kak.exe

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

MalFamily: Azorult **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	828.00 KB (847872 bytes)
Compile time:	2019-08-02 08:12:30
MD5:	b91114eb71f8e3f884381e97c548009f
SHA1:	bd1a4988db9a5bd3018a357b218d50b84edd9f81
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-09-18 19:15:04

URL(s) file hosting

http://laveronicamagazine.com/wp-includes/js/jak/zayn/kak.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-09-17 08:27:38	17/68	

Import library

mscoree.dll

12 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN AZORult Variant.4 Checkin M2

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\filename.exe

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\filename.exe:Zone.Identifier

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
- url: http://techxim.com:443/wp-admin/admin/32/index.php

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

- post_no_referer: HTTP traffic contains a POST request with no referer header
- post_no_useragent: HTTP traffic contains a POST request with no user-agent header
- http_version_old: HTTP traffic uses version 1.0
- suspicious_request: http://techxim.com:443/wp-admin/admin/32/index.php

Dynamic (imported) function loading detected

- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId

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

- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- 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/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- 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: 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: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryW
- DynamicLoader: webengine4.dll/InitializeLibrary
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: MSCOREE.DLL/CorBindToRuntimeHost
- DynamicLoader: mscoreei.dll/CorBindToRuntimeHost_RetAddr
- DynamicLoader: mscoreei.dll/CorBindToRuntimeHost
- DynamicLoader: clr.dll/DllGetClassObjectInternal
- DynamicLoader: webengine4.dll/PerfCounterInitialize
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/ConvertStringSidToSidW
- DynamicLoader: ADVAPI32.dll/IsValidSid
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/CopySid
- DynamicLoader: ADVAPI32.dll/LookupAccountNameW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountNameW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: KERNEL32.dll/CreateWaitableTimerExW

- DynamicLoader: KERNEL32.dll/SetWaitableTimerEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: webengine4.dll/MgdGetIISVersionInformation
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/LocalAllocW
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaLookupSids
- DynamicLoader: webengine4.dll/GetDirMonConfiguration
- DynamicLoader: KERNEL32.dll/FindResource
- DynamicLoader: KERNEL32.dll/FindResourceA
- DynamicLoader: KERNEL32.dll/SizeofResource
- DynamicLoader: KERNEL32.dll/LoadResource
- DynamicLoader: KERNEL32.dll/LockResource
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/VirtualAlloc
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDecrypt
- DynamicLoader: ADVAPI32.dll/CryptDeriveKey
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: apphelp.dll/ApphelpQueryModuleDataEx
- DynamicLoader: apphelp.dll/ApphelpParseModuleData
- DynamicLoader: apphelp.dll/ApphelpCreateAppcompatData
- DynamicLoader: apphelp.dll/SdbInitDatabaseEx
- DynamicLoader: apphelp.dll/SdbReleaseDatabase
- DynamicLoader: apphelp.dll/SdbUnpackAppCompatData
- DynamicLoader: apphelp.dll/SdbQueryContext
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: crypt32.dll/CryptUnprotectData

- DynamicLoader: crtdll.dll/wcscmp
- DynamicLoader: Gdiplus.dll/GdiplusStartup
- DynamicLoader: Gdiplus.dll/GdiplusShutdown
- DynamicLoader: Gdiplus.dll/GdipCreateBitmapFromHBITMAP
- DynamicLoader: Gdiplus.dll/GdipGetImageEncodersSize
- DynamicLoader: Gdiplus.dll/GdipGetImageEncoders
- DynamicLoader: Gdiplus.dll/GdipDisposeImage
- DynamicLoader: Gdiplus.dll/GdipSaveImageToStream
- DynamicLoader: ole32.dll/CreateStreamOnHGlobal
- DynamicLoader: ole32.dll/GetHGlobalFromStream
- DynamicLoader: kernel32.dll/ExpandEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetComputerNameW
- DynamicLoader: kernel32.dll/GlobalMemoryStatus
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/ReadFile
- DynamicLoader: kernel32.dll/GetFileAttributesW
- DynamicLoader: kernel32.dll/CreateMutexA
- DynamicLoader: kernel32.dll/ReleaseMutex
- DynamicLoader: kernel32.dll/GetLastError
- DynamicLoader: kernel32.dll/GetCurrentDirectoryW
- DynamicLoader: kernel32.dll/SetEnvironmentVariableW
- DynamicLoader: kernel32.dll/SetCurrentDirectoryW
- DynamicLoader: kernel32.dll/FindFirstFileW
- DynamicLoader: kernel32.dll/FindNextFileW
- DynamicLoader: kernel32.dll/LocalFree
- DynamicLoader: kernel32.dll/GetTickCount
- DynamicLoader: kernel32.dll/CopyFileW
- DynamicLoader: kernel32.dll/FindClose
- DynamicLoader: kernel32.dll/GlobalMemoryStatusEx
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Process32FirstW
- DynamicLoader: kernel32.dll/Process32NextW
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/SetDllDirectoryW
- DynamicLoader: kernel32.dll/GetLocaleInfoA
- DynamicLoader: kernel32.dll/GetLocalTime
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: kernel32.dll/RemoveDirectoryW
- DynamicLoader: kernel32.dll/DeleteFileW
- DynamicLoader: kernel32.dll/GetLogicalDriveStringsA
- DynamicLoader: kernel32.dll/GetDriveTypeA
- DynamicLoader: kernel32.dll/CreateProcessW
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/LookupAccountSidA
- DynamicLoader: ADVAPI32.dll/CreateProcessAsUserW
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: user32.dll/EnumDisplayDevicesW

- DynamicLoader: user32.dll/wvsprintfA
- DynamicLoader: user32.dll/GetKeyboardLayoutList
- DynamicLoader: shell32.dll/ShellExecuteExW
- DynamicLoader: ntdll.dll/RtlComputeCrc32
- DynamicLoader: sechost.dll/LookupAccountSidLocalA
- DynamicLoader: wininet.dll/InternetOpenA
- DynamicLoader: wininet.dll/InternetConnectA
- DynamicLoader: wininet.dll/HttpOpenRequestA
- DynamicLoader: wininet.dll/HttpAddRequestHeadersA
- DynamicLoader: wininet.dll/HttpSendRequestA
- DynamicLoader: wininet.dll/InternetReadFile
- DynamicLoader: wininet.dll/InternetCloseHandle
- DynamicLoader: wininet.dll/InternetCrackUrlA
- DynamicLoader: wininet.dll/InternetSetOptionA
- DynamicLoader: RASAPI32.dll/RasConnectionNotificationW
- DynamicLoader: sechost.dll/OpenServiceA
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- 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: 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/
- 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: RPCRT4.dll/RpcBindingFree
- DynamicLoader: wsock32.dll/WSAStartup
- DynamicLoader: wsock32.dll/gethostbyname
- DynamicLoader: wsock32.dll/socket
- DynamicLoader: wsock32.dll/send
- DynamicLoader: wsock32.dll/recv
- DynamicLoader: wsock32.dll/htons
- DynamicLoader: wsock32.dll/connect
- DynamicLoader: wsock32.dll/closesocket
- DynamicLoader: RPCRT4.dll/RpcBindingFree

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)

2 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 205.185.216.10
Port: 80
Count: 1

http://techxim.com:443/wp-admin/admin/32/index.php
Hostname: techxim.com
IP Address: 103.94.27.67
Port: 443
Count: 1