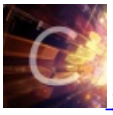
转自“看雪论坛”--NtQuerySystemInformation

转载

lyclowlevel 于 2010-09-27 20:10:00 发布 2273 收藏
分类专栏： win32非界面开发 文章标签： system table


win32非界面开发 专栏收录该内容
22 篇文章 0 订阅
订阅专栏

ProcessExplorer原理分析之句柄处理 by sucsor/RCT
1,如何获得各进程的句柄
使用NtQuerySystemInformation函数的SystemHandleInformation=16号功能.
其相关结构定义如下:

```
typedef struct _SYSTEM_HANDLE_TABLE_ENTRY_INFO{
    USHORT UniqueProcessId;
    USHORT CreatorBackTraceIndex;
    UCHAR ObjectTypeIndex;
    UCHAR HandleAttributes;
    USHORT HandleValue;
    PVOID Object;
    ULONG GrantedAccess;
} SYSTEM_HANDLE_TABLE_ENTRY_INFO, *PSYSTEM_HANDLE_TABLE_ENTRY_INFO;

typedef struct _SYSTEM_HANDLE_INFORMATION{
    ULONG NumberOfHandles;
    SYSTEM_HANDLE_TABLE_ENTRY_INFO Handles[1];
} SYSTEM_HANDLE_INFORMATION, *PSYSTEM_HANDLE_INFORMATION;
```

该功能号获取系统内所有进程的句柄放在Handles里,个数由NumberOfHandles标识,
每个句柄由UniqueProcessId来区分属于那个不同的进程.
2,如何得到句柄的信息
首先ProcessExploer 要打开该进程(OpenProcess),然后根据使用DuplicateHandle,将目标进程的句柄和要关闭的句柄(这不是唯一的办法,不过PE是这样做的)
做为参加传入,得到该句柄执行体对象的在本进程内的句柄,然后通过DeviceIoControl将该句柄传到ProcessExploer的驱动中,
通过使用PsLookupProcessByProcessId得到进程有内核对象,然后使用KeAttachProcess函数切换到进程的上下文中,
再通过使用ObReferenceObjectByHandle得到对象,再通过ObQueryNameString得到对象的名称信息,根据对象的结构,还可以得到其他的相关信息,
比如打开的句柄数和引用计数及一些访问控制信息.

3,如何关闭某进程中的句柄
如同二中提到的通过一系统的函数可以切换到进程的上下文,在该进程上下文中,即可调用ZwClose来关闭本进程的句柄,需要的参数只是句柄,
这个句柄在第一步中已经得到.

4,ObQueryNameString并不是对于所有的对象都能得到名称,对于文件对象的名称可能需要进一步使用文件系统提供的相关函数来获取名称信息.

5,有误之外请各位指正,谢谢.
ProcessExplorer逆向中,不过总体来说只要代码思路有了,相信大家一看便知.
如果可能的话,会将代码按部分贴出来.只是可能....:)