微软在x64系统中推出了DSE保护机制，DSE全称(Driver Signature Enforcement)，该保护机制的核心就是任何驱动程序或者是第三方驱动如果想要在正常模式下被加载则必须要经过微软的认证，当驱动程序被加载到内存时会验证签名的正确性，如果签名不正常则系统会拒绝运行驱动，这种机制也被称为驱动强制签名，该机制的作用是保护系统免受恶意软件的破坏，是提高系统安全性的一种手段。

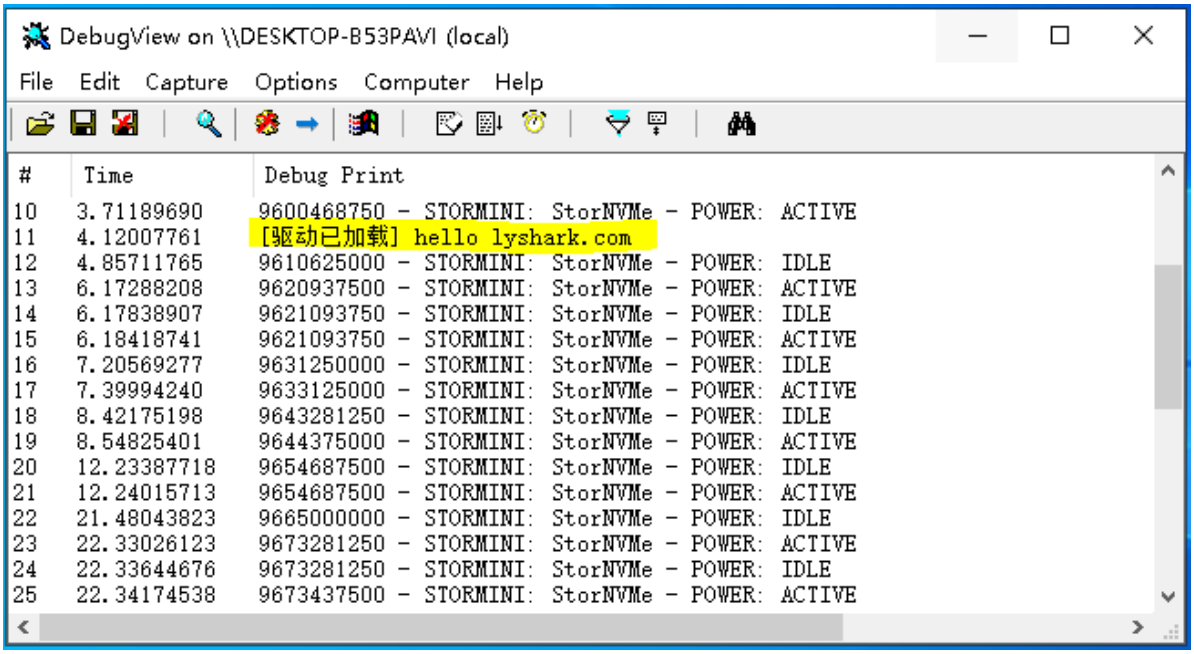
该验证机制即便是在调试模式也需要强制签名，对于一名驱动开发者来说是很麻烦的一件事情，而签名的验证则是在加载时验证驱动入口_KLDR_DATA_TABLE_ENTRY里面的Flags标志，如果此标志被pLdrData->Flags | 0x20置位，则在调试模式下就不会在验证签名了，省去了重复签名的麻烦。

代码的实现非常容易，如下所示:

```
// 署名权
// right to sign one's name on a piece of work
// PowerBy: LyShark
// Email: me@lyshark.com

#include <ntifs.h>

// 绕过签名检查
BOOLEAN BypassCheckSign(PDRIVER_OBJECT pDriverObject)
{
#ifdef _WIN64
    typedef struct _KLDR_DATA_TABLE_ENTRY
    {
        LIST_ENTRY listEntry;
        ULONG64 __Undefined1;
        ULONG64 __Undefined2;
        ULONG64 __Undefined3;
        ULONG64 NonPagedDebugInfo;
        ULONG64 DllBase;
        ULONG64 EntryPoint;
        ULONG SizeOfImage;
        UNICODE_STRING path;
        UNICODE_STRING name;
        ULONG   Flags;
        USHORT  LoadCount;
        USHORT  __Undefined5;
        ULONG64 __Undefined6;
        ULONG   CheckSum;
        ULONG   __padding1;
        ULONG   TimeDateStamp;
        ULONG   __padding2;
    } KLDR_DATA_TABLE_ENTRY, *PKLDR_DATA_TABLE_ENTRY;
#else
    typedef struct _KLDR_DATA_TABLE_ENTRY
    {
        LIST_ENTRY listEntry;
        ULONG unknown1;
        ULONG unknown2;
        ULONG unknown3;
        ULONG unknown4;
        ULONG unknown5;
        ULONG unknown6;
```

```
        ULONG unknown7;
        UNICODE_STRING path;
        UNICODE_STRING name;
        ULONG   Flags;
    } KLDR_DATA_TABLE_ENTRY, *PKLDR_DATA_TABLE_ENTRY;
#endif

    PKLDR_DATA_TABLE_ENTRY pLdrData = (PKLDR_DATA_TABLE_ENTRY)pDriverObject->DriverSection;
    pLdrData->Flags = pLdrData->Flags | 0x20;

    return TRUE;
}

VOID UnDriver(PDRIVER_OBJECT driver)
{

}

NTSTATUS DriverEntry(IN PDRIVER_OBJECT Driver, PUNICODE_STRING RegistryPath)
{
    NTSTATUS status;

    // 绕过签名检查
    // LINKER_FLAGS=/INTEGRITYCHECK
    BypassCheckSign(Driver);

    DbgPrint("[驱动已加载] hello lyshark.com \n");

    Driver->DriverUnload = UnDriver;
    return STATUS_SUCCESS;
}
```

将程序拖入到虚拟机，直接运行即可加载，无需再继续签名：



当然这种方式只能在测试模式下使用，在正常模式也是无效的，只是为了方便测试驱动。