

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"));

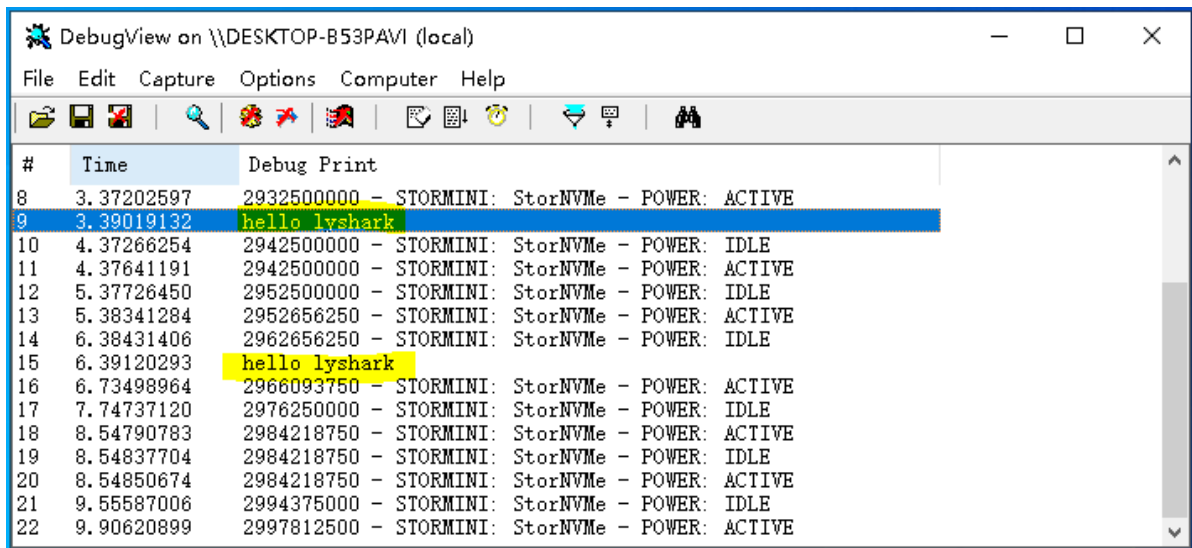
    PLIST_ENTRY pModuleList;
    pModuleList = Driver->DriverSection;

    // 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：



#	Time	Debug Print
8	3.37202597	2932500000 - STORMINI: StorNVMe - POWER: ACTIVE
9	3.39019132	hello lyshark
10	4.37266254	2942500000 - STORMINI: StorNVMe - POWER: IDLE
11	4.37641191	2942500000 - STORMINI: StorNVMe - POWER: ACTIVE
12	5.37726450	2952500000 - STORMINI: StorNVMe - POWER: IDLE
13	5.38341284	2952656250 - STORMINI: StorNVMe - POWER: ACTIVE
14	6.38431406	2962656250 - STORMINI: StorNVMe - POWER: IDLE
15	6.39120293	hello lyshark
16	6.73498964	2966093750 - STORMINI: StorNVMe - POWER: ACTIVE
17	7.74737120	2976250000 - STORMINI: StorNVMe - POWER: IDLE
18	8.54790783	2984218750 - STORMINI: StorNVMe - POWER: ACTIVE
19	8.54837704	2984218750 - STORMINI: StorNVMe - POWER: IDLE
20	8.54850674	2984218750 - STORMINI: StorNVMe - POWER: ACTIVE
21	9.55587006	2994375000 - STORMINI: StorNVMe - POWER: IDLE
22	9.90620899	2997812500 - STORMINI: StorNVMe - POWER: ACTIVE

作者：王瑞 (LyShark)

作者邮箱：me@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！