

zzz.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Clipbanker


MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	36.50 KB (37376 bytes)
Compile time:	2019-09-12 10:10:10
MD5:	8d14a4e9e4ef7f54ceb7516453ba5fb7
SHA1:	164be26324fadd0d382172bbefde56cd680cc96d
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-09-15 14:45:05

URL(s) file hosting

<http://pw.coinpool.fun/zzz.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2019-09-15 12:04:25	34/68	

Import library

mscoree.dll

12

Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: api.ipify.org

Created network traffic indicative of malicious activity

- signature: ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Attempts to create or modify system certificates

Looks up the external IP address

- domain: api.ipify.org

.NET file is packed/obfuscated with Confuser

Reads data out of its own binary image

- self_read: process: zzz.exe, pid: 2664, offset: 0x00000000, length: 0x00001000

- self_read: process: zzz.exe, pid: 2664, offset: 0x00000080, length: 0x00000200

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

- ioc: inetsim.org0

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/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: 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: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- 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: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: psapi.dll/GetModuleInformationW
- DynamicLoader: psapi.dll/GetModuleBaseName
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW



- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: nlsorting.dll/SortGetHandle
- DynamicLoader: nlsorting.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/QueryPerformanceFrequency
- DynamicLoader: KERNEL32.dll/QueryPerformanceCounter
- 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: rasapi32.dll/RasEnumConnections
- DynamicLoader: rasapi32.dll/RasEnumConnectionsW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- 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: ole32.dll/CoTaskMemFree
- 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: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpOpenW
- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: winhttp.dll/WinHttpCloseHandleW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetTimeoutsW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: ole32.dll/CoGetContextToken
- 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: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: KERNEL32.dll/ResetEvent
- DynamicLoader: KERNEL32.dll/GetTimeZoneInformation
- DynamicLoader: KERNEL32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- 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/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: secur32.dll/EnumerateSecurityPackagesW
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: secur32.dll/FreeCredentialsHandle
- DynamicLoader: secur32.dll/AcquireCredentialsHandleW
- DynamicLoader: schannel.dll/SpUserModelInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: secur32.dll/DeleteSecurityContext
- DynamicLoader: secur32.dll/InitializeSecurityContextW
- DynamicLoader: WS2_32.dll/send
- DynamicLoader: WS2_32.dll/recv
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: ncrypt.dll/SslOpenProvider
- DynamicLoader: ncrypt.dll/GetSChannelInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/SslIncrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslImportKey
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: secur32.dll/QueryContextAttributesW
- DynamicLoader: ncrypt.dll/SslLookupCipherSuiteInfo
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertGetCertificateContextProperty
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContextW
- DynamicLoader: CRYPT32.dll/CertCloseStore
- DynamicLoader: CRYPT32.dll/CertDuplicateStore
- DynamicLoader: CRYPT32.dll/CertDuplicateStoreW
- DynamicLoader: CRYPT32.dll/CertEnumCertificatesInStore
- DynamicLoader: CRYPT32.dll/CertEnumCertificatesInStoreW
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertOpenStore
- DynamicLoader: CRYPT32.dll/CertOpenStoreW
- DynamicLoader: CRYPT32.dll/CertAddCertificateLinkToStore
- DynamicLoader: CRYPT32.dll/CertAddCertificateLinkToStoreW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: CRYPT32.dll/CertGetCertificateChain
- DynamicLoader: CRYPT32.dll/CertGetCertificateChainW
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW



- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: cryptnet.dll/I_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: SHLWAPI.dll/UrlGetPartW
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetOption
- DynamicLoader: winhttp.dll/WinHttpCrackUrl
- DynamicLoader: SHLWAPI.dll/StrCmpNW
- DynamicLoader: winhttp.dll/WinHttpConnect
- DynamicLoader: winhttp.dll/WinHttpOpenRequest
- DynamicLoader: winhttp.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: winhttp.dll/WinHttpSendRequest
- DynamicLoader: WS2_32.dll/GetAddrInfoW
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/FreeAddrInfoW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSARecv
- DynamicLoader: WS2_32.dll/WSASend
- DynamicLoader: winhttp.dll/WinHttpReceiveResponse
- DynamicLoader: winhttp.dll/WinHttpQueryHeaders
- DynamicLoader: winhttp.dll/WinHttpQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: winhttp.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- DynamicLoader: KERNEL32.dll/RegCloseKey
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW

- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: CRYPTSP.dll/CryptGetKeyParam
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateChain
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateChainW
- DynamicLoader: KERNEL32.dll/FormatMessage
- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicyW
- DynamicLoader: KERNEL32.dll/SetLastError
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ncrypt.dll/SslDecrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslFreeObject
- DynamicLoader: WS2_32.dll/shutdown
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: diasymreader.dll/DllGetClassObject

Guard pages use detected - possible anti-debugging.

Creates RWX memory

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

- IP: 192.168.56.1:80

SetUnhandledExceptionFilter detected (possible anti-debug)