模拟锁定文件

转载

weixin_33964094 于 2017-08-09 08:30:00 发布 22 收藏
原文链接：http://www.cnblogs.com/yutingliuyl/p/7323302.html

模拟锁定文件的Rring 3下的程序代码,代码来自于看雪中的HWL发表的一份代码中,我仅仅是看了下代码:

```
#include <stdio.h>
```

```
#include <Windows.h>
```

```
void GetAllProcessA(int pids[],int *procount)
```

```
{
```

```
int i=0,c=0;



HANDLE hProcess=0;



for(i=8;i<19996;i+=4)



{



hProcess=OpenProcess(0x10,0,i);



if (hProcess!=0)



{



pids[c]=i;
```

```
    CloseHandle(hProcess);



    c++;



    }



    }



    *procount=c;



}









    int main()



    {
```

```
#define SE_DEBUG_PRIVILEGE 0x14 //DEBUG 权限
```

```
//源码中没有__stdcall,所以一直报checkesp.c line 14的错误
```

```
typedef long (__stdcall *RTLADJUSTPRIVILEGE)(int, bool, bool, int*);
```

```
typedef long (__stdcall *NTDUPLICATEOBJECT)(HANDLE,HANDLE,HANDLE,PHANDLE,ACCESS_MASK,BOOL
```

```
int nEn = 0;
```

```
int pids[4*260];
```

```
int procsnum=0;



char pFile[260];



//得到函数的地址



RTLADJUSTPRIVILEGE getdbg=(RTLADJUSTPRIVILEGE)GetProcAddress(GetModuleHandleW(L"ntdll.d



NTDUPLICATEOBJECT NtDuplicateObject=(NTDUPLICATEOBJECT)GetProcAddress(GetModuleHandleW(



//提升进程权限



getdbg(SE_DEBUG_PRIVILEGE , TRUE, FALSE,&nEn);//SE_DEBUG_PRIVILEGE =20



//getdbg(20,1,0,&bRet);



memset(pids,0,4*260);
```

```
memset(pFile,0,260);



printf("Input the file name you want to protect: ");



scanf("%s",pFile);
```

```
  //新建文件
```

```
  //#define GENERIC_READ (0x80000000L)
```

```
  //HANDLE hsFile = CreateFileA(pFile, 0x80000000, 0, 0, 3, 0, 0);
```

```
HANDLE hsFile = CreateFileA(pFile, GENERIC_READ, 0, NULL, OPEN_EXISTING, FILE_ATTRI
```

```
//SetHandleInformation(hsFile,0,2);
```

```
SetHandleInformation(hsFile, HANDLE_FLAG_PROTECT_FROM_CLOSE, HANDLE_FLAG_PROTECT_FR
```

```
//得到当前存活的进程id列表和进程数目,
```

```
GetAllProcessA(pids,&procsnum);
```

```
//遍历当前存活的进程
```

```
for(int i=0;i<procsnum;i++)
```

```
{
```

```
HANDLE htFile=0;



//HANDLE hProcess = OpenProcess(0x1F0FFF, 0, pids[i]);



//#define STANDARD_RIGHTS_REQUIRED (0x000F0000L)



//#define PROCESS_ALL_ACCESS (STANDARD_RIGHTS_REQUIRED | SYNCHRONIZE | \



0xFFFF)



//#define SYNCHRONIZE (0x00100000L)



//不知道原作者为什么要用这些魔幻数,而不用PROCESS_ALL_ACCESS



HANDLE hProcess = OpenProcess(PROCESS_ALL_ACCESS, 0, pids[i]);
```

```
if (hProcess!=0)

{

//NtDuplicateObject((HANDLE)-1, hsFile, hProcess, &htFile, 0, 0, 4);

NtDuplicateObject((HANDLE)-1, hsFile, hProcess, &htFile, 0, 0, 4); //DUPLICATE_SAME

CloseHandle(hProcess);

}

}

getchar();

printf("OK!\n");
```

```
    getchar();



    return 0;



}
```

代码分析：
遍历当前进程,将文件句柄拷贝到每一个进程中,从而实际锁定文件
转载于:https://www.cnblogs.com/yutingliuyl/p/7323302.html