MAT REPORT

GENERAL INFO

```
----- File Information -----
File Name: sample.exe
Machine Type: 332
Sections Mean Entropy: 3.57
Resources Mean Entropy: 3.03
Number of Exports: 0
■
CreatePropertySheetPageA, PropertySheetA, GetComputerNameA, WriteFile, MoveFileA
SetFileTime, SetEndOfFile, SetFilePointer, GetModuleFileNameA, lstrcatA
CreateDirectoryA, MulDiv, GetCurrentDirectoryA, GetProcAddress, LoadLibraryA
FindClose, FindFirstFileA, FormatMessageA, ReadFile, GetCurrentProcess
GetVersionExA, GetTempPathA, UnmapViewOfFile, MapViewOfFile, CreateFileMappingA
GetFileSize, GetWindowsDirectoryA, GetShortPathNameA, MoveFileExA, GetVersion
LocalFileTimeToFileTime, GetFileAttributesA, lstrcmpiA, SetEnvironmentVariableA
CompareStringW, CompareStringA, GetOEMCP, GetACP, GetCPInfo, GetStringTypeW
GetStringTypeA, LCMapStringW, LCMapStringA, FlushFileBuffers, RtlUnwind
GetEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsW
FreeEnvironmentStringsA, UnhandledExceptionFilter, HeapSize, SetStdHandle
WideCharToMultiByte, GetFileType, GetStdHandle, SetHandleCount, HeapReAlloc
VirtualAlloc, VirtualFree, GetDriveTypeA, CreateFileA, GetFileTime, CloseHandle
CompareFileTime, SetFileAttributesA, DeleteFileA, lstrcpyA, lstrlenA
GetTempFileNameA, GetLastError, SetLastError, DosDateTimeToFileTime, HeapCreate
HeapDestroy, GetEnvironmentVariableA, GetCommandLineA, GetStartupInfoA
HeapAlloc, HeapFree, GetTimeZoneInformation, GetSystemTime, GetLocalTime
MultiByteToWideChar, ExitProcess, TerminateProcess, GetModuleHandleA
GetWindowTextA, MessageBoxA, IsWindow, PeekMessageA, IsDialogMessageA
TranslateMessage, ExitWindowsEx, UpdateWindow, GetDlgCtrlID, GetSysColor
GetSysColorBrush, SetWindowLongA, CheckDlgButton, wsprintfA, ShowWindow
GetParent, PostMessageA, LoadStringA, SetDlgItemTextA, GetDlgItemTextA
SendMessageA, GetDC, ReleaseDC, SendDlgItemMessageA, DestroyWindow, GetDlgItem
DispatchMessageA, SetBkColor, GetDeviceCaps, CreateFontA, DeleteObject
SetTextColor, RegQueryValueExA, RegOpenKeyExA, RegQueryValueA, OpenProcessToken
LookupPrivilegeValueA, AdjustTokenPrivileges, RegCloseKey, SHBrowseForFolderA
SHGetDesktopFolder, SHGetPathFromIDListA, SHGetMalloc
----- Malicious Indicators -----
Status: Potentially Malicious
- Suspicious API imports detected.
```