**如何获得其他进程命令行信息？**

**PEB : Process Environment Block;**

ntdll!\_PEB  
  

typedef struct \_RTL\_USER\_PROCESS\_PARAMETERS

{

ULONG MaximumLength;

ULONG Length;

ULONG Flags;

ULONG DebugFlags;

PVOID ConsoleHandle;

ULONG ConsoleFlags;

PVOID StandardInput;

PVOID StandardOutput;

PVOID StandardError;

[CURDIR](http://www.nirsoft.net/kernel_struct/vista/CURDIR.html) CurrentDirectory;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) DllPath;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) ImagePathName;

[**UNICODE\_STRING**](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) **CommandLine;**

PVOID Environment;

ULONG StartingX;

ULONG StartingY;

ULONG CountX;

ULONG CountY;

ULONG CountCharsX;

ULONG CountCharsY;

ULONG FillAttribute;

ULONG WindowFlags;

ULONG ShowWindowFlags;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) WindowTitle;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) DesktopInfo;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) ShellInfo;

[UNICODE\_STRING](http://www.nirsoft.net/kernel_struct/vista/UNICODE_STRING.html) RuntimeData;

[RTL\_DRIVE\_LETTER\_CURDIR](http://www.nirsoft.net/kernel_struct/vista/RTL_DRIVE_LETTER_CURDIR.html) CurrentDirectores[32];

ULONG EnvironmentSize;

} RTL\_USER\_PROCESS\_PARAMETERS, \*PRTL\_USER\_PROCESS\_PARAMETERS;

**如何获得其他进程的PEB结构体信息。**

**NTSTATUS WINAPI NtQueryInformationProcess(**

**\_\_in HANDLE ProcessHandle,//进程句柄**

**\_\_in PROCESSINFOCLASS ProcessInformationClass,//** ProcessBasicInformation

**\_\_out PVOID ProcessInformation,//** PROCESS\_BASIC\_INFORMATION

**\_\_in ULONG ProcessInformationLength,//前边结构体的大小**

**\_\_out\_opt PULONG ReturnLength//返回值的大小。**

**);**