Undocumented Structures

Introduction

When referencing the Windows documentation for a structure, one may encounter several *reserved* members within the structure. These reserved members are often presented as arrays of `BYTE` or `PVOID` data types. This practice is implemented by Microsoft to maintain confidentiality and prevent users from understanding the structure to avoid modifications to these reserved members.

With that being said, throughout this course, it will be necessary to work with these undocumented members. Therefore, some modules will avoid using Microsoft's documentation and instead use other websites that have the full undocumented structure, which was likely derived through reverse engineering.

PEB Structure Example

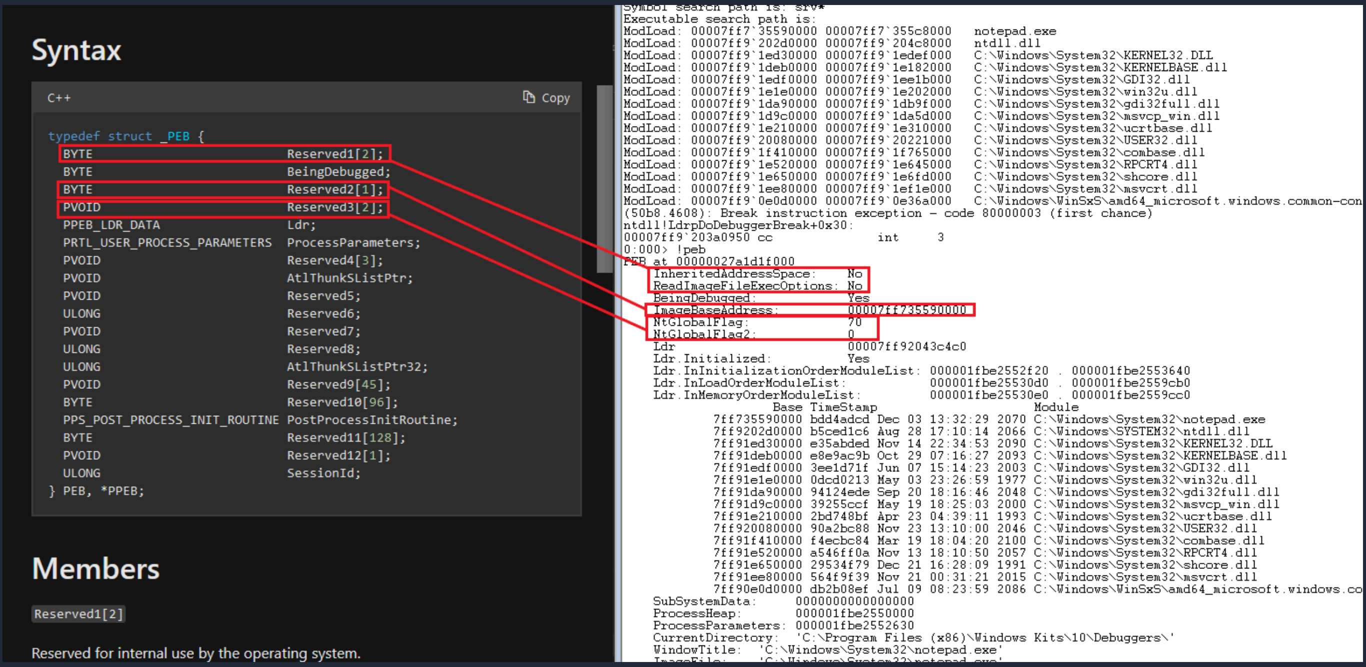
As mentioned in an earlier module, the Process Environment Block or PEB is a data structure that holds information about a Windows process. However, Microsoft's documentation on the PEB structure shows several reserved members. This makes it difficult to access the members of the structure.

```
typedef struct _PEB {
  BYTE                          Reserved1[2];
  BYTE                          BeingDebugged;
  BYTE                          Reserved2[1];
  PVOID                         Reserved3[2];
  PPEB_LDR_DATA                 Ldr;
  PRTL_USER_PROCESS_PARAMETERS  ProcessParameters;
  PVOID                         Reserved4[3];
  PVOID                         AtlThunkSListPtr;
  PVOID                         Reserved5;
  ULONG                         Reserved6;
  PVOID                         Reserved7;
  ULONG                         Reserved8;
  ULONG                         AtlThunkSListPtr32;
  PVOID                         Reserved9[45];
  BYTE                          Reserved10[96];
  PPS_POST_PROCESS_INIT_ROUTINE PostProcessInitRoutine;
```

```
    BYTE                          Reserved11[128];
    PVOID                         Reserved12[1];
    ULONG                         SessionId;
  } PEB, *PPEB;
```

Finding Reserved Members

One way to determine what the PEB's reserved members hold is through the `!peb` command in WinDbg.



Syntax

```
C++
typedef struct _PEB {
  BYTE                          Reserved1[2];
  BYTE                          BeingDebugged;
  BYTE                          Reserved2[1];
  PVOID                         Reserved3[2];
  PPEB_LDR_DATA                 Ldr;
  PRTL_USER_PROCESS_PARAMETERS  ProcessParameters;
  PVOID                         Reserved4[3];
  PVOID                         AtlThunkSListPtr;
  PVOID                         Reserved5;
  ULONG                         Reserved6;
  PVOID                         Reserved7;
  ULONG                         Reserved8;
  ULONG                         AtlThunkSListPtr32;
  PVOID                         Reserved9[45];
  BYTE                          Reserved10[96];
  PPS_POST_PROCESS_INIT_ROUTINE PostProcessInitRoutine;
  BYTE                          Reserved11[128];
  PVOID                         Reserved12[1];
  ULONG                         SessionId;
} PEB, *PPEB;
```

Members

`Reserved1[2]`

Reserved for internal use by the operating system.

```
Symbol search path is: srv*
Executable search path is:
ModLoad: 00007ff7`35590000 00007ff7`355c8000   notepad.exe
ModLoad: 00007ff9`202d0000 00007ff9`204c8000   ntdll.dll
ModLoad: 00007ff9`1ed30000 00007ff9`1edef000   C:\Windows\System32\KERNEL32.DLL
ModLoad: 00007ff9`1deb0000 00007ff9`1e182000   C:\Windows\System32\KERNELBASE.dll
ModLoad: 00007ff9`1edf0000 00007ff9`1ee1b000   C:\Windows\System32\GDI32.dll
ModLoad: 00007ff9`1e1e0000 00007ff9`1e202000   C:\Windows\System32\win32u.dll
ModLoad: 00007ff9`1da90000 00007ff9`1db9f000   C:\Windows\System32\gdi32full.dll
ModLoad: 00007ff9`1d9c0000 00007ff9`1da5d000   C:\Windows\System32\msvcp_win.dll
ModLoad: 00007ff9`1e210000 00007ff9`1e310000   C:\Windows\System32\ucrtbase.dll
ModLoad: 00007ff9`20080000 00007ff9`20221000   C:\Windows\System32\USER32.dll
ModLoad: 00007ff9`1f410000 00007ff9`1f765000   C:\Windows\System32\combase.dll
ModLoad: 00007ff9`1e520000 00007ff9`1e645000   C:\Windows\System32\RPCRT4.dll
ModLoad: 00007ff9`1e650000 00007ff9`1e6fd000   C:\Windows\System32\shcore.dll
ModLoad: 00007ff9`1ee80000 00007ff9`1ef1e000   C:\Windows\System32\msvcrt.dll
ModLoad: 00007ff9`0e0d0000 00007ff9`0e36a000   C:\Windows\WinSxS\amd64_microsoft.windows.common-con
(50b8.4608): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ff9`203a0950 cc              int     3
0:000> !peb
PEB at 00000027a1d1f000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            Yes
    ImageBaseAddress:         00007ff735590000
    NtGlobalFlag:             70
    NtGlobalFlag2:            0
    Ldr                       00007ff92043c4c0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000001fbe2552f20 . 000001fbe2553640
    Ldr.InLoadOrderModuleList:           000001fbe25530d0 . 000001fbe2559cb0
    Ldr.InMemoryOrderModuleList:         000001fbe25530e0 . 000001fbe2559cc0
                    Base TimeStamp                     Module
            7ff735590000 bdd4adcd Dec 03 13:32:29 2070 C:\Windows\System32\notepad.exe
            7ff9202d0000 b5ced1c6 Aug 28 17:10:14 2066 C:\Windows\SYSTEM32\ntdll.dll
            7ff91ed30000 e35abded Nov 14 22:34:53 2090 C:\Windows\System32\KERNEL32.DLL
            7ff91deb0000 e8e9ac9b Oct 29 07:16:27 2093 C:\Windows\System32\KERNELBASE.dll
            7ff91edf0000 3ee1d71f Jun 07 15:14:23 2003 C:\Windows\System32\GDI32.dll
            7ff91e1e0000 0dcd0213 May 03 23:26:59 1977 C:\Windows\System32\win32u.dll
            7ff91da90000 94124ede Sep 20 18:16:46 2048 C:\Windows\System32\gdi32full.dll
            7ff91d9c0000 39255ccf May 19 18:25:03 2000 C:\Windows\System32\msvcp_win.dll
            7ff91e210000 2bd748bf Apr 23 04:39:11 1993 C:\Windows\System32\ucrtbase.dll
            7ff920080000 90a2bc88 Nov 23 13:10:00 2046 C:\Windows\System32\USER32.dll
            7ff91f410000 f4ecbc84 Mar 19 18:04:20 2100 C:\Windows\System32\combase.dll
            7ff91e520000 a546ff0a Nov 13 18:10:50 2057 C:\Windows\System32\RPCRT4.dll
            7ff91e650000 29534f79 Dec 21 16:28:09 1991 C:\Windows\System32\shcore.dll
            7ff91ee80000 564f9f39 Nov 21 00:31:21 2015 C:\Windows\System32\msvcrt.dll
            7ff90e0d0000 db2b08ef Jul 09 08:23:59 2086 C:\Windows\WinSxS\amd64_microsoft.windows.co
    SubSystemData:     0000000000000000
    ProcessHeap:       000001fbe2550000
    ProcessParameters: 000001fbe2552630
    CurrentDirectory:  'C:\Program Files (x86)\Windows Kits\10\Debuggers\'
    WindowTitle:  'C:\Windows\System32\notepad.exe'
    ImageFile:    'C:\Windows\System32\notepad.exe'
```

For a more complete PEB structure, refer to Process Hacker's PEB structure.

Alternative Documentation

As previously mentioned, some modules will avoid using Microsoft's documentation and instead use other documentation sources.

- Process Hacker's Header Files
- undocumented.ntinternals.net - Some structures may be outdated
- Reac#'s Documentation
- Vergilius Project - Although mainly for Windows kernel structures, it remains a valuable resource.

Considerations

When choosing a structure definition, it's important to be mindful of the following points.

- Some structure definitions only work for a specific architecture, either x86 or x64. If that's the case, ensure the appropriate structure definition is chosen.

- In certain cases, it may be necessary to define multiple structures due to the concept of nested structures. For example, a structure such as PEB may contain a member that acts as a pointer to another structure. Therefore, it becomes important to include the definition of the latter structure to ensure its correctly interpreted by the program.
- When using a custom definition of a structure, it is not possible to include its original definition found in the Windows SDK simultaneously. For example, Microsoft's definition of the PEB structure is located in Winternl.h. If one intends to use a different definition from one of the above-mentioned documentation sources, then attempting to include `Winternl.h` in the program will result in redefinition errors thrown by Visual Studio's compiler. To avoid this, select only one definition of the structure.

Previous Modules Complete Next