2021/06/03_Windows64位内核_第4课_强制删除文件

笔记本： Windows64位内核
创建时间： 2021/6/5 星期六 0:17
作者： ileemi

操作其他进程的句柄

> 进程中的句柄存储在进程的句柄表（EPROCESS + 0x200处）中

强制删除文件

系统判定文件是否被占用的条件：被打开文件相关属性，是否共享等。

从操作系统的角度，当使用CreateFile创建一个文件，会创建一个文件对象，Ring3层操作该文件需要使用该文件的文件句柄。操作文件句柄就相当于操作文件对象，文件句柄可以有多个，而文件对象只有一个。每创建、关闭文件句柄时，文件对象对应的文件句柄的引用计数都会加加、减减。当对应的引用计数为0时，文件对象释放。

当创建的文件模式为不共享时，且创建的文件句柄不进行关闭，文件句柄存在进程问题（每个进程都有对应的句柄表，记录进程所产生的句柄表），产生的文件就不能被其它进程进行操作。

> 进程中的句柄存储在进程的句柄表（EPROCESS + 0x200位置）中
>
> ```
> +0x200 ObjectTable       : Ptr64 _HANDLE_TABLE
> ```

每个进程的使用CloseHandle时只能关闭自己句柄表中的进程句柄。

KeStackAttachProcess：切换进程
ZwClose
KeUnstackDetachProcess

文件打开次数以及场景不确定，CreateFile（Ring3）、ZwCreateFile（Ring0）都会产生对应的句柄，但是Ring0层打开文件产生的句柄Ring3层无法关闭（没有权限）。

InitializeObjectAttributes
ObQueryNameString：在内核中使用参数4（返回的字节长度）必须使用。
ZwCreateFile --> NtCreateFile --> IopCreateFile

ZwDuplicateObject（ntdll.dll）：通过进程句柄拷贝进程对象到当前进程中