MAT REPORT

GENERAL INFO

----- File Information -----
File Name: mal1.exe
Machine Type: 332
Sections Mean Entropy: 3.02
Resources Mean Entropy: 4.17
Number of Exports: 0
■
lstrlenW, CreateMailslotW, GetLastError, GetProcAddress, LoadLibraryW
VirtualProtect, DuplicateHandle, CloseHandle, GetTickCount, GetFileAttributesExA
LocalAlloc, LockFile, GetStartupInfoW, RaiseException, RtlUnwind
TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter
SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WriteFile
WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers
DeleteCriticalSection, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection
GetModuleHandleW, Sleep, ExitProcess, GetStdHandle, GetModuleFileNameA
GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW
GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, TlsGetValue
TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError
GetCurrentThreadId, InterlockedDecrement, GetCurrentThread, HeapCreate
HeapDestroy, VirtualFree, QueryPerformanceCounter, GetCurrentProcessId
GetSystemTimeAsFileTime, SetFilePointer, GetCPInfo, GetACP, GetOEMCP
IsValidCodePage, VirtualAlloc, HeapReAlloc, WriteConsoleA, GetConsoleOutputCP
WriteConsoleW, MultiByteToWideChar, SetStdHandle
InitializeCriticalSectionAndSpinCount, CreateFileA, HeapSize
SetConsoleCtrlHandler, FreeLibrary, InterlockedExchange, LoadLibraryA
LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeFormatA
GetDateFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA
IsValidLocale, SetEndOfFile, GetProcessHeap, ReadFile, GetLocaleInfoW
GetTimeZoneInformation, CompareStringA, CompareStringW, SetEnvironmentVariableA
OpenSCManagerA, SetAclInformation, AreAnyAccessesGranted
----- Malicious Indicators -----
Status: Potentially Malicious
- Suspicious API imports detected.