

File Analysis Report

Generated on: 2025-05-18 16:45:01

=====

File Information

=====

Filename: AgentTesla.exe
Size: 2,932,642 bytes
Type: PE32

=====

File Hashes

=====

MD5: cce284cab135d9c0a2a64a7caec09107
SHA1: e4b8f4b6cab18b9748f83e9fffd275ef5276199e
SHA256: 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

=====

PE Header Information

=====

Entry Point: 0x33c4
Image Base: 0x400000
Sections: 5

=====

PE Sections

=====

Section: .text
Virtual Address: 0x1000
Virtual Size: 0x631a
Raw Size: 0x6400
Section: .rdata
Virtual Address: 0x8000
Virtual Size: 0x1384
Raw Size: 0x1400
Section: .data
Virtual Address: 0xa000
Virtual Size: 0x20318
Raw Size: 0x600
Section: .ndata
Virtual Address: 0x2b000
Virtual Size: 0x1c000

Raw Size: 0x0

Section: .rsrc

Virtual Address: 0x47000

Virtual Size: 0x4260

Raw Size: 0x4400

Imported DLLs and Functions

■ KERNEL32.dll

- SetEnvironmentVariableW
- SetFileAttributesW
- Sleep
- GetTickCount
- GetFileSize
- GetModuleFileNameW
- GetCurrentProcess
- CopyFileW
- SetCurrentDirectoryW
- GetFileAttributesW
- GetWindowsDirectoryW
- GetTempPathW
- GetCommandLineW
- GetVersion
- SetErrorMode
- lstrlenW
- lstrcpynW
- GetDiskFreeSpaceW
- ExitProcess
- MoveFileW
- CreateThread
- GetLastError
- CreateDirectoryW
- CreateProcessW
- RemoveDirectoryW
- lstrcmpiA
- CreateFileW
- GetTempFileNameW
- WriteFile
- lstrcpyA
- MoveFileExW
- lstrcatW
- GetSystemDirectoryW

- GetProcAddress
- GetModuleHandleA
- GetExitCodeProcess
- lstrcmpiW
- lstrcmpW
- GetFullPathNameW
- GetShortPathNameW
- SearchPathW
- CompareFileTime
- SetFileTime
- CloseHandle
- ExpandEnvironmentStringsW
- GlobalFree
- GlobalLock
- GlobalUnlock
- GlobalAlloc
- DeleteFileW
- FindFirstFileW
- FindNextFileW
- FindClose
- SetFilePointer
- ReadFile
- MulDiv
- lstrlenA
- WideCharToMultiByte
- MultiByteToWideChar
- WritePrivateProfileStringW
- FreeLibrary
- GetPrivateProfileStringW
- GetModuleHandleW
- LoadLibraryExW

■ USER32.dll

- GetWindowRect
- GetSystemMenu
- SetClassLongW
- IsWindowEnabled
- SetWindowPos
- GetSysColor
- GetWindowLongW
- SetCursor
- LoadCursorW
- CheckDlgButton

- GetMessagePos
- CallWindowProcW
- IsWindowVisible
- CloseClipboard
- SetClipboardData
- EmptyClipboard
- OpenClipboard
- TrackPopupMenu
- ScreenToClient
- EnableMenuItem
- GetDlgItem
- SetDlgItemTextW
- GetDlgItemTextW
- MessageBoxIndirectW
- CharPrevW
- CharNextA
- wsprintfA
- DispatchMessageW
- PeekMessageW
- GetDC
- ReleaseDC
- EnableWindow
- InvalidateRect
- SendMessageW
- DefWindowProcW
- BeginPaint
- GetClientRect
- FillRect
- SystemParametersInfoW
- EndDialog
- RegisterClassW
- DialogBoxParamW
- CreateWindowExW
- GetClassInfoW
- DestroyWindow
- CharNextW
- ExitWindowsEx
- SetWindowTextW
- LoadImageW
- SetTimer
- ShowWindow
- PostQuitMessage

- wsprintfW
- SetWindowLongW
- FindWindowExW
- IsWindow
- CreatePopupMenu
- AppendMenuW
- GetSystemMetrics
- DrawTextW
- EndPaint
- CreateDialogParamW
- SendMessageTimeoutW
- SetForegroundWindow

■ GDI32.dll

- SelectObject
- SetTextColor
- SetBkMode
- CreateFontIndirectW
- CreateBrushIndirect
- DeleteObject
- GetDeviceCaps
- SetBkColor

■ SHELL32.dll

- ShellExecuteExW
- SHGetPathFromIDListW
- SHGetSpecialFolderLocation
- SHGetFileInfoW
- SHFileOperationW
- SHBrowseForFolderW

■ ADVAPI32.dll

- AdjustTokenPrivileges
- RegCreateKeyExW
- RegOpenKeyExW
- SetFileSecurityW
- OpenProcessToken
- LookupPrivilegeValueW
- RegEnumValueW
- RegDeleteKeyW
- RegDeleteValueW
- RegCloseKey
- RegSetValueExW
- RegQueryValueExW
- RegEnumKeyW

■ COMCTL32.dll

- ImageList_Create
- ImageList_AddMasked
- Ordinal 17
- ImageList_Destroy

■ ole32.dll

- OleUninitialize
- OleInitialize
- CoTaskMemFree
- CoCreateInstance

Extracted Strings

1. !This program cannot be run in DOS mode.
2. .text
3. `.rdata
4. @.data
5. .ndata
6. .rsrc
7. s495L
8. tZj\V
9. >FFf;
10. jHjZW
11. VQSPW
12. SQVPW
13. 8u/j!
14. v#Vh`.@
15. Instu`
16. softuW
17. NulluN
18. YtS9]
19. j@Vh@
20. SVWj _3
21. j [f;
22. Aj"A[f
23. D\$ Ph0
24. D\$\$SPS
25. Vj%SSS
26. tWf="
27. WPWj0
28. D\$\$+D\$
29. D\$,+D\$\$P

- 30. UUUUW
- 31. t\$,VW
- 32. WWWWjn
- 33. uDWWH
- 34. Ph4T@
- 35. FFC;]
- 36. \u f9O
- 37. ^\PN
- 38. f!>_^
- 39. @_^[]
- 40. 90u'AAf
- 41. v%Ph|
- 42. SVWj"
- 43. UXTHEME
- 44. USERENV
- 45. SETUPAPI
- 46. APPHELP
- 47. PROPSYS
- 48. DWMAPI
- 49. CRYPTBASE
- 50. OLEACC
- 51. CLBCATQ
- 52. NTMARTA
- 53. RichEd32
- 54. RichEd20
- 55. MulDiv
- 56. DeleteFileW
- 57. FindFirstFileW
- 58. FindNextFileW
- 59. FindClose
- 60. SetFilePointer
- 61. ReadFile
- 62. MultiByteToWideChar
- 63. lstrlenA
- 64. WideCharToMultiByte
- 65. GetPrivateProfileStringW
- 66. WritePrivateProfileStringW
- 67. FreeLibrary
- 68. LoadLibraryExW
- 69. GetModuleHandleW
- 70. GlobalAlloc
- 71. GlobalFree

- 72. ExpandEnvironmentStringsW
- 73. lstrcmpW
- 74. lstrcmpiW
- 75. CloseHandle
- 76. SetFileTime
- 77. CompareFileTime
- 78. SearchPathW
- 79. GetShortPathNameW
- 80. GetFullPathNameW
- 81. MoveFileW
- 82. SetCurrentDirectoryW
- 83. GetFileAttributesW
- 84. SetFileAttributesW
- 85. Sleep
- 86. GetTickCount
- 87. GetFileSize
- 88. GetModuleFileNameW
- 89. GetCurrentProcess
- 90. CopyFileW
- 91. ExitProcess
- 92. SetEnvironmentVariableW
- 93. GetWindowsDirectoryW
- 94. GetTempPathW
- 95. GetCommandLineW
- 96. GetVersion
- 97. SetErrorMode
- 98. lstrlenW
- 99. lstrcpynW
- 100. GetDiskFreeSpaceW

[+] ... and 12775 more strings not shown.