Windows Windows

Windows 1

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

Windows

2

DLL

PEB

(PEB) Window PEB IPPID) Windows

```
typedef struct _PEB {
                                 Reserved1[2];
 BYTE
 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

Beging Debugged

Debug 1 (TRUE) 0 (FALSE)

LDR

Ldr PEBEB_LDR_DATA DLL DLDMindows DLL LDR DLL

PEB_LDR_DATA

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

```
PV0ID Reserved2[3];
LIST_ENTRY InMemoryOrderModuleList;
} PEB_LDR_DATA, *PPEB_LDR_DATA;
```

LDR DLL **GettModuleHain(le**kernel32.dll)

ProcessParameters

ProcessParameters PEB Windows PEB RTProdess_PARAMETERS

ProcessParameter

PostProcessInitRoutine

PEB PostProcessInitRoutine) TLS (

SessionId

PEB SessionID

TEB

TEB () Windows/indows

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

TIsSlots

(TLS) TIsSlots 64

TIsExpansionSlots

64 TLS TIsExpansionSlots

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