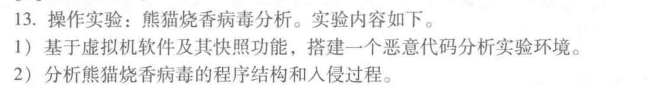
## 选取题目：

P239 12

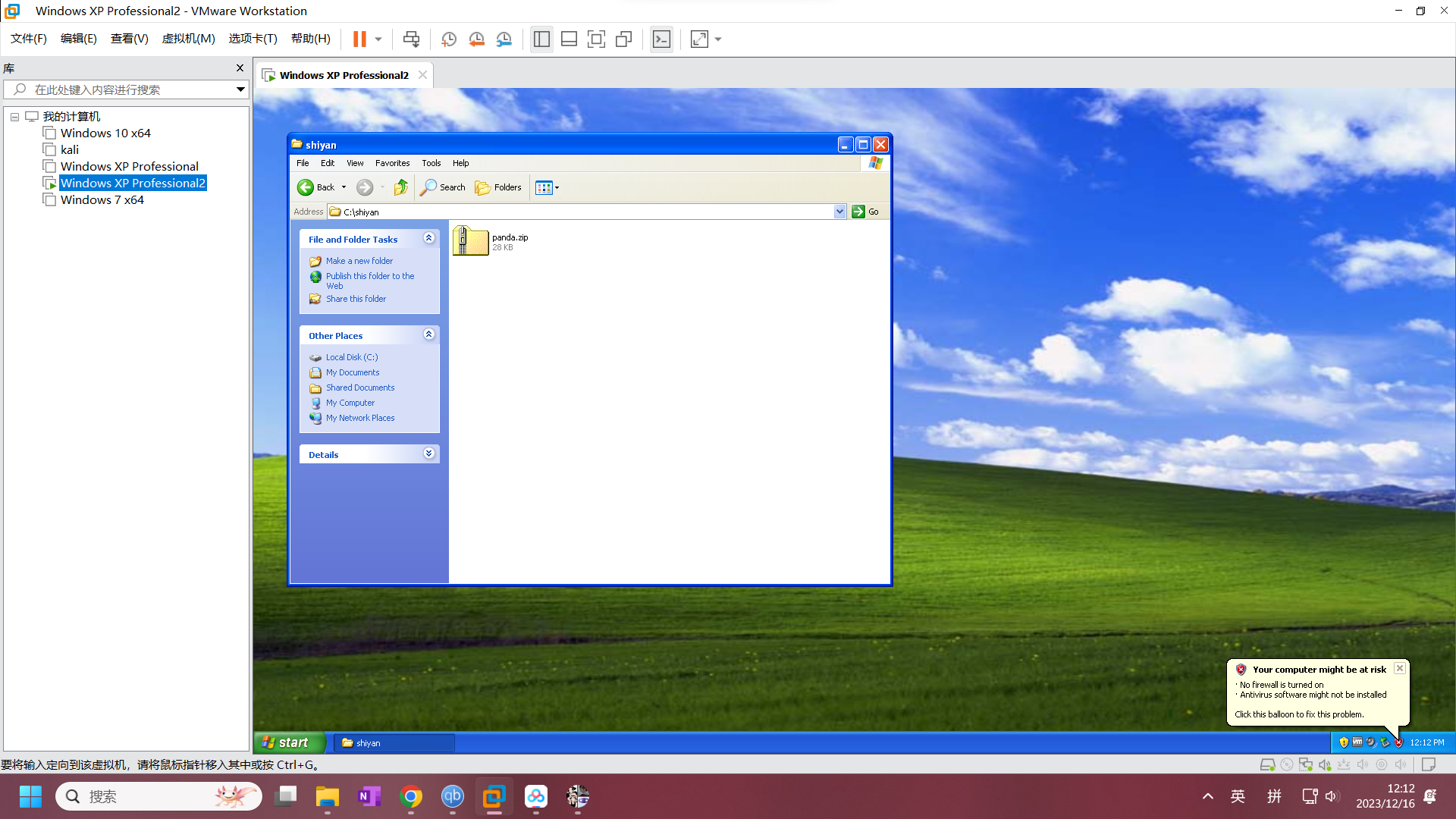


## 软件安装：

安装windows xp虚拟机

从网盘上下载熊猫烧香病毒文件放入xp虚拟机中





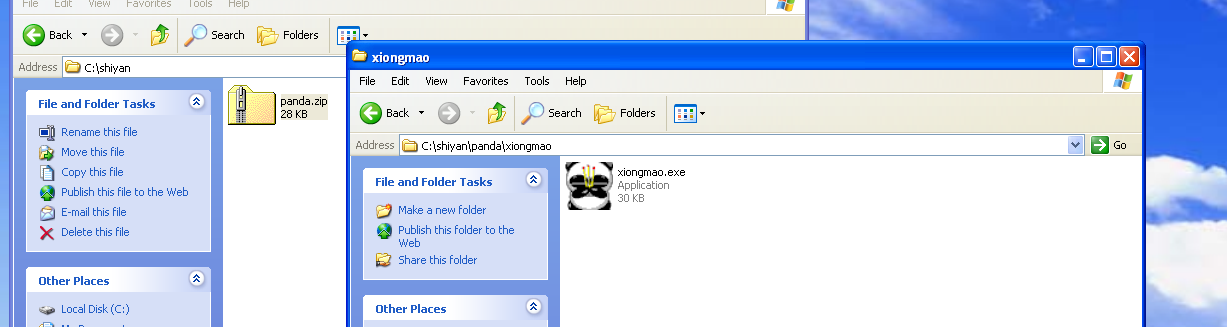
为当前虚拟机的状态拍摄快照



## 分析

### 执行病毒文件后先简单查看下虚拟机出现了哪些变化

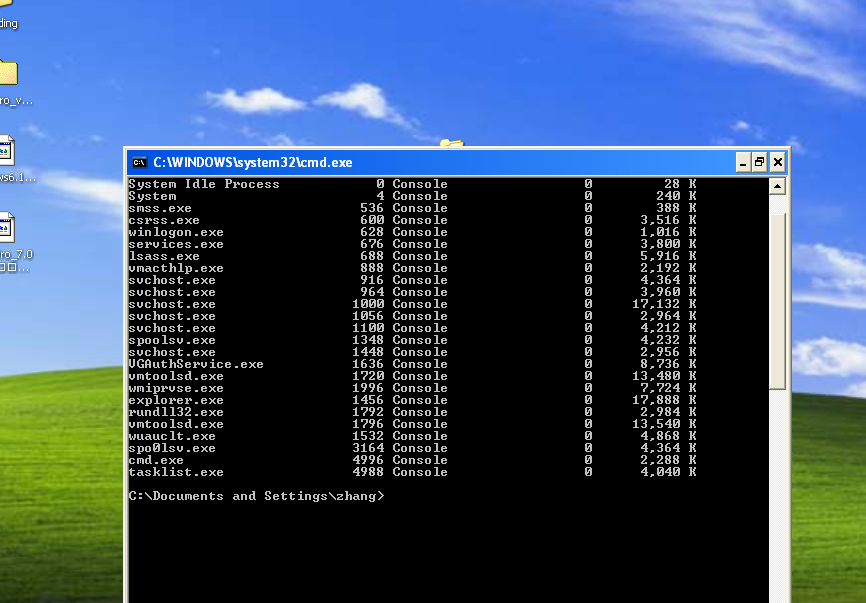
解压文件并把病毒文件扩展名改为exe



执行病毒文件

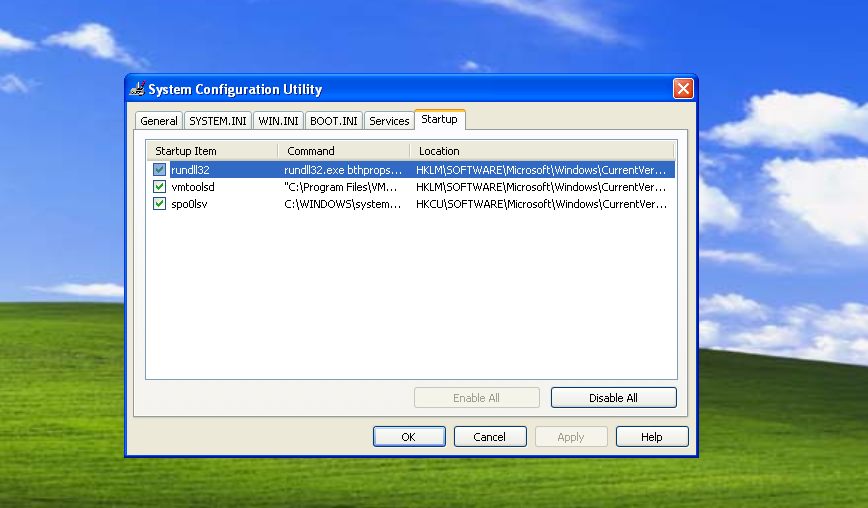
尝试打开资源管理器发现是打不开的，打开也立马闪退了

资源管理器用不了，用cmd查看当前的进程



可以明显看到多了spoolsv.exe这个程序，应该是病毒创造出来的进程

再查看启动项



可以看到多出来了一个spoolsv的启动项，而且是在system32下的，并且在注册表中是注册过的

不仅如此，查看启动项的界面还会闪退，应该也是病毒的影响

想看看注册表里面相应的是不是有这个变化，但是注册表打开就闪退，没办法看了。

还是在cmd下面看看system32\drivers下面有没有这个exe吧：

Cd到对应位置用dir查看



可以看到是有的

想在文件管理器里面查看，但是一直点c盘点不开，应该也是病毒搞得

在cmd里面看看c盘怎么了：



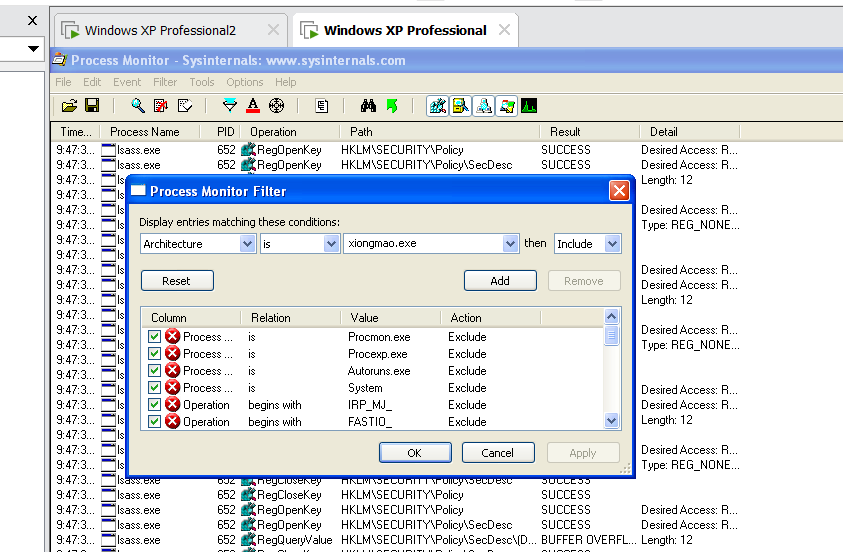
通过/ah找一下c盘下的隐藏文件，看到这个autorun应该是帮助病毒自启动的文件，setup应该是病毒执行文件

### 病毒入侵过程

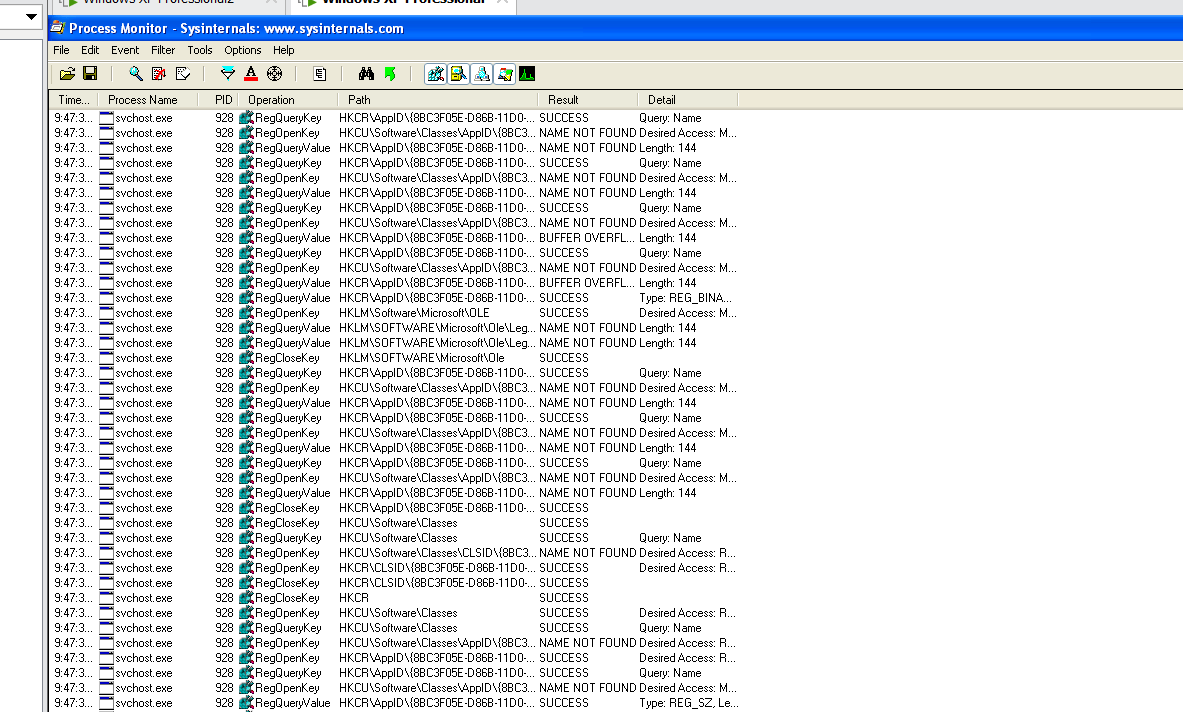
使用ProcessMonitor进行分析

先把虚拟机恢复到病毒运行前的状态

在工具中筛选，只选择病毒文件

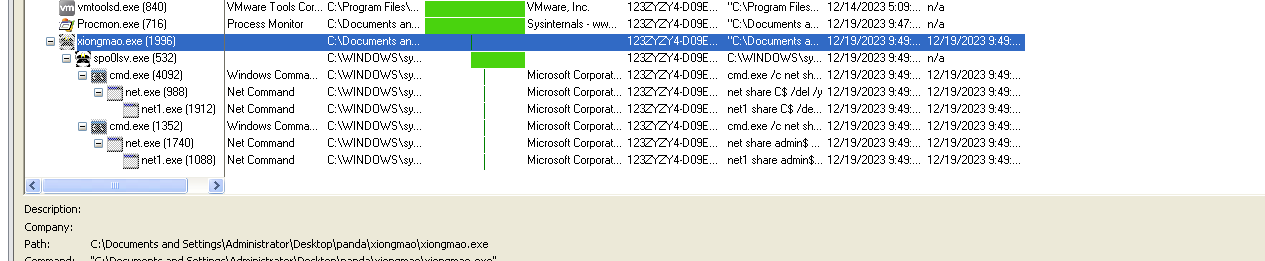


再次执行病毒，打开分析工具

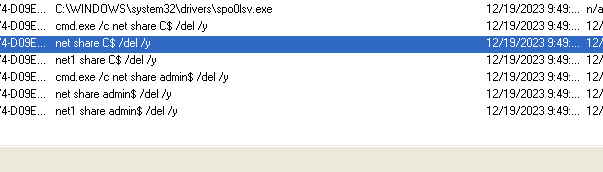


可以看到捕获到了相当多的信息

查看下进程树

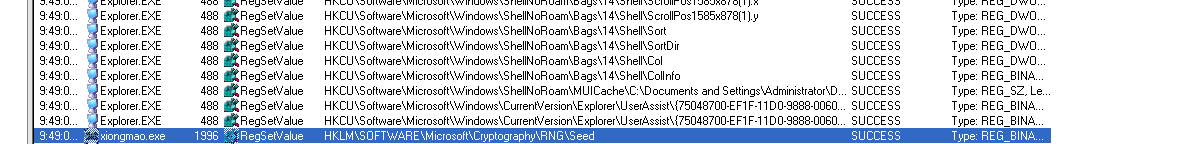
这里可以看到病毒程序涉及到了哪些内容

从进程树中看到xiongmao病毒下的spoolsv打开了两个cmd，看一下分别都是干嘛的：



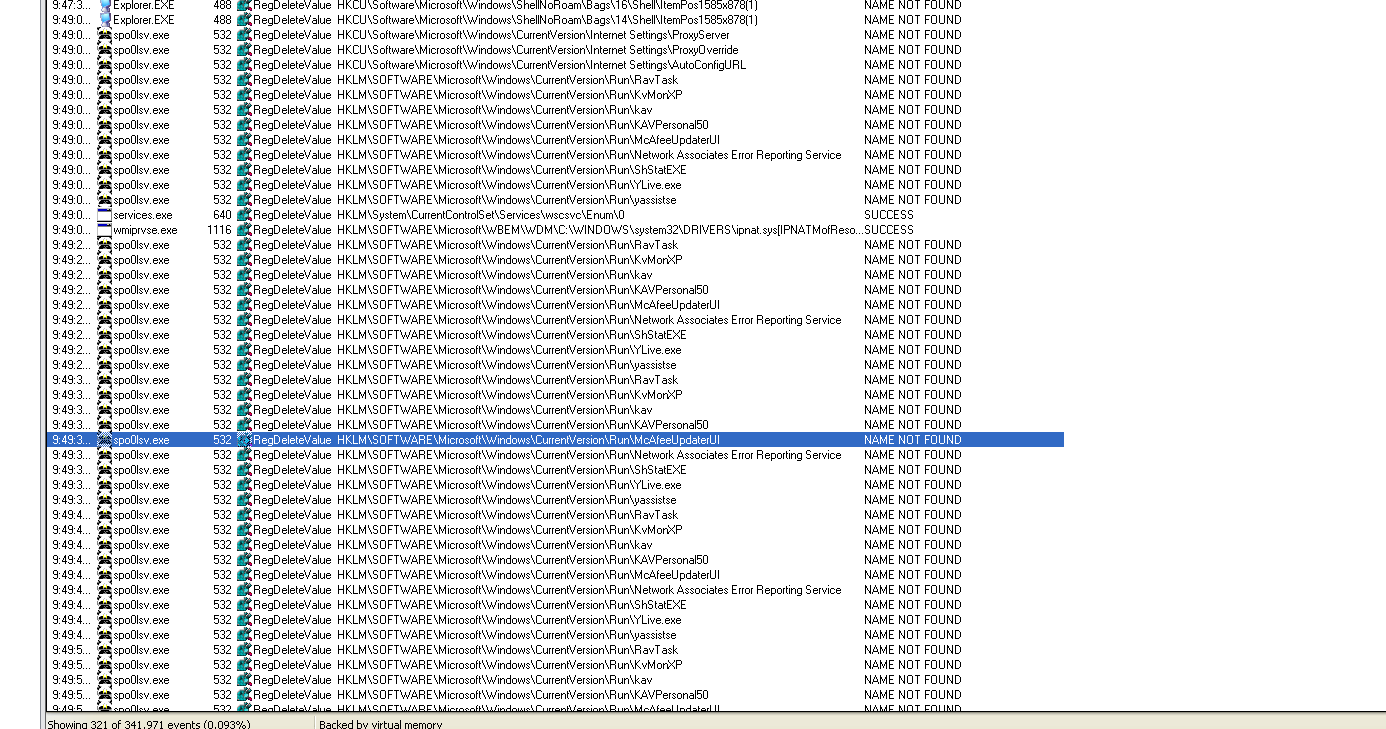
可以看到，两个command都是net share，删除了两个位置的共享资源

回到工具首页，通过筛选器查看病毒对注册表的修改



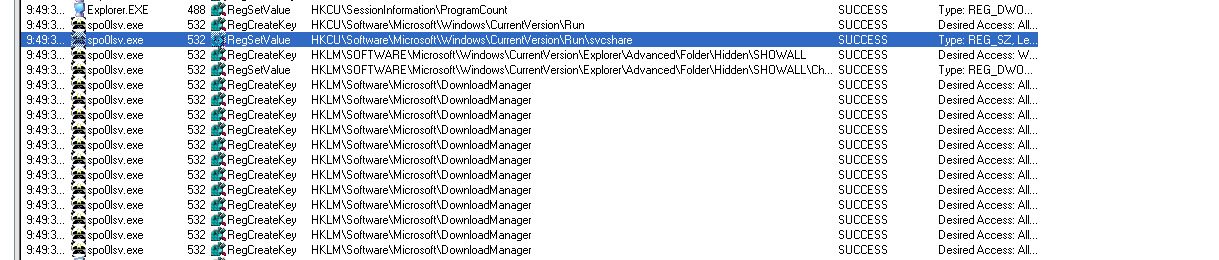
改变了seed即随机数种子

再看看对注册表的删除



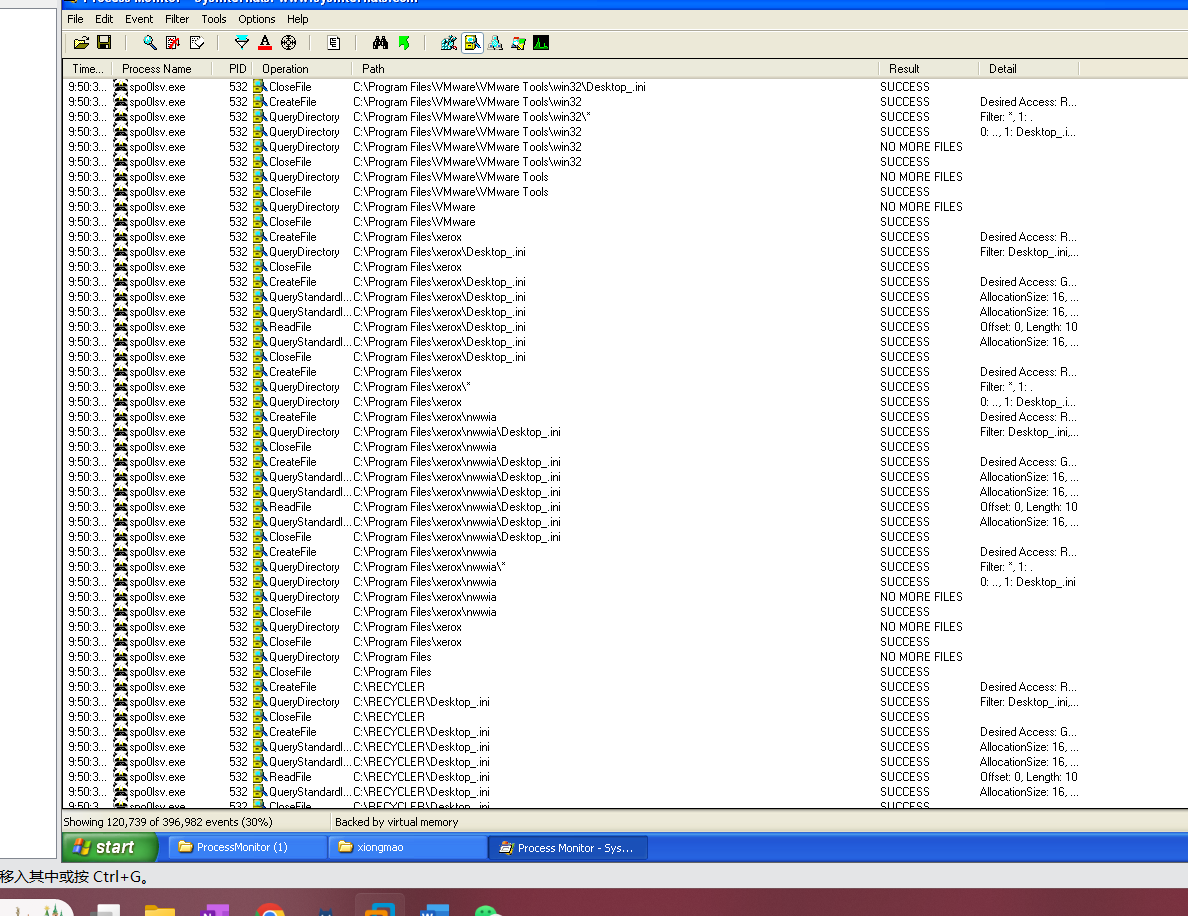
有特别多，看名字应该是删除了注册表中杀毒软件相关启动项让这些杀毒软件失效

再看看病毒在注册表中创建了哪些



最明显的是创建了一个自启动项，并且对自己进行了隐藏处理

在看看对文件的修改

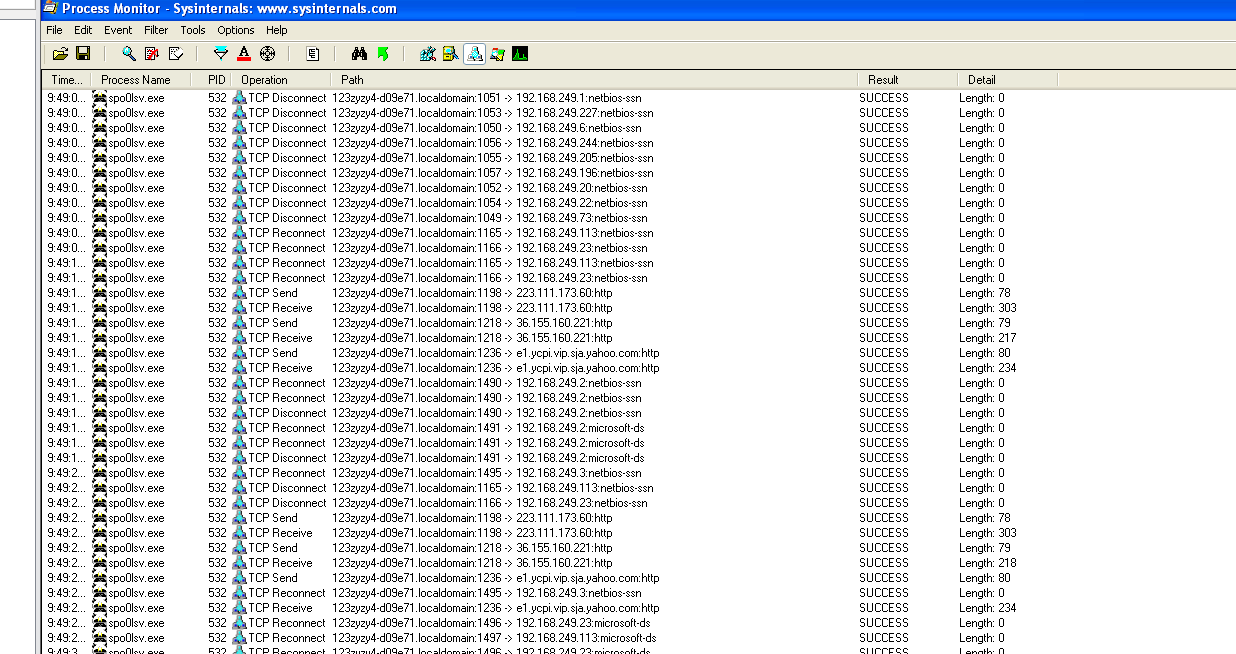


改了太多了根据截图不完

里面最终要的应该是：

这里在c盘根目录下创建了病毒启动相关程序

再看看对网络的修改：

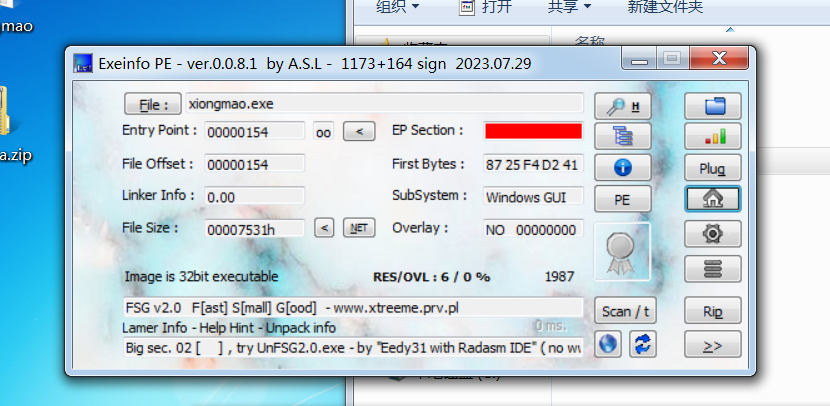


也是非常多

从图里可以看出，病毒程序一直在尝试与局域网中的其他主机连接，这也是病毒的入侵行为之一。

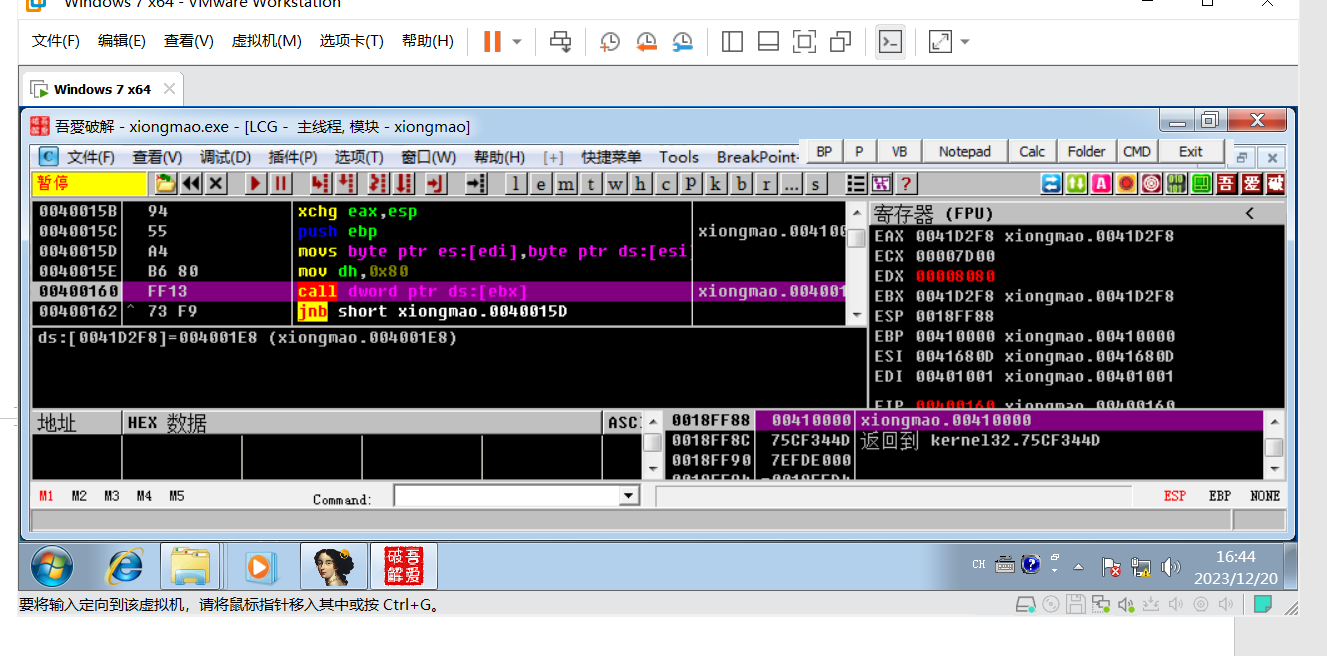
### 病毒的程序结构分析

首先使用exeinfo pe对病毒程序进行查壳：

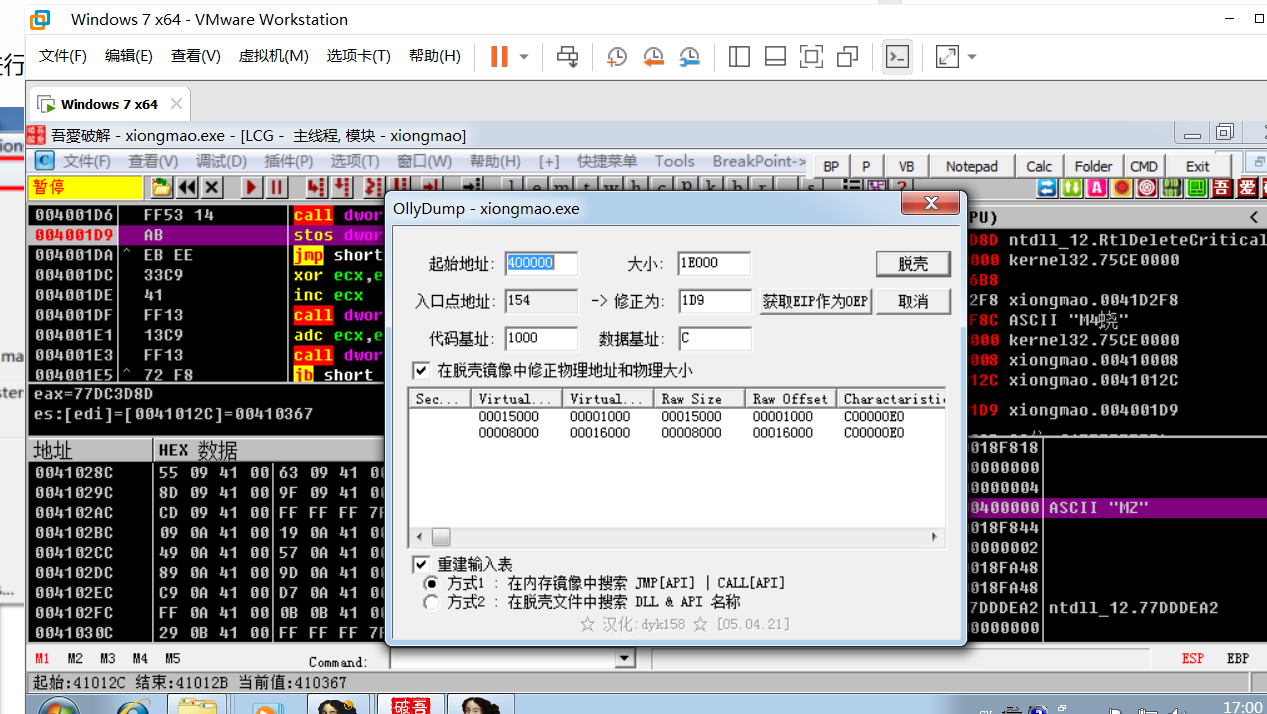


看到使用的是fsg2.0的壳。（FSG（Fast Small Good）是一种著名的壳（packer），用于对可执行文件进行保护）

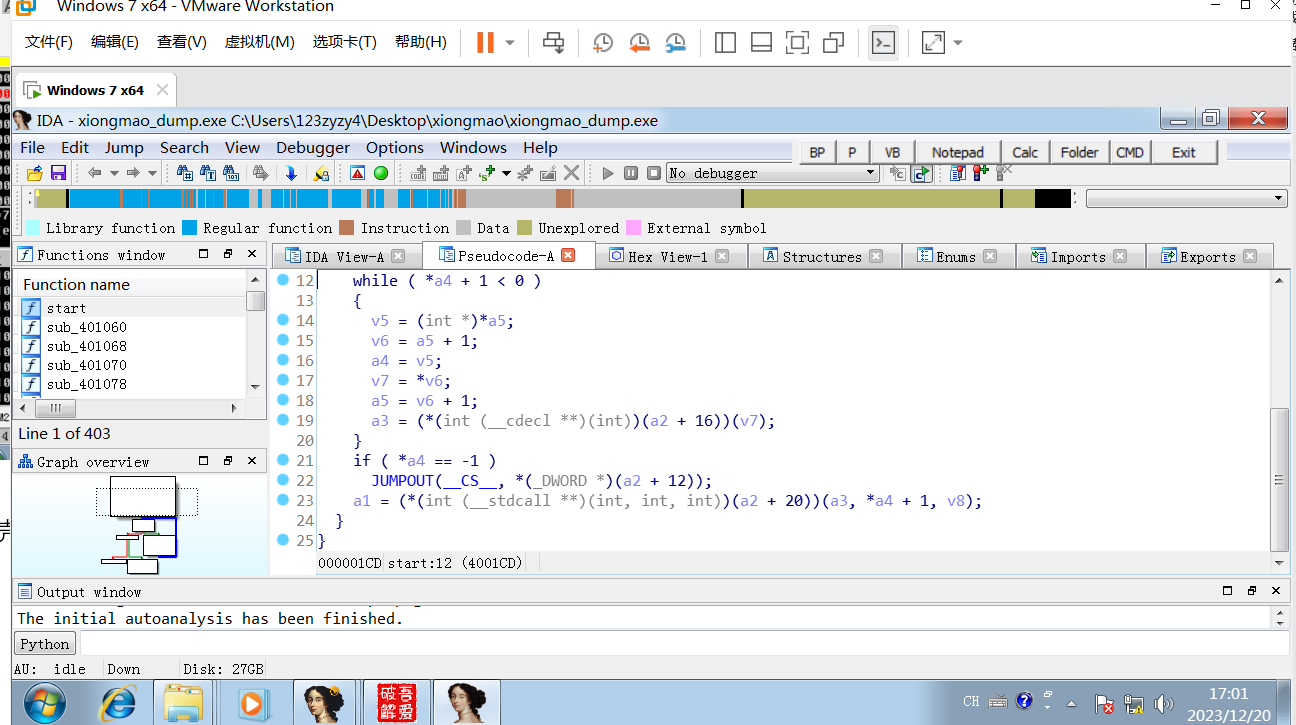
打开之前安装过ollydbg的win7虚拟机，把病毒文件拖到od中



使用od的插件对程序进行脱壳：

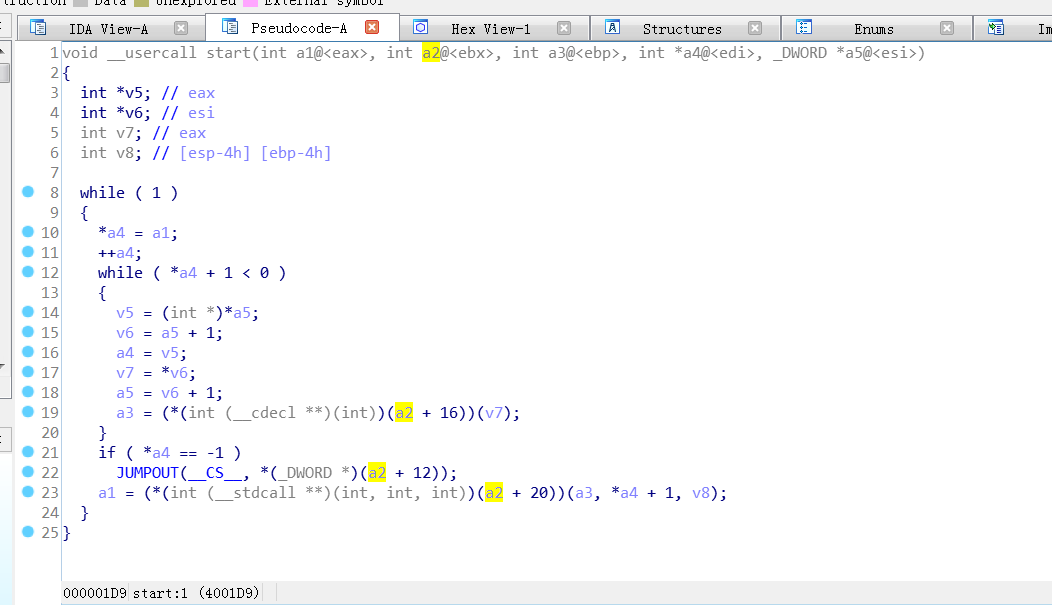


把脱壳后的程序放到ida中：



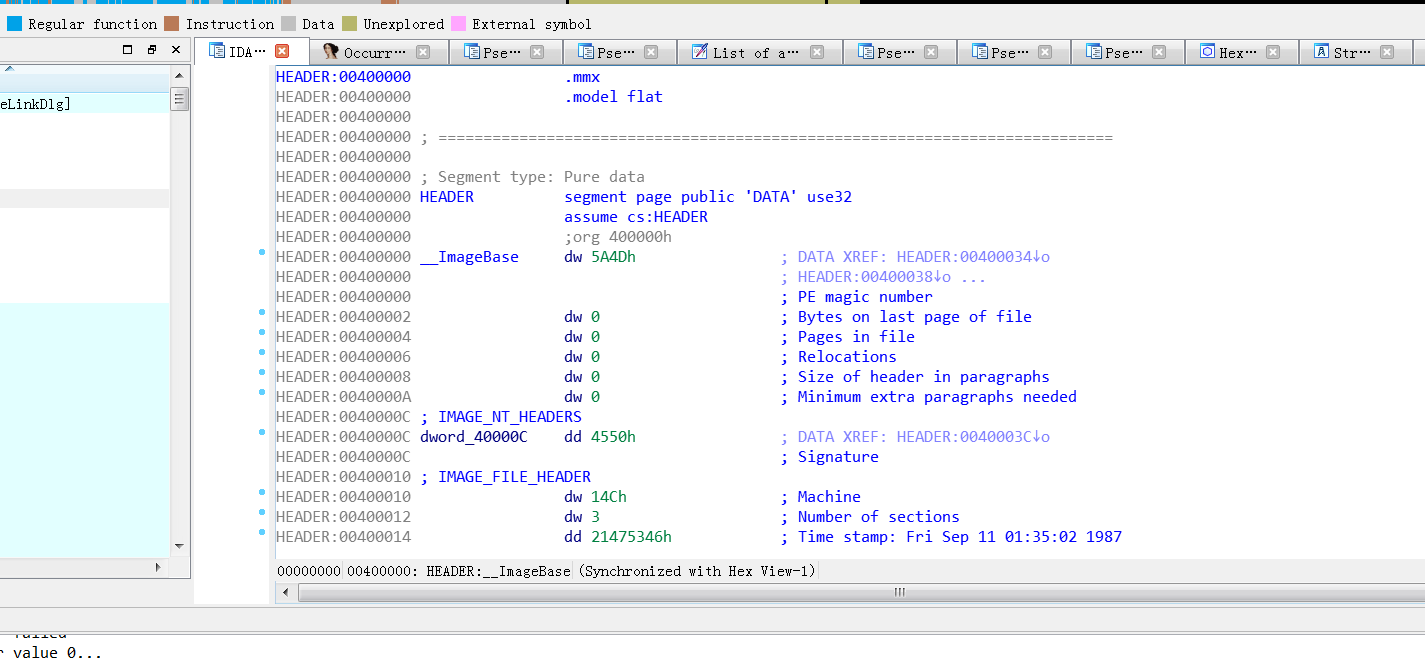
看到左边的子程序就知道脱壳是没啥问题的，另外使用f5反编译

下面分析具体程序;

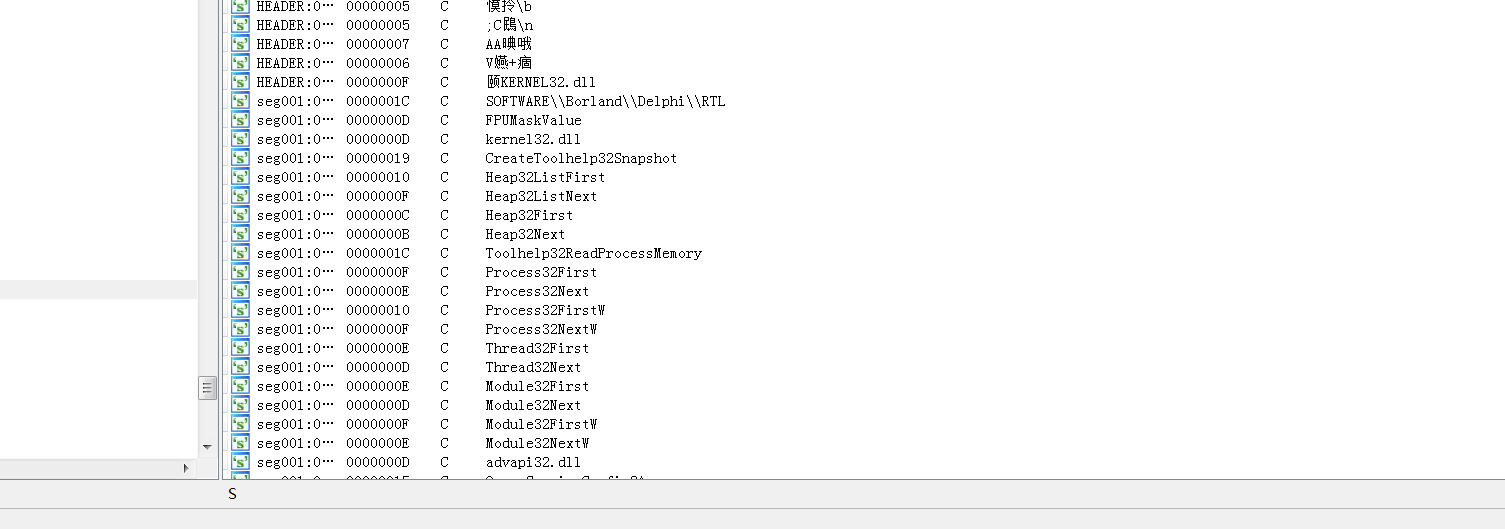


从图可以看出start大概先定义了一堆变量然后进入了一个死循环（怪不得的od中单步调试一直没法往下推）

转化为原本的模式：



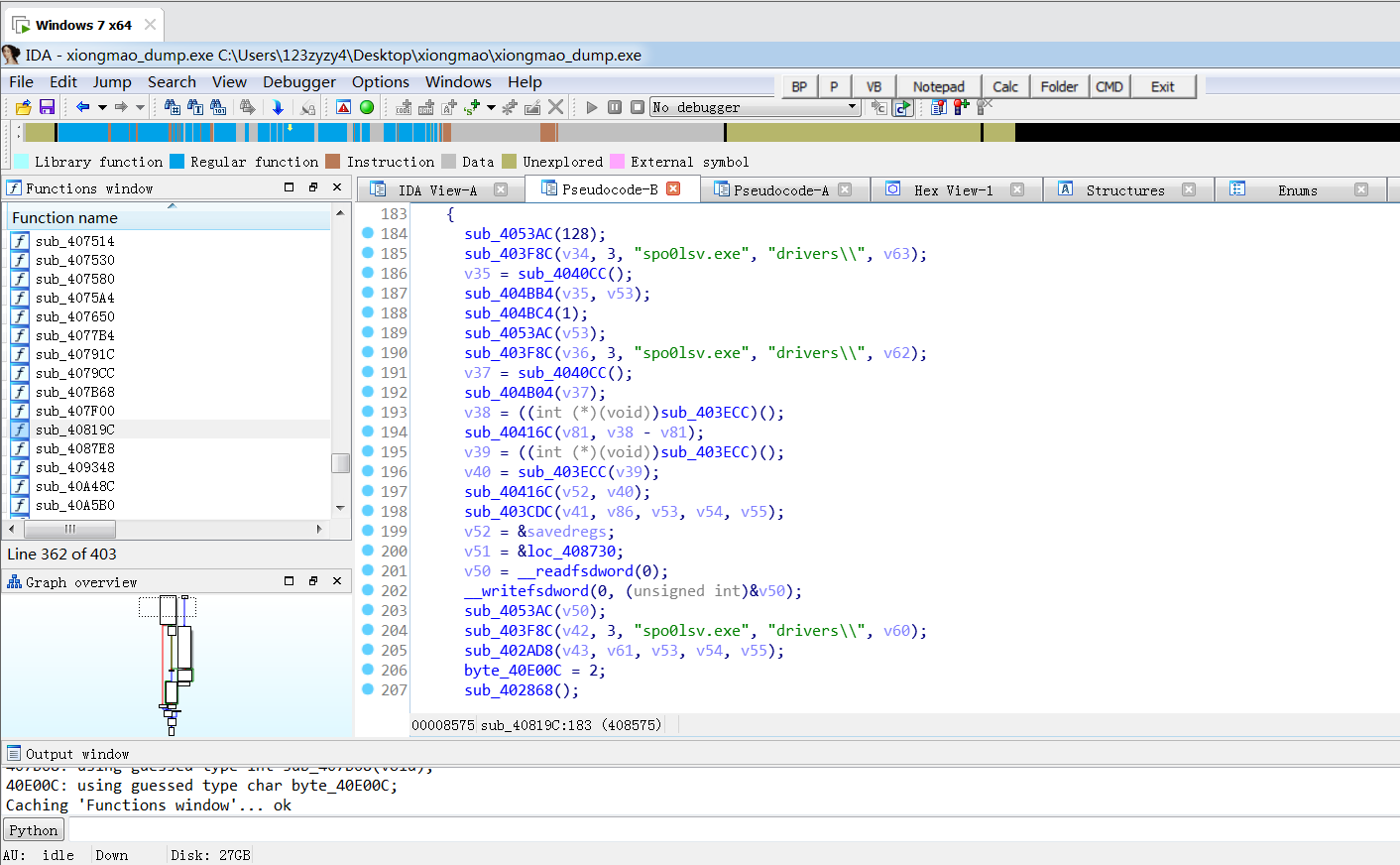
内容太多了，通过字符串搜索的方法筛选一批有重要字符串的，只关注里面调用的比较重要的函数：



从这些中找出start函数call的部分

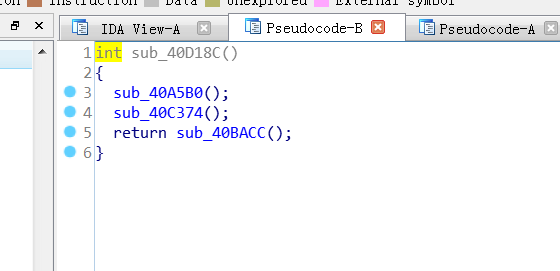
寻找到的第一个重要的函数-sub\_40819c

****

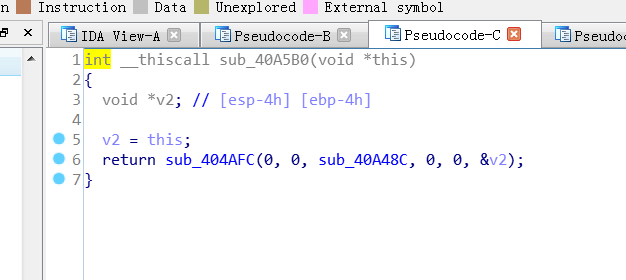


从图中可以看到出现了两个字符串一个是desktop.ini一个是spo0lsv.exe，这个函数大概的作用应该是创造这两个文件并执行，分别执行桌面文件的入侵和病毒程序的启动。

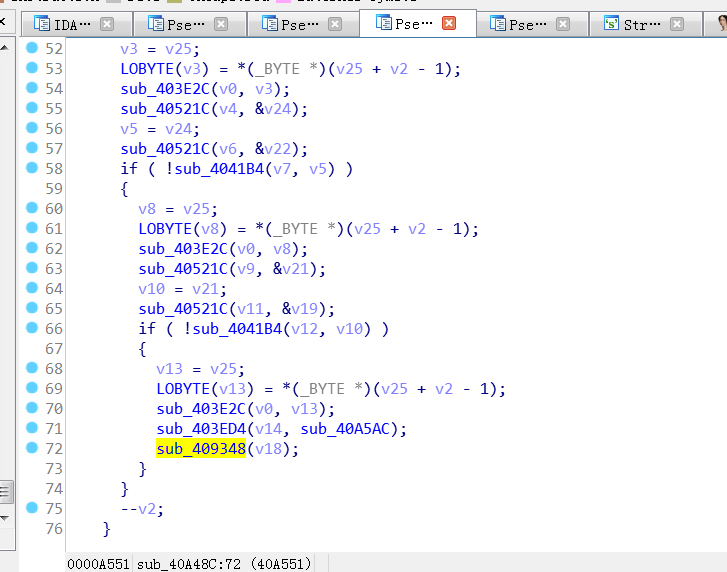
第二个比较重要的函数是sub\_40D18C：



进入sub\_40A5B0



进入sub\_40A48C:

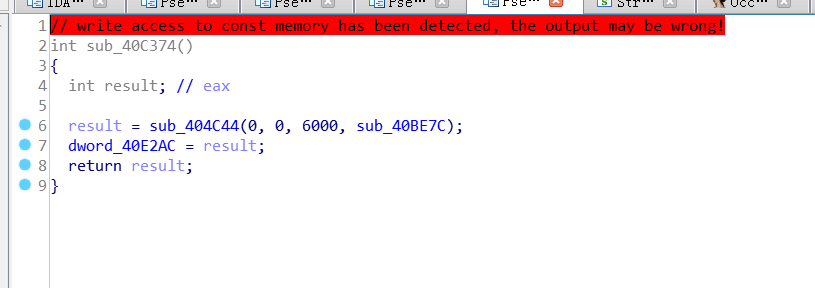


进入sub\_409348：

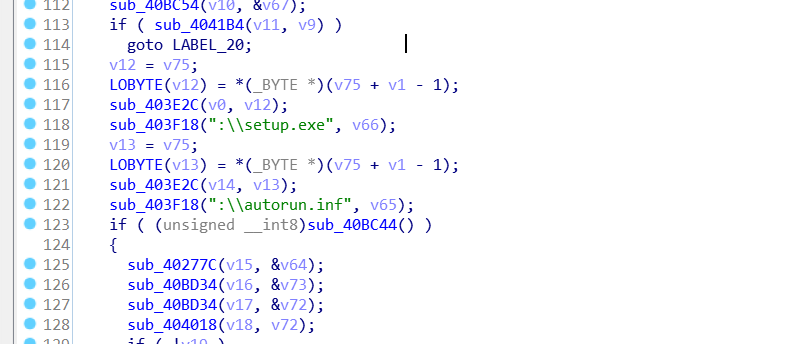


找到了在字符串查找中出现的另一个出现desktop.ini的地方了

但是这不是关注的重点，继续进入里面的sub\_40C374



进入sub\_40BE7C：



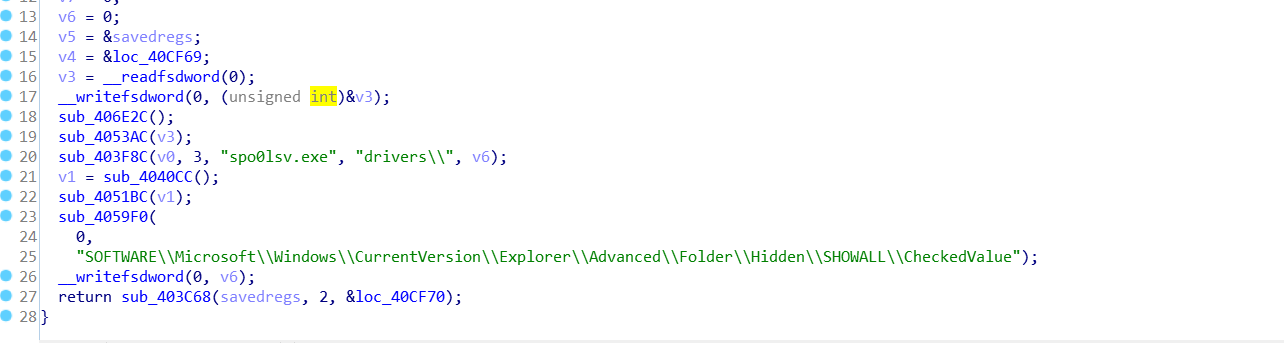
这个是上面一直进入函数后找到的函数，可以看到里面出现了setup.exe和autorun.inf，在病毒行为分析那一块写过这两个文件可能起到的作用这里就不多写了，这个函数大概的作用应该就是创建了这两个文件。

下一个出现的比较重要（有入侵过程中见到过的字符串）的函数是sub\_40D088



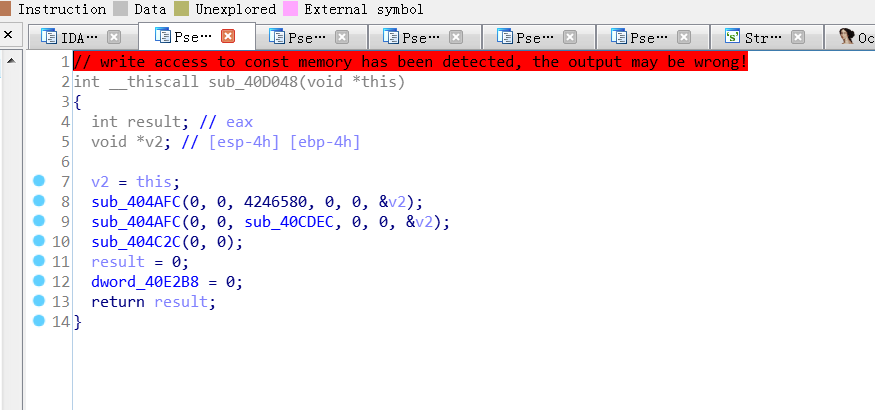
这个函数基本负责了病毒攻击部分的大部分内容，下面细说

进入sub\_40CEE4

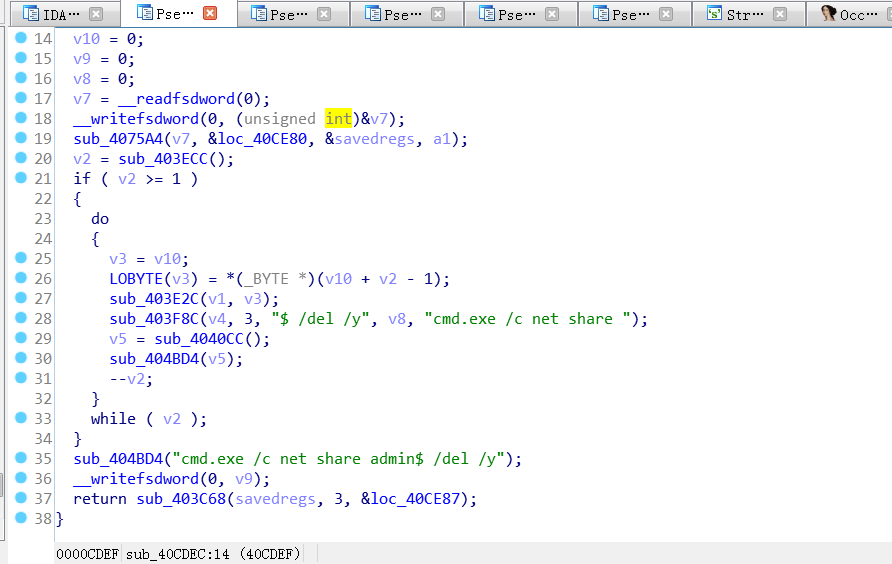


从字符串不难看出是做了病毒隐藏的操作（hidden）

进入sub\_40D048

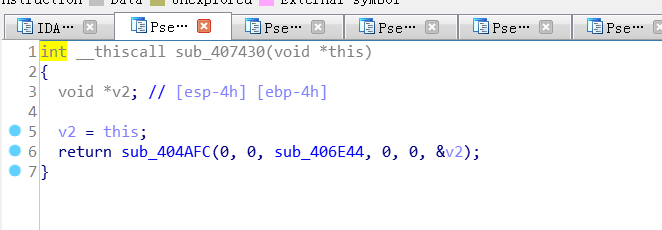


进入sub\_40CDEC

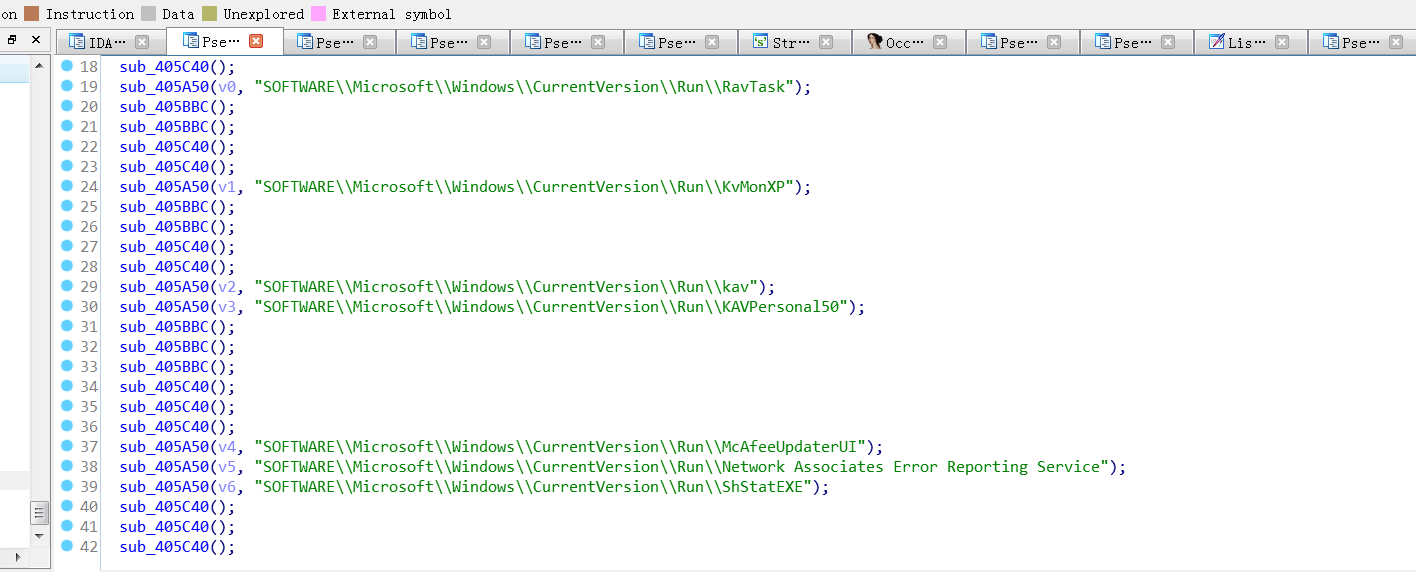


在这里通过cmd中net share指令进行了共享的删除（这个上面入侵过程也提到过）

从最开始的sub\_40D088进入sub\_407430函数



再进入sub\_406E44函数



原来把注册表里面常见杀毒软件自动的项目删除是在这里进行的

至此大部分入侵过程中提到的病毒对计算机的修改操作在代码里面都有了对应，分析过程就写到这里。