****

**分析报告**

|  |  |
| --- | --- |
| **样本名** |  |
| **班级** | **42期** |
| **作者** | **王昊** |
| **时间** |  |
| **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 2](#_Toc19916)

[1.1 样本信息 2](#_Toc23761)

[1.2 测试环境及工具 3](#_Toc17493)

[1.3 导入表 3](#_Toc187)

[1.4 查壳 4](#_Toc8353)

[2． 具体行为分析 5](#_Toc30680)

[2.1 文件操作 5](#_Toc27371)

[2.2 行为监控 7](#_Toc3904)

[2.3 网络监控 9](#_Toc12935)

[2.4 执行监控 9](#_Toc15627)

[2.5 注册表监控 10](#_Toc4324)

[3.恶意代码分析 11](#_Toc2526)

[3.1 脱壳 11](#_Toc5457)

[3.2 整体流程 13](#_Toc21503)

[3.3 代码块405250分析 14](#_Toc26708)

[3.4 代码块40819C分析 16](#_Toc8170)

[3.5 代码块40D18C分析 18](#_Toc10837)

[3.6 代码块40D088分析 23](#_Toc2755)

[4． 解决方案 26](#_Toc28893)

[参考文献 29](#_Toc21780)

# 1．样本概况

## 1.1 样本信息

病毒名称：熊猫烧香病毒

所属家族：

MD5值： 512301C535C88255C9A252FDF70B7A03

SHA1值： CA3A1070CFF311C0BA40AB60A8FE3266CFEFE870

CRC32： E334747C

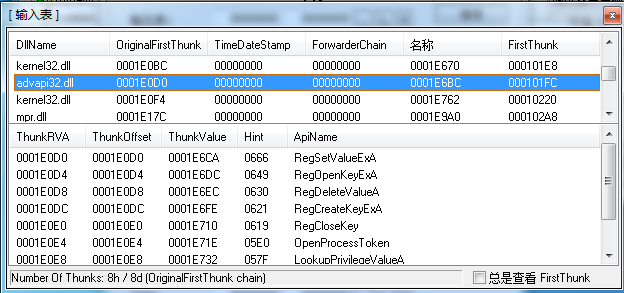
病毒行为：

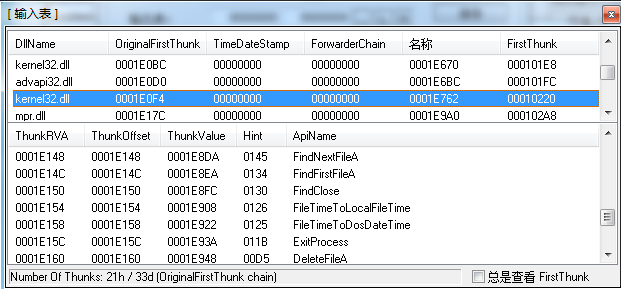
添加系统自启项，感染文件，拷贝程序到系统目录

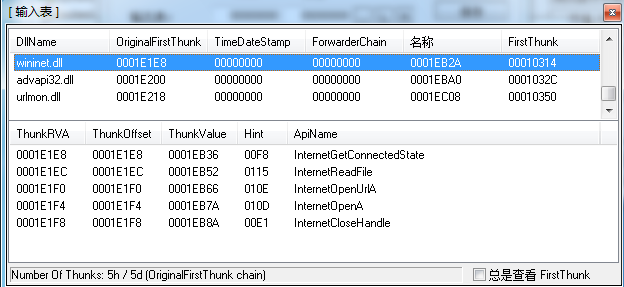
## 1.2 测试环境及工具

32位win7，火绒剑，OD，PEiD，exeinfo，IDA

**1.3 导入表**

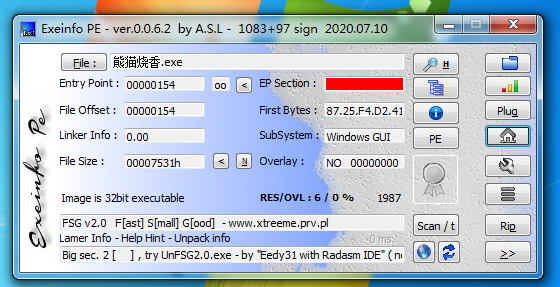




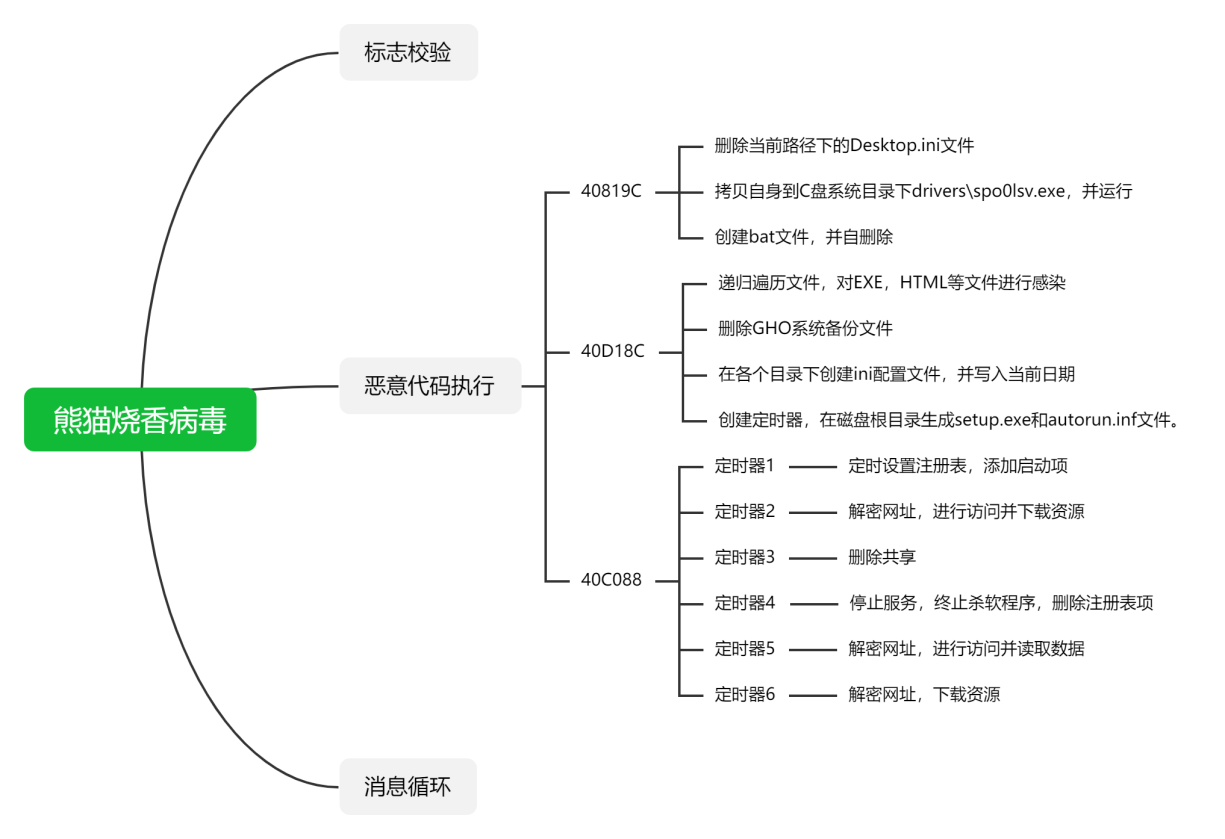


## 1.4 查壳

Exeinfope工具进行壳查询：结果为FSG v2.0压缩壳。



其思维导图大致如下：



# 具体行为分析

## 2.1 文件操作

主要行为有：

1.在各个文件目录下创建后缀名为ini的隐藏文件，其内容为记录的是当前日期。

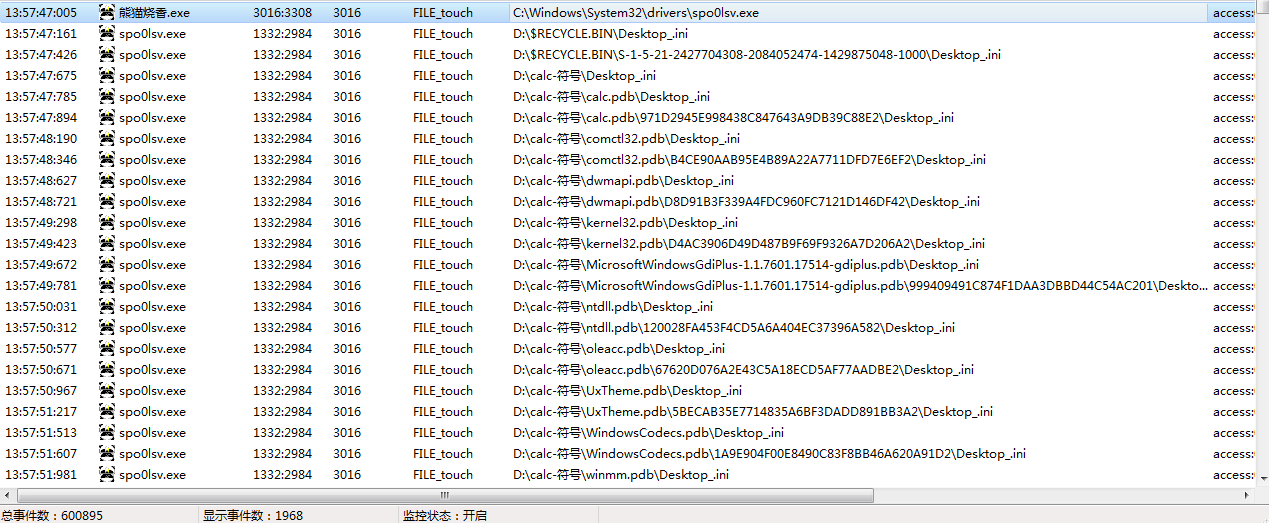
2.拷贝一份病毒文件，并以隐藏的方式放到C盘系统目录。

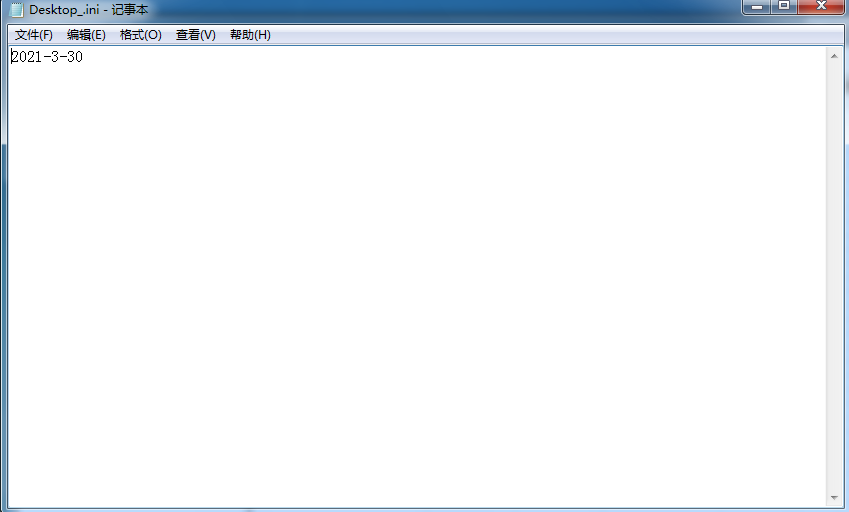
3.在Temp文件目录下创建图像为熊猫烧香的图片

4.感染后缀名为exe的PE文件以及html的文件

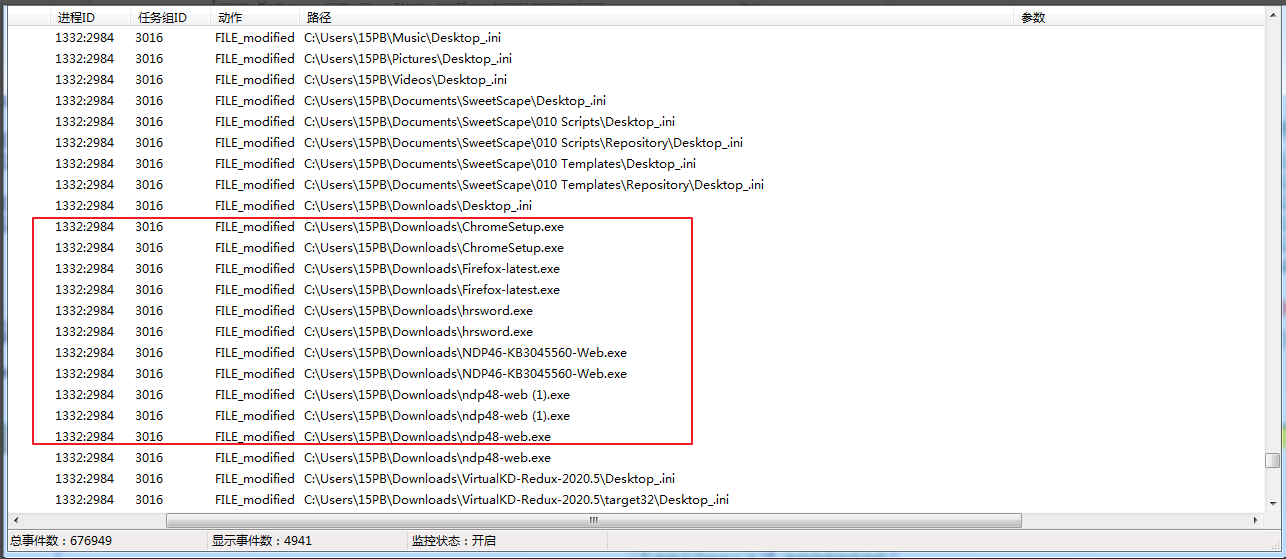
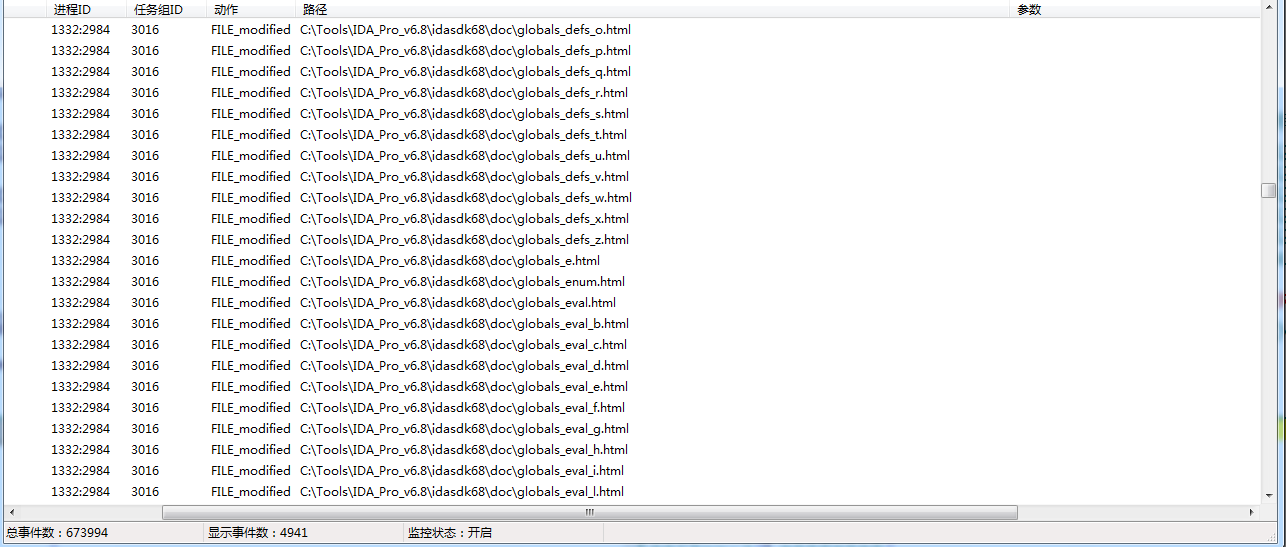
5.删掉了部分图片

1.在各个文件目录下创建后缀名为ini的隐藏文件，其内容为记录的是当前日期。

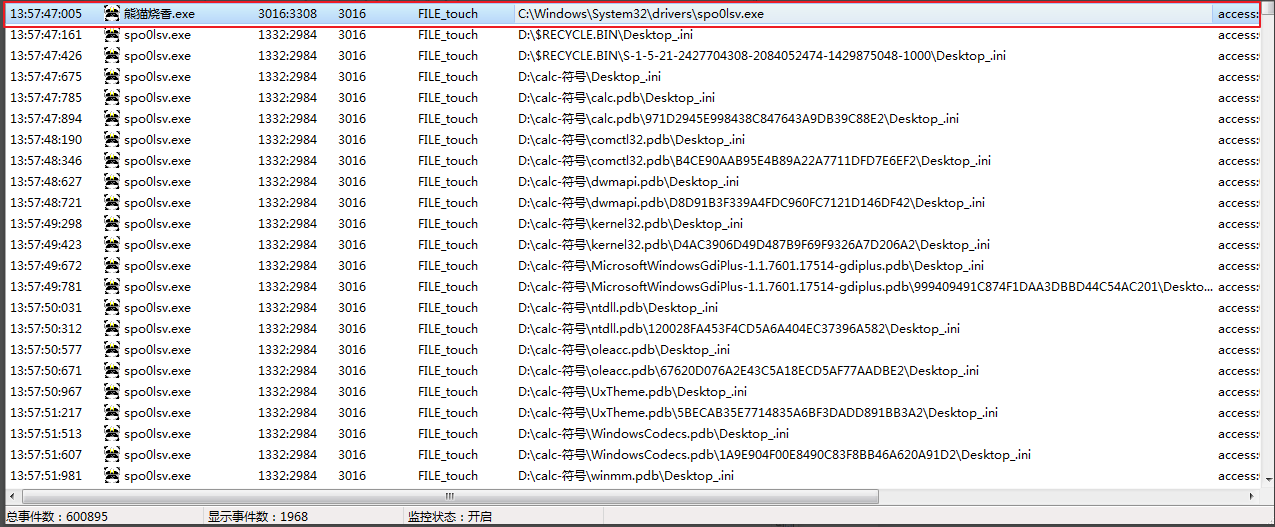


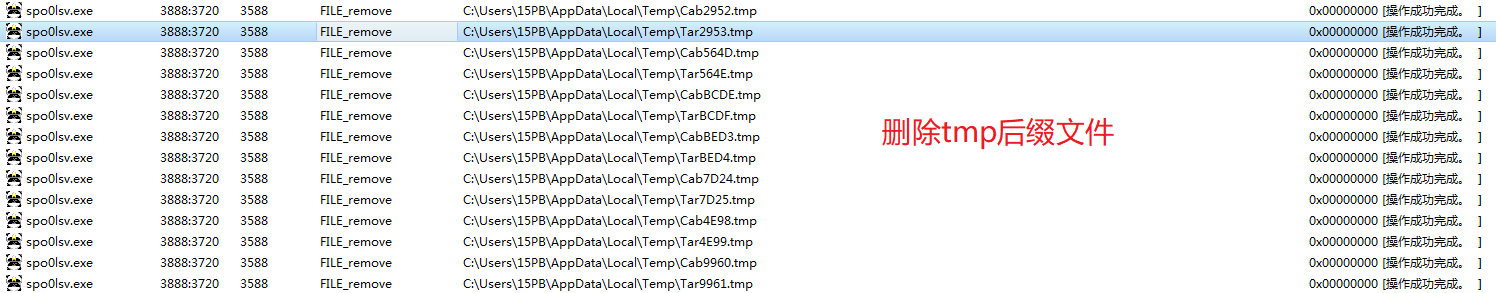


2.感染后缀名为exe的PE文件以及html的文件



1. 拷贝一份病毒文件，并以隐藏的方式放到C盘系统目录。





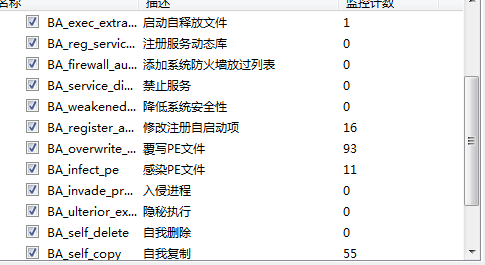
## 2.2 行为监控

1.自我复制，并拷贝到C盘系统目录下（隐藏），并启动

2.修改注册自启动项，将病毒程序添加到自启项中

3.感染PE文件，并进行重写覆盖

4.自我复制setup.exe到各个文件目录下（隐藏）





## 2.3 网络监控

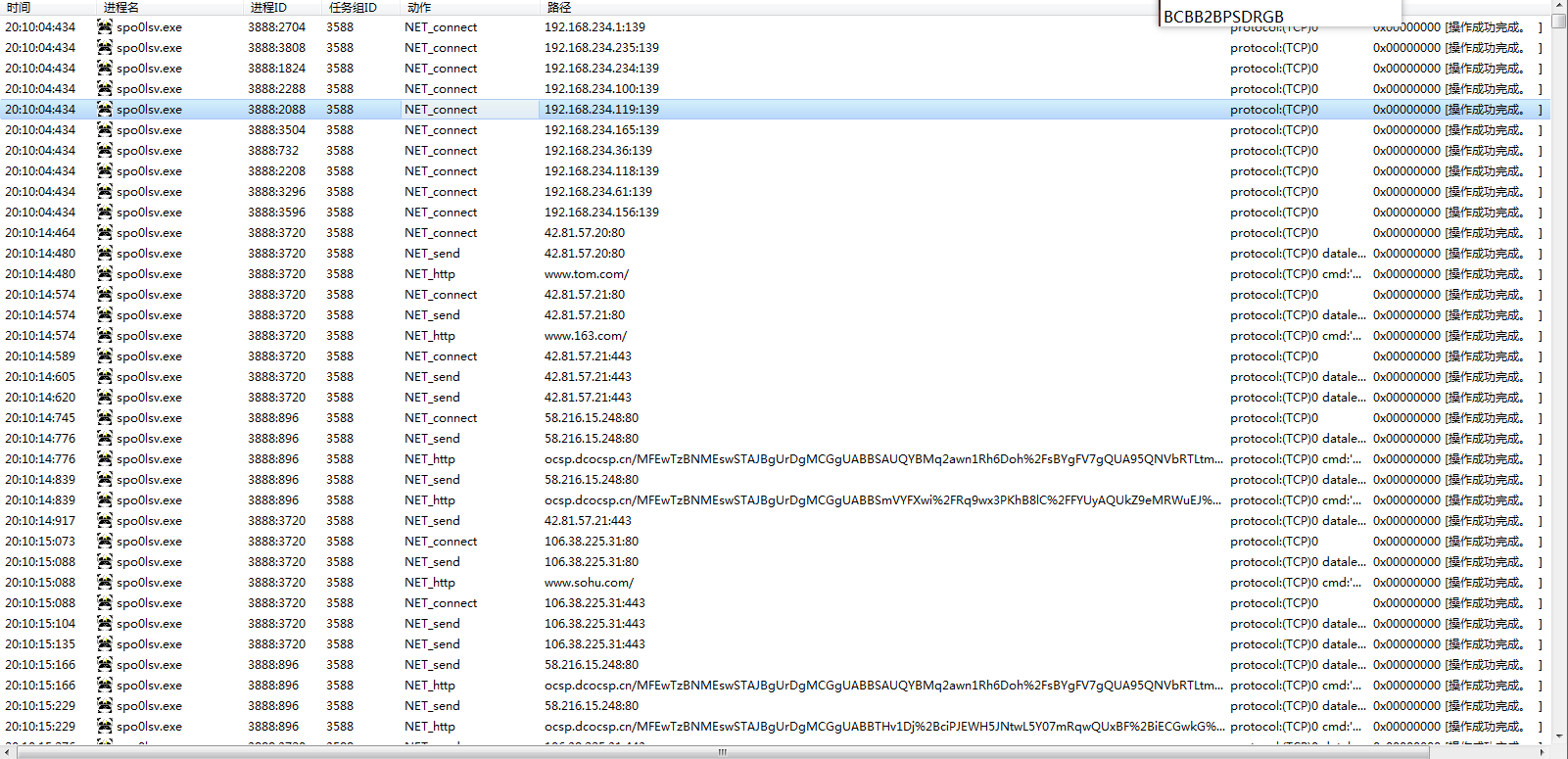
存在大量http请求可以实施DDos攻击，也可以发送数据包，以便上传私密信息到服务器，存在网络连接，以便用户从服务器下载木马等恶意程序。

其大体行为主要分为：

1.对局域网内的ip进行了访问

2.对外网42.81.57.16:80进行了连接访问

3.向相关网址发送数据



## 2.4 执行监控

主要行为有：

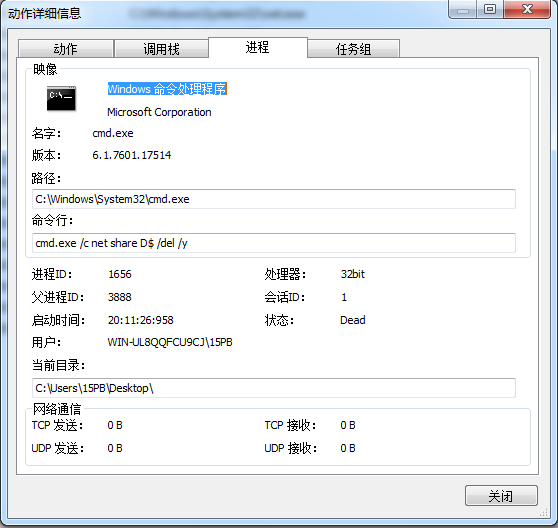
1.创建子进程并结束掉熊猫烧香主进程

2.打开cmd命令用于删除网络共享

3.建立相关网络连接

4.执行完毕后，结束cmd命令和网络连接





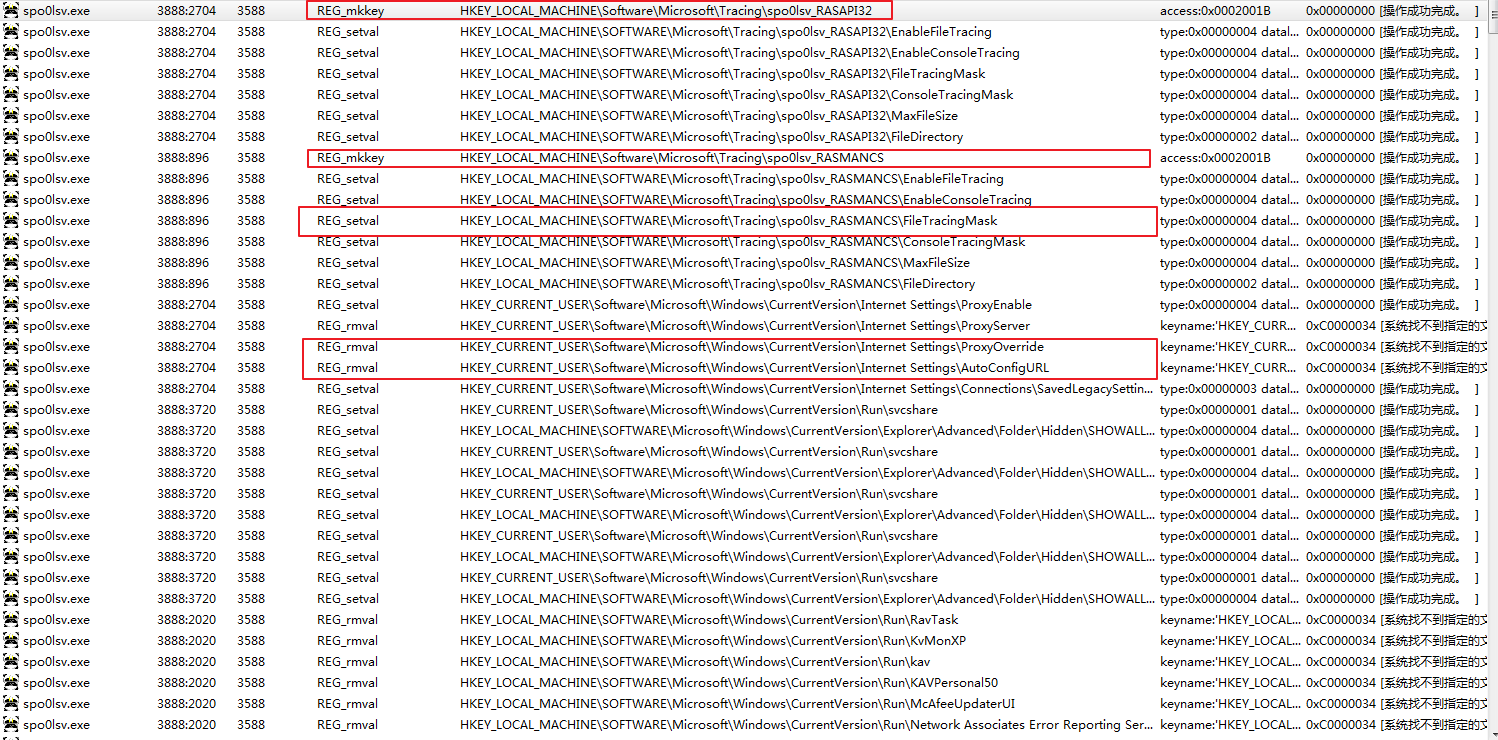
通过cmd命令删除了网络共享。

## 2.5 注册表监控

主要行为有：

1.删除一些注册表启动项（猜测是杀毒软件相关的exe）

2.将病毒自身程序添加至系统自启项



# 3.恶意代码分析

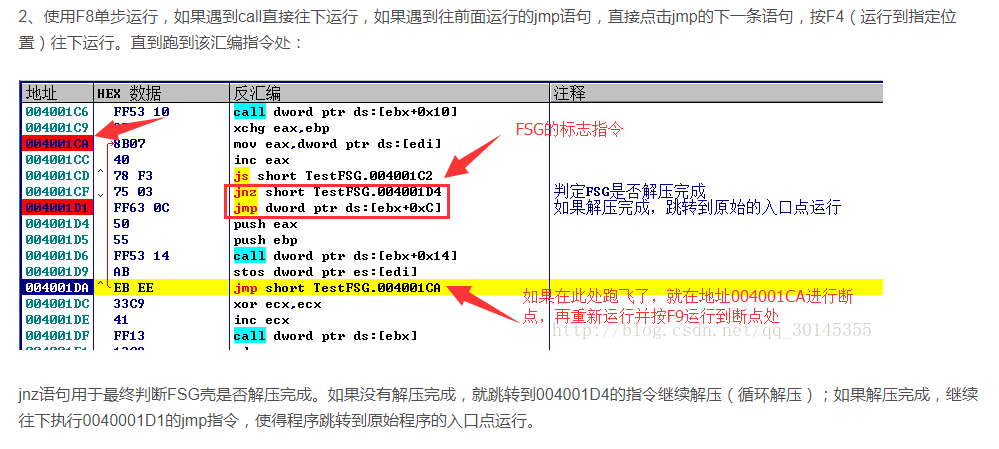
## 3.1 脱壳

进行手工脱壳：

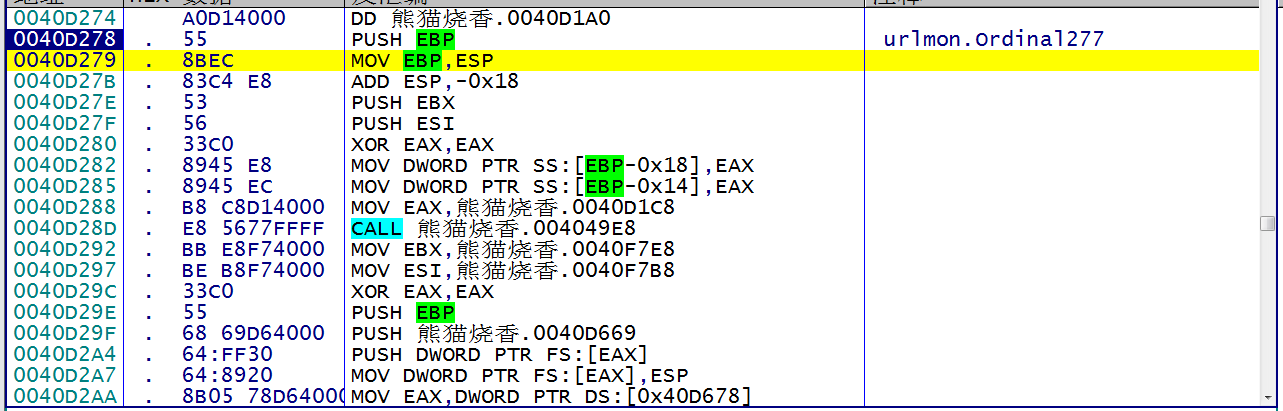
通过查阅资料可以查到，FSG跳转到OEP处附近的特征码：

78 F3 Jnz short TestFSG.004001D4

75 83 Jmp dword ptr ds:[ebx+0xC]

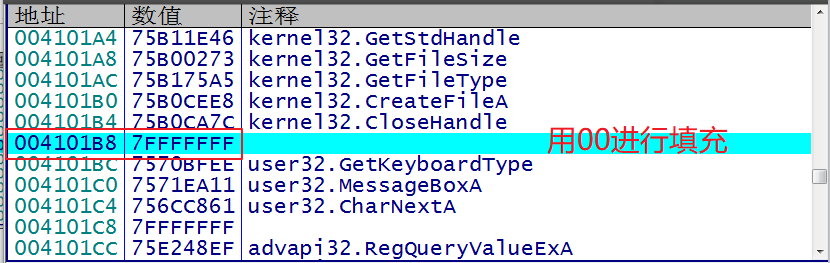


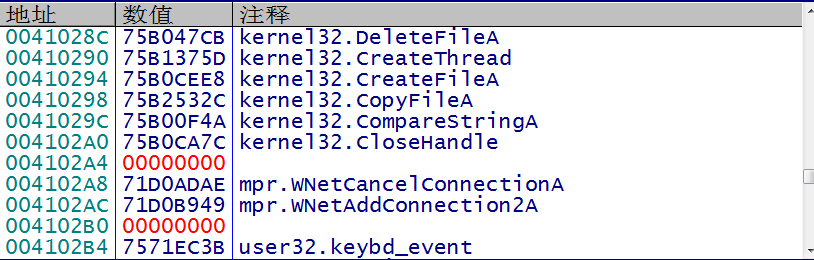
跳转到OEP后，进行Dump：



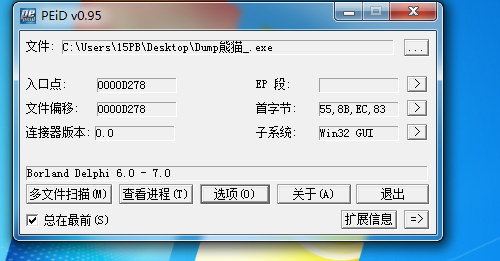
Dump之后进行IAT修复：

由于该程序对IAT做了处理，需要改回来：





Dump完毕后，PEID深度扫描查看编写语言：（Delphi调用约定：fastcall，寄存器传参）。



## 3.2 整体流程

脱壳后使用IDA进行静态分析，并导入Delphi标签

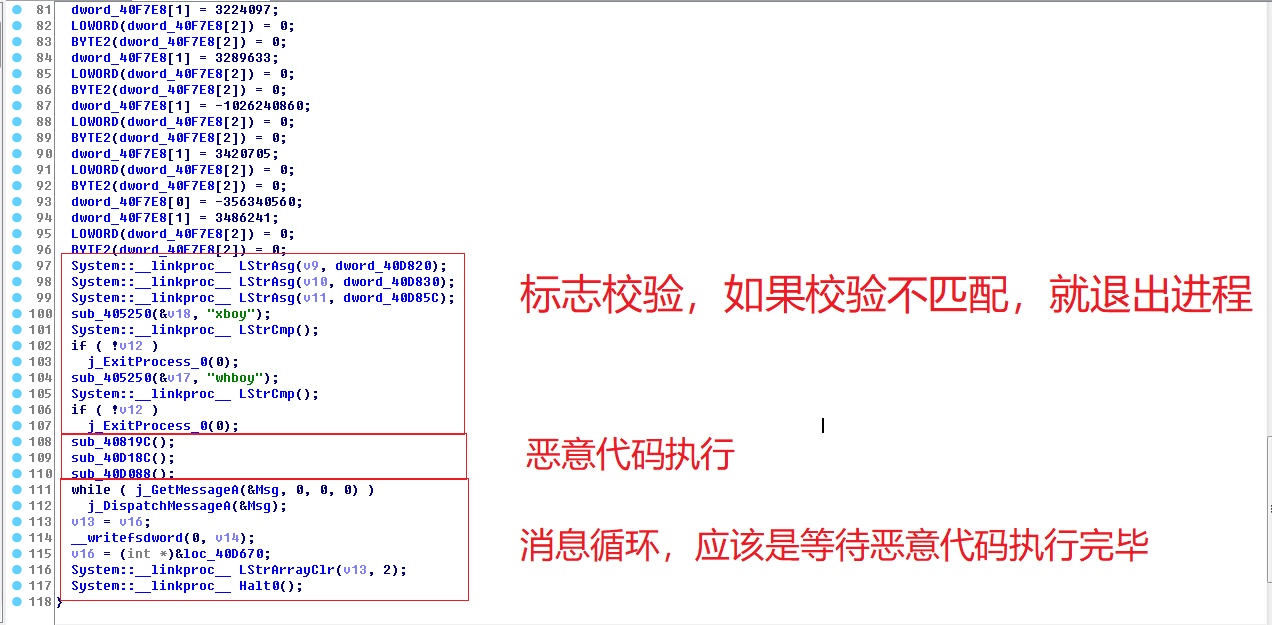
可以将程序分为以下几个阶段：

1.数据初始化段

2.字符串校验段，对获取的标识进行校验，如果相同则执行后续的代码，如果不相同，则退出进程

3.代码执行段，可以明显看到后面的while消息循环，循环结束应该就是恶意代码执行完毕。

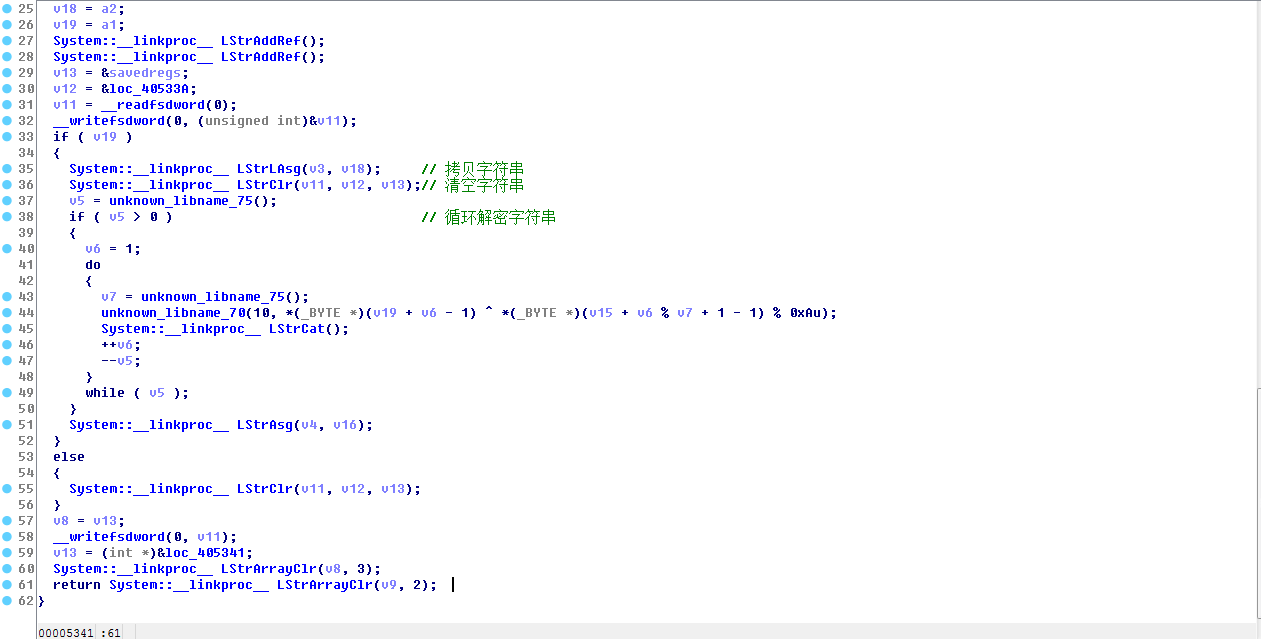




## 3.3 代码块405250分析

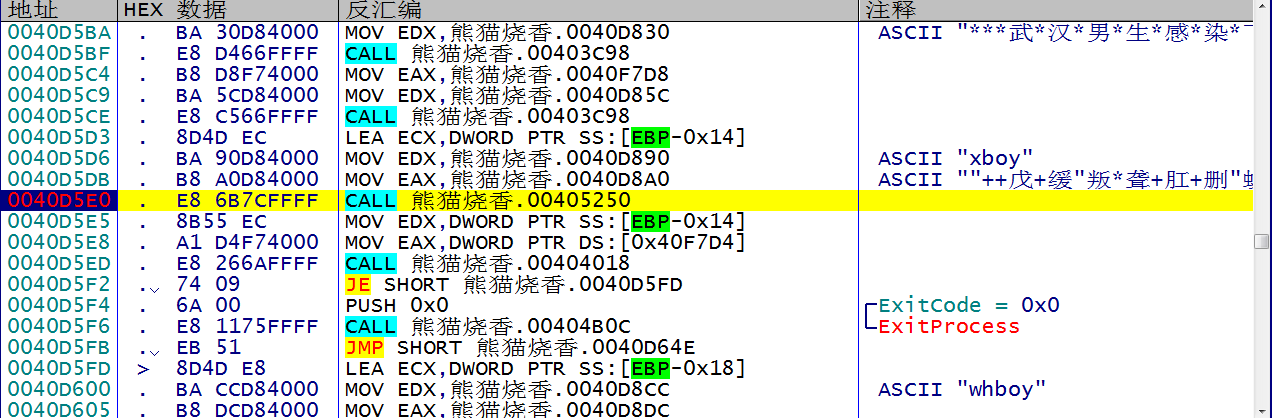
主要是为了进行标志位校验

IDA静态分析



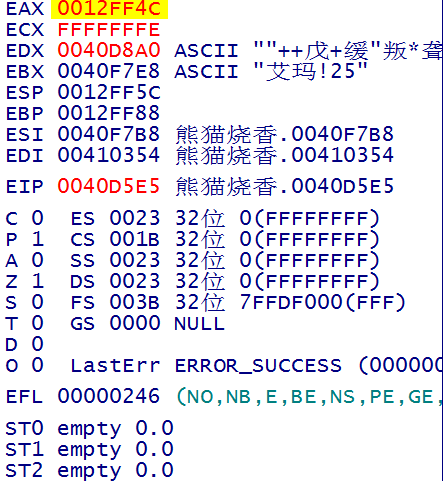
OD进行动态调试：

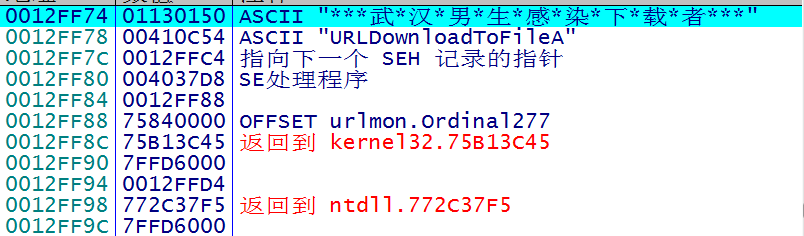
参数：ECX（局部变量应该是），EDX，EAX



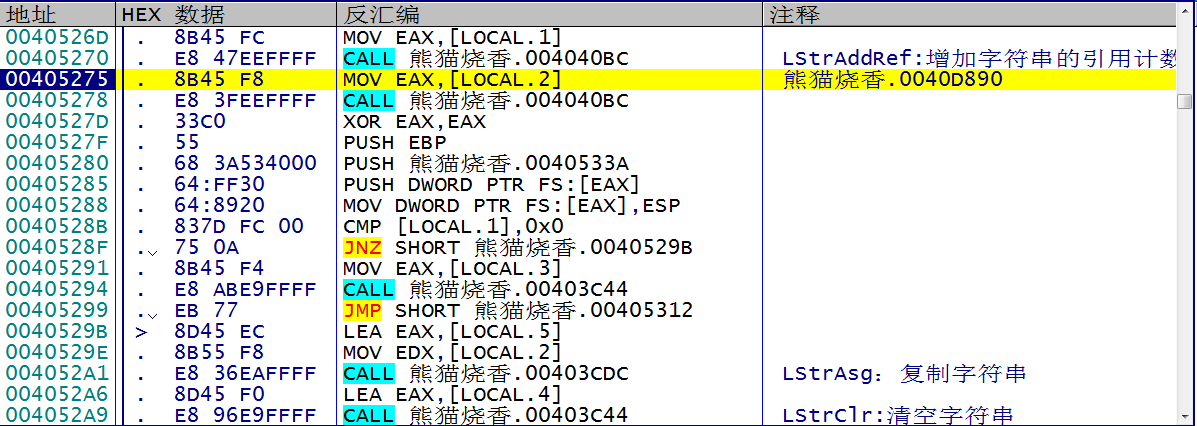
单步步过查看寄存器以及堆栈情况：

发现，该函数获取了一个字符串保存至参数1：EBP-0x14中

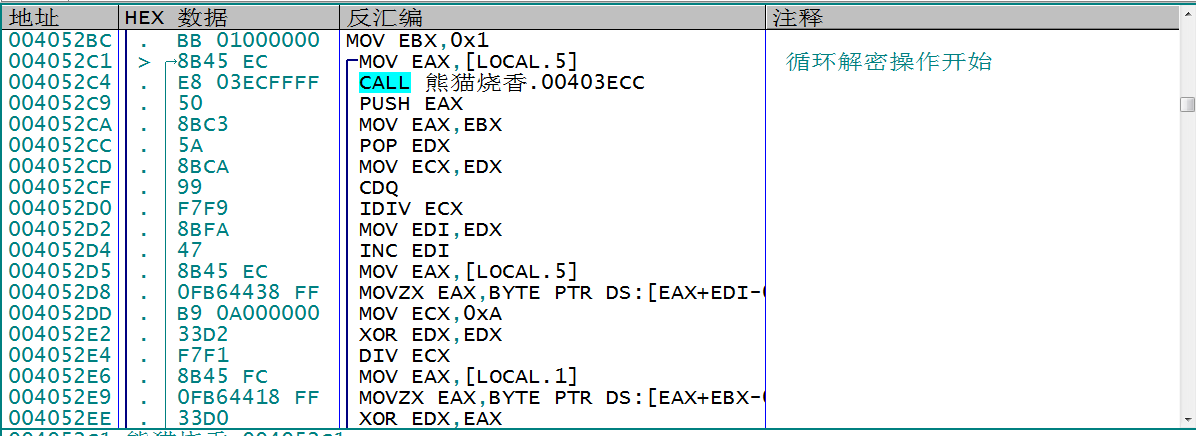


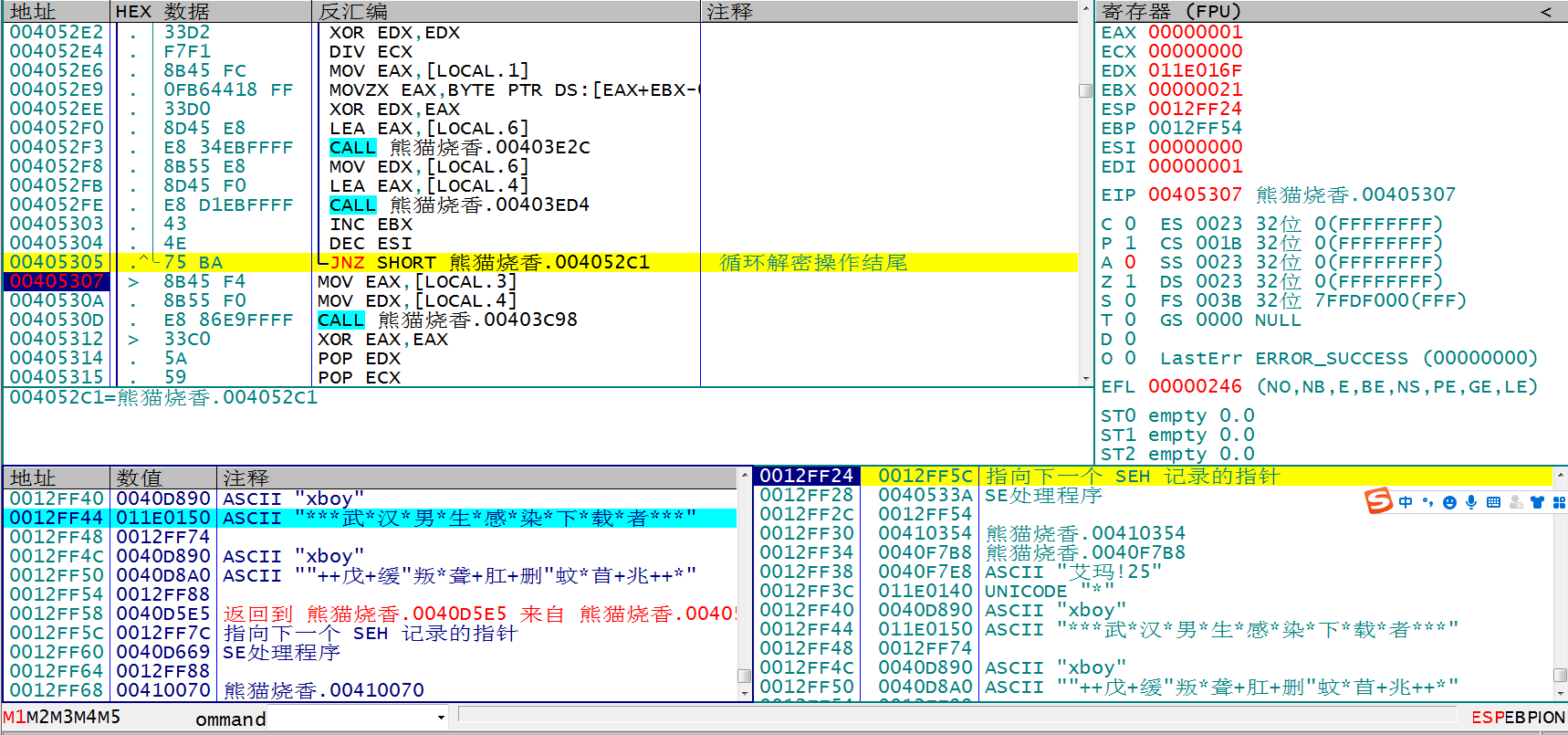


函数内部分析：



函数内部有一个循环，单步跟踪分析后，发现应该是字符串解密操作：





## 3.4 代码块40819C分析

主要功能：首先判断当前目录下是否存在Desktop.ini，若存在则删除，然后判断启动的病毒文件是否在C盘系统目录，不在则结束该进程，并自我拷贝一份文件复制到C盘系统目录下drivers\spo0lsv.exe，并启动该路径下的病毒程序。创建bat文件，并自删除。

### 3.4.1判断当前目录下是否存在ini文件，若存在则删除



### 3.4.2判断启动的病毒文件是否在C盘系统目录：

不在则结束该进程，并自我拷贝一份文件复制到C盘系统目录下drivers\spo0lsv.exe，并启动该路径下的病毒程序。



### 3.4.3 若本程序是在该系统路径运行的：

对读取的自身PE文件，判断是否存在标志字符串"WhBoy...."字符串，如果当前运行的程序有这个字符串，说明当前运行的程序是被感染的文件 (感染：在原程序的PE文件前面写入病毒程序),若当前运行的是被感染的文件，则读取自身，将原文件的PE拷贝出来，以附加的方式写入到文件中,并编写并执行bat批处理文件：意思就是删除被感染的文件，运行原文件创建bat文件，并自删除



创建并写入bat文件：

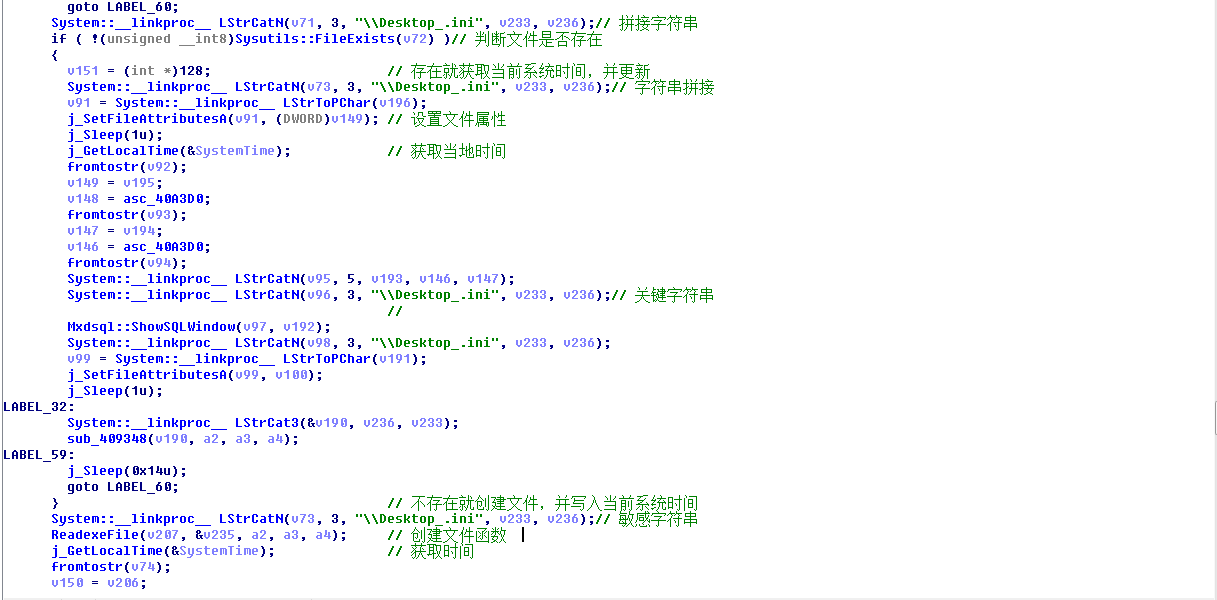


## 3.5 代码块40D18C分析

主要功能：递归遍历文件，对EXE,HTML等文件进行感染。删除GHO系统备份文件。创建ini配置文件，更新当前日期。创建定时器，在磁盘根目录生成setup.exe和autorun.inf文件。

创建线程，通过139，445端口感染局域网主机。

### 3.5.1判断各个目录下是否存在ini文件，不存在就创建，存在就更新当前日期。

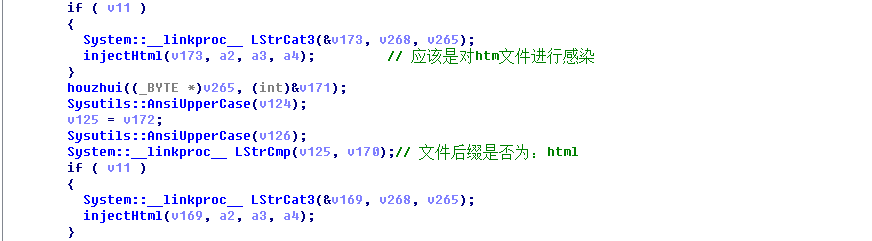




### 3.5.2 递归遍历文件，对EXE,HTML等文件进行感染。删除GHO系统备份文件。







InjectExe感染EXE，SRC，COM，PIF:在文件开头捆绑病毒程序，并在文件结尾加入”whBoy...”字样



InjectHtml感染htm、html、asp、php、jsp文件：解密一串字符串，并写入文件



### 3.5.3 创建定时器，在磁盘根目录生成setup.exe和autorun.inf文件。

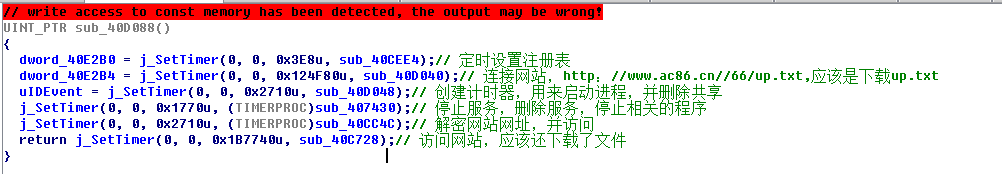




### 3.5.4创建线程，通过139，445端口感染局域网主机。



## 3.6 代码块40D088分析



主要功能：设置注册表自启项，解密URL，下载资源并运行。删除共享，停止并删除杀毒软件服务。

### 3.6.1 定时设置注册表，添加启动项



### 3.6.2 解密网址，进行访问并下载资源



### 3.6.2 创建计时器，启动进程，删除共享，并且调用了之前的访问网址操作



### 3.6.3停止服务，终止杀软程序，删除注册表项



### 3.6.4解密网址，访问网站，读取访问的内容



### 3.6.5解密网址，访问网站，下载资源



# 解决方案

**4.1-病毒特征**

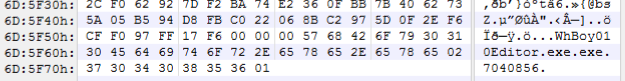
病毒文件的哈希值如下：

MD5: 512301C535C88255C9A252FDF70B7A03

SHA1: CA3A1070CFF311C0BA40AB60A8FE3266CFEFE870

CRC32: E334747C

被感染文件中，文件最后有感染表示标识：WhBoy + 原文件名 + exe + + ascii码为1的字符 + 随机数+ ascii码为2的字符



**4.2-解决思路**

1.结束相关进程

2.修复注册表

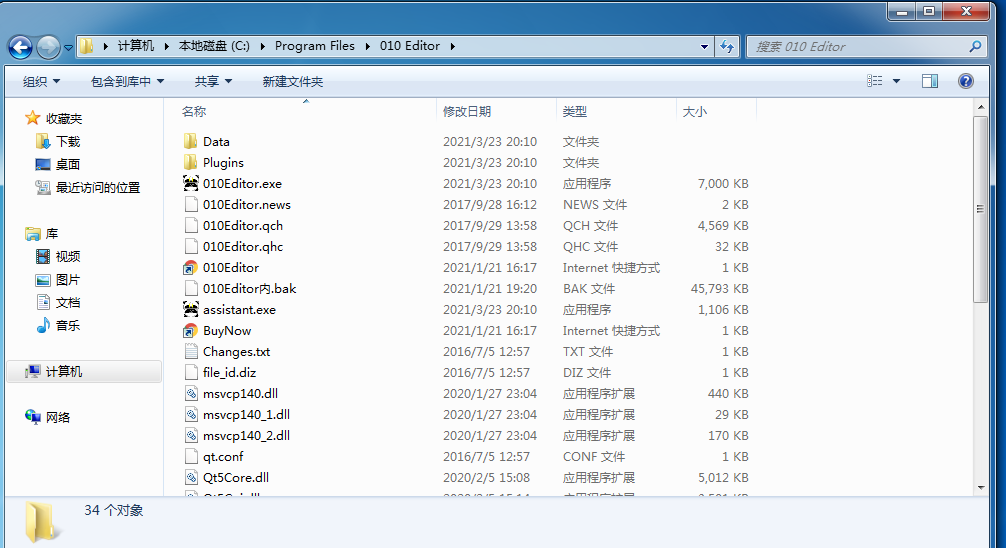
3.删除相关ini文件

4.恢复PE文件

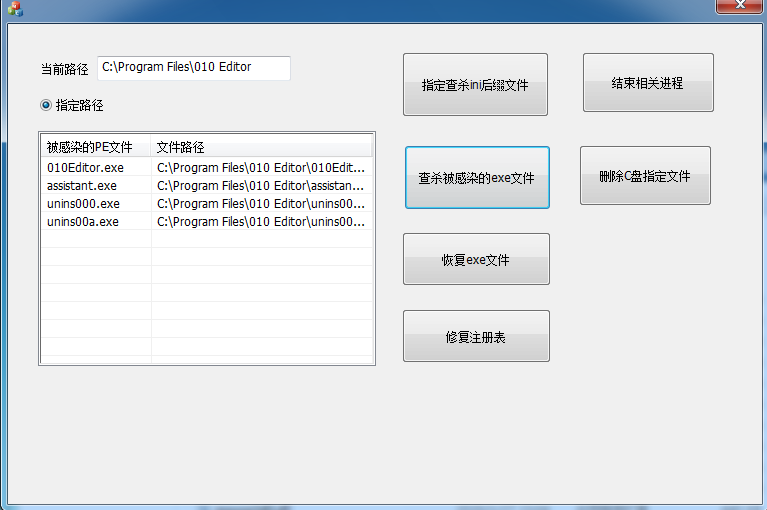
5.删除释放在C盘根目录下的spo0lsv.exe病毒程序。

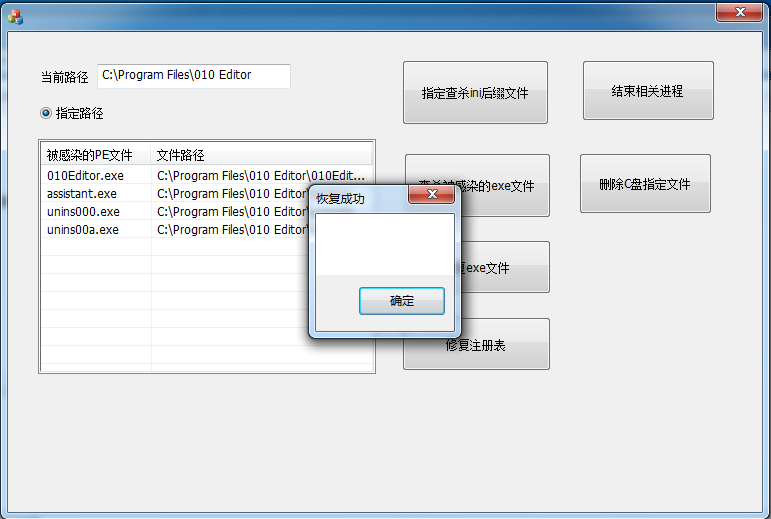
**4.3-专杀工具**

修复前：

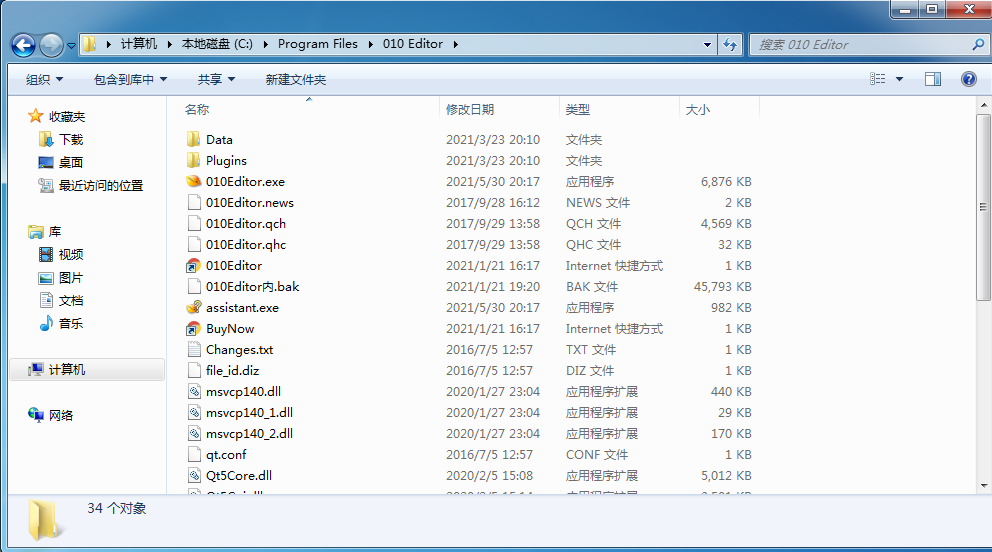


运行程序截图：





修复后的效果：



参考文献

1. 看雪学院
2. HACK编程技术详解
3. 吾爱破解