

not_a_rat.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Bladabindi

MalScore: 100


File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	23.50 KB (24064 bytes)
Compile time:	2019-01-03 20:06:39
MD5:	7f3fdb1ee65c60e68b13e7727e2f43da
SHA1:	1086420a42105169ac11daae480e860c6be13c6b
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-01-17 13:42:04

URL(s) file hosting

https://cdn.discordapp.com/attachments/529465302472458253/530493472072007691/not_a_rat.exe

https://cdn.discordapp.com/attachments/529465302472458253/530623531244060672/not_a_rat.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-01-04 07:33:44	58/70	

Import library

mscoree.dll

11

Behaviors detected by system signatures

Creates a copy of itself



- copy: C:\Users\Seven01\AppData\Local\Temp\loldab.exe
- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\08df3c98cd8b4f56293066bd6bee67e0.exe

Installs itself for autorun at Windows startup

- key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\08df3c98cd8b4f56293066bd6bee67e0
- data: "C:\Users\Seven01\AppData\Local\Temp\loldab.exe" ..
- key:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\08df3c98cd8b4f56293066bd6bee67e0
- data: "C:\Users\Seven01\AppData\Local\Temp\loldab.exe" ..
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\08df3c98cd8b4f56293066bd6bee67e0.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\08df3c98cd8b4f56293066bd6bee67e0.exe

Sniffs keystrokes

- GetAsyncKeyState: Process: loldab.exe(2192)

Uses Windows utilities for basic functionality

- command: netsh firewall add allowedprogram "C:\Users\Seven01\AppData\Local\Temp\loldab.exe" "loldab.exe" ENABLE

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\loldab.exe

Reads data out of its own binary image

- self_read: process: not_a_rat.exe, pid: 2064, offset: 0x00000000, length: 0x00005e00

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/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcr7.dll/_set_error_mode
- DynamicLoader: msvcr7.dll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcr7.dll/_get_terminate
- DynamicLoader: KERNEL32.dll/FindActCtxSectionStringW
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: MSCOREE.DLL/IEE
- DynamicLoader: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: MSCOREE.DLL/GetStartupFlags
- DynamicLoader: mscoreei.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscoreei.dll/GetStartupFlags
- DynamicLoader: MSCOREE.DLL/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetCORVersion_RetAddr



- DynamicLoader: mscoreei.dll/GetCORVersion
- DynamicLoader: MSCOREE.DLL/GetCORSystemDirectory
- DynamicLoader: mscoreei.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: KERNEL32.dll/IsWow64Process
- 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/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/AddVectoredContinueHandler
- DynamicLoader: KERNEL32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/GetWriteWatch
- DynamicLoader: KERNEL32.dll/ResetWriteWatch
- DynamicLoader: KERNEL32.dll/CreateMemoryResourceNotification
- DynamicLoader: KERNEL32.dll/QueryMemoryResourceNotification
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface



- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegSetValueEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/RtlMoveMemory
- DynamicLoader: KERNEL32.dll/RtlMoveMemoryW
- DynamicLoader: shell32.dll/ShellExecuteEx
- DynamicLoader: shell32.dll/ShellExecuteExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- 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: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.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: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister
- 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/UrIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsGetValue



- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcr7.dll/_set_error_mode
- DynamicLoader: msvcr7.dll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcr7.dll/_get_terminate
- DynamicLoader: KERNEL32.dll/FindActCtxSectionStringW
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscorcli.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscorcli.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: MSCOREE.DLL/IEE
- DynamicLoader: mscorcli.dll/IEE_RetAddr
- DynamicLoader: mscorcli.dll/IEE
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: MSCOREE.DLL/GetStartupFlags
- DynamicLoader: mscorcli.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscorcli.dll/GetStartupFlags
- DynamicLoader: MSCOREE.DLL/GetHostConfigurationFile
- DynamicLoader: mscorcli.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscorcli.dll/GetHostConfigurationFile
- DynamicLoader: mscorcli.dll/GetCORVersion_RetAddr
- DynamicLoader: mscorcli.dll/GetCORVersion
- DynamicLoader: MSCOREE.DLL/GetCORSystemDirectory
- DynamicLoader: mscorcli.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscorcli.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscorcli.dll/CreateConfigStream
- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: KERNEL32.dll/IsWow64Process
- 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/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/AddVectoredContinueHandler
- DynamicLoader: KERNEL32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/GetWriteWatch



- DynamicLoader: KERNEL32.dll/ResetWriteWatch
- DynamicLoader: KERNEL32.dll/CreateMemoryResourceNotification
- DynamicLoader: KERNEL32.dll/QueryMemoryResourceNotification
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/Istrlen
- DynamicLoader: KERNEL32.dll/IstrlenW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegSetValueEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: USER32.dll/SendMessageTimeout
- DynamicLoader: USER32.dll/SendMessageTimeoutA
- DynamicLoader: KERNEL32.dll/GetStartupInfo
- DynamicLoader: KERNEL32.dll/GetStartupInfoW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- DynamicLoader: KERNEL32.dll/WaitForSingleObject
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: shfolder.dll/SHGetFolderPath
- DynamicLoader: shfolder.dll/SHGetFolderPathW



- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/SwitchToThread
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: USER32.dll/GetAsyncKeyState
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: USER32.dll/GetKeyState
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: USER32.dll/GetSystemMetrics
- 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: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- 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: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/PeekMessage
- DynamicLoader: USER32.dll/PeekMessageW
- 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/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: MSCOREE.DLL/ND_R12
- DynamicLoader: mscoreei.dll/ND_R12_RetAddr
- DynamicLoader: mscoreei.dll/ND_R12
- DynamicLoader: ws2_32.dll/WSAStartup
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- 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: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CreateFileMapping
- DynamicLoader: KERNEL32.dll/CreateFileMappingW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/MapViewOfFile
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/VirtualQuery
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSidW
- DynamicLoader: KERNEL32.dll/WaitForSingleObject
- DynamicLoader: KERNEL32.dll/OpenMutex
- DynamicLoader: KERNEL32.dll/OpenMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: KERNEL32.dll/GetProcessTimes
- DynamicLoader: KERNEL32.dll/GetProcessTimesW
- DynamicLoader: ws2_32.dll/setsockopt
- DynamicLoader: ws2_32.dll/inet_addr
- DynamicLoader: ws2_32.dll/WSAConnect
- DynamicLoader: KERNEL32.dll/FormatMessage
- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: USER32.dll/GetKeyState
- DynamicLoader: USER32.dll/GetKeyboardState
- DynamicLoader: USER32.dll/MapVirtualKey
- DynamicLoader: USER32.dll/MapVirtualKeyA
- DynamicLoader: USER32.dll/GetForegroundWindow
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/GetKeyboardLayout
- DynamicLoader: USER32.dll/ToUnicodeEx
- 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: KERNEL32.dll/GetExitCodeProcess
- DynamicLoader: KERNEL32.dll/GetExitCodeProcessW
- DynamicLoader: KERNEL32.dll/GetProcessWorkingSetSize
- DynamicLoader: KERNEL32.dll/GetProcessWorkingSetSizeW
- DynamicLoader: KERNEL32.dll/SetProcessWorkingSetSize
- DynamicLoader: KERNEL32.dll/SetProcessWorkingSetSizeW
- DynamicLoader: ws2_32.dll/shutdown
- DynamicLoader: USER32.dll/GetWindowTextLengthA
- DynamicLoader: USER32.dll/GetWindowTextA
- DynamicLoader: KERNEL32.dll/GlobalMemoryStatusEx
- DynamicLoader: ADVAPI32.dll/RegCreateKeyEx



- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: RASMONTR.DLL/InitHelperDll
- DynamicLoader: NSHWFP.DLL/InitHelperDll
- DynamicLoader: DHCPMONITOR.DLL/InitHelperDll
- DynamicLoader: WSHHELPER.DLL/InitHelperDll
- DynamicLoader: NSHHTTP.DLL/InitHelperDll
- DynamicLoader: FWCFG.DLL/InitHelperDll
- DynamicLoader: AUTHFWCFG.DLL/InitHelperDll
- DynamicLoader: IFMON.DLL/InitHelperDll
- DynamicLoader: NETIOHLP.DLL/InitHelperDll
- DynamicLoader: WHHELPER.DLL/InitHelperDll
- DynamicLoader: HNETMON.DLL/InitHelperDll
- DynamicLoader: RPCNSH.DLL/InitHelperDll
- DynamicLoader: DOT3CFG.DLL/InitHelperDll
- DynamicLoader: NAPMONTR.DLL/InitHelperDll
- DynamicLoader: NSHIPSEC.DLL/InitHelperDll
- DynamicLoader: P2PNETSH.DLL/InitHelperDll
- DynamicLoader: WLANCFG.DLL/InitHelperDll
- DynamicLoader: PEERDISTSH.DLL/InitHelperDll
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: CRYPTSP.dll/CryptEnumProvidersW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: RpcRtRemote.dll/_RpcExtInitializeExtensionPoint
- DynamicLoader: HTTPAPI.dll/HttpInitialize
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: USERENV.dll/UnregisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: MPRMSG.dll/MprmsgGetErrorString
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: HTTPAPI.dll/HttpTerminate
- DynamicLoader: GPAPI.dll/UnregisterGPNotificationInternal
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: comctl32.dll/

Guard pages use detected - possible anti-debugging.


Creates RWX memory

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

- IP: 152.44.44.237:6969 (United States)

SetUnhandledExceptionFilter detected (possible anti-debug)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
152.44.44.237 		152-44-44-237.us-sjo1.upcloud.host.

1 Countr(y|ies) detected

Hosts	Country
1	United States 