

Forum:[Hack Forums](#)

Thread: [PEB walk example](#)

Biggy_Asian - October 9, 2024, 4:16 pm

PEB is a very useful thing to learn. You can learn it by visiting the below github. The github blog goes in depth on each part of PEB and explains its structure well.

<https://github.com/Faran-17/Windows-Internals/blob/main/Processes%20and%20Jobs/Processes/PEB%20-%20Part%201.md>

Code (NOT mine.):

Code // Read the blog -

<https://github.com/Faran-17/Windows-Internals/blob/main/Processes%20and%20Jobs/Processes/PEB%20-%20Part%202.md>

```
#include <Windows.h>
```

```
#include <winternl.h>
```

```
#include <stdio.h>
```

```
// Redefined PEB Structure
```

```
typedef struct _MY_PEB_LDR_DATA {
```

```
    ULONG Length;
```

```
    BOOL Initialized;
```

```
    PVOID SsHandle;
```

```
    LIST_ENTRY InLoadOrderModuleList;
```

```
    LIST_ENTRY InMemoryOrderModuleList;
```

```
    LIST_ENTRY InInitializationOrderModuleList;
```

```
} MY_PEB_LDR_DATA, * PMY_PEB_LDR_DATA;
```

```
typedef struct _MY_LDR_DATA_TABLE_ENTRY
```

```
{
```

```
    LIST_ENTRY InLoadOrderLinks;
```

```
    LIST_ENTRY InMemoryOrderLinks;
```

```
    LIST_ENTRY InInitializationOrderLinks;
```

```
    PVOID DllBase;
```

```
    PVOID EntryPoint;
```

```
    ULONG SizeOfImage;
```

```
    UNICODE_STRING FullDllName;
```

```
    UNICODE_STRING BaseDllName;
```

```
} MY_LDR_DATA_TABLE_ENTRY, * PMY_LDR_DATA_TABLE_ENTRY;
```

```
int main()
```

```
{
```

```
    // Fetching PEB Address
```

```
    PPEB PEB_Address = (PPEB) __readgsqword( 0x60 );
```

```
    // Fetching PEB_LDR_DATA Structure Address
```

```
    PMY_PEB_LDR_DATA P_Ldr = (PMY_PEB_LDR_DATA) PEB_Address->Ldr;
```

```

// Getting the 1st InLoadOrderModuleList Entry
PLIST_ENTRY P_NextModule = P_Ldr->InLoadOrderModuleList.Flink;

// parse it to LDR_DATA_TABLE_ENTRY structure
PMY_LDR_DATA_TABLE_ENTRY P_DataTableEntry = (PMY_LDR_DATA_TABLE_ENTRY)
P_NextModule;

while (P_DataTableEntry->DllBase != NULL)
{
    // Fetch module base address
    PVOID P_ModuleBase = P_DataTableEntry->DllBase;

    // Fetch module name
    UNICODE_STRING BaseDllName = P_DataTableEntry->BaseDllName;

    // Printing the output
    printf("DLL Name : %ls\n", BaseDllName.Buffer);
    printf("DLL Base Address: %p\n", P_ModuleBase);
    printf("\n");

    // Load the next entry
    P_DataTableEntry = (PMY_LDR_DATA_TABLE_ENTRY)
P_DataTableEntry->InLoadOrderLinks.Flink;
}
return 0;
}

```

Bastille - October 9, 2024, 10:10 pm

Really interesting, could be useful for me for malware analysis I guess, thanks for the share !

Biggy_Asian - October 10, 2024, 5:00 am

(Oct 9, 2024 10:10 PM)Bastille Wrote: [\[CITE\]](#) Really interesting, could be useful for me for malware analysis I guess, thanks for the share !

UAC Bypass + Shell by abusing another util but mainly because of peb ;) <3

n1k7 - November 23, 2024, 11:55 pm

Great for EDR evasions as well as Reconnaissance into ones' own process at runtime, so there is a free will for the malware developer to do whole lot with it.

- - Good day.