

Mozilla.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Malicious

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	408.50 KB (418304 bytes)
Compile time:	2019-08-06 04:39:52
MD5:	c26ab151f1b6c679564b3795f0b90465
SHA1:	ab14be07f13a0d4ca15c650c97c28e93978dcdc2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-08-12 11:45:04

URL(s) file hosting

<http://13.67.107.73/yzuv/Mozilla.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2019-08-06 15:17:33	20/66	

Import library

mscoree.dll

22

Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: checkip.amazonaws.com



Sniffs keystrokes

- SetWindowsHookExW: Process: Mozilla.exe(2772)

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (476) called API NtQuerySystemTime 411126 times
- Spam: services.exe (476) called API GetSystemTimeAsFileTime 1688986 times

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\lbZHhBYQ.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\lbZHhBYQ.url

Retrieves Windows ProductID, probably to fingerprint the sandbox

Checks the CPU name from registry, possibly for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\Windows\Window.exe

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
- file: C:\Users\Seven01\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect*.xml
- file: C:\Users\Seven01\AppData\Roaming\FTPGetter\servers.xml
- file: C:\Users\Seven01\AppData\Roaming\lpswitch\WS_FTP\Sites\ws_ftp.ini
- file: C:\cftp\Ftplist.txt
- key: HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Roaming\Thunderbird\profiles.ini
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP

Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password

- key:
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

- key:
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

Collects information to fingerprint the system

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.69, characteristics:
IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size:
0x00064800, virtual_size: 0x00064604

Creates RWX memory

Guard pages use detected - possible anti-debugging.

A process attempted to delay the analysis task.

- Process: Mozilla.exe tried to sleep 567 seconds, actually delayed analysis time by 0 seconds

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/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/GetCurrentPackageld
- 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/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- 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: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo



- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: SHELL32.dll/SHGetFolderPath
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetCurrentDirectory
- DynamicLoader: KERNEL32.dll/GetCurrentDirectoryW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CreateDirectory
- DynamicLoader: KERNEL32.dll/CreateDirectoryW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- 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: KERNEL32.dll/CreateMutexW
- 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: KERNEL32.dll/GetProcessId
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: psapi.dll/EnumProcesses
- DynamicLoader: psapi.dll/EnumProcessesW
- 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/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc



- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/MkParseDisplayName
- DynamicLoader: KERNEL32.dll/GetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/SetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLocaleName
- DynamicLoader: ole32.dll/BindMoniker
- DynamicLoader: SXS.DLL/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: SXS.DLL/SxsOleAut32MapConfiguredClsidToReferenceClsid
- DynamicLoader: SXS.DLL/SxsLookupClrGuid
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: mscoreei.dll/_CorDllMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorDllMain
- DynamicLoader: MSCOREE.DLL/GetTokenForVTableEntry
- DynamicLoader: MSCOREE.DLL/SetTargetForVTableEntry
- DynamicLoader: MSCOREE.DLL/GetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry



- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry
- DynamicLoader: KERNEL32.dll/GetLastError
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: wminet_utils.dll/ResetSecurity
- DynamicLoader: wminet_utils.dll/SetSecurity
- DynamicLoader: wminet_utils.dll/BlessWBemServices
- DynamicLoader: wminet_utils.dll/BlessWBemServicesObject
- DynamicLoader: wminet_utils.dll/GetPropertyHandle
- DynamicLoader: wminet_utils.dll/WritePropertyValue
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/VerifyClientKey
- DynamicLoader: wminet_utils.dll/GetQualifierSet
- DynamicLoader: wminet_utils.dll/Get
- DynamicLoader: wminet_utils.dll/Put
- DynamicLoader: wminet_utils.dll/Delete
- DynamicLoader: wminet_utils.dll/GetNames
- DynamicLoader: wminet_utils.dll/BeginEnumeration
- DynamicLoader: wminet_utils.dll/Next
- DynamicLoader: wminet_utils.dll/EndEnumeration
- DynamicLoader: wminet_utils.dll/GetPropertyQualifierSet
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/GetObjectText
- DynamicLoader: wminet_utils.dll/SpawnDerivedClass
- DynamicLoader: wminet_utils.dll/SpawnInstance
- DynamicLoader: wminet_utils.dll/CompareTo
- DynamicLoader: wminet_utils.dll/GetPropertyOrigin
- DynamicLoader: wminet_utils.dll/InheritsFrom
- DynamicLoader: wminet_utils.dll/GetMethod
- DynamicLoader: wminet_utils.dll/PutMethod
- DynamicLoader: wminet_utils.dll/DeleteMethod
- DynamicLoader: wminet_utils.dll/BeginMethodEnumeration
- DynamicLoader: wminet_utils.dll/NextMethod
- DynamicLoader: wminet_utils.dll/EndMethodEnumeration
- DynamicLoader: wminet_utils.dll/GetMethodQualifierSet
- DynamicLoader: wminet_utils.dll/GetMethodOrigin
- DynamicLoader: wminet_utils.dll/QualifierSet_Get
- DynamicLoader: wminet_utils.dll/QualifierSet_Put
- DynamicLoader: wminet_utils.dll/QualifierSet_Delete
- DynamicLoader: wminet_utils.dll/QualifierSet_GetNames
- DynamicLoader: wminet_utils.dll/QualifierSet_BeginEnumeration
- DynamicLoader: wminet_utils.dll/QualifierSet_Next
- DynamicLoader: wminet_utils.dll/QualifierSet_EndEnumeration
- DynamicLoader: wminet_utils.dll/GetCurrentApartmentType
- DynamicLoader: wminet_utils.dll/GetDemultiplexedStub
- DynamicLoader: wminet_utils.dll/CreateInstanceEnumWmi



- DynamicLoader: wminet_utils.dll/CreateClassEnumWmi
- DynamicLoader: wminet_utils.dll/ExecQueryWmi
- DynamicLoader: wminet_utils.dll/ExecNotificationQueryWmi
- DynamicLoader: wminet_utils.dll/PutInstanceWmi
- DynamicLoader: wminet_utils.dll/PutClassWmi
- DynamicLoader: wminet_utils.dll/CloneEnumWbemClassObject
- DynamicLoader: wminet_utils.dll/ConnectServerWmi
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: KERNEL32.dll/GetTimeZoneInformation
- DynamicLoader: KERNEL32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: SHELL32.dll/SHGetFolderPath
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFileMUIPath
- DynamicLoader: KERNEL32.dll/LoadLibraryEx
- DynamicLoader: KERNEL32.dll/LoadLibraryExW
- DynamicLoader: KERNEL32.dll/FreeLibrary
- DynamicLoader: KERNEL32.dll/FreeLibraryW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess



- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: KERNEL32.dll/TerminateProcess
- DynamicLoader: KERNEL32.dll/TerminateProcessW
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: KERNEL32.dll/CreateWaitableTimerExW
- DynamicLoader: KERNEL32.dll/SetWaitableTimerEx
- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/EnumCalendarInfoExEx
- DynamicLoader: KERNEL32.dll/GetCalendarInfoEx
- DynamicLoader: KERNEL32.dll/GetSystemTimeAsFileTime
- DynamicLoader: USER32.dll/GetLastInputInfo
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/EnumTimeFormatsEx
- DynamicLoader: KERNEL32.dll/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: KERNEL32.dll/QueryPerformanceFrequency
- DynamicLoader: KERNEL32.dll/QueryPerformanceCounter
- DynamicLoader: rasapi32.dll/RasEnumConnections
- DynamicLoader: rasapi32.dll/RasEnumConnectionsW
- DynamicLoader: rtutils.dll/TraceRegisterExA
- DynamicLoader: rtutils.dll/TracePrintfExA
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: WS2_32.dll/WSAStartup
- DynamicLoader: WS2_32.dll/WSASocket



- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/setsockopt
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/closesocket
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: KERNEL32.dll/FormatMessage
- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: rasapi32.dll/RasConnectionNotification
- DynamicLoader: rasapi32.dll/RasConnectionNotificationW
- DynamicLoader: ADVAPI32.dll/RegOpenCurrentUser
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: MLANG.dll/
- DynamicLoader: winhttp.dll/WinHttpOpenW
- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: winhttp.dll/WinHttpCloseHandleW
- DynamicLoader: WININET.dll/FindFirstUrlCacheEntryA
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandle
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetTimeoutsW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: urlmon.dll/CreateUri
- DynamicLoader: KERNEL32.dll/InitializeSRWLock
- DynamicLoader: KERNEL32.dll/AcquireSRWLockExclusive
- DynamicLoader: KERNEL32.dll/AcquireSRWLockShared
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockExclusive
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockShared
- DynamicLoader: KERNEL32.dll/InitializeSRWLock
- DynamicLoader: KERNEL32.dll/AcquireSRWLockExclusive
- DynamicLoader: KERNEL32.dll/AcquireSRWLockShared
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockExclusive
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockShared
- DynamicLoader: WININET.dll/FindNextUrlCacheEntryA
- DynamicLoader: WININET.dll/FindCloseUrlCache
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContext
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptReleaseContextW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: vaultcli.dll/VaultEnumerateVaults
- DynamicLoader: ADVAPI32.dll/EventSetInformation



- DynamicLoader: KERNEL32.dll/ResetEvent
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: IPHLPAPI.DLL/GetNetworkParams
- DynamicLoader: DNSAPI.dll/DnsQueryConfig
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: IPHLPAPI.DLL/GetIpInterfaceEntry
- DynamicLoader: IPHLPAPI.DLL/GetBestInterfaceEx
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2_32.dll/GetAddrInfoW
- DynamicLoader: WS2_32.dll/freeaddrinfo
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2_32.dll/WSAConnect
- DynamicLoader: WS2_32.dll/send
- DynamicLoader: WS2_32.dll/setsockopt
- DynamicLoader: WS2_32.dll/recv
- DynamicLoader: WS2_32.dll/shutdown
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: KERNEL32.dll/FindFirstFile
- DynamicLoader: KERNEL32.dll/FindFirstFileW
- DynamicLoader: KERNEL32.dll/FindClose
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyEx
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: USER32.dll/SetClipboardViewer
- DynamicLoader: USER32.dll/SetClipboardViewerW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/OleGetClipboard
- DynamicLoader: KERNEL32.dll/GlobalLock
- DynamicLoader: KERNEL32.dll/GlobalUnlock
- DynamicLoader: KERNEL32.dll/GlobalFree
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SetWindowsHookEx
- DynamicLoader: USER32.dll/SetWindowsHookExW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryW
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/PeekMessage
- DynamicLoader: USER32.dll/PeekMessageW
- DynamicLoader: USER32.dll/IsWindowUnicode
- DynamicLoader: USER32.dll/GetMessageW
- DynamicLoader: USER32.dll/TranslateMessage
- DynamicLoader: USER32.dll/DispatchMessageW
- DynamicLoader: USER32.dll/WaitMessage
- DynamicLoader: KERNEL32.dll/GetTempPath
- DynamicLoader: KERNEL32.dll/GetTempPathW
- DynamicLoader: ole32.dll/CoGetObjectContext



- DynamicLoader: KERNEL32.dll/GlobalMemoryStatusEx
- DynamicLoader: KERNEL32.dll/GlobalMemoryStatusExW
- DynamicLoader: OLEAUT32.dll/SysAllocStringLen
- DynamicLoader: OLEAUT32.dll/SysAllocStringLenW
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: ADVAPI32.dll/SystemFunction041
- DynamicLoader: ADVAPI32.dll/SystemFunction041W
- DynamicLoader: ADVAPI32.dll/SystemFunction040
- DynamicLoader: ADVAPI32.dll/SystemFunction040W
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/CreateSemaphore
- DynamicLoader: KERNEL32.dll/CreateSemaphoreA
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: FastProx.dll/DllGetClassObject
- DynamicLoader: FastProx.dll/DllCanUnloadNow
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: WMI.DLL/WmiQueryAllDataW
- DynamicLoader: WMI.DLL/WmiQuerySingleInstanceW
- DynamicLoader: WMI.DLL/WmiSetSingleItemW
- DynamicLoader: WMI.DLL/WmiSetSingleInstanceW
- DynamicLoader: WMI.DLL/WmiExecuteMethodW
- DynamicLoader: WMI.DLL/WmiNotificationRegistrationW
- DynamicLoader: WMI.DLL/WmiMofEnumerateResourcesW
- DynamicLoader: WMI.DLL/WmiFileHandleToInstanceNameW
- DynamicLoader: WMI.DLL/WmiDevInstToInstanceNameW
- DynamicLoader: WMI.DLL/WmiQueryGuidInformation
- DynamicLoader: WMI.DLL/WmiOpenBlock



- DynamicLoader: WMI.DLL/WmiCloseBlock
- DynamicLoader: WMI.DLL/WmiFreeBuffer
- DynamicLoader: WMI.DLL/WmiEnumerateGuids
- DynamicLoader: WINBRAND.dll/BrandingLoadString
- DynamicLoader: SECURITY.DLL/InitSecurityInterfaceW
- DynamicLoader: CRYPTSP.dll/SystemFunction035
- DynamicLoader: schannel.DLL/SpUserModelInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/NtSetSystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtQuerySystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQueryDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtOpenDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: ntdll.dll/NtOpenFile
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtFsControlFile
- DynamicLoader: ntdll.dll/NtQueryVolumeInformationFile
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupSetInfo
- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetLocalGroupSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupGetUsers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetMembers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupEnum
- DynamicLoader: NETAPI32.DLL/NetShareEnum
- DynamicLoader: NETAPI32.DLL/NetShareGetInfo
- DynamicLoader: NETAPI32.DLL/NetShareAdd
- DynamicLoader: NETAPI32.DLL/NetShareEnumSticky
- DynamicLoader: NETAPI32.DLL/NetShareSetInfo
- DynamicLoader: NETAPI32.DLL/NetShareDel
- DynamicLoader: NETAPI32.DLL/NetShareDelSticky
- DynamicLoader: NETAPI32.DLL/NetShareCheck
- DynamicLoader: NETAPI32.DLL/NetUserEnum
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: NETAPI32.DLL/NetUserSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetApiBufferFree
- DynamicLoader: NETAPI32.DLL/NetQueryDisplayInformation
- DynamicLoader: NETAPI32.DLL/NetServerSetInfo
- DynamicLoader: NETAPI32.DLL/NetServerGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetDCName
- DynamicLoader: NETAPI32.DLL/NetWkstaGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetAnyDCName
- DynamicLoader: NETAPI32.DLL/NetServerEnum
- DynamicLoader: NETAPI32.DLL/NetUserModalsGet
- DynamicLoader: NETAPI32.DLL/NetScheduleJobAdd
- DynamicLoader: NETAPI32.DLL/NetScheduleJobDel
- DynamicLoader: NETAPI32.DLL/NetScheduleJobEnum
- DynamicLoader: NETAPI32.DLL/NetScheduleJobGetInfo
- DynamicLoader: NETAPI32.DLL/NetUseGetInfo
- DynamicLoader: NETAPI32.DLL/NetEnumerateTrustedDomains
- DynamicLoader: NETAPI32.DLL/DsGetDcNameW



- DynamicLoader: NETAPI32.DLL/DsRoleGetPrimaryDomainInformation
- DynamicLoader: NETAPI32.DLL/DsRoleFreeMemory
- DynamicLoader: NETAPI32.DLL/NetRenameMachineInDomain
- DynamicLoader: NETAPI32.DLL/NetJoinDomain
- DynamicLoader: NETAPI32.DLL/NetUnjoinDomain
- DynamicLoader: WKSCLI.DLL/NetWkstaGetInfo
- DynamicLoader: cscapi.dll/CscNetApiGetInterface
- DynamicLoader: kernel32.dll/GetDiskFreeSpaceExW
- DynamicLoader: kernel32.dll/GetVolumePathNameW
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Heap32ListFirst
- DynamicLoader: kernel32.dll/GlobalMemoryStatusEx
- DynamicLoader: kernel32.dll/GetSystemDefaultUILanguage
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: RPCRT4.dll/UuidFromStringW
- DynamicLoader: radarrs.dll/WdiDiagnosticModuleMain
- DynamicLoader: radarrs.dll/WdiHandleInstance
- DynamicLoader: radarrs.dll/WdiGetDiagnosticModuleInterfaceVersion

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: 0.0.0.0
- ioc: kgxypqcbglg.resources
- ioc: 5.ekf
- ioc: 25.ea
- ioc: 4.ejf
- ioc: 7.eif
- ioc: 27.ec
- ioc: 6.ehf
- ioc: 26.eb
- ioc: 1.eof
- ioc: 21.ee
- ioc: 0.enf
- ioc: 20.ed
- ioc: 3.emf
- ioc: 23.eg
- ioc: 2.elf
- ioc: 22.ef
- ioc: ke.co
- ioc: kd.cn
- ioc: kg.cm
- ioc: 9.cgf
- ioc: kf.cl
- ioc: 8.cff
- ioc: ka.ck



- ioc: kc.ci
- ioc: kb.ch
- ioc: km.cg
- ioc: 3.cmf
- ioc: kl.cf
- ioc: 5.dkf
- ioc: 2.clf
- ioc: 35.da
- ioc: je.bo
- ioc: jd.bn
- ioc: jg.bm
- ioc: 9.bgf
- ioc: jf.bl
- ioc: 8.bff
- ioc: ja.bk
- ioc: jc.bi
- ioc: jb.bh
- ioc: jm.bg
- ioc: 3.bmf
- ioc: jl.bf
- ioc: 4.djf
- ioc: 2.blf
- ioc: ie.ao
- ioc: id.an
- ioc: ig.am
- ioc: 9.agf
- ioc: if.al
- ioc: 8.aff
- ioc: ia.ak
- ioc: ic.ai
- ioc: ib.ah
- ioc: im.ag
- ioc: 3.amf
- ioc: il.af
- ioc: 7.dif
- ioc: 2.alf
- ioc: 37.dc
- ioc: 6.dhf
- ioc: 36.db
- ioc: oe.go
- ioc: od.gn
- ioc: og.gm
- ioc: 9.ggf
- ioc: of.gl
- ioc: 8.gff
- ioc: oa.gk
- ioc: oc.gi
- ioc: ob.gh
- ioc: om.gg
- ioc: 3.gmf
- ioc: ol.gf
- ioc: 1.dof
- ioc: 2.glf
- ioc: 31.de
- ioc: ne.fo
- ioc: nd.fn
- ioc: ng.fm
- ioc: 9.fgf
- ioc: nf.fl
- ioc: 8.fff
- ioc: na.fk
- ioc: nc.fi
- ioc: nb.fh

- ioc: nm.fg
- ioc: 3.fmf
- ioc: nl.ff
- ioc: 0.dnf
- ioc: 2.flf
- ioc: 30.dd
- ioc: me.eo
- ioc: md.en
- ioc: mg.em
- ioc: 9.egf
- ioc: mf.el
- ioc: 8.eff
- ioc: ma.ek
- ioc: mc.ei
- ioc: mb.eh
- ioc: mm.eg
- ioc: ml.ef
- ioc: 3.dmf
- ioc: 33.dg
- ioc: le.do
- ioc: ld.dn
- ioc: lg.dm
- ioc: 9.dgf
- ioc: lf.dl
- ioc: 8.dff
- ioc: la.dk
- ioc: lc.di
- ioc: lb.dh
- ioc: lm.dg
- ioc: ll.df
- ioc: 2.dlf
- ioc: 32.df

Reads data out of its own binary image

- self_read: process: Mozilla.exe, pid: 2684, offset: 0x00065e00, length: 0x00000400

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://checkip.amazonaws.com/

Performs some HTTP requests

- url: http://checkip.amazonaws.com/

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

- IP: 192.168.56.1:587

SetUnhandledExceptionFilter detected (possible anti-debug)

1 HTTP Request(s) detected

<http://checkip.amazonaws.com/>

Hostname: checkip.amazonaws.com

IP Address: 10.1.26.180

Port: 80

Count: 1