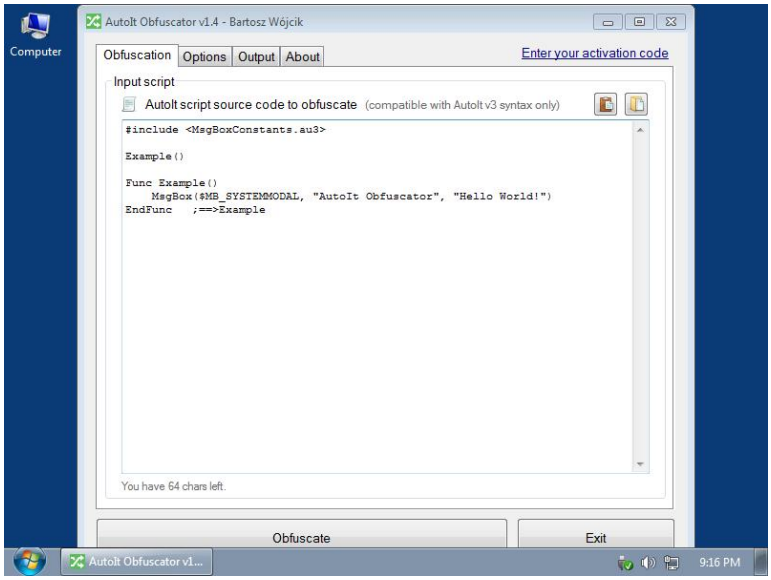

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:17 PM

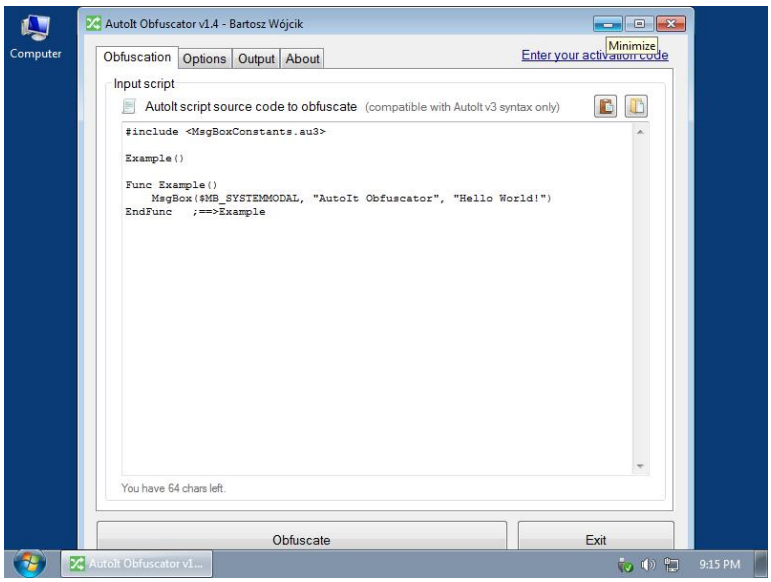

Computer
ERROR! - InvalidCastException
System.InvalidCastException: Specified cast is not valid.
at 321B4446.65510F0C(0E093457 73182507, Object 64751818)
at 321B4446.49167924(0E093457 73182507, 6023723B& 57306371)
at 321B4446.2F151F2F(0E093457 73182507)
at 1E4B4F64.2F151F2F(Void* 212F5900, UInt64 52665024, UInt64 48744D2B, UInt64 4C50794B, Char*[] 3F466001, Boolean 5C163323)
OK
ERROR! - InvalidCast...
9:14 PM

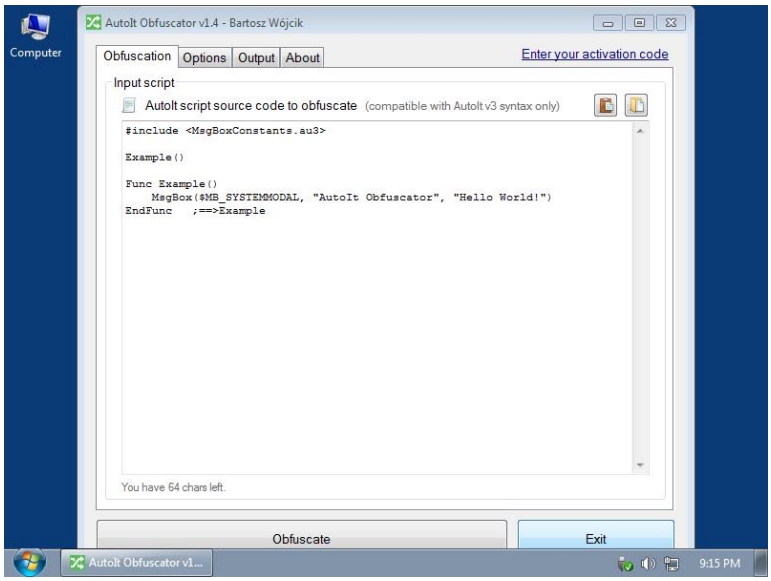

Computer
9:14 PM

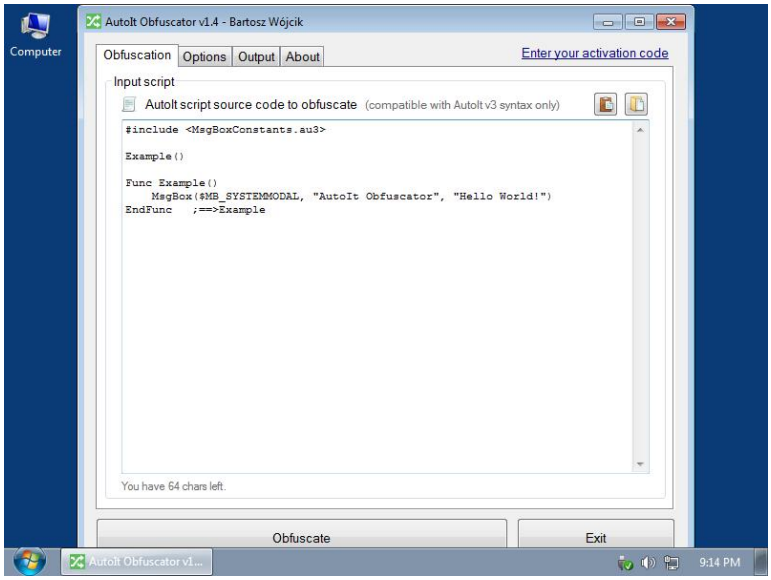

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

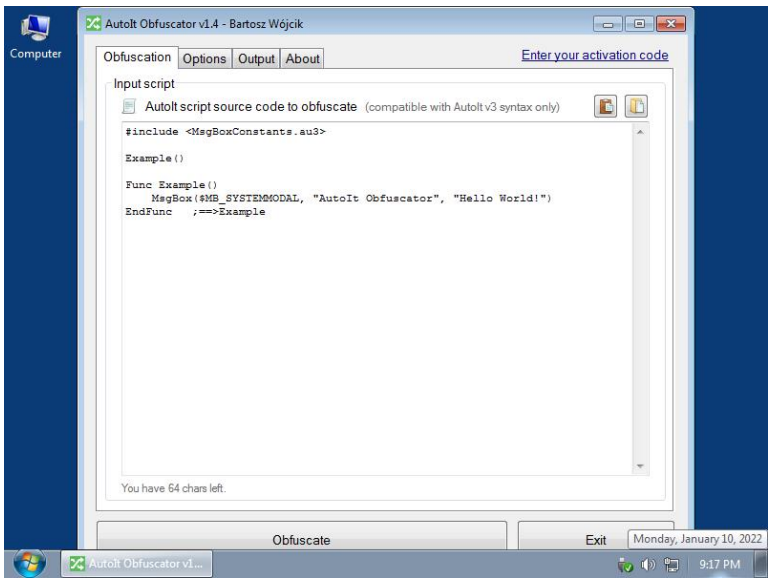

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

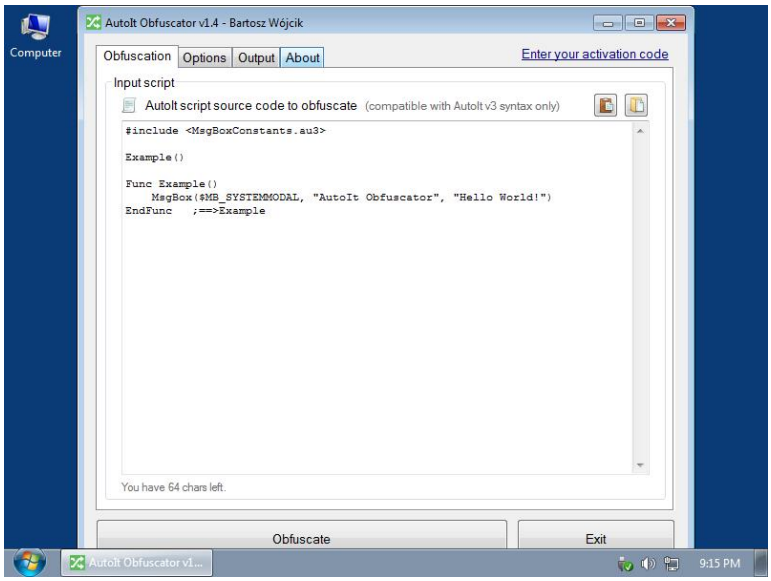

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM

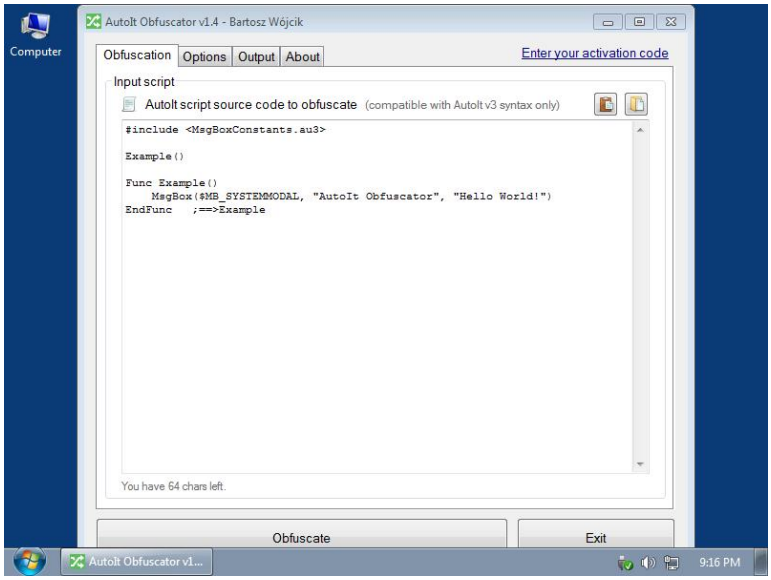

Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Minimize
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:15 PM

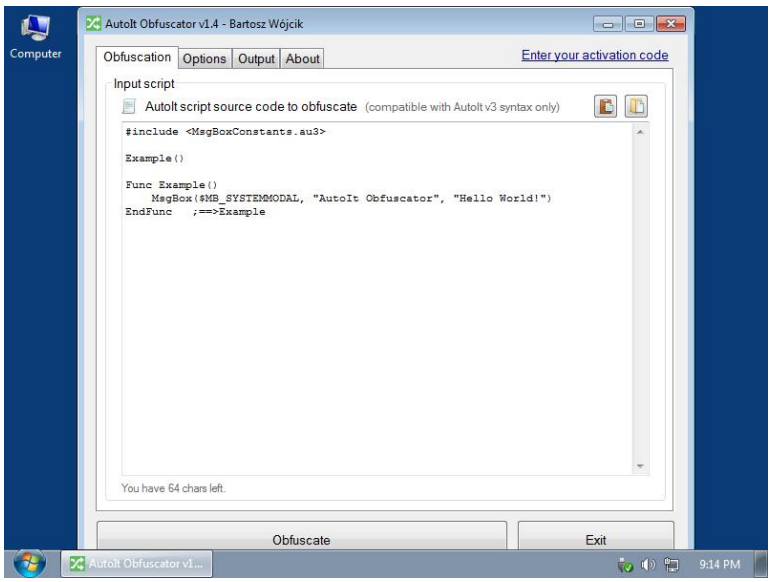

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
9:15 PM

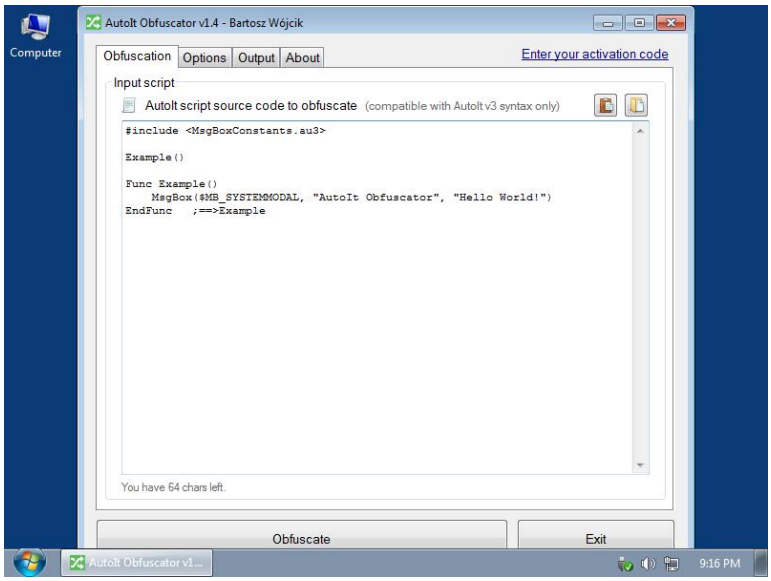

AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
9:14 PM


AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
Monday, January 10, 2022
9:17 PM


AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
9:15 PM


AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
9:16 PM


AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
9:14 PM


Computer
AutoIt Obfuscator v1.4 - Bartosz Wójcik
Obfuscation
Options
Output
About
Enter your activation code
Input script
AutoIt script source code to obfuscate (compatible with AutoIt v3 syntax only)
#include <MsgBoxConstants.au3>
Example()
Func Example()
MsgBox($MB_SYSTEMMODAL, "AutoIt Obfuscator", "Hello World!")
EndFunc ;==>Example
You have 64 chars left.
Obfuscate
Exit
AutoIt Obfuscator v1...
9:16 PM