|  |
| --- |
| HANDLE WINAPI CreateRemoteThread(  \_\_in HANDLE hProcess,  \_\_in LPSECURITY\_ATTRIBUTES lpThreadAttributes,  \_\_in SIZE\_T dwStackSize,  \_\_in LPTHREAD\_START\_ROUTINE lpStartAddress,  \_\_in LPVOID lpParameter,  \_\_in DWORD dwCreationFlags,  \_\_out LPDWORD lpThreadId  ); |

### [折叠](http://baike.so.com/doc/6950512-7172913.html)hProcess[in]

线程所属进程的进程句柄.

该句柄必须具有 PROCESS\_CREATE\_THREAD, PROCESS\_QUERY\_INFORMATION,

PROCESS\_VM\_OPERATION,

PROCESS\_VM\_WRITE,

PROCESS\_VM\_READ 访问权限.

### [折叠](http://baike.so.com/doc/6950512-7172913.html)lpThreadAttributes[in]

一个指向 [SECURITY\_ATTRIBUTES](http://baike.so.com/doc/1090506.html" \t "http://baike.so.com/doc/_blank) 结构的指针, 该结指定了线程的安全属性.

### [折叠](http://baike.so.com/doc/6950512-7172913.html)dwStackSize[in]

线程初始大小,以字节为单位,如果该值设为0,那么使用系统默认大小.

### [折叠](http://baike.so.com/doc/6950512-7172913.html)lpStartAddress[in]

在远程进程的地址空间中,该线程的线程函数的起始地址.

### [折叠](http://baike.so.com/doc/6950512-7172913.html)lpParameter[in]

指向传给线程函数的参数，指针是远程进程的地址

### [折叠](http://baike.so.com/doc/6950512-7172913.html)dwCreationFlags[in]

线程的创建标志.

|  |  |
| --- | --- |
| 值 | 含义 |
| 0 | 线程创建后﻿立即运行 |
| CREATE\_SUSPENDED  0x00000004 | 线程创建后先将线程挂起,直到 [ResumeThread](http://baike.so.com/doc/6952955.html" \t "http://baike.so.com/doc/_blank) 被调用. |
| STACK\_SIZE\_PARAM\_IS\_A\_RESERVATION  0x00010000 | *dwStackSize* 参数指定为线程栈预订大小,如果﻿STACK\_SIZE\_PARAM\_IS\_A\_RESERVATION没有被指定,﻿*dwStackSize* 参数指定为线程栈分配大小. |

### [折叠](http://baike.so.com/doc/6950512-7172913.html)lpThreadId[out]

指向所创建线程句柄的指针,如果创建失败,该参数为NULL.

返回值

如果调用成功,返回新线程句柄.

如果失败,返回NULL.

例

HANDLE hRemoteThread;

if ((hRemoteThread = CreateRemoteThread(hRemoteProcess, NULL, 0,

pLoadLibraryAddr, pszLibFileRemote, 0, NULL)) == NULL)

{

MessageBox(NULL, L"创建远程线程失败", L"Error", MB\_OK);

return FALSE;

}