# 与断链隐藏进程功能类似，关于断链进程隐藏可参考 《驱动开发：DKOM 实现进程隐藏》 这一篇文章，断链隐藏驱动自身则用于隐藏自身SYS驱动文件，当驱动加载后那么使用ARK工具扫描将看不到自身驱动模 块，此方法可能会触发PG会蓝屏，在某些驱动辅助中也会使用这种方法隐藏自己。

驱动实现代码如下所示:

#include <ntifs.h>



HANDLE hThread;

VOID ThreadRun(PVOID StartContext)

{

LARGE\_INTEGER times; PDRIVER\_OBJECT pDriverObject;

// 等待3秒 单位是纳秒

times.QuadPart = -30 1000 1000;

KeDelayExecutionThread(KernelMode, FALSE, &times); pDriverObject = (PDRIVER\_OBJECT)StartContext;

// 修改模块信息

pDriverObject->DriverSize = 0; pDriverObject->DriverSection = NULL; pDriverObject->DriverExtension = NULL; pDriverObject->DriverStart = NULL; pDriverObject->DriverInit = NULL; pDriverObject->FastIoDispatch = NULL; pDriverObject->DriverStartIo = NULL;

ZwClose(hThread);

}

VOID UnDriver(PDRIVER\_OBJECT driver)

{

DbgPrint(("Uninstall Driver Is OK \n"));

}

NTSTATUS DriverEntry(IN PDRIVER\_OBJECT Driver, PUNICODE\_STRING RegistryPath)

{

DbgPrint(("hello lyshark \n"));

PLIST\_ENTRY pModuleList; pModuleList = Driver->DriverSection;

// 前一个模块的Flink=本模块的Flink

pModuleList->Blink->Flink = pModuleList->Flink;

// 前一个模块的Blink=本模块的Blink

pModuleList->Flink->Blink = pModuleList->Blink; PsCreateSystemThread(&hThread, GENERIC\_ALL, NULL, NULL, NULL, ThreadRun,

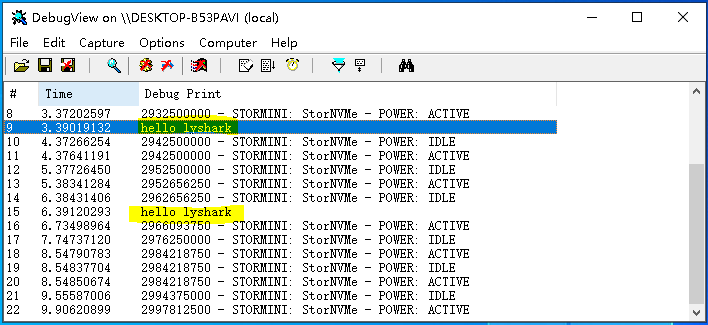
Driver);

Driver->DriverUnload = UnDriver;

return STATUS\_SUCCESS;

}

# 输出效果如下，驱动每隔3秒执行一次模块修改：



作者： 王瑞 (LyShark)

作者邮箱： m [e@lyshark.com](mailto:e@lyshark.com)

版权声明：本博客文章与代码均为学习时整理的笔记，文章 [均为原创] 作品，转载文章请遵守

《中华人民共和国著作权法》相关法律规定或遵守《署名CC BY-ND 4.0国际》规范，合理合规携带原创出处转载，如果不携带文章出处，并恶意转载多篇原创文章被本人发现，本人保留起诉权！