# 《软件安全技术》综合实验

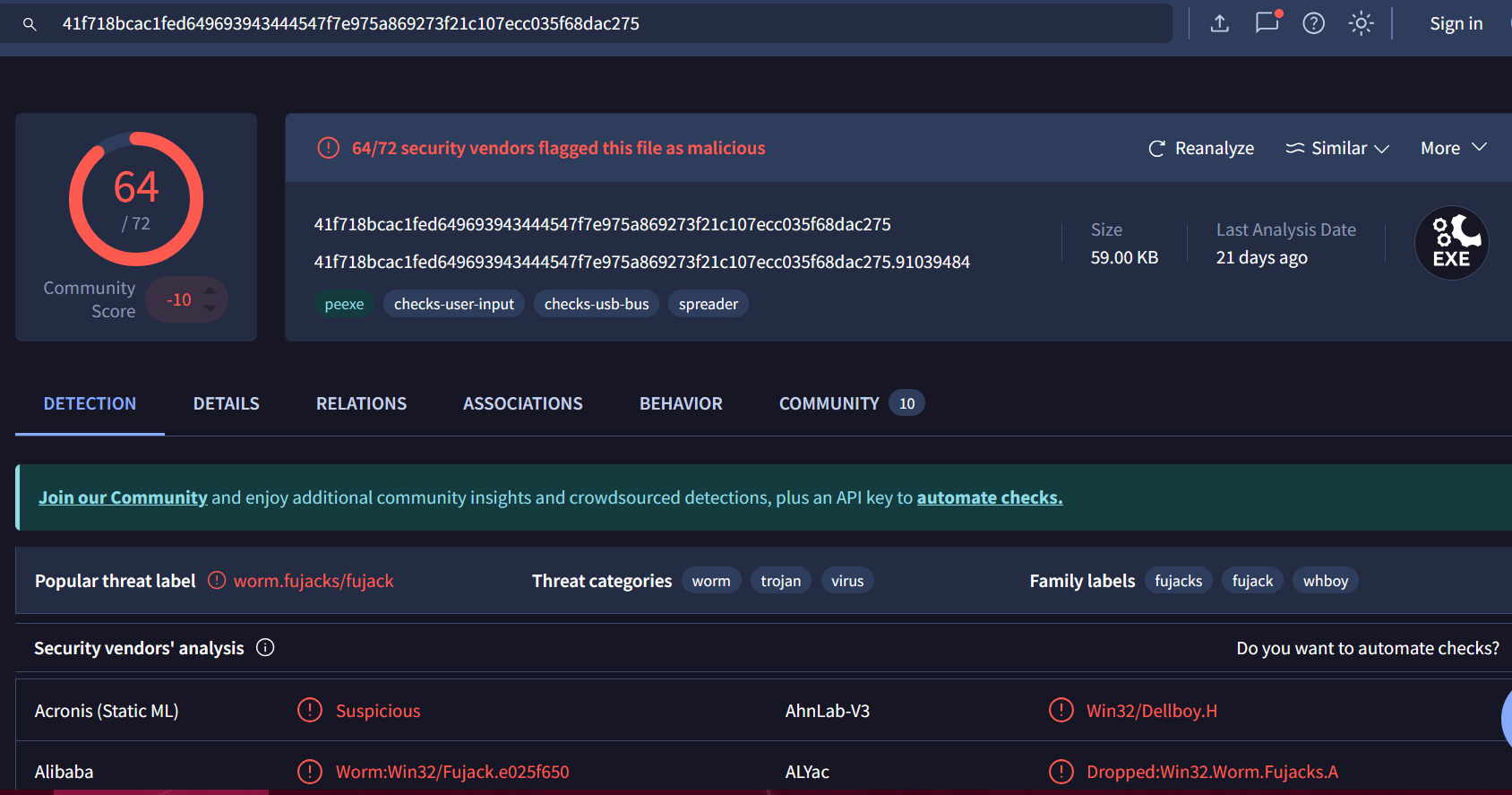
## 实验五：熊猫烧香病毒分析

## 作者：谭九鼎

## 学号：522024320137

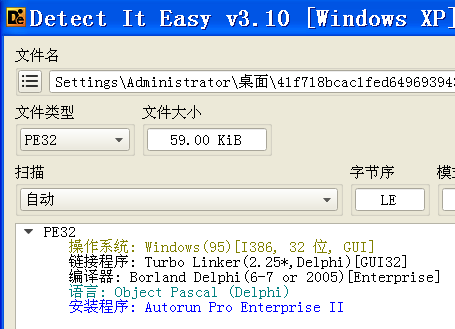
## 时间：2024年12月

使用VirusTotal多引擎在线查毒：

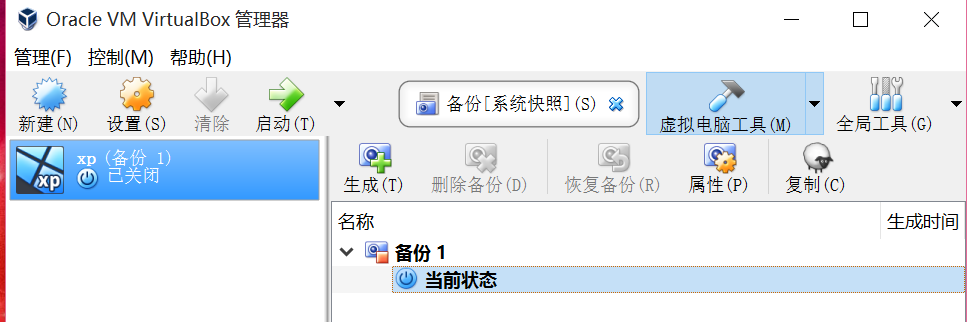


其中AliCloud没有报毒

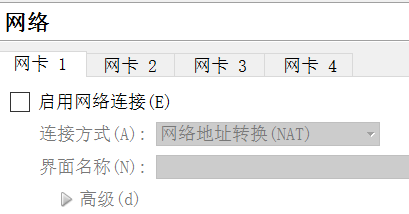
使用Detect-it-Easy检查语言和框架：



创建还原点：



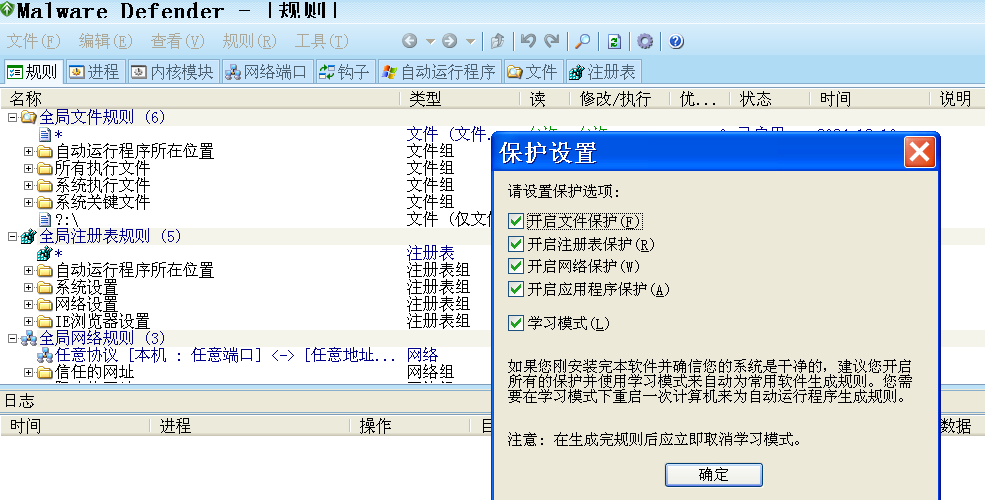
禁用网卡防止传播：



下载反编译软件IDA pro 6.8: <https://sourceforge.net/projects/doccument/files/> 实测无法启动



下载安全工具Malware Defender HIPS：<https://www.xiazaiba.com/html/1860.html>

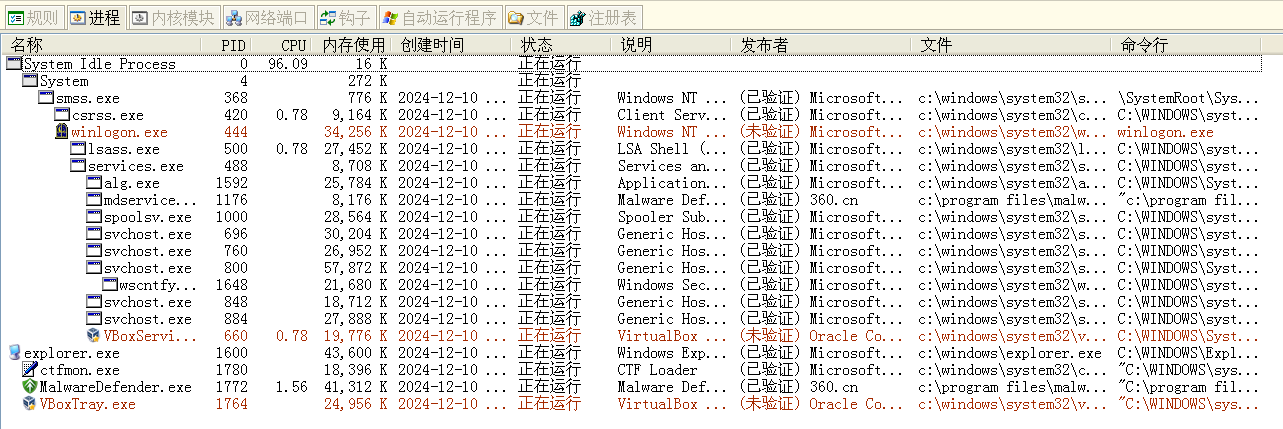


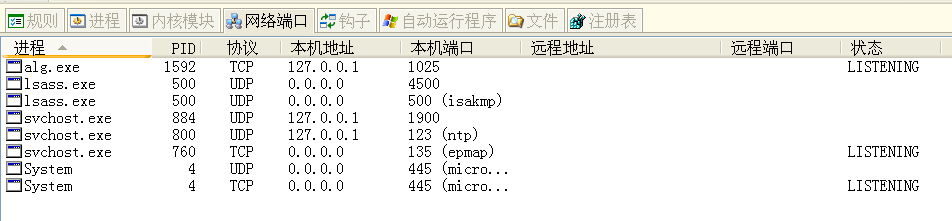
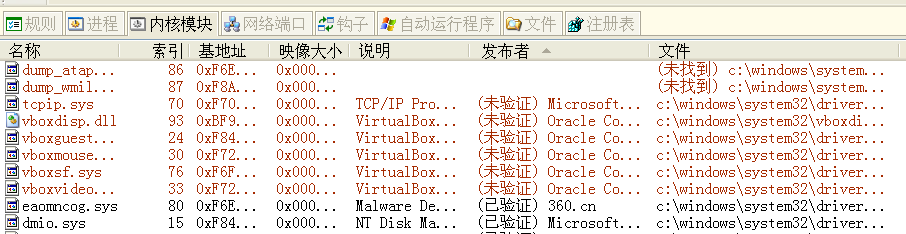
先使用学习模式，添加允许正常程序行为的规则。之后再切换到普通模式。

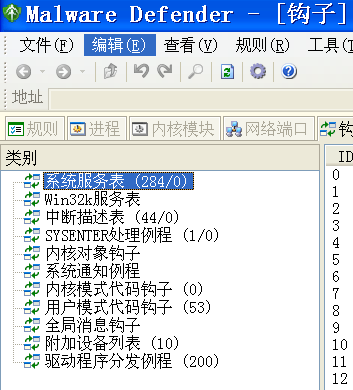
设定记录文件的写、修改、删除，注册表的修改、网络的访问

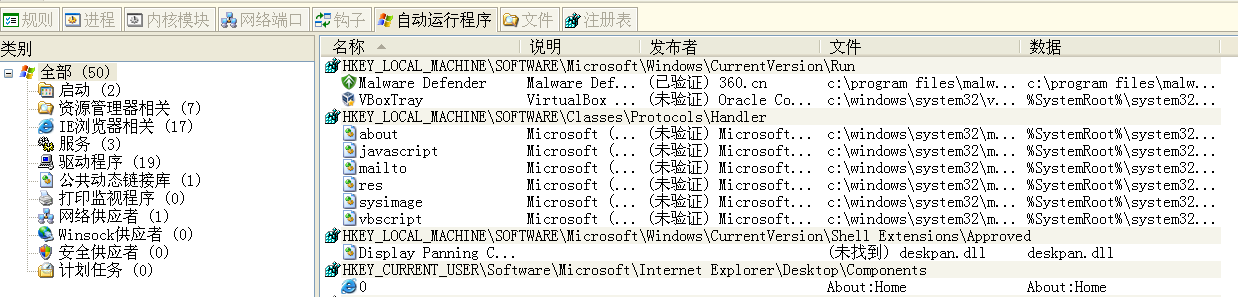


运行病毒前的状态：





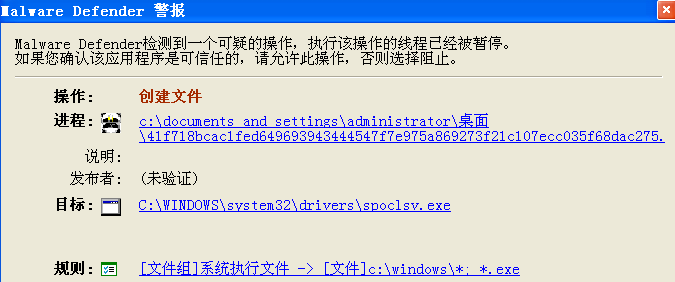


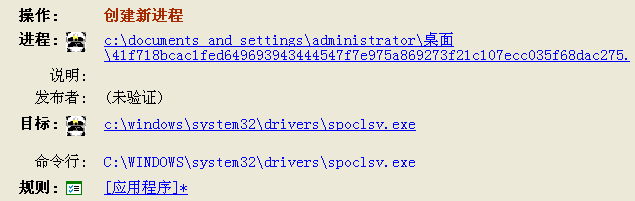


双击运行病毒：

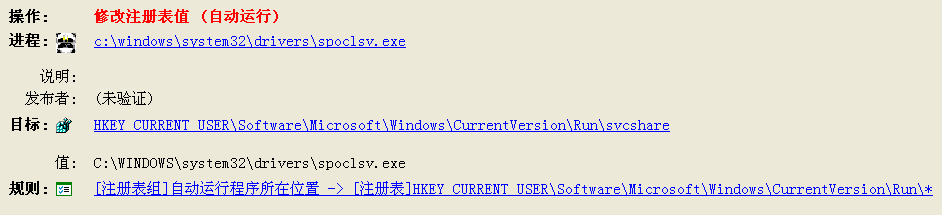


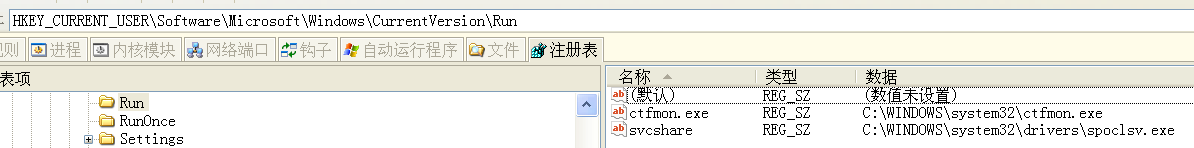
允许explorer运行病毒。



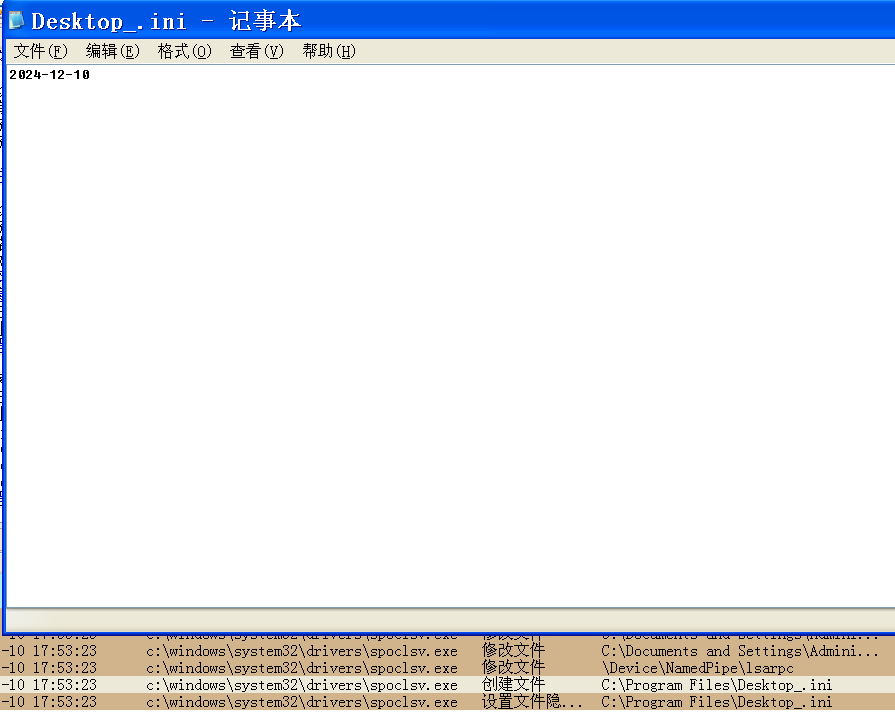


病毒创建spoclsv.exe文件并运行。

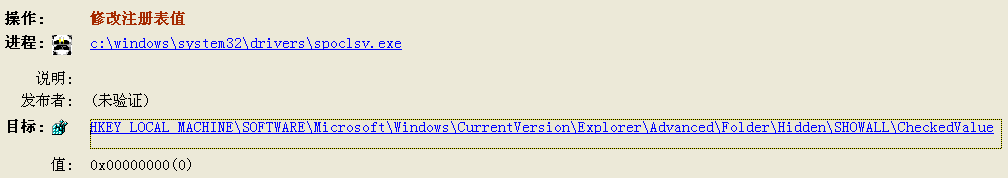




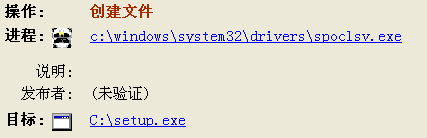
添加自启，并且定时重复运行



修改了一些ie的设置。在各个文件夹中创建Desktop\_.ini

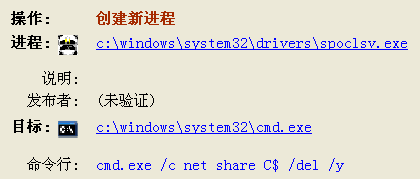


禁止显示隐藏文件，并且定时重复运行

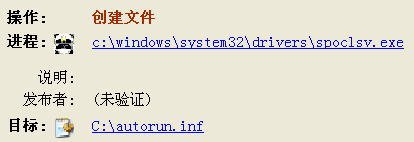




创建复制体



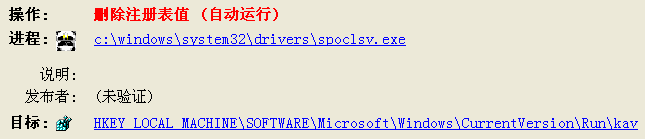
删除共享（多次出现，不知道有什么用）







创建双击磁盘运行病毒的功能

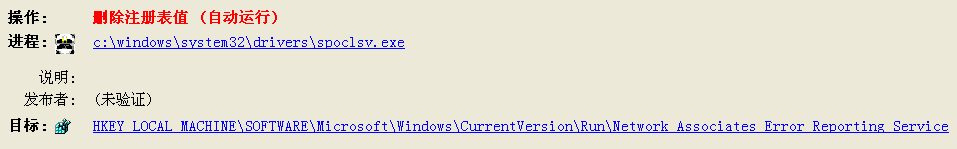






删除一些杀软的自启项，并且定时重复运行



删除网络错误报告服务



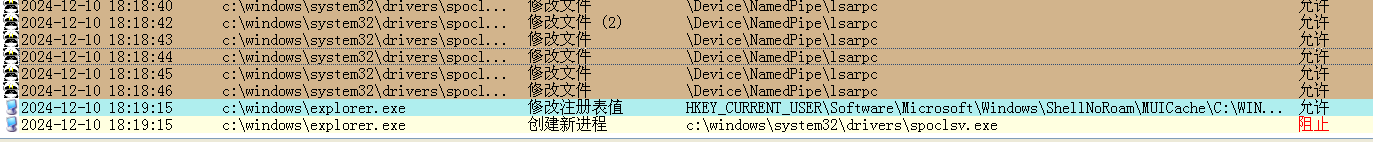


禁止wscsvc运行

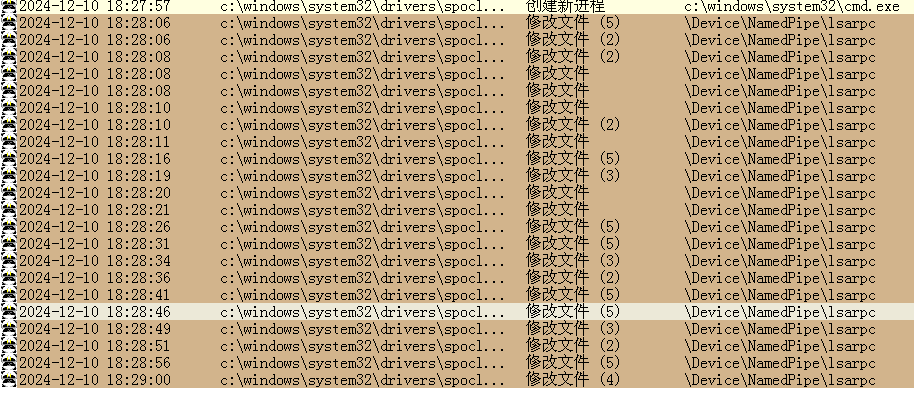
至此已经结束，没有进一步动作。接下来重启。



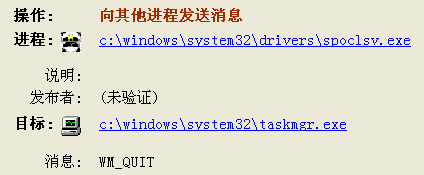
不清楚是否和病毒有关。



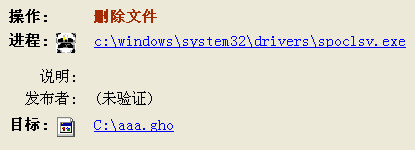
本来病毒已经启动了，但因为MD的默认规则，explorer启动程序要询问，但因为上一条消息太多，自动拒绝了，导致病毒被关闭了。创建允许规则再重启。



持续访问lsarpc命名管道。查询资料得知与SMB有关。根据其他分析，这个就是用于传播到其他电脑。



如果运行任务管理器，会被关闭。



会删除gho文件

持续运行近半小时，没有发现感染exe的行为。



最后恢复备份，回到未运行病毒的时候。

使用Binary Ninja在线静态反编译成C伪代码：

