****

**分析报告**

|  |  |
| --- | --- |
| **样本名** | **xiongmao.exe** |
| **班级** | **软安41期** |
| **作者** | **张海龙** |
| **时间** | **2020-12-30** |
| **平台** | **Windows 7** |

15PB信息安全研究院(病毒分析报告)

**目录**

[1．样本概况 4](#_Toc419)

[1.1 样本信息 4](#_Toc21701)

[1.2 测试环境及工具 5](#_Toc3875)

[1.3 分析目标 5](#_Toc299)

[2． 利用pchunter和wsexploer敏感信息 5](#_Toc21082)

[2.1 查看可疑进程 5](#_Toc2281)

[2.2 查看可疑启动项 6](#_Toc18204)

[2.3 查看驱动/服务可疑项 6](#_Toc1616)

[2.4 查看其他可疑项 6](#_Toc15613)

[2.5 查看可疑流量 7](#_Toc22279)

[3． 利用火绒剑监控软件行为 7](#_Toc15844)

[3.2 文件监控 8](#_Toc23761)

[3.3 注册表监控 8](#_Toc28209)

[3.4 进程监控 9](#_Toc30087)

[3.5 网络监控 9](#_Toc23380)

[3.6 行为监控 10](#_Toc27634)

[4． 具体分析病毒行为 10](#_Toc5050)

[4.1 使用die进行查壳 12](#_Toc28777)

[4.2 使用OD进行手动脱壳 13](#_Toc31610)

[4.3 遍历文件进行感染 15](#_Toc24410)

[4.4 感染可执行文件 17](#_Toc11058)

[4.5 感染网页文件 18](#_Toc3372)

[4.6 复制病毒母体并写入配置文件 19](#_Toc21228)

[4.7 创建定时器保护自身 21](#_Toc18968)

[4.8 SafeSelfThreadProc 22](#_Toc10497)

[4.9 从指定网址查看链接并访问内容，下载病毒，然后执行 24](#_Toc9710)

[4.10 攻击注册表 24](#_Toc27996)

[5． 解决方案 24](#_Toc31459)

[致 谢 25](#_Toc2953)

# 1．样本概况

## 1.1 样本信息

----------------------

病毒名称：512301C535C88255C9A252FDF70B7A03

所属家族：蠕虫

MD5值：512301C535C88255C9A252FDF70B7A03

SHA1值：CA3A1070CFF311C0BA40AB60A8FE3266CFEFE870

CRC32：E334747C

病毒行为：  
 1.将自身拷贝到C:\Windows\System32\drivers\spo0lsv.exe，然后结束自身  
 2.在每个目录下释放隐藏文件Desktop\_.txt（内容，感染日期）

3.创建C:\Windows\System32\drivers\spo0lsv.exe自启动

4.复制病毒文件到C盘根目录setup.exe，并且写入可疑文件autorun.inf

5.autorun.inf文件注册启动项

6.感染文件,将应用程序的图标替换成熊猫烧香的图标(原因，熊猫烧香的PE文件在原 可执行文件之前，原PE文件作为了熊猫烧香的附加段在文件中，系统识别可执行程序 识别的是熊猫烧香的。所以图标被替换了)

## 1.2 测试环境及工具

测试环境：win7

使用工具：pchunter、wsexplorer、火绒剑、die、ida、od、importrec、hash

## 1.3 分析目标

1、提取病毒样本，手工清理机器

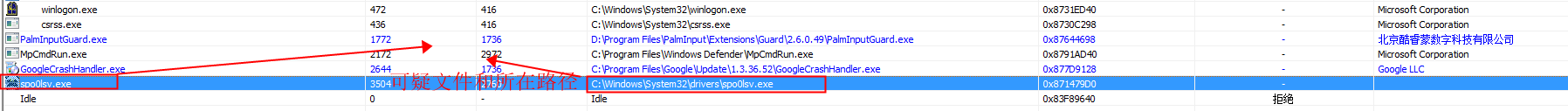
2、行为分析，获取病毒行为

3、详细分析，找到行为恶意代码

4、提出解决方案、编写专杀工具

# 利用pchunter和wsexploer敏感信息

## 2.1 查看可疑进程

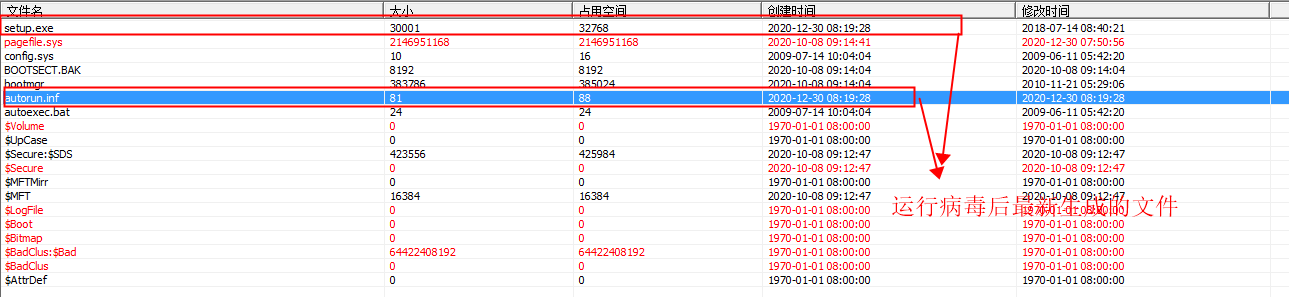


## 2.2 查看可疑启动项

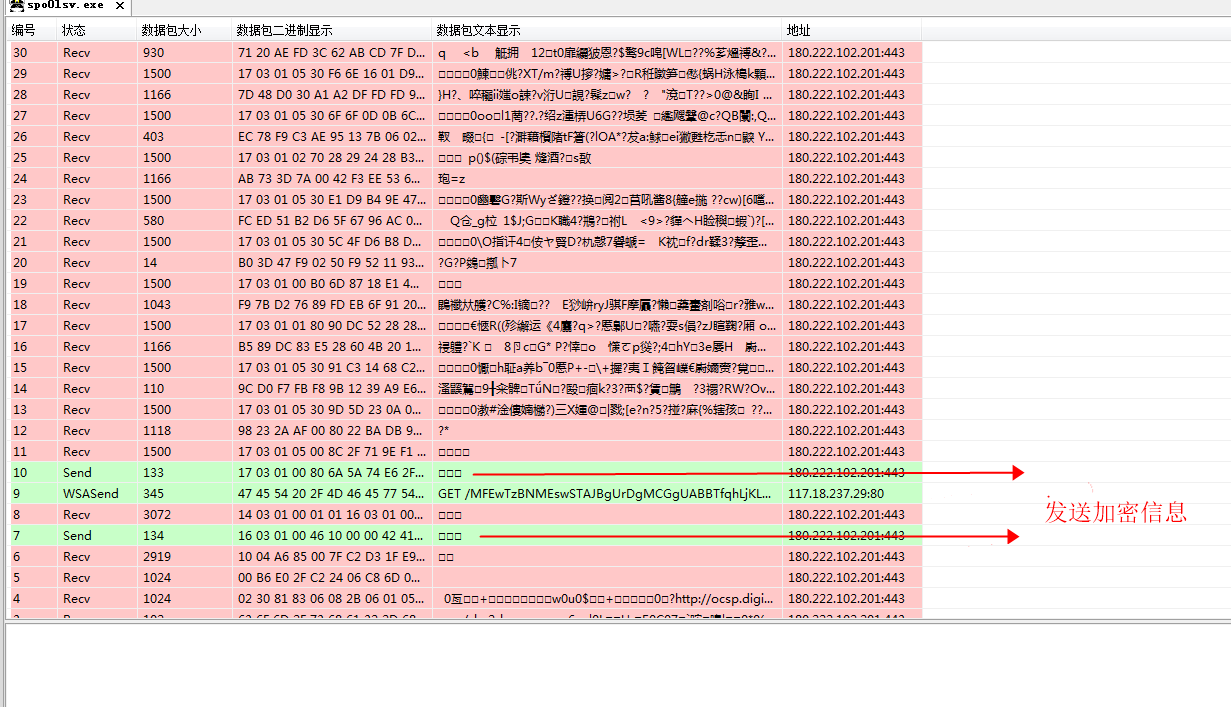
## 2.3 查看驱动/服务可疑项

无

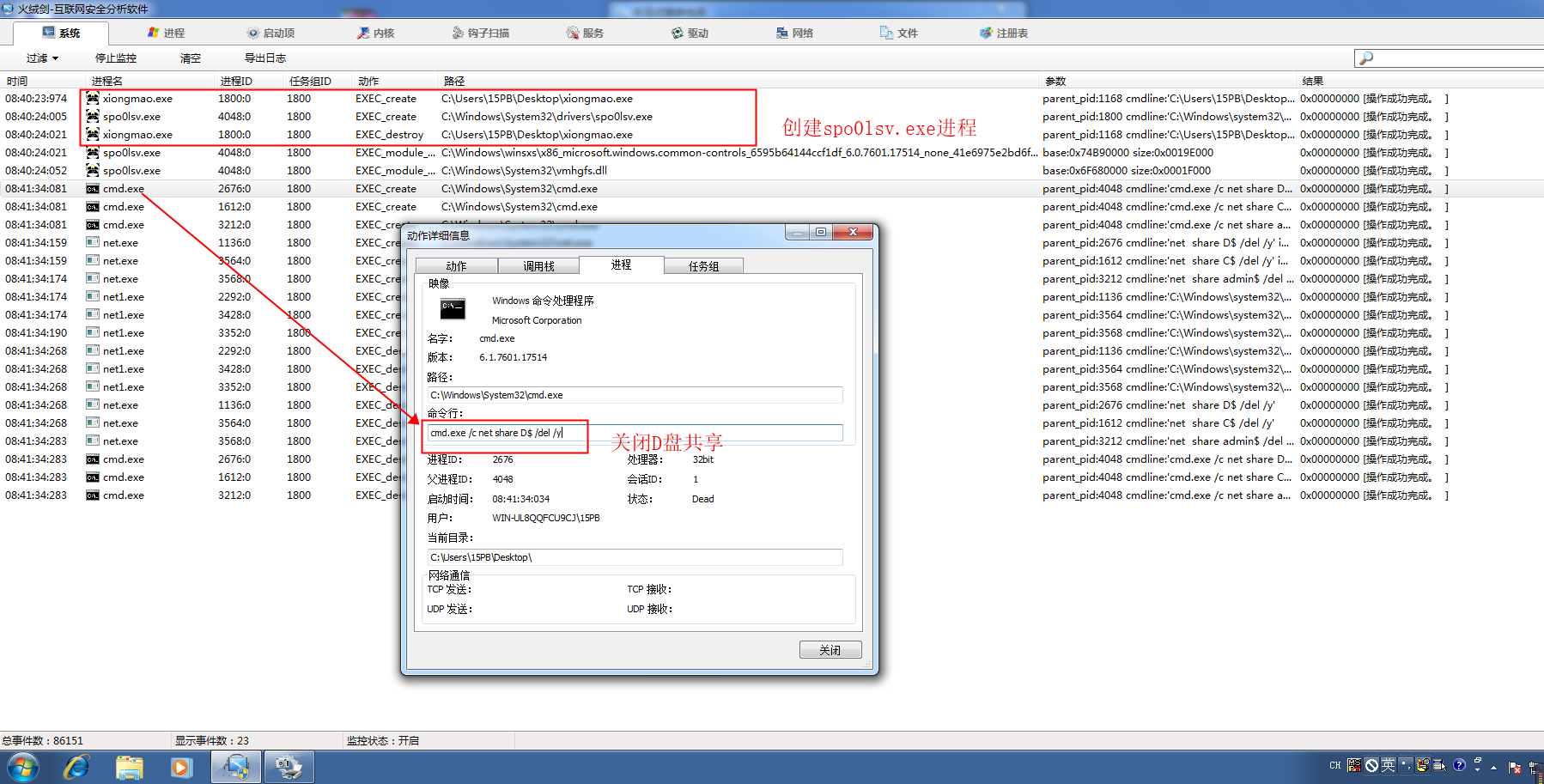
## 2.4 查看其他可疑项



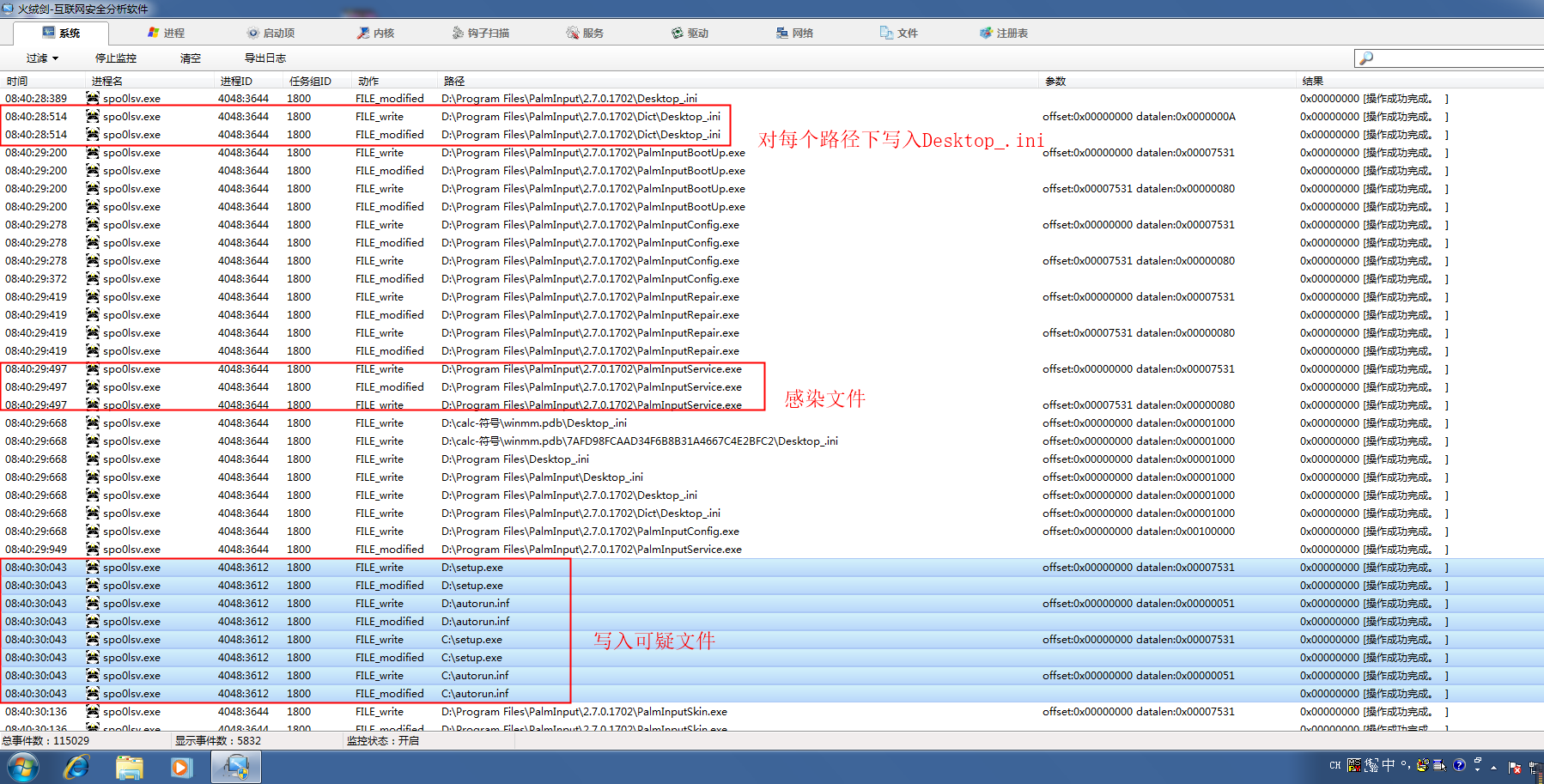
## 2.5 查看可疑流量



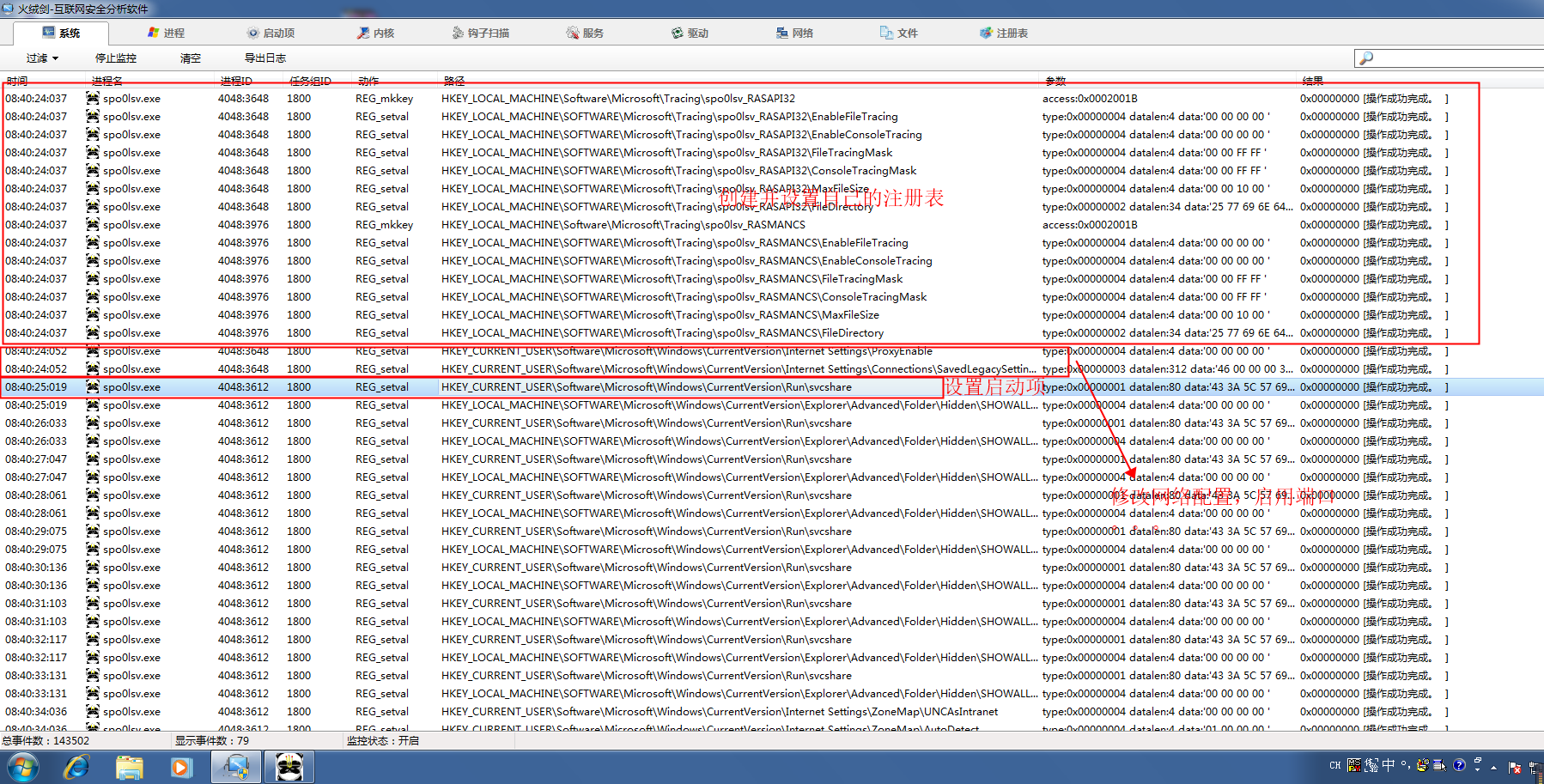
# 利用火绒剑监控软件行为

**3.1 执行监控**

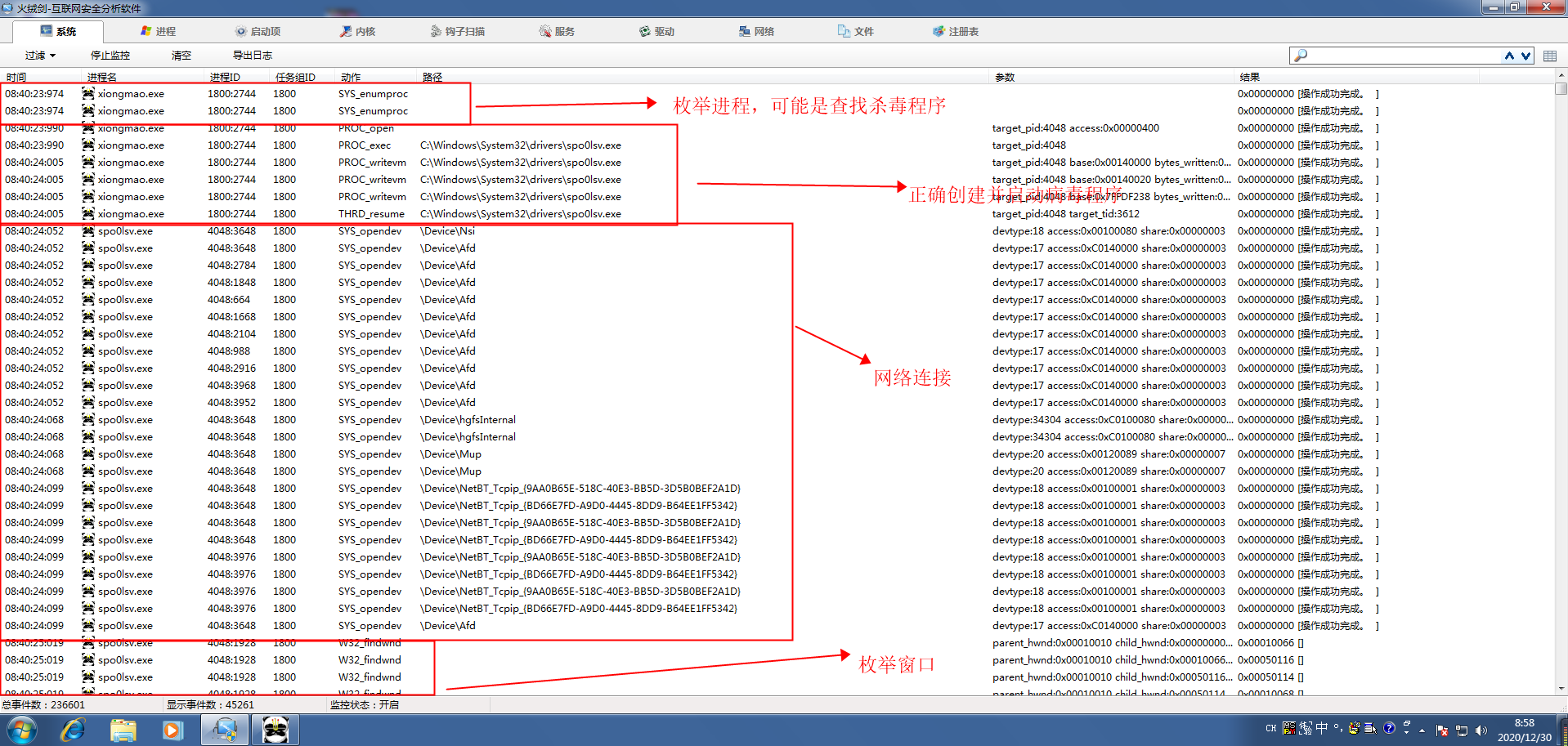
## 3.2 文件监控



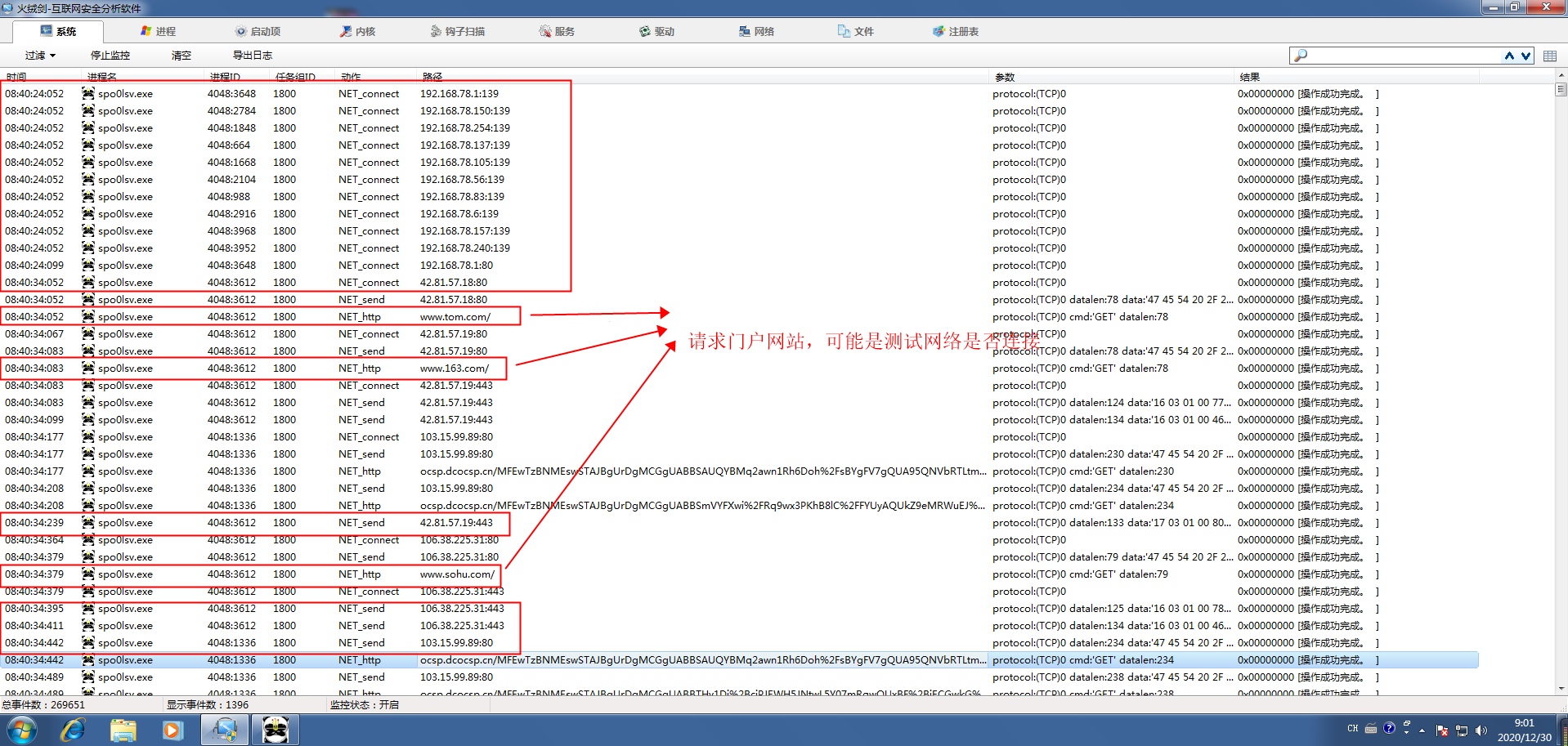
## 3.3 注册表监控



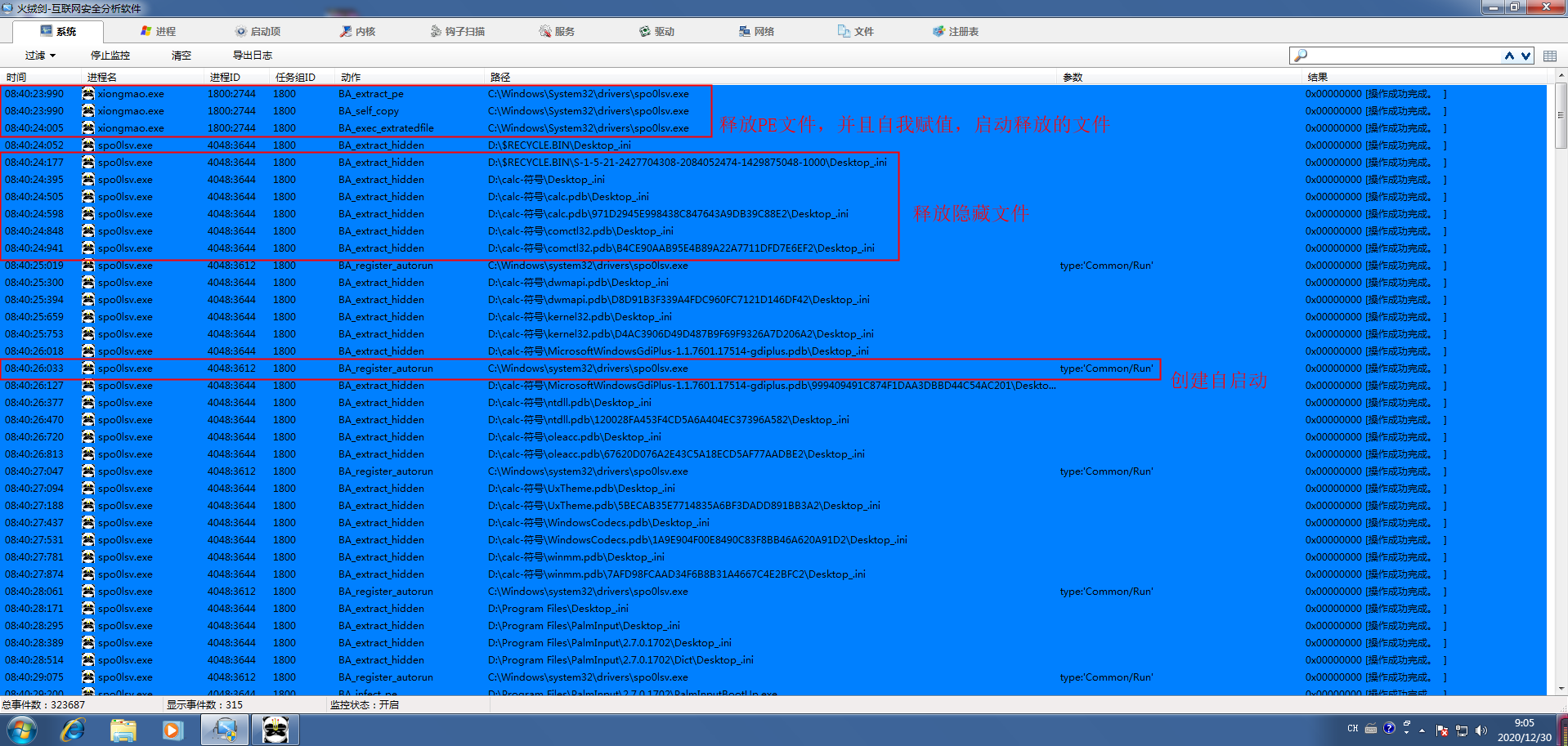
## 3.4 进程监控

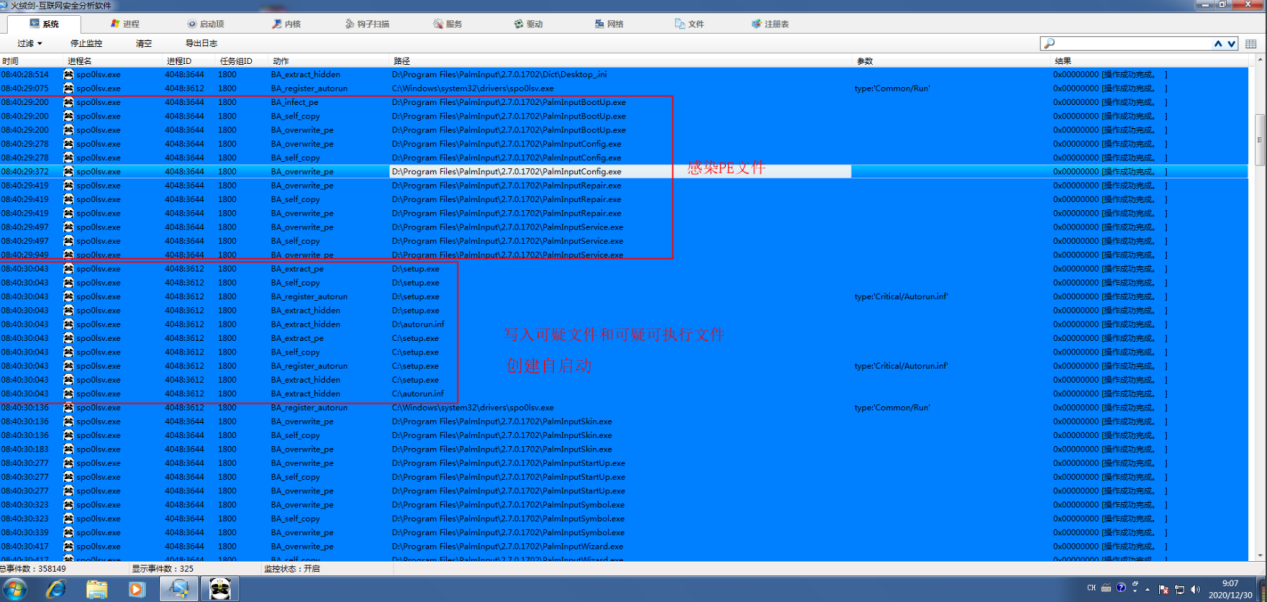


## 3.5 网络监控



## 3.6 行为监控





# 具体分析病毒行为

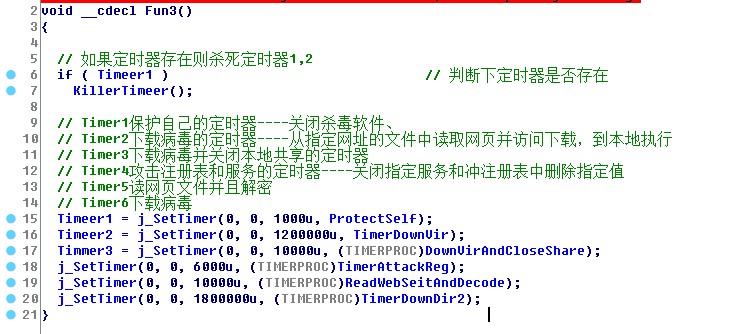
Fun1功能简介



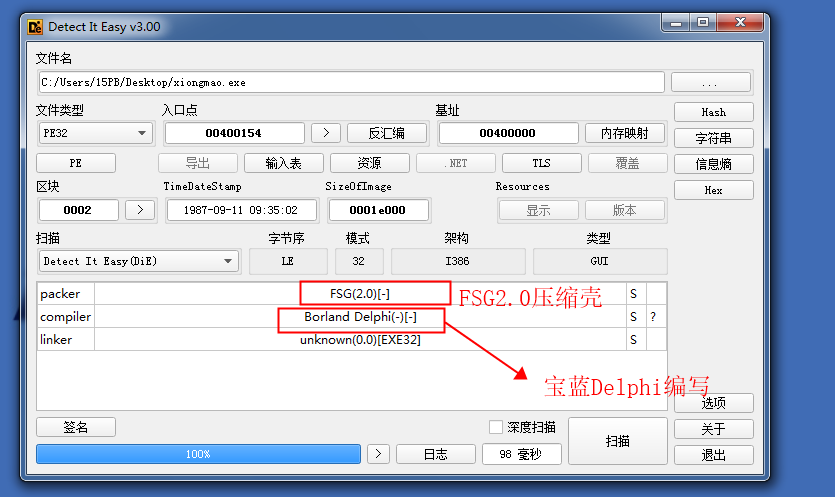
Fun2功能简介



Fun3功能简介



## 4.1 使用die进行查壳



获得情报1：病毒程序加了FSG2.0压缩壳。

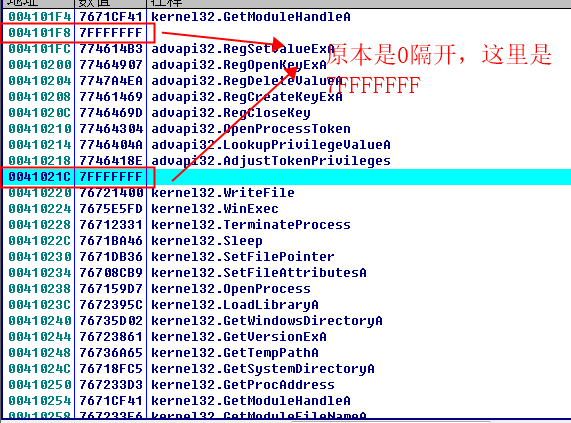
获得情报2：病毒程序加了使用Borland Delphi编写

## 4.2 使用OD进行手动脱壳



跳转oep关键点处进行下断点，直接F9运行到此处，跳转到oep

查看IAT表是否有问题。



修复IAT表的隔开数据

使用dump插件dump文件

并使用ImportREC修复IAT



## 4.3 遍历文件进行感染



## 4.4 感染可执行文件

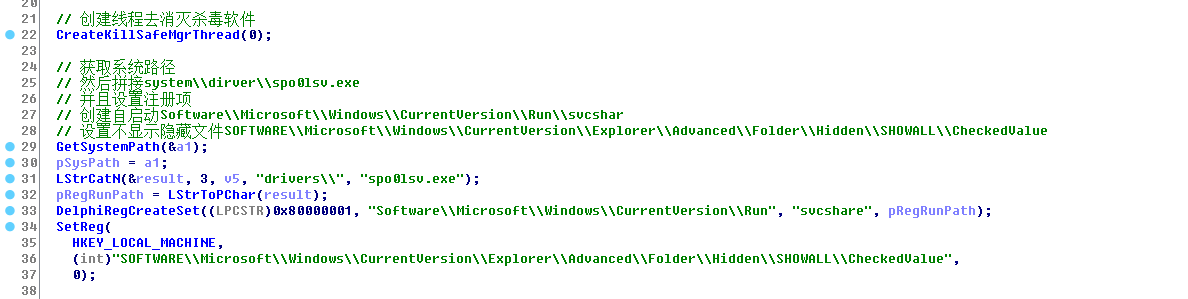


## **4.5 感染网页文件**

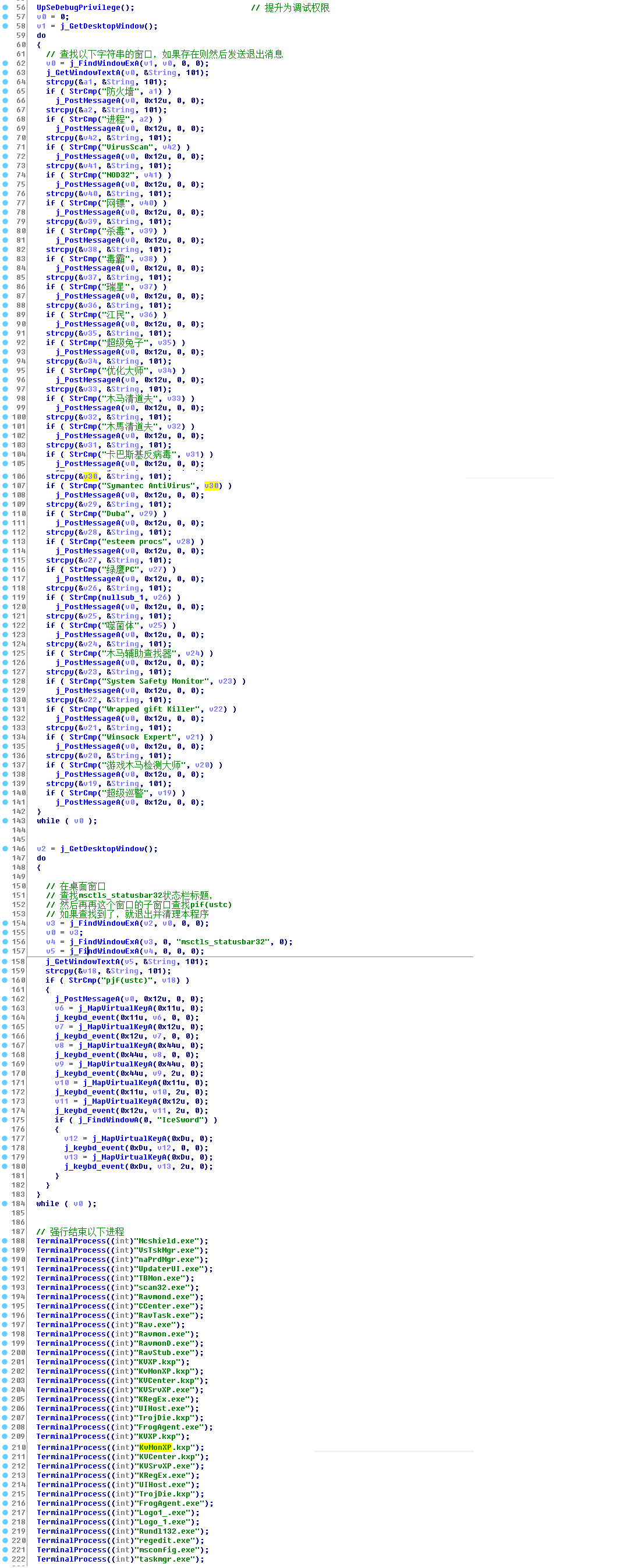


## **4.6 复制病毒母体并写入配置文件**

## **4.7 创建定时器保护自身**

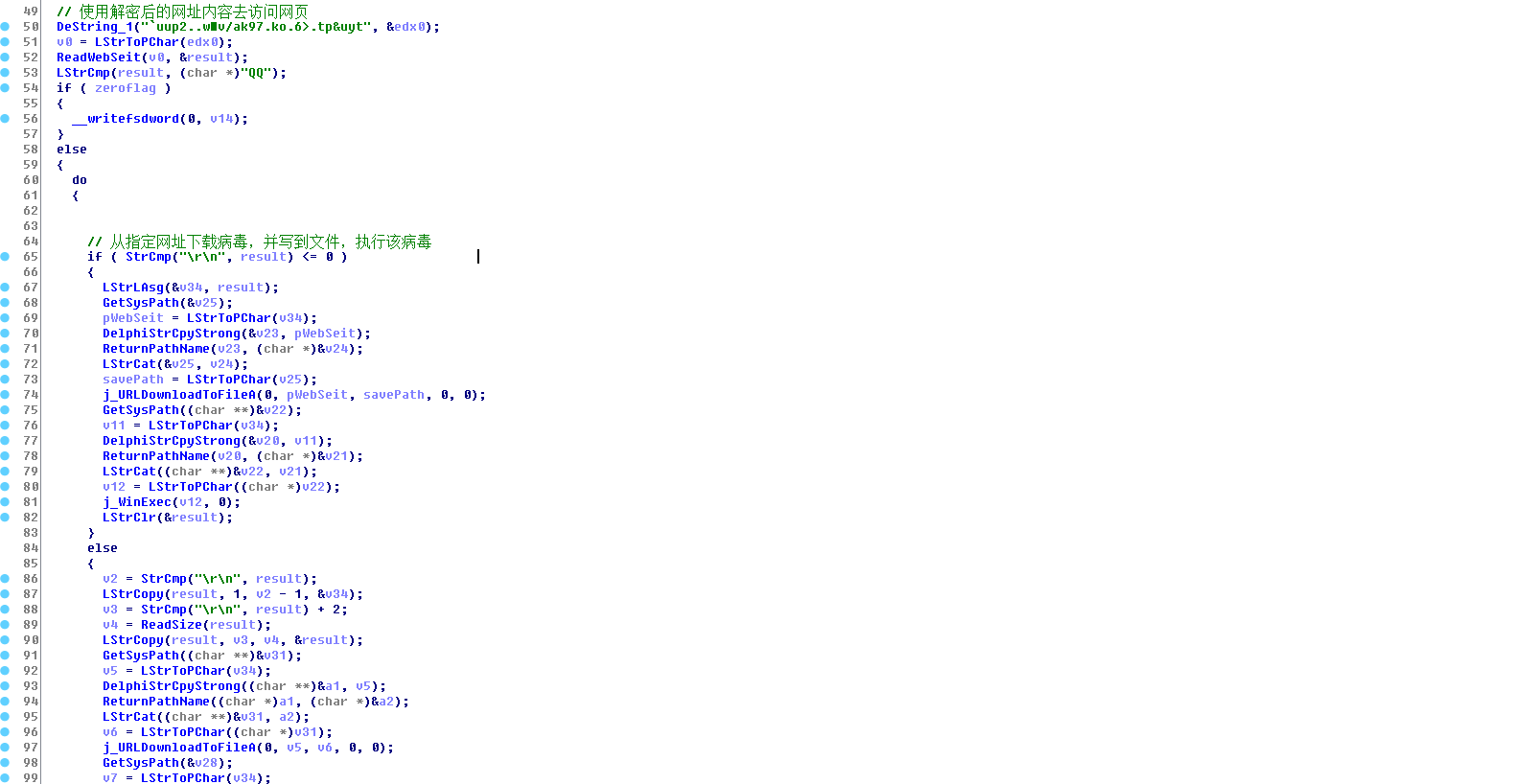


## **4.8 SafeSelfThreadProc**



注册快捷键ctrl+alt+d并发送退出消息

## **4.9 从指定网址查看链接并访问内容，下载病毒，然后执行**



## **4.10 攻击注册表**



# 解决方案

**1、查杀思路**

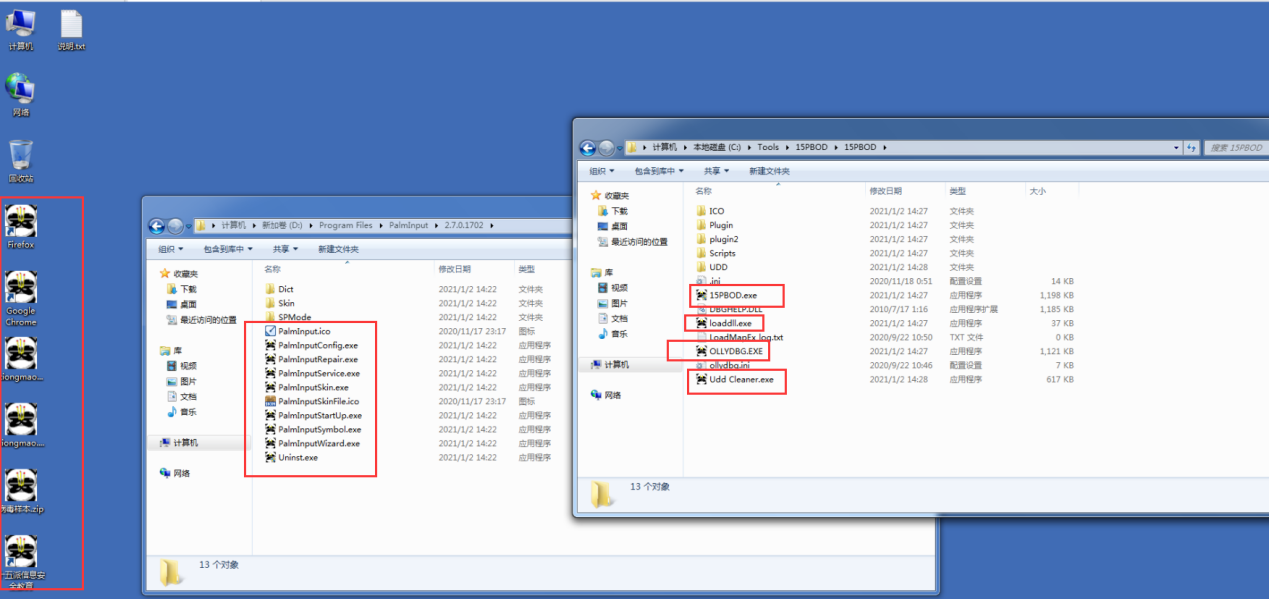
①结束病毒进程spo0lsv.exe进程

②修复注册表，包括删除病毒自启动项svcshare、修复文件的隐藏显示

③删除C盘下的autorun.inf、setup.exe、spo0lsv.exe

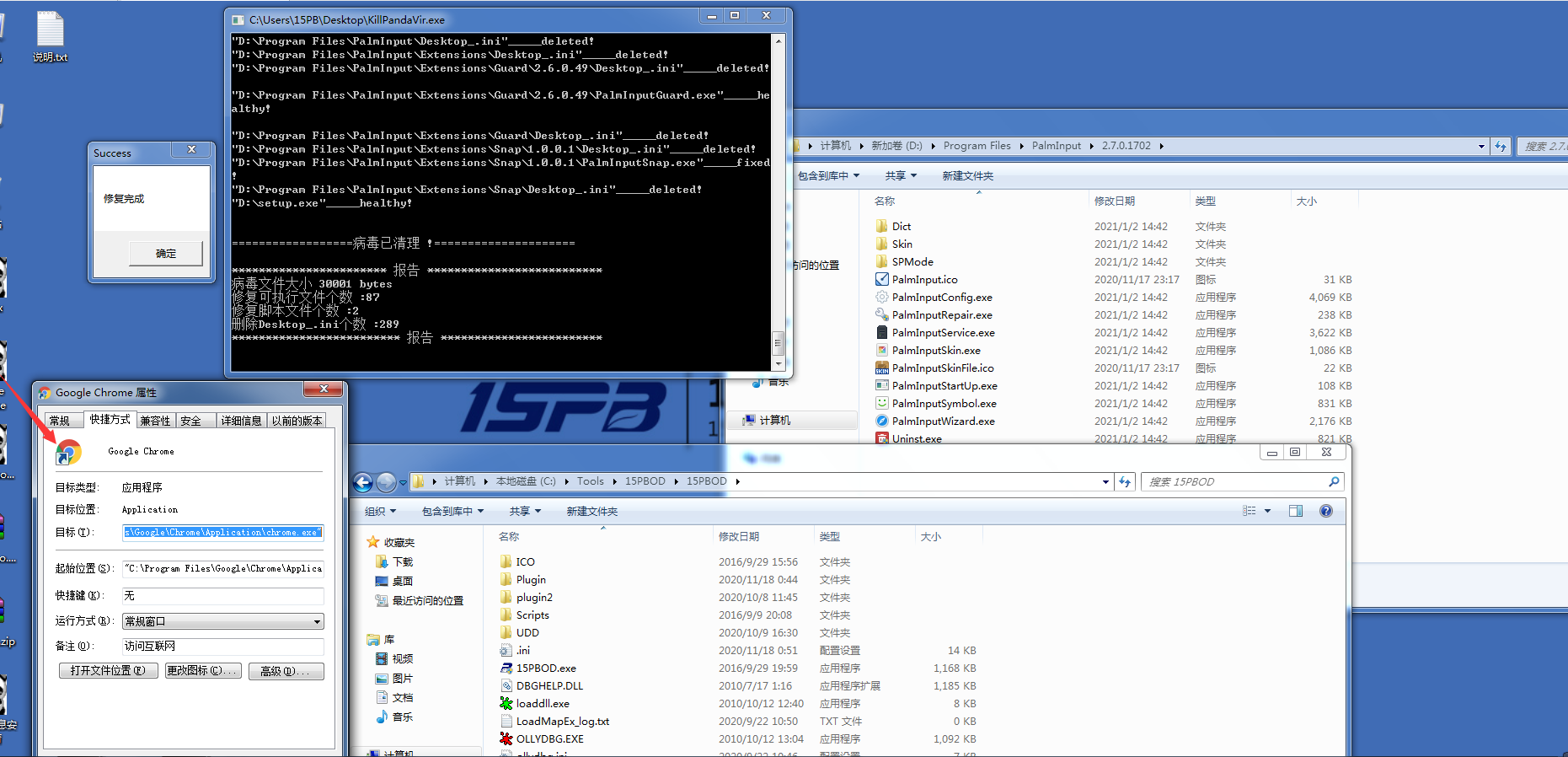
④遍历全盘删除Desktop\_.ini,修复受感染的文件，二进制文件和脚本文件要区别处理

**2、编写专杀工具，完成对恶意代码的清理与修复**



电脑已经成功感染熊猫烧香病毒

现在我们运行专杀工具来修复



这里快捷方式的图标没有改变是因为需要重启后才能恢复。

致 谢

正文用宋体小四，内容限1页，一律向15PB信息安全研究院谢意。