









Windows

Windows

Windows 1

▼ 	msedge.exe	34156	0.02	109.33 MB
	msedge.exe	31044		2.1 MB
	msedge.exe	4040		55.95 MB
	msedge.exe	40724		11.07 MB
	msedge.exe	30572		7.54 MB
	msedge.exe	39948		13.61 MB
	msedge.exe	36952		18.65 MB
	msedge.exe	35164		51.52 MB

Windows

2

DLL

PEB

(PEB) WindowDLL PEB IDPID) 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_LDR_DATA 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

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;
```

PEB PEB

(TLS) TlsSlots	64
----------------	----

64 TLS TlsExpansionSlots

```
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