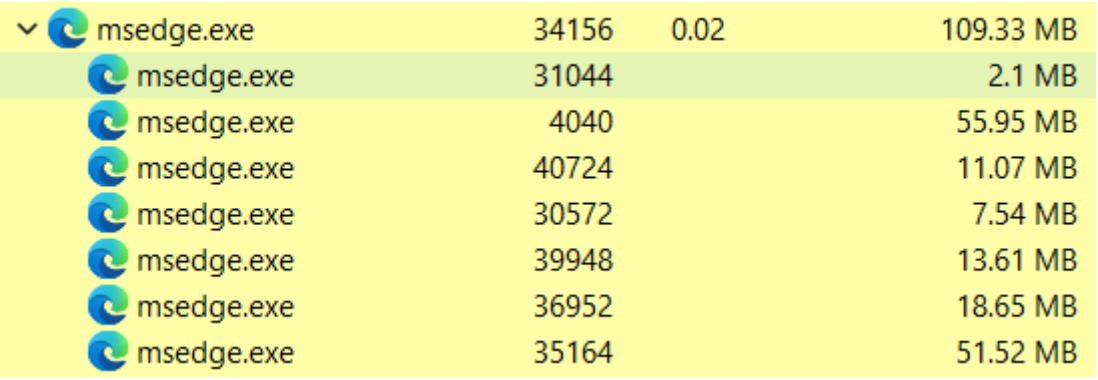
Windows Windows

Windows 1



Windows

2

DLL

PEB

(PEB) Windows DLL PEB ID PID) Windows

PEB C PEB

```
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;
```

PEB

BegingDebugged

Debug 1 (TRUE) 0 (FALSE)

LDR

Ldr PEB **PEB_LDR_DATA** **DLL** DLL Windows DLL LDR DLL

PEB_LDR_DATA

```
typedef struct _PEB_LDR_DATA {
  BYTE       Reserved1[8];
```

```
  PVOID      Reserved2[3];
  LIST_ENTRY InMemoryOrderModuleList;
} PEB_LDR_DATA, *PPEB_LDR_DATA;
```

LDR DLL **GetModuleHandle** kernel32.dll)

ProcessParameters

ProcessParameters PEB Windows PEB **RTL_USER_PROCESS_PARAMETERS**

```
typedef struct _RTL_USER_PROCESS_PARAMETERS {
  BYTE           Reserved1[16];
  PVOID          Reserved2[10];
  UNICODE_STRING ImagePathName;
  UNICODE_STRING CommandLine;
} RTL_USER_PROCESS_PARAMETERS, *PRTL_USER_PROCESS_PARAMETERS;
```

ProcessParameter

PostProcessInitRoutine

PEB PostProcessInitRoutine) TLS (

SessionId

PEB SessionID

TEB

TEB ( ) Windows Windows

C TEB

```
typedef struct _TEB {
  PVOID Reserved1[12];
  PPEB  ProcessEnvironmentBlock;
  PVOID Reserved2[399];
  BYTE  Reserved3[1952];
  PVOID TlsSlots[64];
  BYTE  Reserved4[8];
  PVOID Reserved5[26];
  PVOID ReservedForOle;
  PVOID Reserved6[4];
  PVOID TlsExpansionSlots;
} TEB, *PTEB;
```

TEB

ProcessEnvironmentBlock

PEB PEB

TlsSlots

(TLS) TlsSlots 64

TlsExpansionSlots

64 TLS TlsExpansionSlots

Windows PID ID

OpenProcess OpenThread

```
HANDLE OpenProcess(
  [in] DWORD dwDesiredAccess,
  [in] BOOL  bInheritHandle,
  [in] DWORD dwProcessId
);
```

```
HANDLE OpenThread(
  [in] DWORD dwDesiredAccess,
  [in] BOOL  bInheritHandle,
  [in] DWORD dwThreadId
);
```

Revision #5
Created 21 June 2023 01:59:17 by
Updated 28 January 2024 05:09:08 by