****

**分析报告**

|  |  |
| --- | --- |
| **样本名** | **3601病毒** |
| **班级** | **43期** |
| **作者** | **王昊** |
| **时间** | **2021.5.29** |
| **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 3](#_Toc29946)

[1.1 样本信息 3](#_Toc12547)

[1.2 测试环境及工具 4](#_Toc17848)

[1.3 分析目标 5](#_Toc12569)

[1.4 查壳 5](#_Toc9897)

[1.5 脱壳 5](#_Toc16978)

[2．具体行为分析 6](#_Toc20473)

[2.1 文件操作 6](#_Toc17420)

[2.2 行为监控 8](#_Toc5101)

[2.3 网络监控 9](#_Toc22121)

[2.4 注册表监控 10](#_Toc5448)

[2.5 进程监控 10](#_Toc12198)

[3．恶意代码分析 12](#_Toc24012)

[3.1 整体流程 13](#_Toc5386)

[3.2 对函数sub\_405A52进行跟进分析： 14](#_Toc15853)

[3.3 对函数sub\_405B6E进行跟进分析： 14](#_Toc23645)

[3.4 对函数sub\_40561A进行跟进分析： 17](#_Toc26350)

[3.5 对函数dra33.dll进行跟进分析： 29](#_Toc16907)

[4．总结 33](#_Toc31480)

[4.1 dll劫持原理 33](#_Toc344)

[4.2 特征码提取 33](#_Toc27380)

[参考文献 34](#_Toc18265)

# **1．样本概况**

## 1.1 样本信息

病毒名称：lpk劫持病毒

文件: C:\Users\15PB\Desktop\3601.exe

大小: 24576 bytes

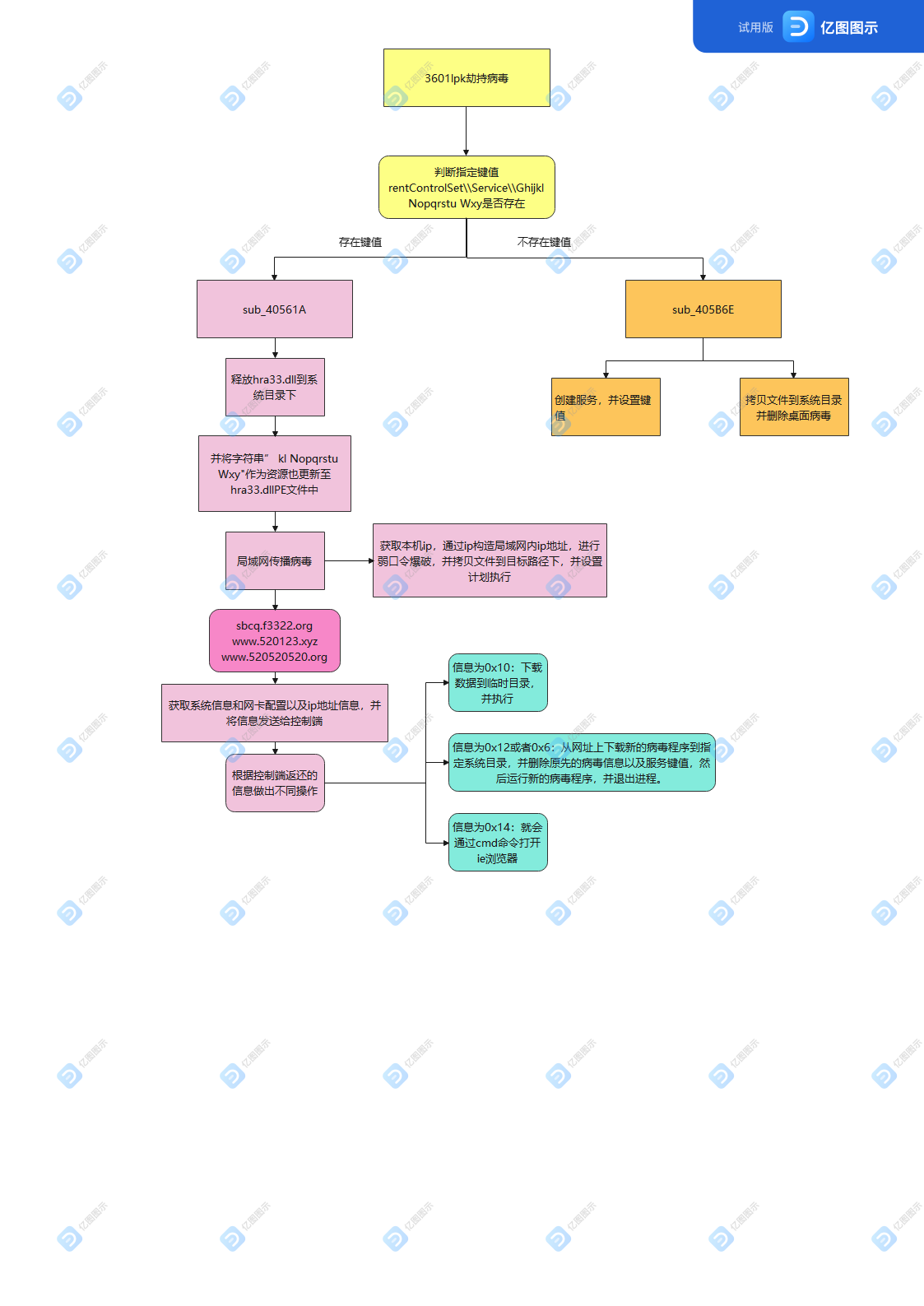
文件版本:7.02.2600.5512 (xpsp.080413-0852)

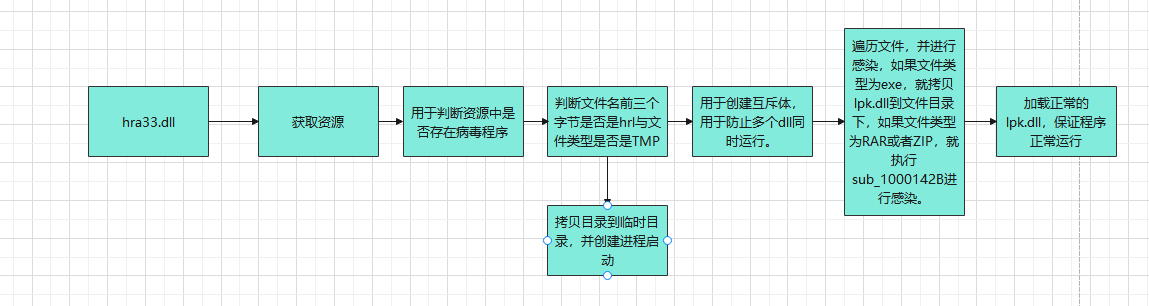
修改时间: 2015年9月29日, 13:10:48

MD5: B5752252B34A8AF470DB1830CC48504D

SHA1: AEC38ADD0AAC1BC59BFAAF1E43DBDAB10E13DB18

CRC32: 4EDB317F





## 1.2 测试环境及工具

32位win7，火绒剑，OD，PEiD，exeinfo，IDA

## 1.3 分析目标

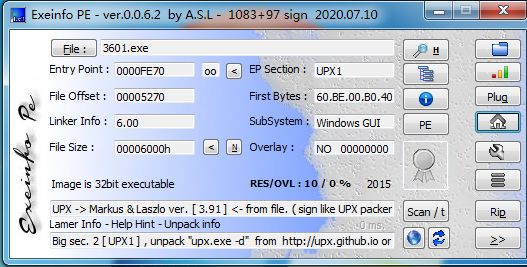
1.提取病毒样本

2.分析病毒行为

3.分析病毒代码细节，获取其执行流程

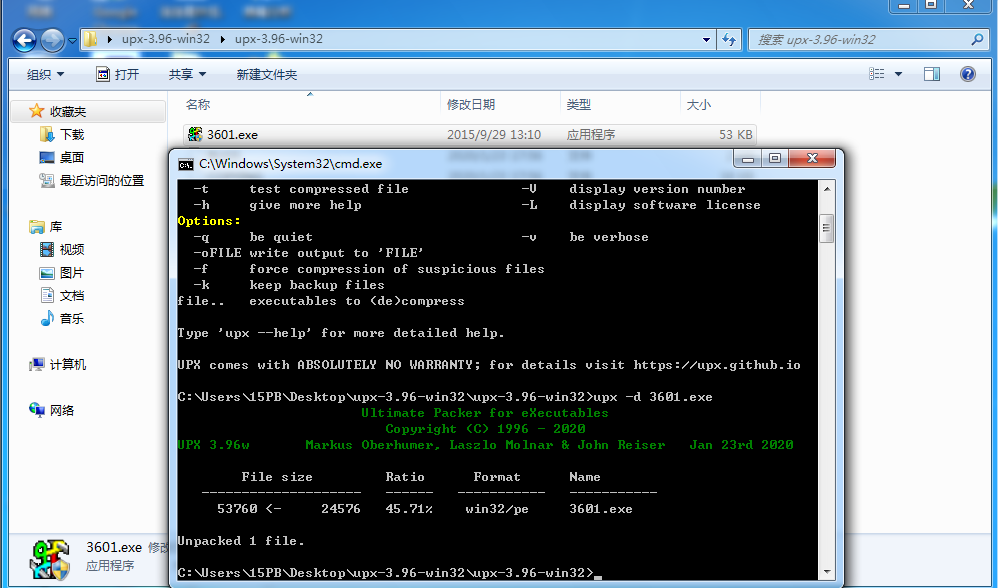
## 1.4 查壳

Exeinfope工具进行壳查询：结果为UPX压缩壳。



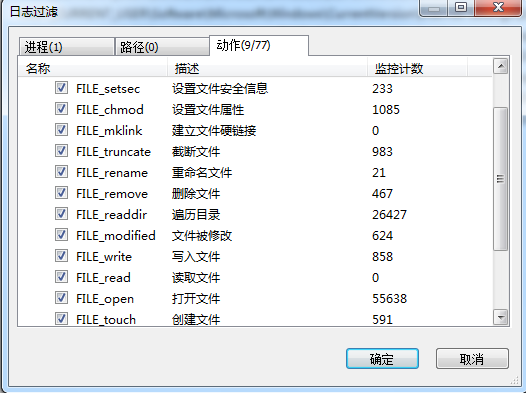
## 1.5 脱壳

通过网上UPX官网下载脱壳工具，进行脱壳，脱壳后，原病毒文件体积变大。

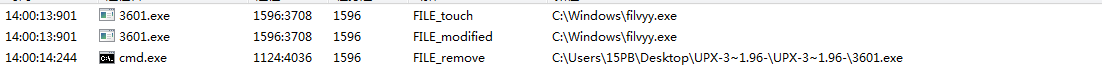


# 2．具体行为分析

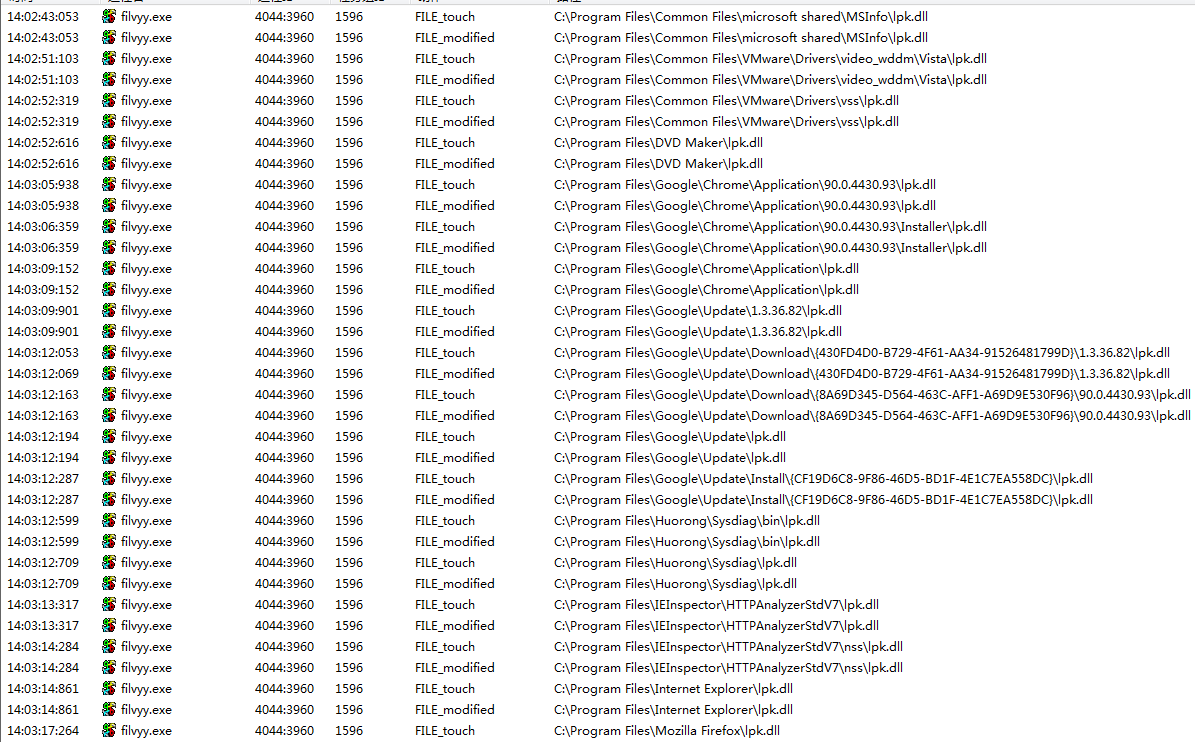
## 2.1 文件操作



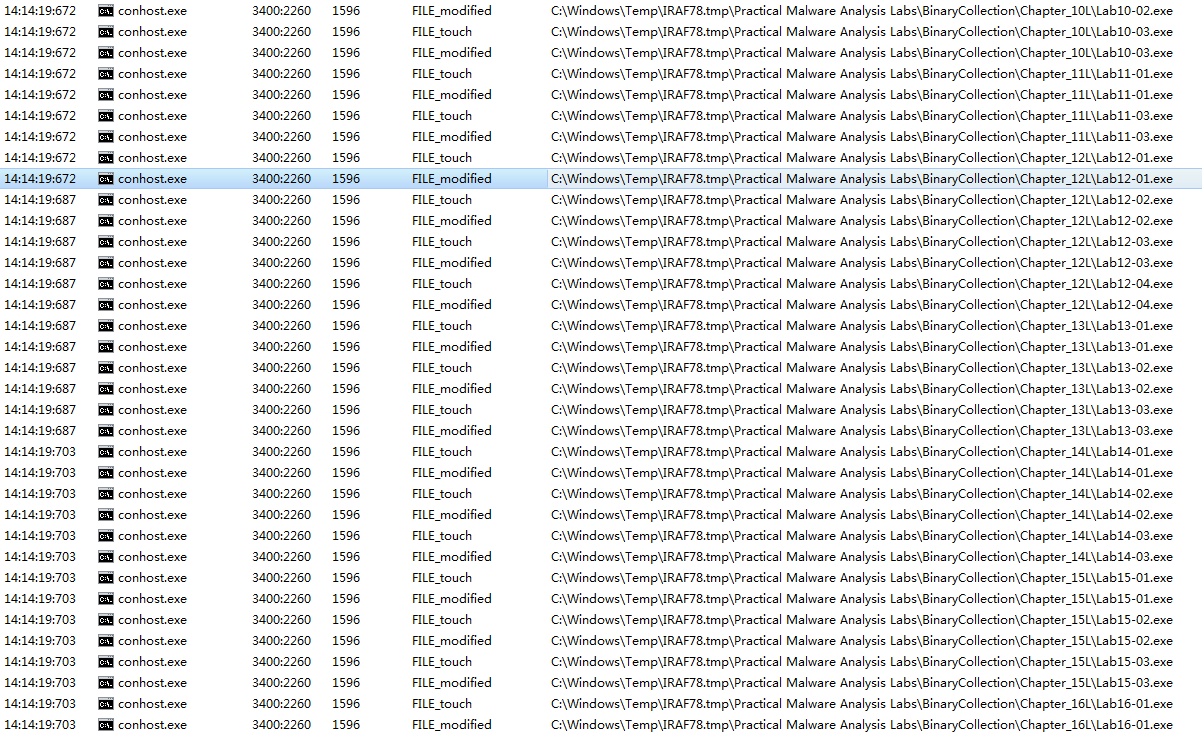
1.在C盘Windows目录下创建文件，并写入内容，然后自我删除在桌面上的病毒文件。

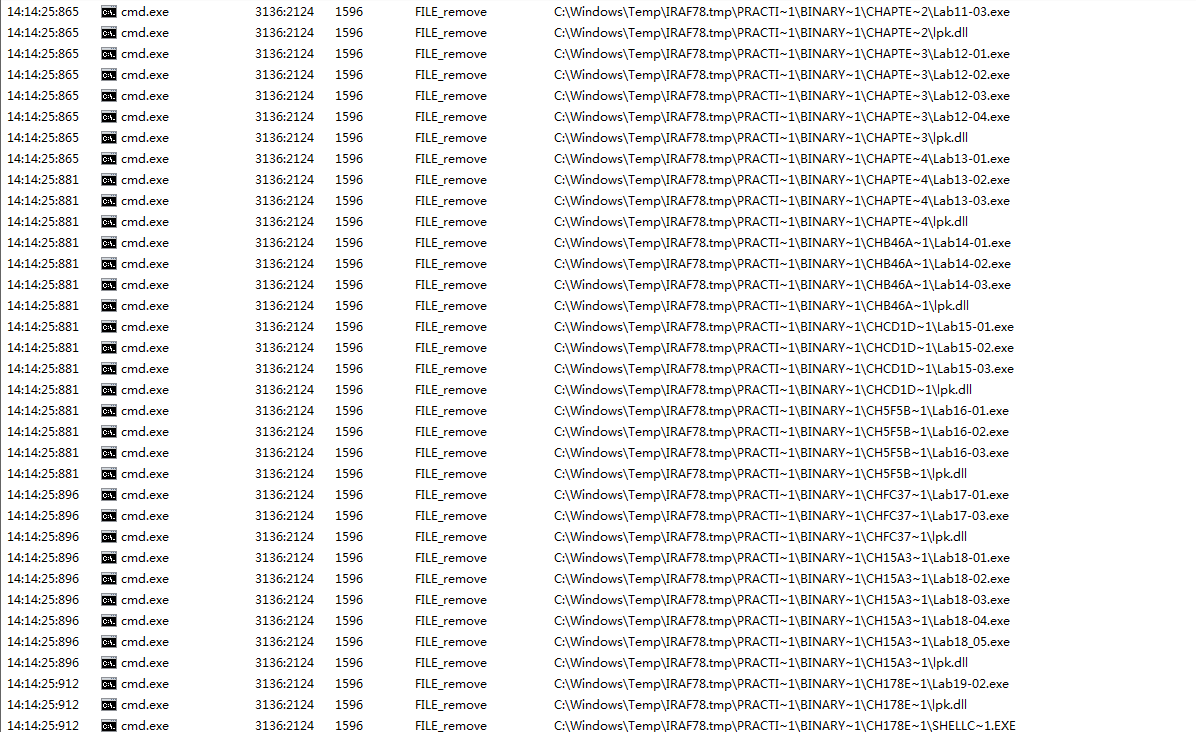


1. 在各个目录下创建lpk.dll，并写入内容



1. 创建大量的文件并写入内容，然后删除





## 2.2 行为监控



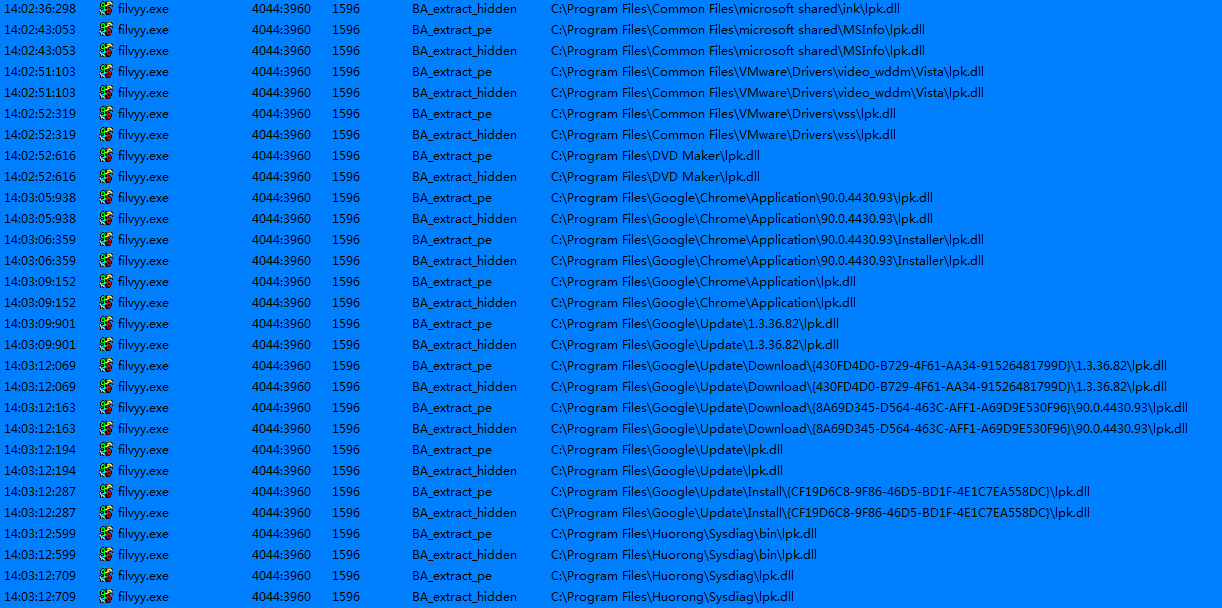
1. 自我复制到C盘Windows目录下，并释放PE文件filvyy.exe



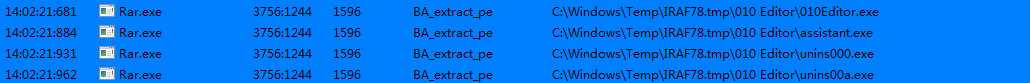
1. 释放hra33.dll到C盘系统目录下，释放RCXA266.tmp文件到C盘目录下。



1. 并遍历文件，释放lpk.dll到各个文件目录下。



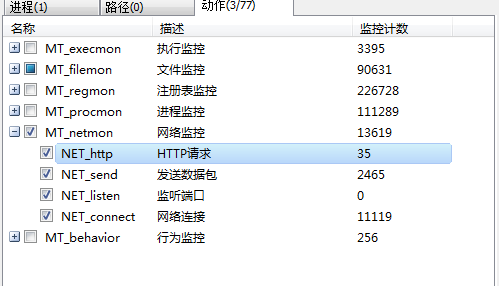
4.创建cmd，Rar，conhost等进程



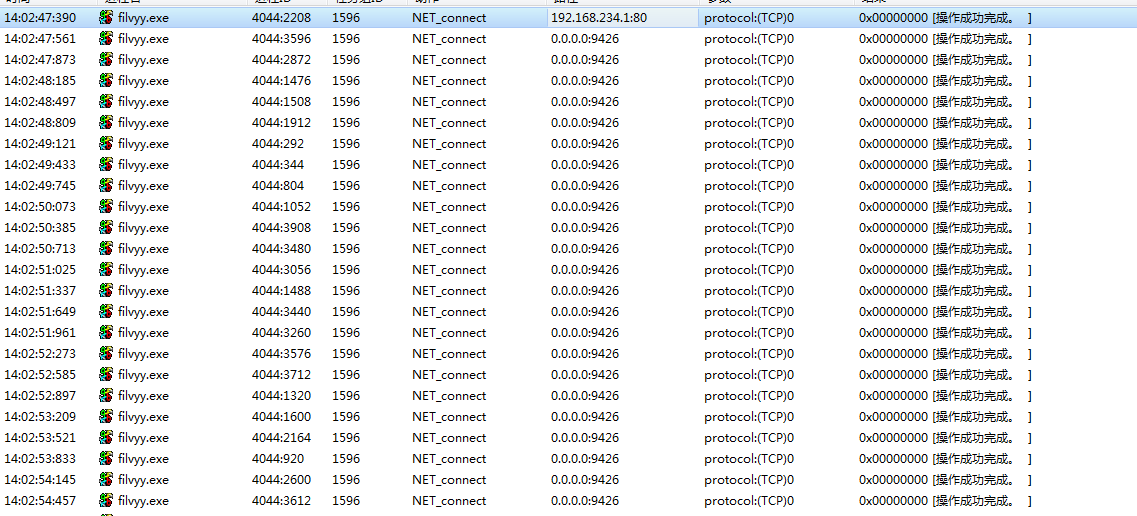




## 2.3 网络监控

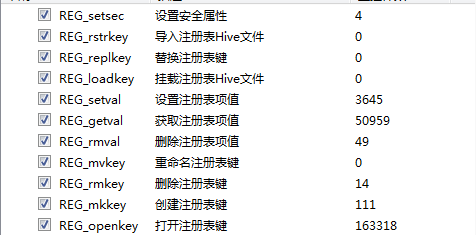
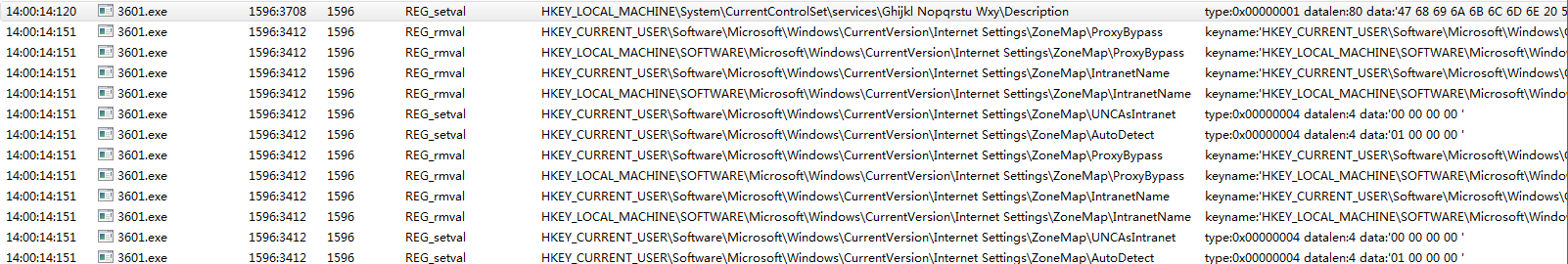


对ip为192.168.234.1：80进行网络连接并发送数据包



## 2.4 注册表监控

修改了注册表项值，并创建了注册表键

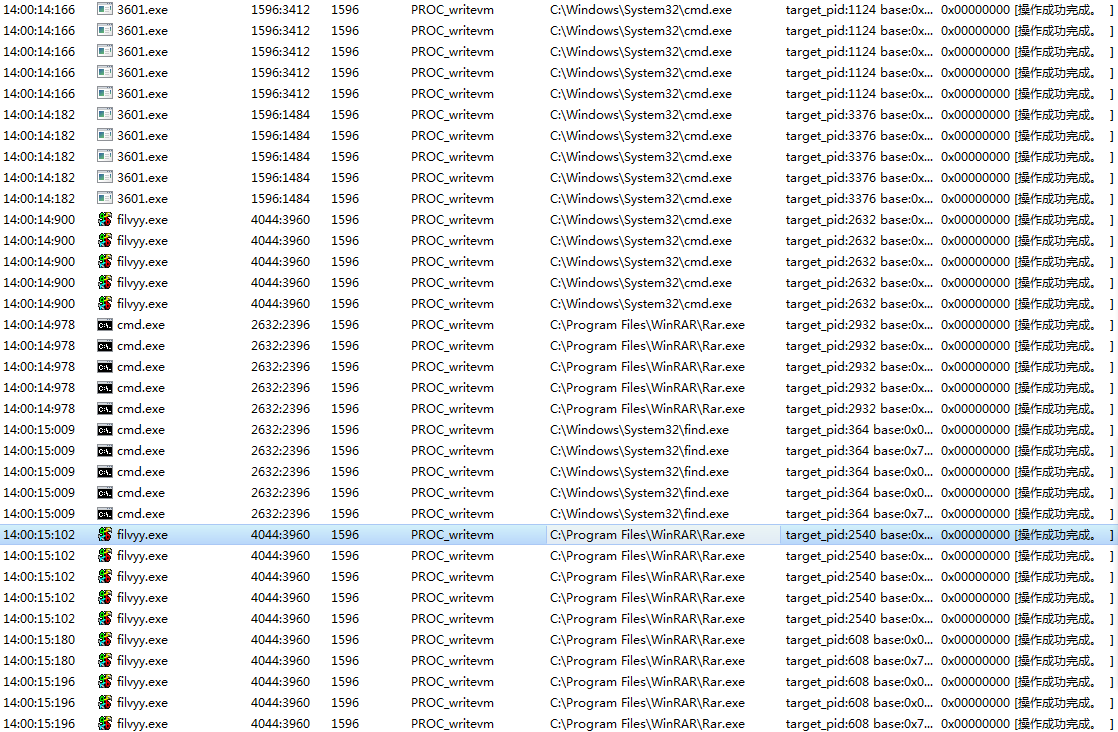


## 2.5 进程监控

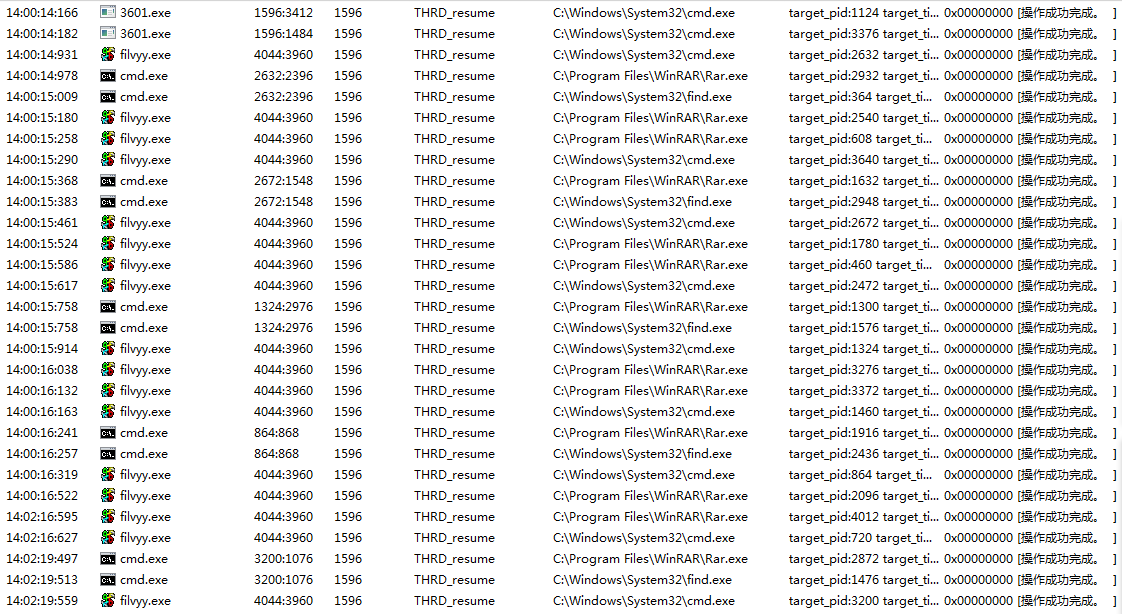
1. 创建cmd，Rar，find等进程



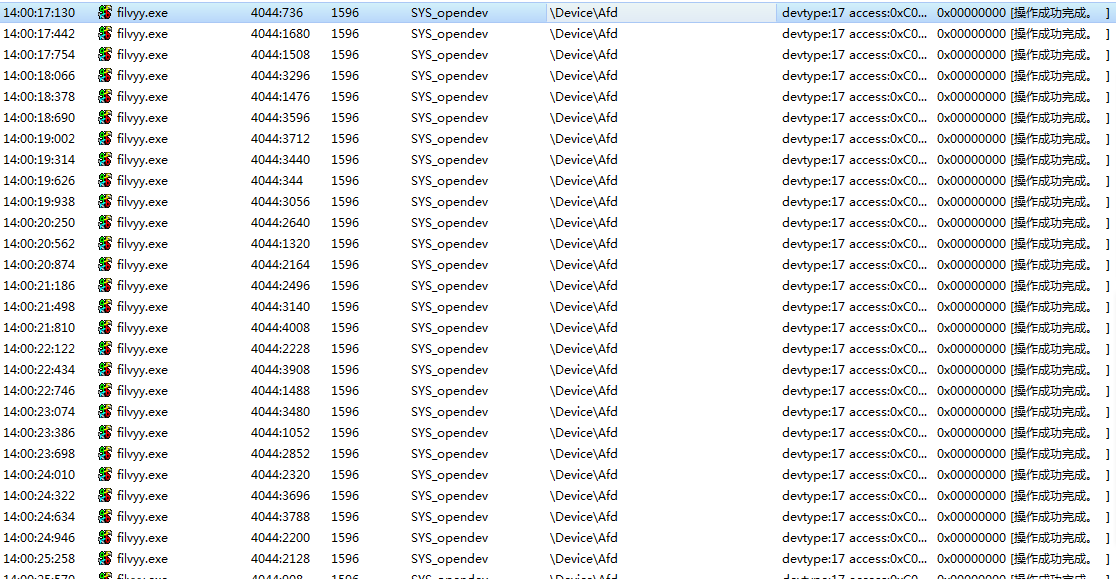
1. 并对创建的进程进行跨进程写入



1. 跨进程恢复挂起的线程



1. 打开设备，用于将数据包传输到局域网和Internet。

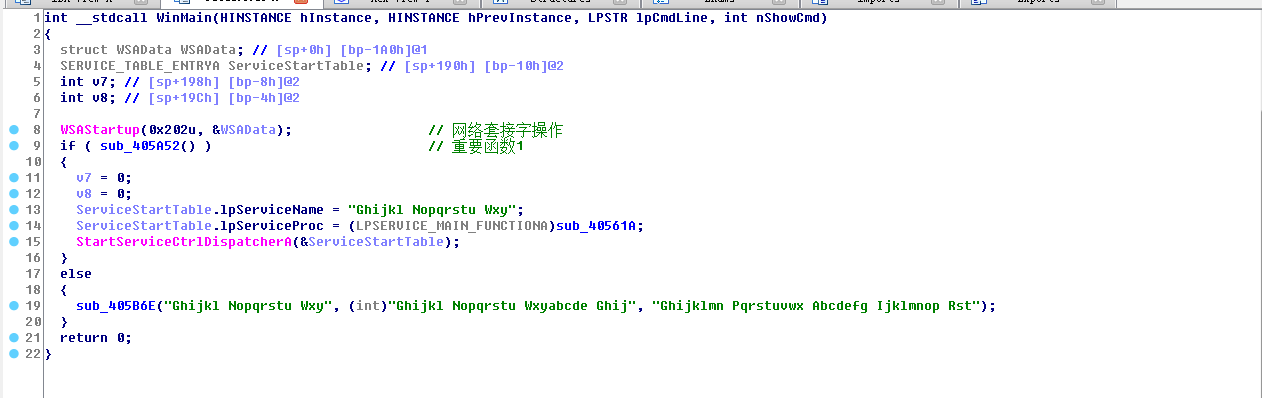


# 3．恶意代码分析

分析导图如下：



## 3.1 整体流程



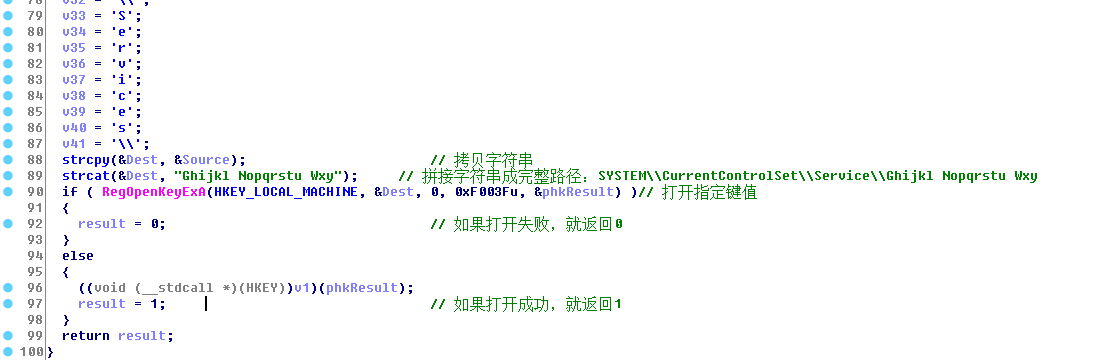
1.打开注册表指定键值，判断该键值是否存在

2.若键值不存在，就执行405B6E。

3.若键值存在，就执行40561A

## 3.2 对函数sub\_405A52进行跟进分析：





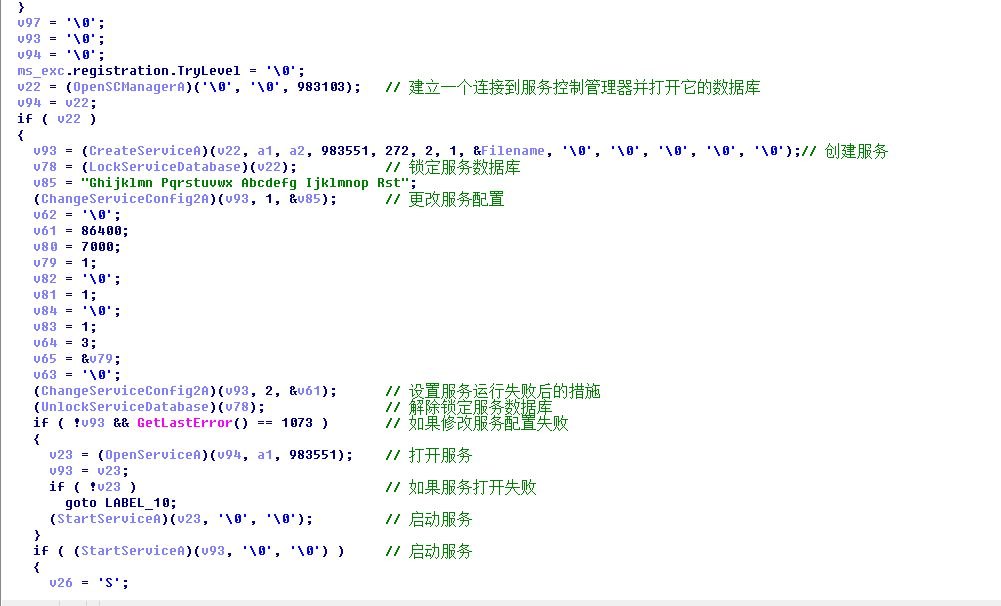
可以分析出，该函数的作用是用于判断指定键值是否存在。

## 3.3 对函数sub\_405B6E进行跟进分析：

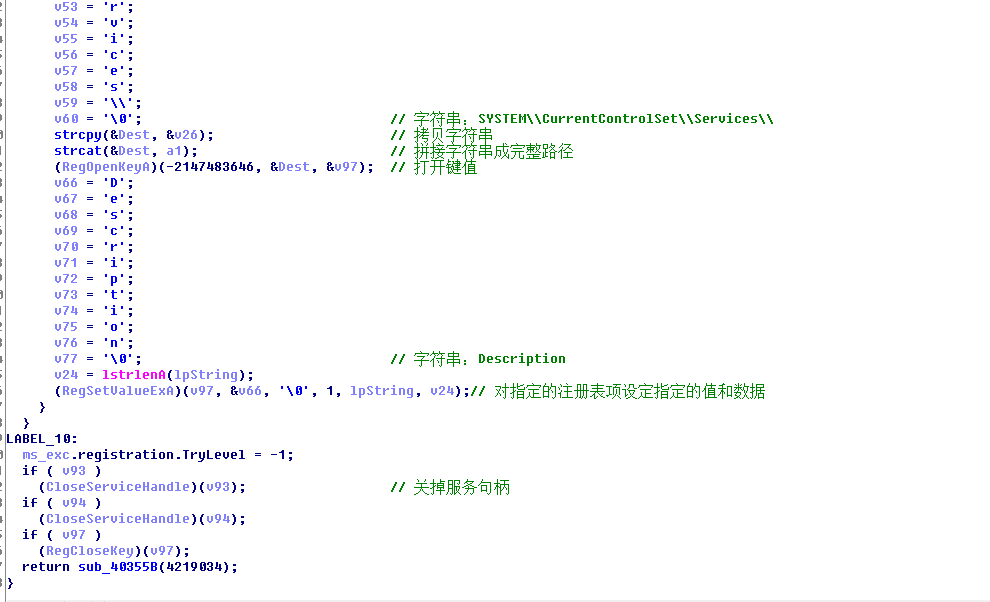
**3.3.1 第一部分：**加载相关模块，与获取相关API的函数地址。然后判断当前进程是否运行在系统目录下，如果没有，就随机生成字符串用于组成文件名，并拼接成完整路径，再将病毒程序拷贝至拼接的路径下。



**3.3.2 第二部分**：打开服务管理器，然后创建服务，并锁定服务数据库，并对服务的相关配置进行修改和设置，然后释放对服务数据库的锁定。如果服务创建失败，就再次去打开服务，并尝试启动服务。



**3.3.3 第三部分**：把服务名与指定路径进行拼接，拼接成完整路径，并打开该路径下的注册表键值，然后将指定的数据与值填入该注册表项中。



**3.3.4 第四部分（跟进sub\_40355B）:**通过执行cmd命令完成对桌面病毒文件的删除，并设置相关进程和线程优先级。



## 3.4 对函数sub\_40561A进行跟进分析：

**3.4.1 第一部分：**

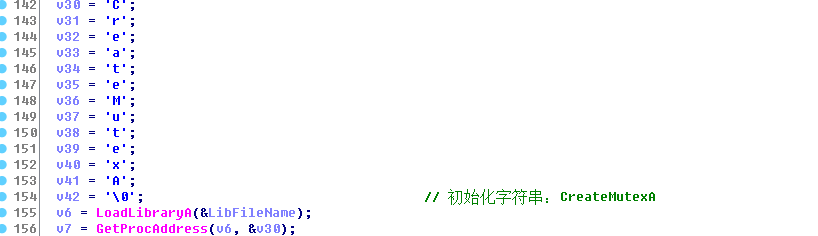
加载了相关的模块以及获取相关函数地址，并通过API来设置服务状态。



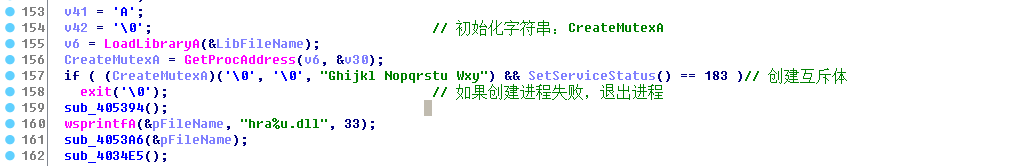
**3.4.2 第二部分：**

获取相关函数地址：其中包括：GetLastError;GetCurrentThreadId;CreateMutexA

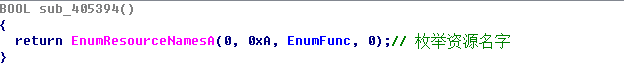




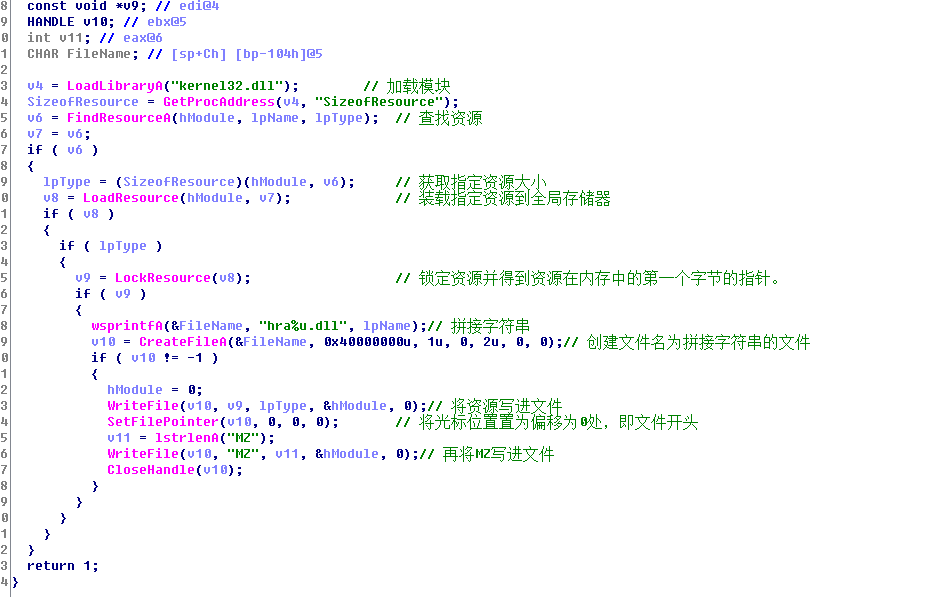
**3.4.2 第三部分：**



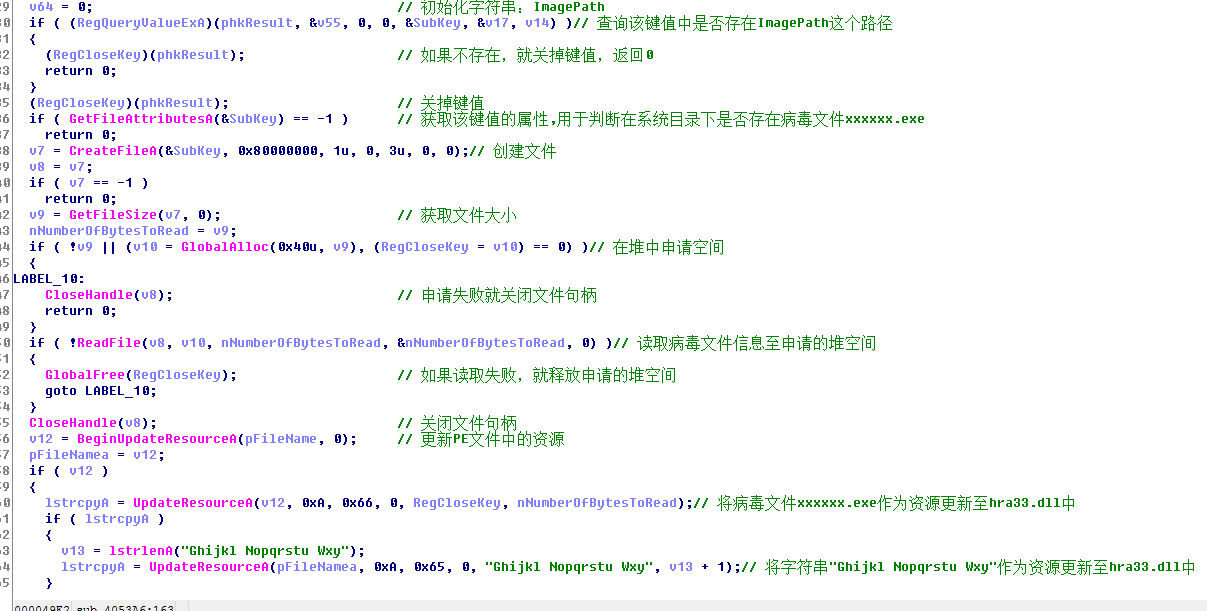
**3.4.2.1跟进sub\_405394:**



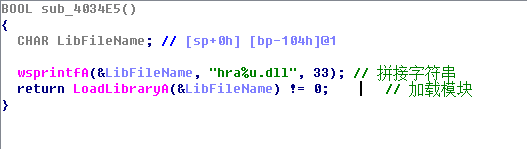
继续跟进，分析回调函数EnumFunc：将指定模块作为资源写进创建的hra33.dll文件中，并在文件开头写入MZ字符串。



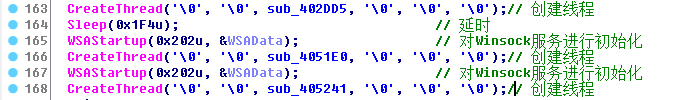
**3.4.2.2跟进sub\_4053A6**:申请堆空间用于接收病毒文件信息，然后将病毒本身作为资源更新至hra33.dllPE文件中，并将字符串” kl Nopqrstu Wxy"作为资源也更新至hra33.dllPE文件中，最后释放申请的堆空间。



**3.4.2.3跟进sub\_4034E5:**

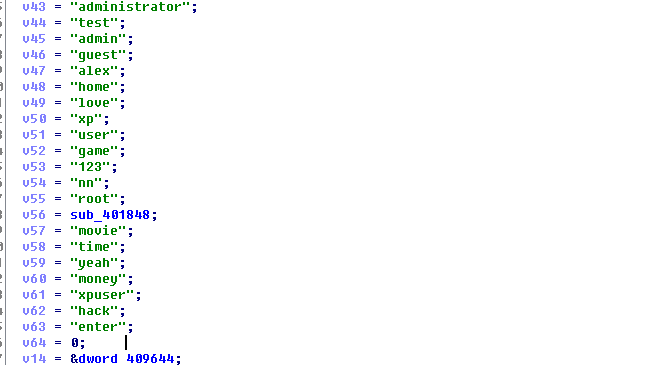


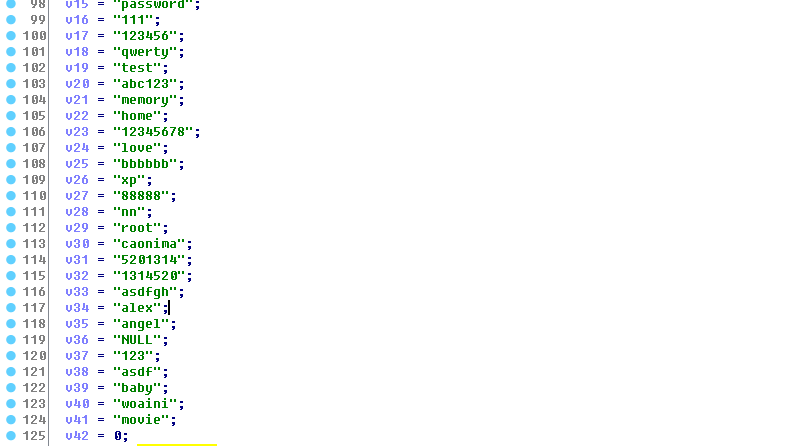
**3.4.3 第四部分：**



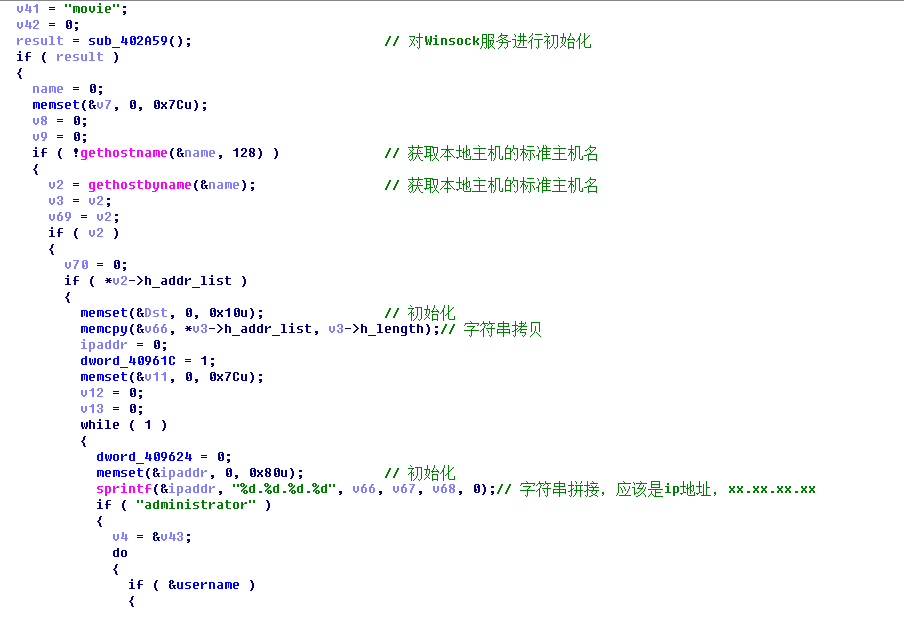
**3.4.3.1：**对第一个线程回调函数sub\_402DD5进行分析：

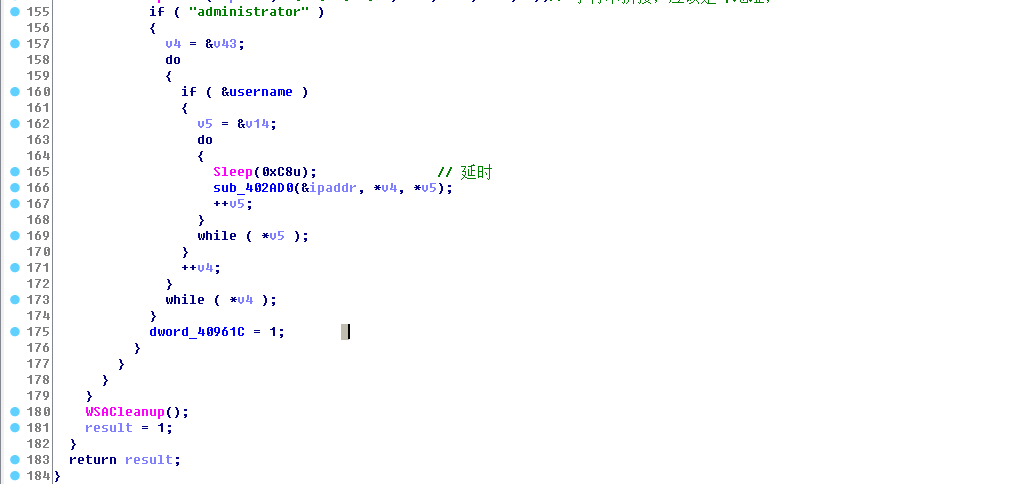
（1）发现一串类似于账号和密码的字符串，猜测可能是要进行账号和密码的暴力破解。





（2）应该是获取本地主机ip地址，并转换成字符串，作为参数传入函数sub\_402AD0





1. 跟进sub\_402AD0

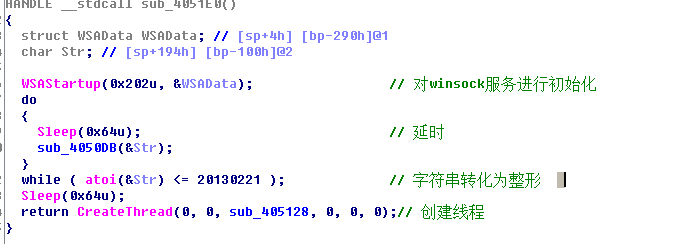
1.建立ipc连接，如果建立成功，就获取病毒文件的文件名，并将其拷贝到各个系统根目录下。



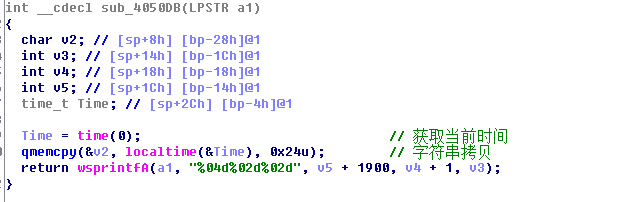
2.获取本地系统时间，用过cmd命令，设置定时启动程序。



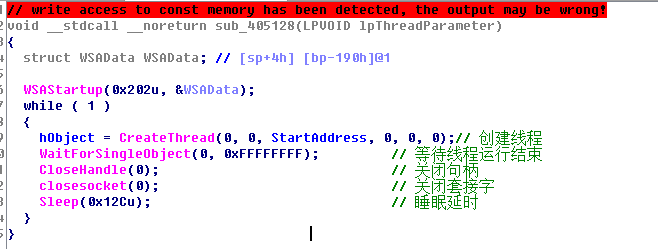
**3.4.3.2：**对第二个线程回调函数sub\_4051E0进行分析：



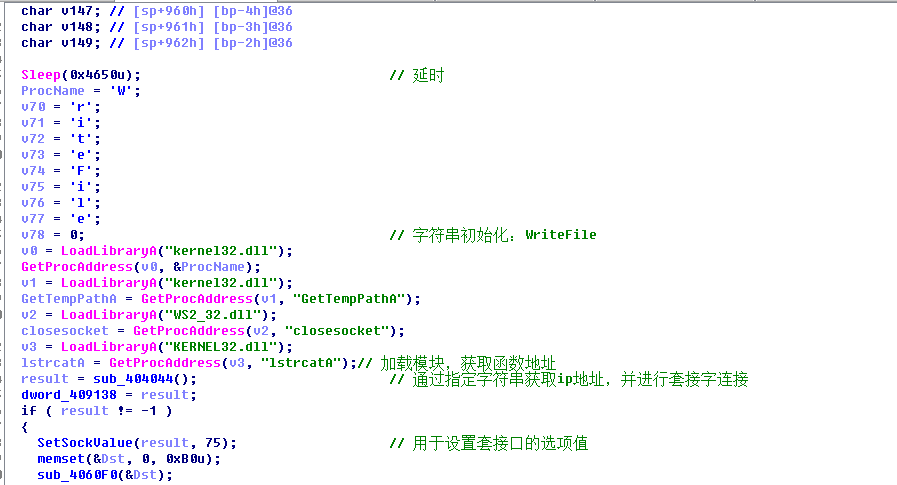
1. 跟进sub\_4050DB:获取了下当地时间，并返回一串拼接好的字符串



1. 跟进线程回调函数sub\_405128:创建了一个线程，并等待其执行完毕

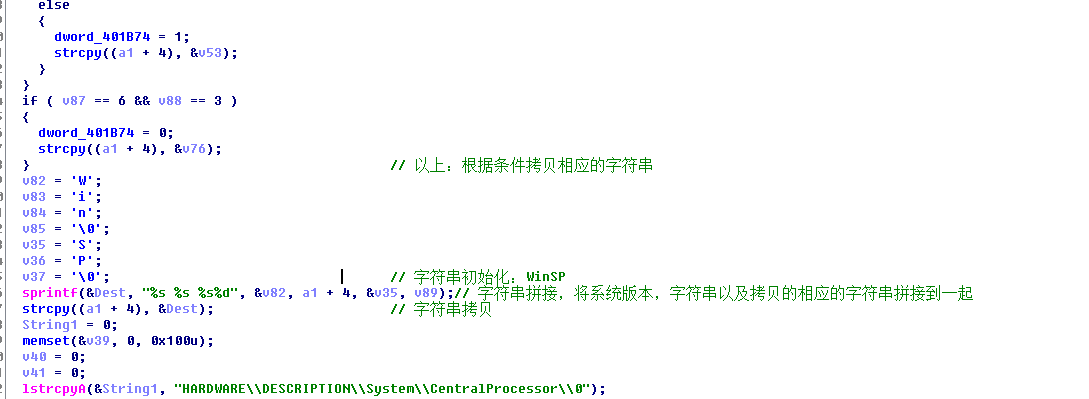


继续跟进线程回调函数StartAddress：



跟进sub\_4060F0：主要是获取系统信息和网卡配置以及ip地址信息

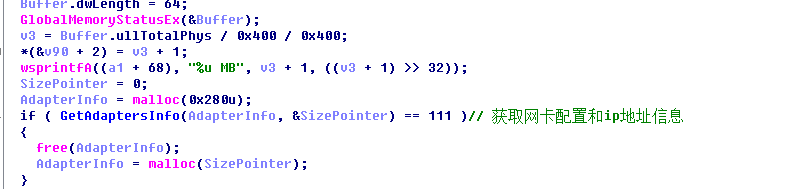
获取了系统信息



获取了CPU相关信息

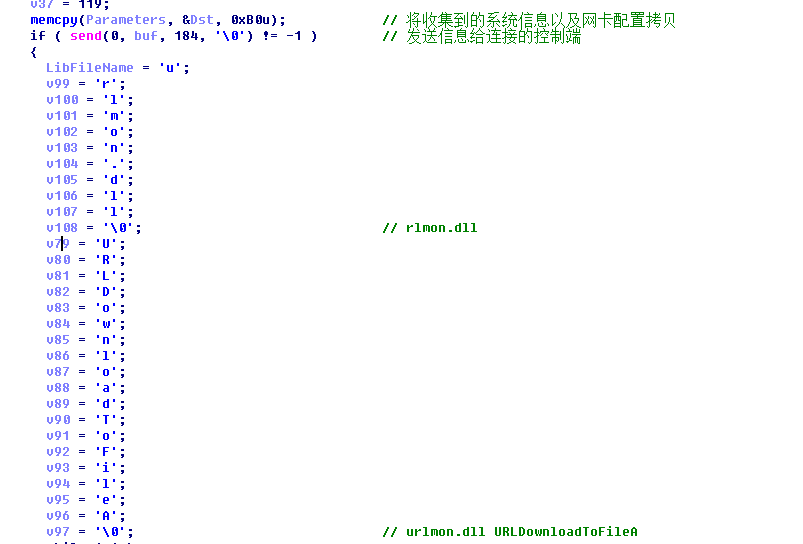


获取网卡配置和ip地址信息：



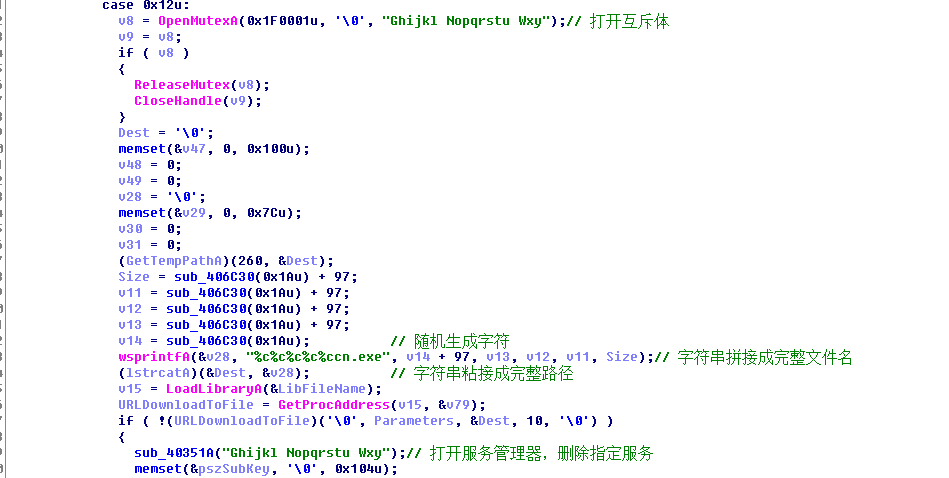
返回继续分析StartAddress：

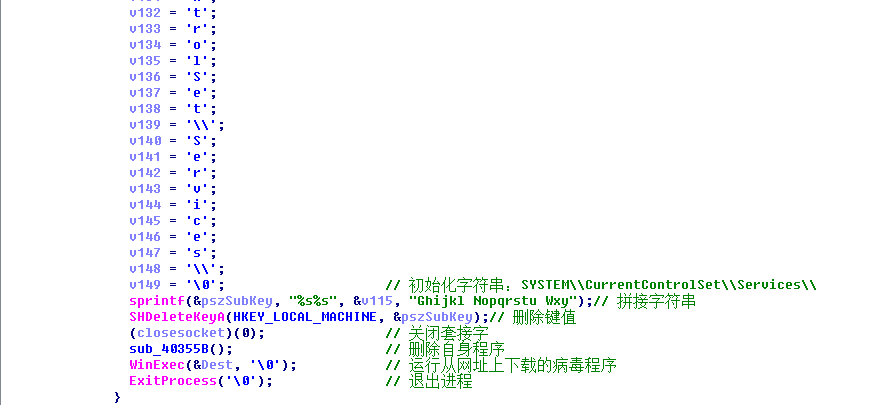
将收集到的信息发送给控制端，并等待控制端返还信息，如果信息为0x10，就从指定网址下载恶意代码并执行。





如果信息为0x12：从网址上下载新的病毒程序到指定系统目录，并删除原先的病毒信息以及服务键值，然后运行新的病毒程序，并退出进程。





如果信息为0x14：就会通过cmd命令打开ie浏览器

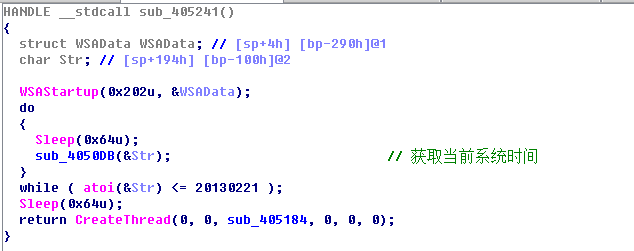


如果信息为0x6，会执行与0x12相同的操作。

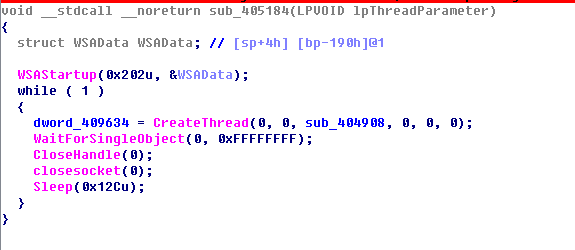
如果信息为其他：就会进行一系列的套接字初始化操作



**3.4.3.3：**对第三个线程回调函数进行分析：

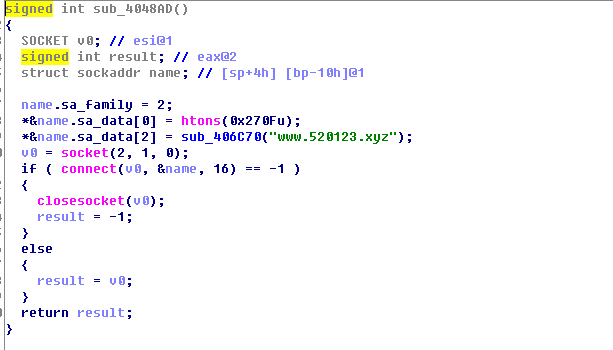


跟进线程回调函数sub\_405184:同样创建了一个线程

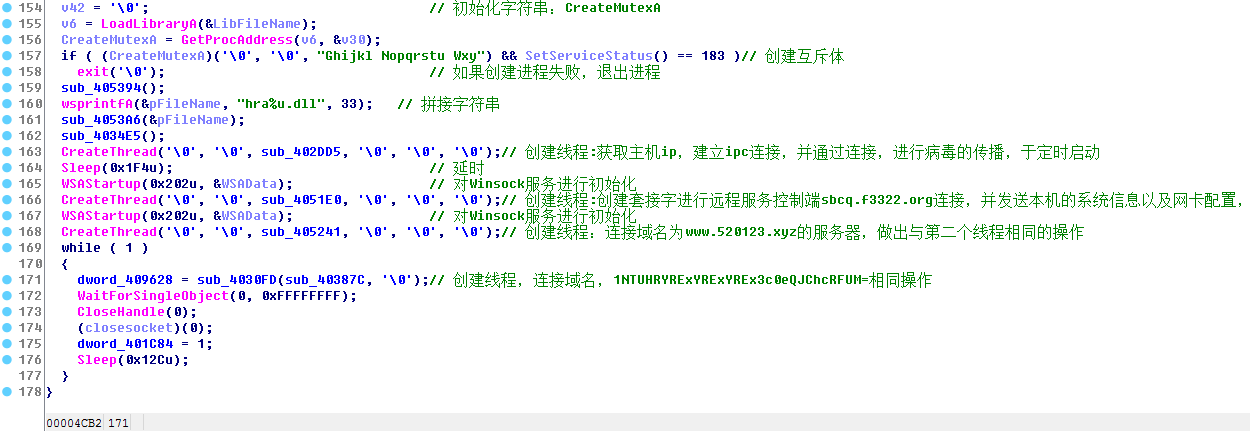


继续跟进线程回调函数sub\_404908:发现该回调函数和之前的第二个线程回调函数基本一样。但是访问的域名发生了变化：[www.520123.xyz](http://www.520123.xyz)





**3.4.4 第五部分：**同样创建了一个线程，进行域名连接，但是域名应该是被加了密的，然后连接域名后，做出与第3个线程同样的操作



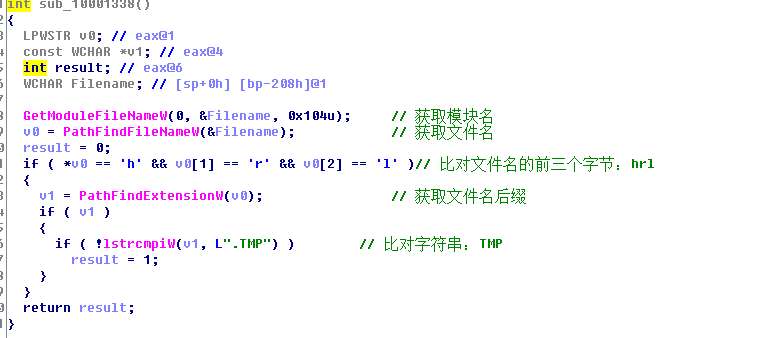
## 3.5 对函数dra33.dll进行跟进分析：



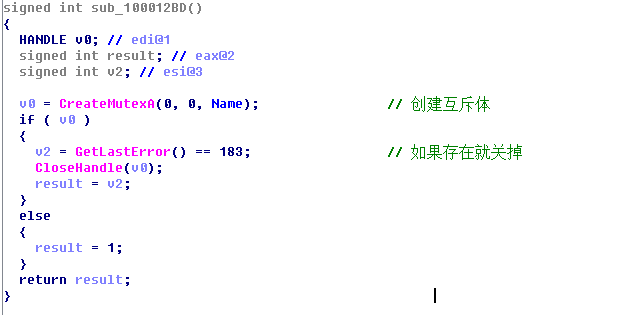
**3.5.1 sub\_10001134:**用于判断资源中是否存在病毒程序



**3.5.2 sub\_10001338:**用于判断文件名前三个字节是否是hrl与文件类型是否是TMP



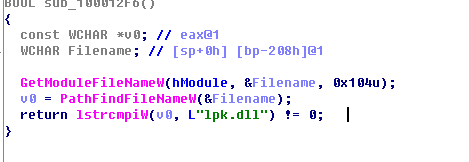
**3.5.3 sub\_100012BD:**用于创建互斥体，用于防止多个dll同时运行。



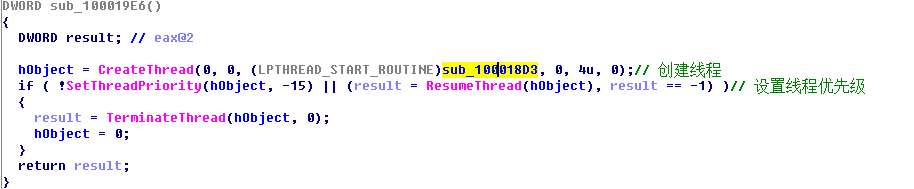
**3.5.4 sub\_10001193:**用于加载病毒文件并运行



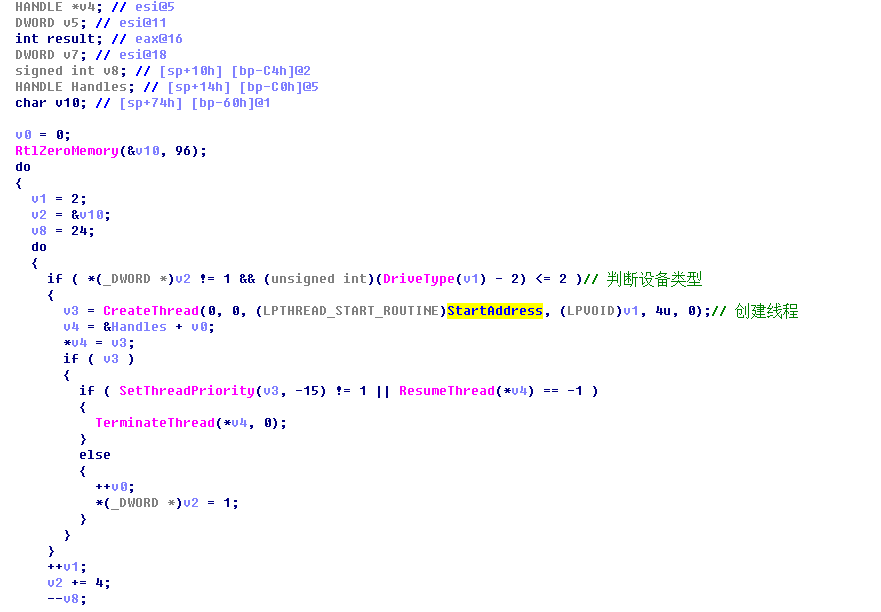
**3.5.5 sub\_100012F6:**用于比较文件名是否是lpk.dll



**3.5.6 sub\_100019E6:**创建了线程并设置了线程的优先级



跟进线程回调函数100018D3：同样创建了一个线程



继续跟进StartAddress：用于遍历文件，并进行感染，如果文件类型为exe，就拷贝lpk.dll到文件目录下，如果文件类型为RAR或者ZIP，就执行sub\_1000142B进行感染。



sub\_1000142B:主要是在压缩包内插入或替换带病毒程序的lpk.dll



# 4．总结

## 4.1 dll劫持原理

DLL劫持技术的原理是当一个可执行文件运行时，Windows加载器将可执行模块映射到进 程的地址空间中，加载器分析可执行模块的输入表，并设法找出需要的DLL,并将它们映射到 进程的地址空间中。由于输入表中只包含DLL名而没有它的路径名，因此加载程序必须在磁盘 上搜索DLL文件。搜索DLL文件的顺序如下所示。

1.程序所在目录。

2.系统目录。

3.16位系统目录。

4.Windows 目录。

5.当前目录。

6.PATH环境变量中的各个目录。

首先系统会尝试从当前程序所在的目录中加载DLL;如果没找到，则在系统目录中查找； 如果没找到，则在16位系统目录中寻找；如果没找到，在Windows系统目录中查找；如果没 找到，则在当前目录中查找；如果没找到，则在环境变量列出的各个目录下查找。

利用搜索路径的这个特点，先伪造一个与系统同名的DLL,提供同样的输出表，并使每个 输出函数转向真正的系统DLLo程序调用系统DLL时会先调用当前程序所在目录下的伪造的 DLL,完成相关功能后，再跳到系统DLL同名函数里执行。这个过程就是DLL劫持。

为了使程序在加载了劫持的DLL后还能正常执行，劫持DLL导出函数的名称和功能必须 要与原来的DLL相同。可以有两种方式来调用原来DLL的导出函数。一种是直接转发DLL函 数，另一种是调用DLL函数。

## 4.2 特征码提取

字符串：sbcq.f3322.org

www.520123.xyz

www.520520520.org:9426

Ghijkl Nopqrstu Wxy

参考文献

1. 看雪学院
2. HACK编程技术详解
3. 吾爱破解