30

[旧帖] [原创]关于拦截“通过WMI读取硬件序列号”的一些心得

0.00元 优

夜鹰fly

极客

2010-12-27 14:17

大家都知道，WMI（Windows Management Instrumentation,Windows 管理规范）是一项核心的 Windows 管理技术；用户可以使用 WMI 管理本地和远程计算机，在这里只讨论它的硬件信息管理功能。

所有硬件设备的信息要能被WMI收集，其编写的驱动程序必须符合WMI规范，即WMI相当于这些硬件信息的管理员。通过IRPTrace这个工具可以很方便看到，当ring3有读取硬件序列号的动作，传到ring0层是这样：WMIDataDevice内核设备会收到一个名叫IRP_MJ_SYSTEM_CONTROL的通知，当然该通知还会附加着一个类似于IRP_MN_QUERY_ALL_DATA的通知。只要有一定驱动编程基础的人都知道，该通知会层层传递下去，得到结果后返回上来。

所以，我的拦截思路很简单，编写一个过滤驱动设备，附载在WMIDataDevice内核设备上，我的过滤驱动只对IRP_MJ_SYSTEM_CONTROL进行过滤：

```
NTSTATUS DriverEntry(
    IN PDRIVER_OBJECT  DriverObject,
    IN PUNICODE_STRING RegistryPath
    )
{
.................
        for (i = 0; i < IRP_MJ_MAXIMUM_FUNCTION; i++) {

        DriverObject->MajorFunction[i] = LS2capDispatchGeneral;
    }

    //
    // Our read function is where we do our real work.
    //


    DriverObject->MajorFunction[IRP_MJ_SYSTEM_CONTROL] = LS2DispatchSystemControl;
    return LS2capInit( DriverObject );
}
```

然后再设置完成例程，目的是等该通知取到序列号后可以拦截并任意修改序列号。

主要就是编写NTSTATUS LS2DispatchSystemControl(

```
    IN PDEVICE_OBJECT DeviceObject,
    IN PIRP           Irp
    )
{
....
```

}例程。

代码如下：

```
NTSTATUS  LS2DispatchSystemControl(
    IN PDEVICE_OBJECT DeviceObject,
    IN PIRP           Irp
    )
{
        //PAGED_CODE();
```

```
    NTSTATUS status ;
PDEVICE_EXTENSION   devExt;
UCHAR minorFunc;
PIO_STACK_LOCATION       IrpSp;
    char teststr2[34]="IRP_MN_QUERY_ALL_DATA";
    char teststr3[34]="IRP_MN_QUERY_SINGLE_INSTANCE";
    char teststr0[34]="NOTHING";
IrpSp = IoGetCurrentIrpStackLocation( Irp );
    devExt = (PDEVICE_EXTENSION) DeviceObject->DeviceExtension;
    status = STATUS_SUCCESS ;


minorFunc = IrpSp->MinorFunction;
    switch(minorFunc)
    {
    case IRP_MN_QUERY_ALL_DATA:
          devExt->controlcode=2;
          currentIrpStack = IoGetCurrentIrpStackLocation(Irp);
    nextIrpStack = IoGetNextIrpStackLocation(Irp);
*nextIrpStack = *currentIrpStack;
IoSetCompletionRoutine( Irp, Ctrl2capWMIComplete,
                    DeviceObject, TRUE, TRUE, TRUE );

    WriteFileTest(teststr2,34);
       break;
case IRP_MN_QUERY_SINGLE_INSTANCE:
       devExt->controlcode=3;
       currentIrpStack = IoGetCurrentIrpStackLocation(Irp);
nextIrpStack = IoGetNextIrpStackLocation(Irp);
*nextIrpStack = *currentIrpStack;
IoSetCompletionRoutine( Irp, Ctrl2capWMIComplete,
                    DeviceObject, TRUE, TRUE, TRUE );

    WriteFileTest(teststr3,34);
       break;
case IRP_MN_REGINFO:
case IRP_MN_REGINFO_EX:
case IRP_MN_CHANGE_SINGLE_INSTANCE:
case IRP_MN_CHANGE_SINGLE_ITEM:
 case IRP_MN_EXECUTE_METHOD:
 case IRP_MN_DISABLE_EVENTS:
 case IRP_MN_ENABLE_COLLECTION:
 case IRP_MN_DISABLE_COLLECTION:
 case IRP_MN_ENABLE_EVENTS:
 default:
#if WIN2K
    IoSkipCurrentIrpStackLocation(Irp);
#else // WIN2K
//
// This is the equivalent of the IoSkipCurrentIrpStackLocation macro,
// which doesn't exist in the NT 4 DDK.
//
    Irp->CurrentLocation++;
    Irp->Tail.Overlay.CurrentStackLocation++;
#endif // WIN2K
          WriteFileTest(teststr0,34);
```

```
>TopOfStack, Irp);
                break;
        }
        // 完成IRP
        /*
        Irp->IoStatus.Status = status;
        Irp->IoStatus.Information = 0;                  // bytes xfered
        IoCompleteRequest( Irp, IO_NO_INCREMENT );          //结束IRP请求，即不再往下传递

    return status;
    */
        return IoCallDriver( devExt->TopOfStack, Irp );

}
```

为了方便检测是否过滤成功，可以创建一个文本文件，并往里写入标记。本人已实现对硬盘，主板，MAC地址等读取拦截。主要思路和代码就是这些，请各位多多指教。

最新回复 (9)

西风X 2010-12-27 19:41　2 楼　0

很强悍了，驱动级拦截，一劳永逸的做法，
我也想这样做，就是写驱容易蓝屏，这个头痛得很
LZ有没有好的方法，防止蓝屏的

夜鹰fly 2010-12-28 08:56　3 楼　0

调试驱动程序是不可避免蓝屏的，但是可以减少：1，在Ring0级下读写内存时应格外小心，可以在读写一段内存前对其进行读写检测；2，尽量不要在实体主机上进行调试，建议构建WinDbg+虚拟机平台，我习惯利用WinDbg+VMWare进行驱动调试。

glspj 2010-12-28 11:21　4 楼　0

看起来真的很麻烦啊~~~

偶是猪猪 2010-12-28 13:56　5 楼　0

支持一下！虽然看不懂！呵呵！

sulepluto 2011-8-10 15:01　6 楼　0

最近正在做过滤进程通过WMI获取系统信息的事情，
楼主的方法刚好能用上，非常感谢！

zengde 2011-8-10 15:07　7 楼　0

强悍

最新回复 (9)

jasonnbfan 8 2012-6-2 19:08 8 楼 0

感谢楼主共享。

大牛

寒欣 2012-6-2 22:06 9 楼 0

很不错的经验，谢谢！

极客

算法newren 2014-12-18 09:18 10 楼 0

挺好的，就是win7 之后64位的驱动要签名才能使用。
此路越来越窄了。

极客

游客

登录 | 注册 方可回帖

回帖 表情 高级回复

返回