MAT REPORT

GENERAL INFO

----- File Information -----
File Name: trojan.exe
Machine Type: 332
Sections Mean Entropy: 4.31
Resources Mean Entropy: 4.38
Number of Exports: 3
■
lstrlenA, CommConfigDialogA, HeapAlloc, SetEnvironmentVariableW, FlushViewOfFile
GetTickCount, GetCommConfig, GetPrivateProfileStringW, GetWindowsDirectoryA
GetMailslotInfo, GetCompressedFileSizeA, lstrcatA, GetOverlappedResult
GetVolumePathNameA, EnumSystemLocalesA, GetLastError, GetProcAddress
GetNumaHighestNodeNumber, LoadLibraryA, LocalAlloc, IsWow64Process
BuildCommDCBAndTimeoutsW, WaitForMultipleObjects, FindFirstVolumeMountPointA
GetProcessAffinityMask, CreateMailslotA, GetConsoleCursorInfo
ScrollConsoleScreenBufferA, GetVolumeNameForVolumeMountPointW, CreateFileW
CloseHandle, EncodePointer, DecodePointer, EnterCriticalSection
LeaveCriticalSection, DeleteCriticalSection, WideCharToMultiByte
MultiByteToWideChar, GetStringTypeW, IsDebuggerPresent
IsProcessorFeaturePresent, GetCommandLineA, RaiseException, RtlUnwind, HeapFree
UnhandledExceptionFilter, SetUnhandledExceptionFilter, SetLastError
InitializeCriticalSectionAndSpinCount, Sleep, GetCurrentProcess
TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW
GetModuleHandleW, GetCPInfo, LCMapStringW, ExitProcess, GetModuleHandleExW
HeapSize, GetCurrentThreadId, GetProcessHeap, GetStdHandle, GetFileType
GetModuleFileNameA, WriteFile, GetModuleFileNameW, QueryPerformanceCounter
GetCurrentProcessId, GetSystemTimeAsFileTime, GetEnvironmentStringsW
FreeEnvironmentStringsW, GetACP, HeapReAlloc, IsValidCodePage, GetOEMCP
LoadLibraryExW, OutputDebugStringW, GetConsoleCP, GetConsoleMode
SetFilePointerEx, FlushFileBuffers, SetStdHandle, WriteConsoleW, GetClipCursor
----- Malicious Indicators -----
Status: Potentially Malicious
- Suspicious API imports detected.