镜像劫持

定义

所谓的镜像劫持，就是在注册表的

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options]处新建一个以杀毒软件主程序命名的项，例如 Rav.exe。然后再创建一个子键“Debugger="C:\WINDOWS\system32\drivers\”。以后只要用户双击 Rav.exe 就会运行 OSO 的病毒文件，类似文件关联的效果。

有关操作

autorun.inf 和 oobtwtr.exe 手动去除法:

1．首先下载 autoruns

2．然后打开运行　镜像劫持；

3．接下来单击开始|运行|输入 cmd，回车|x：回车（x 是你的盘符）

4．输入 attrib autorun.inf -s -h -r

attrib oobtwtr.exe -s -h -r (去隐藏属性)；

5．输入 del　autorun.inf

del　oobtwtr.exe（删除）

用镜像劫持防病毒

把 system.rar 解压后的文件在 d:\sysset\menu 目录下后上传参数就行了。

易游开机会自动导入这个注册表文件的.

可以在百度上搜一下就知道了.

什么是镜像劫持（IFEO）？

所谓的 IFEO 就是 Image File Execution Options

在是位于注册表的:

由于这个项主要是用来调试程序用的，对一般用户意义不大。默认是只有管理员和 local system 有权读写修改

先看看常规病毒等怎么修改注册表吧。。

那些病毒、蠕虫和，木马等仍然使用众所皆知并且过度使用的注册表键值，如下：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunHKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit_DLLs

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

等等。

随着网友的安全意识提高和众多安全软件的针对，都可以很容易的对上面的恶意启动项进行很好的处理

那就是 IFEO。

实验：开始-运行-regedit,展开到 IFEO：

然后选上 Image File Execution Options，新建个项，然后，把这个项（默认在最后面）然后改成 123.exe。

Click here to open new windowCTRL+Mouse wheel to zoom in/out

选上 123.exe 这个项，然后默认右边是空白的，我们点右键，新建个“字串符”，然后改名为“Debugger"。

这一步要做好，然后回车，就可以。。。再双击该键，修改数据数值（其实就是路径）。

把它改为 C:\windows\system32\CMD.exe

在此之前，记得先把“隐藏以知文件类型扩展名”的勾去掉！

然后找个扩展名为 EXE 的，（我这里拿 IcesWord.exe 做实验），改名为 123.exe。

然后运行之。一次简单的恶作剧就成了。

同理，病毒等也可以利用这样的方法，把杀软、安全工具等名字再进行重定向，指向病毒路径

SO..如果你把病毒清理掉后，重定向项没有清理的话，由于 IFEO 的作用，没被损坏的程序一样运行不了！