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.

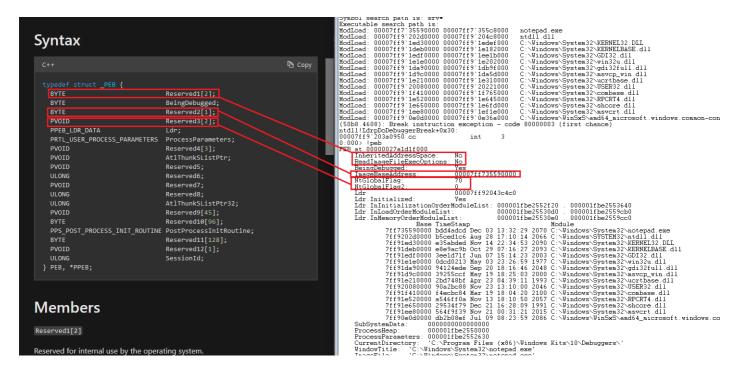
PEB Structure Example

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;
                                Reserved2[1];
BYTE
PVOID
                                Reserved3[2];
PPEB LDR DATA
PRTL USER PROCESS PARAMETERS ProcessParameters;
PVOID
                                Reserved4[3];
 PVOID
                                AtlThunkSListPtr;
                                Reserved5;
 PVOID
ULONG
                                Reserved6;
                                Reserved7;
 PVOID
ULONG
                                Reserved8;
ULONG
                                AtlThunkSListPtr32;
PVOID
                                Reserved9[45];
BYTE
                                Reserved10[96];
PPS POST PROCESS INIT ROUTINE PostProcessInitRoutine;
BYTE
                                Reserved11[128];
 PVOID
                                Reserved12[1];
                                SessionId;
ULONG
PEB, *PPEB;
```

Finding Reserved Members

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



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
- ReactOS'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.