MO.exe

Is DLL | Packer | Anti Debug | Anti VM | Signed | XOR

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	501.00 KB (513024 bytes)
Compile time:	2019-08-16 20:41:31
MD5:	202a5d15ae9926a1dec141ed13065ad5
SHA1:	97a84b26c9f2f8a89fbbd8e3c35f673d17704fdf
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-10-02 18:30:03

URL(s) file hosting

http://gnomingroam.com/MO.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-10-02 13:50:08	18/59	

Import library

mscoree.dll

10 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: Traffico Anomalo ? Start Traffico)

- signature: SURICATA HTTP Unexpected Request body
- signature: Traffico Anomalo: Traffico verso host malevolo, GET HTTP Content "db" (Soc-Rule)

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.59, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00078800, virtual_size: 0x00078744

Performs some HTTP requests

- url: http://www.nvdough.com/um/?h0DlqZ5=4Yw0gXJLQ90lLTIcB32djYjt2OEtXmxfjudlzqbkDDM3xccXyWmYEu+3ADGrfiKhTQcYLOd4&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.gigiart.ltd/um/?h0DlqZ5=zUMRnHHqEvHnhlxv7ul0o7duYCXQP/NigJilWumFZpB6G299GKUjOq9fAlbdo2F2L7pGQWeh&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.gigiart.ltd/um/
- url: http://www.rose-blencha.com/um/?h0DlqZ5=2VdfU7Odx+rtBodd3PYu50TC0dyalmO/xythd4qT1goRQUlE+v7j52oMCAw5RqfGqYGtotUw&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.rose-blencha.com/um/
- url: http://www.7thgenerationrabble.com/um/?h0DlqZ5=qCg2acAoFw3NIIKzrJKi/r6+hA6w7uaHvFNkheLyk0npNZrc1dV4b2rlHsmrmKgqGNsRWHU3&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.7thgenerationrabble.com/um/
- url: http://www.scaker.com/um/?h0DlqZ5=+yOKJmfs2AUMMiwIhJjF3ftzrHyWcdWbdT8U21VoR7BW7cK2j+HNvQ6sQGRkAxI0XcLNdYEE&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.scaker.com/um/
- url: http://www.realtec-project.com/um/?h0DlqZ5=7FCCdwWhlApNdbQrvmlzi/aJ1zSbxBli3wT7PF1mjYNAnEhK0bE5sd6+77kxD1K4JQGjVHq5&MJBx=FdCxIn0H-pvHhbPP
- url: http://www.realtec-project.com/um/

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://www.nvdough.com/um/?h0DlqZ5=4Yw0gXJLQ90lLTIcB32djYjt2OEtXmxfjudlzqbkDDM3xccXyWmYEu+3ADGrfiKhTQcYLOd4&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.gigiart.ltd/um/?h0DlqZ5=zUMRnHHqEvHnhlxv7ul0o7duYCXQP/NigJilWumFZpB6G299GKUjOq9fAlbdo2F2L7pGQWeh&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.gigiart.ltd/um/
- suspicious_request: http://www.rose-blencha.com/um/?h0DlqZ5=2VdfU7Odx+rtBodd3PYu50TC0dyalmO/xythd4qT1goRQUlE+v7j52oMCAw5RqfGqYGtotUw&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.rose-blencha.com/um/
- suspicious_request: http://www.7thgenerationrabble.com/um/?h0DlqZ5=qCg2acAoFw3NIIKzrJKi/r6+hA6w7uaHvFNkheLyk0npNZrc1dV4b2rlHsmrmKgqGNsRWHU3&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.7thgenerationrabble.com/um/
- suspicious_request: http://www.scaker.com/um/?h0DlqZ5=+yOKJmfs2AUMMiwIhJjF3ftzrHyWcdWbdT8U21VoR7BW7cK2j+HNvQ6sQGRkAxI0XcLNdYEE&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.scaker.com/um/
- suspicious_request: http://www.realtec-project.com/um/?h0DlqZ5=7FCCdwWhlApNdbQrvmlzi/aJ1zSbxBli3wT7PF1mjYNAnEhK0bE5sd6+77kxD1K4JQGjVHq5&MJBx=FdCxIn0H-pvHhbPP
- suspicious_request: http://www.realtec-project.com/um/

Network activity detected but not expressed in API logs

Dynamic (imported) function loading detected

- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrlIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue

- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce

- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdipLoadImageFromStream
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdipImageForceValidation
- DynamicLoader: gdiplus.dll/GdipGetImageType
- DynamicLoader: gdiplus.dll/GdipGetImageRawFormat
- DynamicLoader: gdiplus.dll/GdipGetImageWidth
- DynamicLoader: gdiplus.dll/GdipGetImageHeight
- DynamicLoader: gdiplus.dll/GdipBitmapGetPixel
- DynamicLoader: gdiplus.dll/GdipDisposeImage
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/VirtualAlloc
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDecrypt

- DynamicLoader: ADVAPI32.dll/CryptDeriveKey
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: apphelp.dll/ApphelpQueryModuleDataEx
- DynamicLoader: apphelp.dll/ApphelpParseModuleData
- DynamicLoader: apphelp.dll/ApphelpCreateAppcompatData
- DynamicLoader: apphelp.dll/SdbInitDatabaseEx
- DynamicLoader: apphelp.dll/SdbReleaseDatabase
- DynamicLoader: apphelp.dll/SdbUnpackAppCompatData
- DynamicLoader: apphelp.dll/SdbQueryContext
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ADVAPI32.dll/EventUnregister

Guard pages use detected - possible anti-debugging.

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

16 HTTP Request(s) detected

http://www.nvdough.com/um/?h0DlqZ5=4Yw0gXJLQ90lLTIcB32djYjt2OEtXmxfjudlzqbkDDM3xccXyWmYEu+3ADGrfiKhTQcYLOd4&MJBx=FdCxIn0H-pvHhbPP

Hostname: www.nvdough.com

IP Address:

Port: 80

Count: 1

http://www.gigiart.ltd/um/?h0DlqZ5=zUMRnHHqEvHnhlxv7ul0o7duYCXQP/NigJilWumFZpB6G299GKUjOq9fAlbdo2F2L7pGQWeh&MJBx=FdCxIn0H-pvHhbPP

Hostname: www.gigiart.ltd

IP Address: 94.136.40.51

Port: 80

Count: 1

http://www.gigiart.ltd/um/

Hostname: www.gigiart.ltd
IP Address: 94.136.40.51
Port: 80
Count: 1

http://www.gigiart.ltd/um/
Hostname: www.gigiart.ltd
IP Address: 94.136.40.51
Port: 80
Count: 1

http://www.rose-blencha.com/um/?h0DlqZ5=2VdfU7Odx+rtBodd3PYu50TC0dyalmO/xythd4qT1goRQUlE+v7j52oMCAw5RqfGqYGtotUw&MJBx=FdCxIn0H-pvHhbPP
Hostname: www.rose-blencha.com
IP Address:
Port: 80
Count: 1

http://www.rose-blencha.com/um/
Hostname: www.rose-blencha.com
IP Address:
Port: 80
Count: 1

http://www.rose-blencha.com/um/
Hostname: www.rose-blencha.com
IP Address:
Port: 80
Count: 1

http://www.7thgenerationrabble.com/um/?h0DlqZ5=qCg2acAoFw3NIlKzrJKi/r6+hA6w7uaHvFNkheLyk0npNZrc1dV4b2rlHsmrmKgqGNsRWHU3&MJBx=FdCxIn0H-pvHhbPP
Hostname: www.7thgenerationrabble.com
IP Address: 198.54.117.216
Port: 80
Count: 1

http://www.7thgenerationrabble.com/um/
Hostname: www.7thgenerationrabble.com
IP Address: 198.54.117.216
Port: 80
Count: 1

http://www.7thgenerationrabble.com/um/
Hostname: www.7thgenerationrabble.com
IP Address: 198.54.117.216
Port: 80
Count: 1

http://www.scaker.com/um/?h0DlqZ5=+yOKJmfs2AUMMiwIhJjF3ftzrHyWcdWbdT8U21VoR7BW7cK2j+HNvQ6sQGRkAxI0XcLNdYEE&MJBx=FdCxIn0H-pvHhbPP
Hostname: www.scaker.com
IP Address: 198.54.112.128
Port: 80
Count: 1

http://www.scaker.com/um/
Hostname: www.scaker.com
IP Address: 198.54.112.128
Port: 80
Count: 1

http://www.scaker.com/um/
Hostname: www.scaker.com
IP Address: 198.54.112.128
Port: 80
Count: 1

http://www.realtec-project.com/um/?h0DlqZ5=7FCCdwWhlApNdbQrvmlzi/aJ1zSbxBli3wT7PF1mjYNAnEhK0bE5sd6+77kxD1K4JQGjVHq5&MJBx=FdCxIn0H-pvHhbPP
Hostname: www.realtec-project.com
IP Address: 85.13.135.136
Port: 80
Count: 1

http://www.realtec-project.com/um/
Hostname: www.realtec-project.com
IP Address: 85.13.135.136
Port: 80
Count: 1

http://www.realtec-project.com/um/
Hostname: www.realtec-project.com
IP Address: 85.13.135.136
Port: 80
Count: 1