****

**分析报告**

|  |  |
| --- | --- |
| **样本名** | **3601.exe&har33.dll** |
| **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 8](#_Toc25736)

[1.1 样本信息 8](#_Toc18142)

[1.2 测试环境及工具 8](#_Toc17592)

[1.3 分析目标 8](#_Toc10245)

[2 上传微步查看运行结果 9](#_Toc17724)

[3 火绒监控程序操作 11](#_Toc16177)

[3.1 执行监控 11](#_Toc10166)

[3.2 文件监控 11](#_Toc18792)

[3.3 进程监控 12](#_Toc30526)

[3.4 网络监控 12](#_Toc1769)

[3.5 行为监控 13](#_Toc22162)

[4 3601.exe具体分析 13](#_Toc19723)

[4.1 服务回调函数 15](#_Toc21749)

[4.1.1 ConcentHostDownExecVir线程回调 17](#_Toc26660)

[4.1.2 DownVirAndExec和sub\_405241和sub\_40387C 以上函数执行功能基本一至 21](#_Toc9985)

[4.1.3 枚举资源回调 23](#_Toc21914)

[4.1.4 更新资源函数 24](#_Toc19181)

[4.2 CopyVirAndCreateVirServiceWriteReg函数 26](#_Toc24461)

[5. lpk.dll具体分析 28](#_Toc7188)

[5.1 DllEntryPoint函数 28](#_Toc11960)

[5.2 LpkLoadRes 29](#_Toc14285)

[5.3 LpkExtensionIsTmp 30](#_Toc19584)

[5.4 LpkMutexIsExist 30](#_Toc26054)

[5.5 LpkCreateSrc0x66Process 31](#_Toc7748)

[5.6 LpkFileIslpk\_DLL 32](#_Toc2185)

[5.7 LpkBinWriteAndDecom 32](#_Toc27759)

[5.8 LpkCreateThreadForExeAndDecompression 33](#_Toc32466)

[5.9 LplWriteExeAndDecompressionFile 35](#_Toc23259)

[5.10 LpkDecompressionFile 37](#_Toc25816)

[5.11 LpkRunCommand 37](#_Toc9604)

[5.12 LpkGetLpkFunction\_ 38](#_Toc23751)

[5.13 LpkGetLpkFunction 39](#_Toc19358)

[5.14 LpkGetProcAddress 39](#_Toc32745)

[致 谢 39](#_Toc25735)

# 1．样本概况

## 1.1 样本信息

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

病毒名称：B5752252B34A8AF470DB1830CC48504D

所属家族：Trojan

MD5值：B5752252B34A8AF470DB1830CC48504D

SHA1: AEC38ADD0AAC1BC59BFAAF1E43DBDAB10E13DB18

CRC32: 4EDB317F

病毒行为：

在每个exe程序的路径下释放病毒lpk.dll，替换系统的lpk。

## 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、hash

## 1.3 分析目标

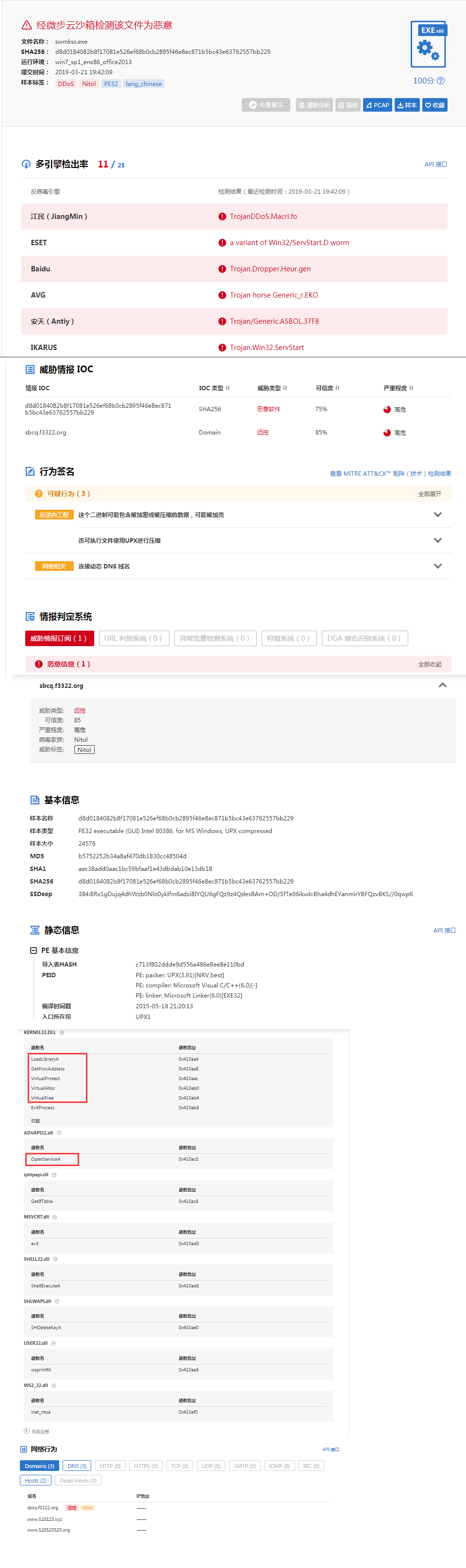
1、提取病毒样本，手工清理机器

2、行为分析，获取病毒行为

3、详细分析，找到行为恶意代码

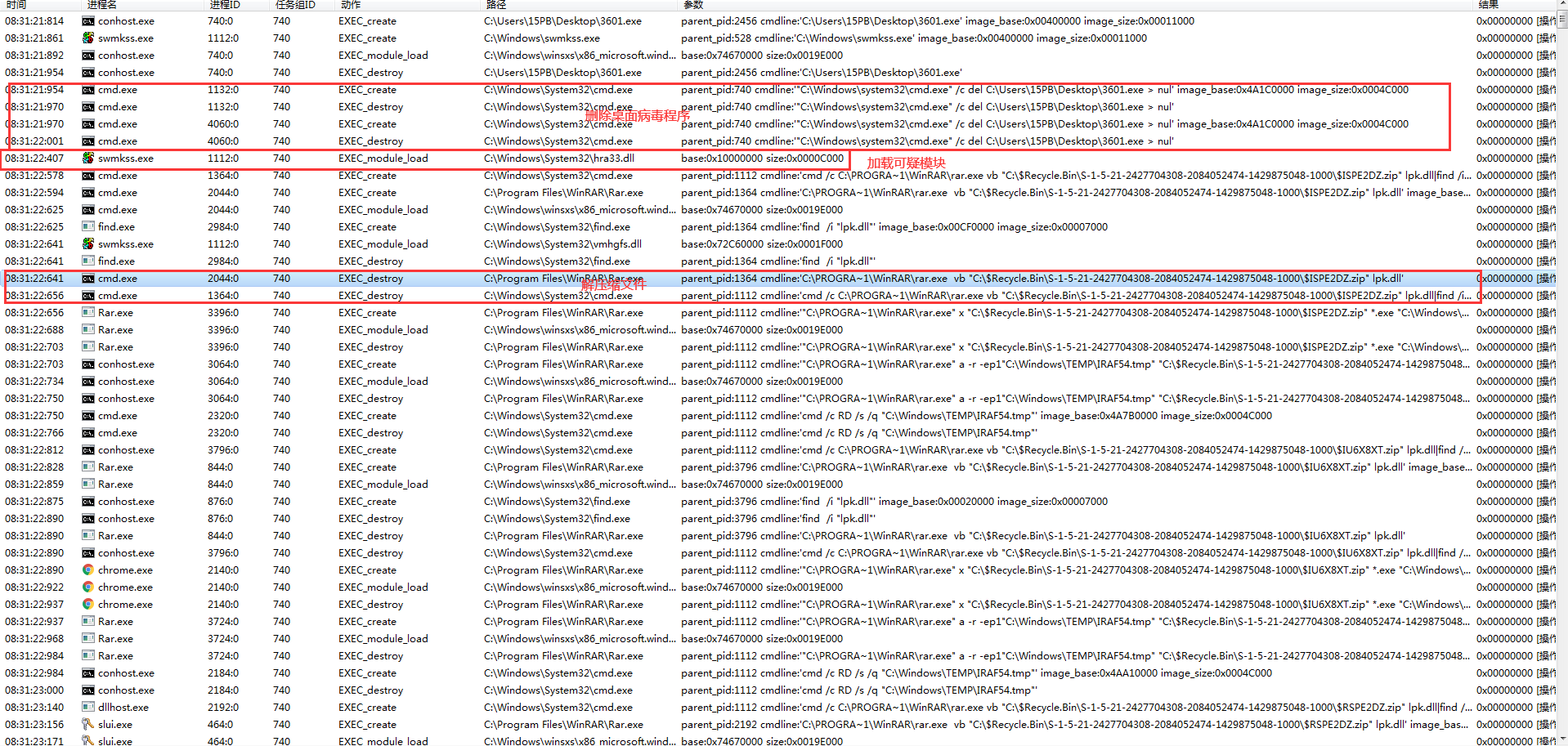
4、提出解决方案、编写专杀工具

# **2 上传微步查看运行结果**



# **3 火绒监控程序操作**

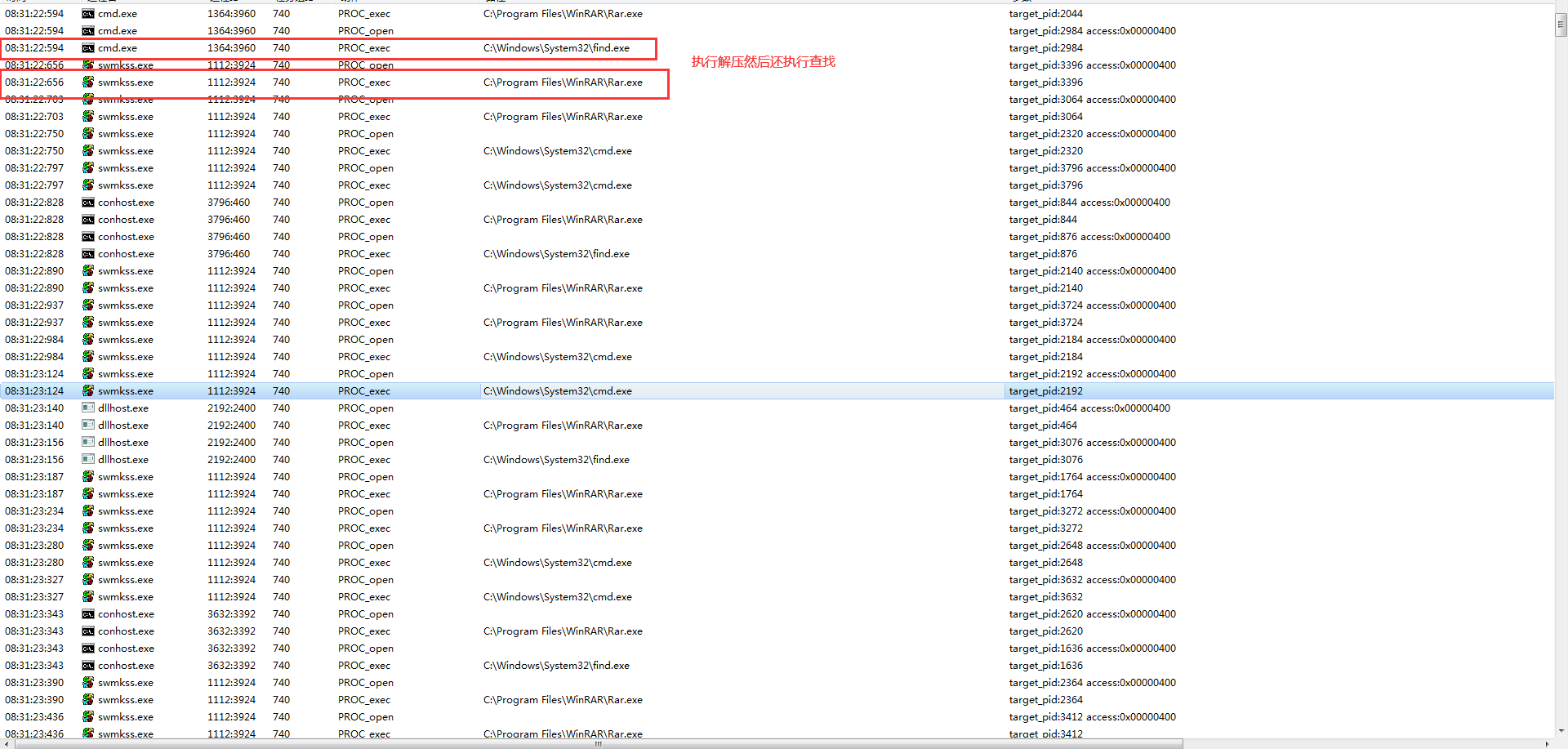
## 3.1 执行监控



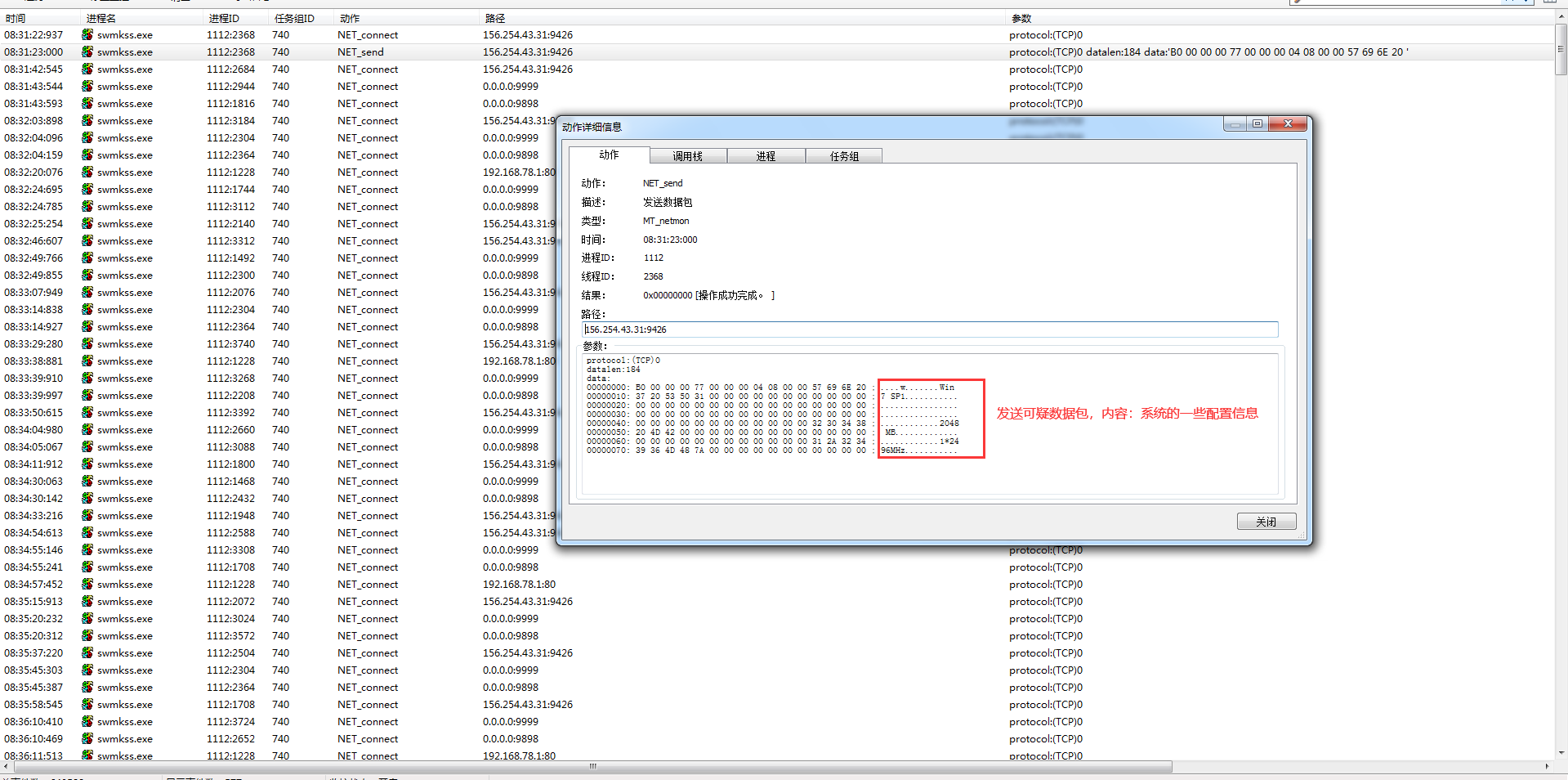
## **3.2 文件监控**



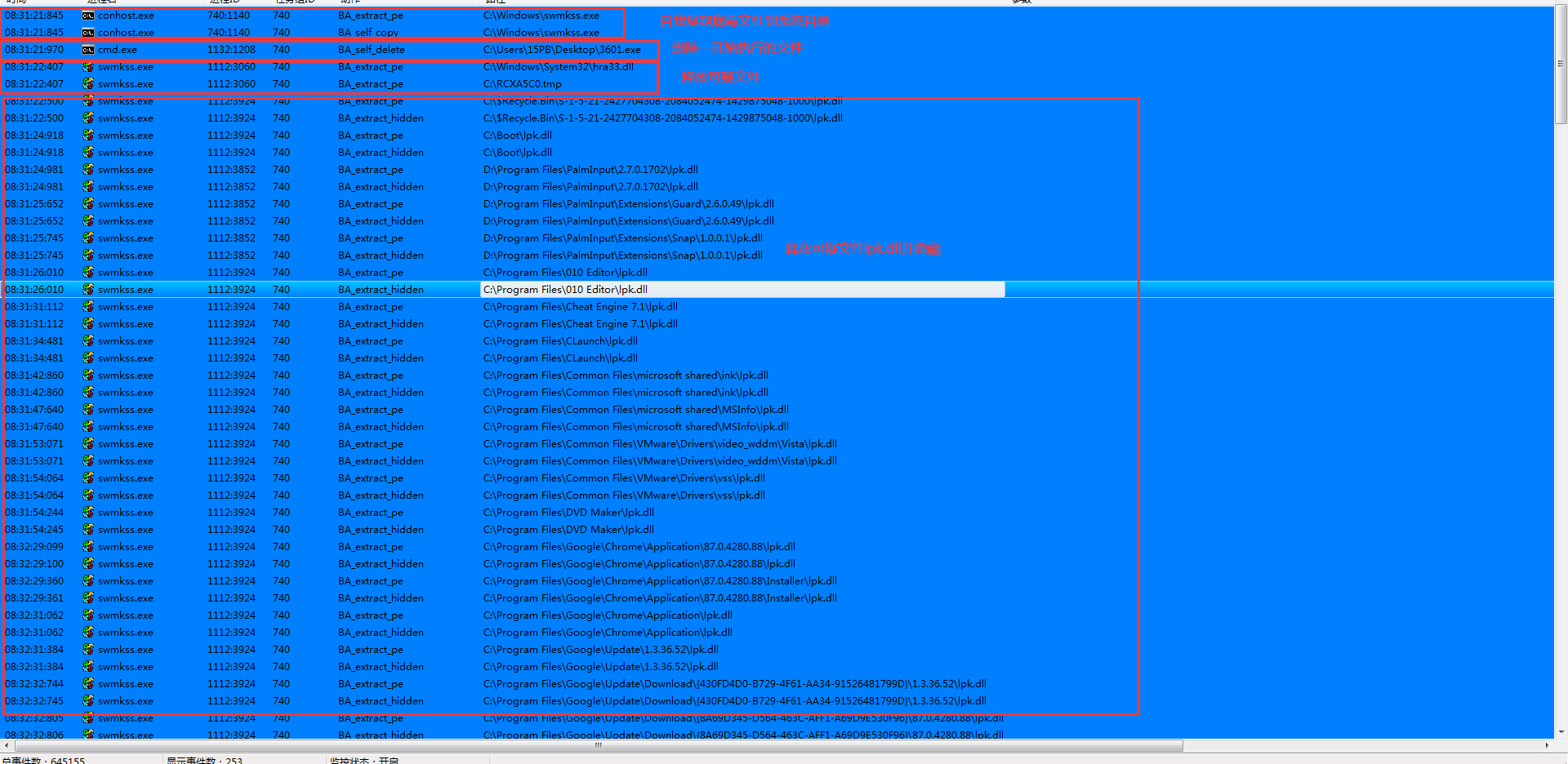
## **3.3 进程监控**



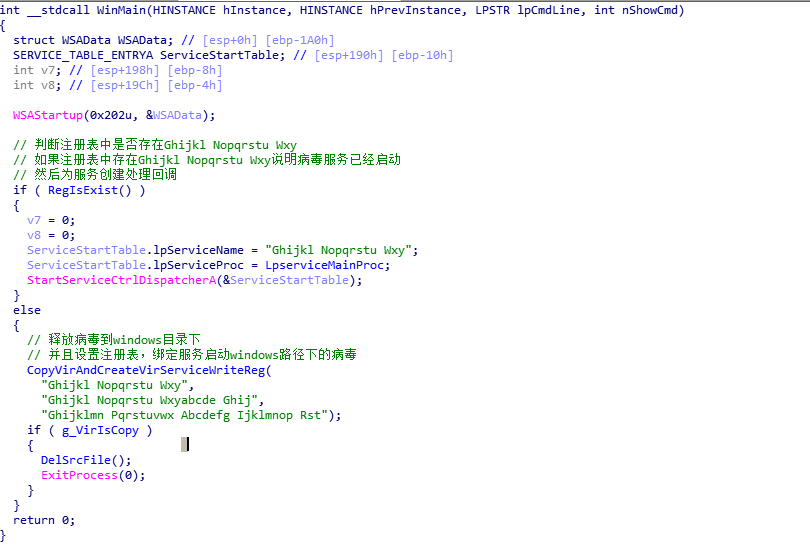
## **3.4 网络监控**



## **3.5 行为监控**



# **4 3601.exe具体分析**

整体概括

第二个服务器地址sbcq.f3322.org

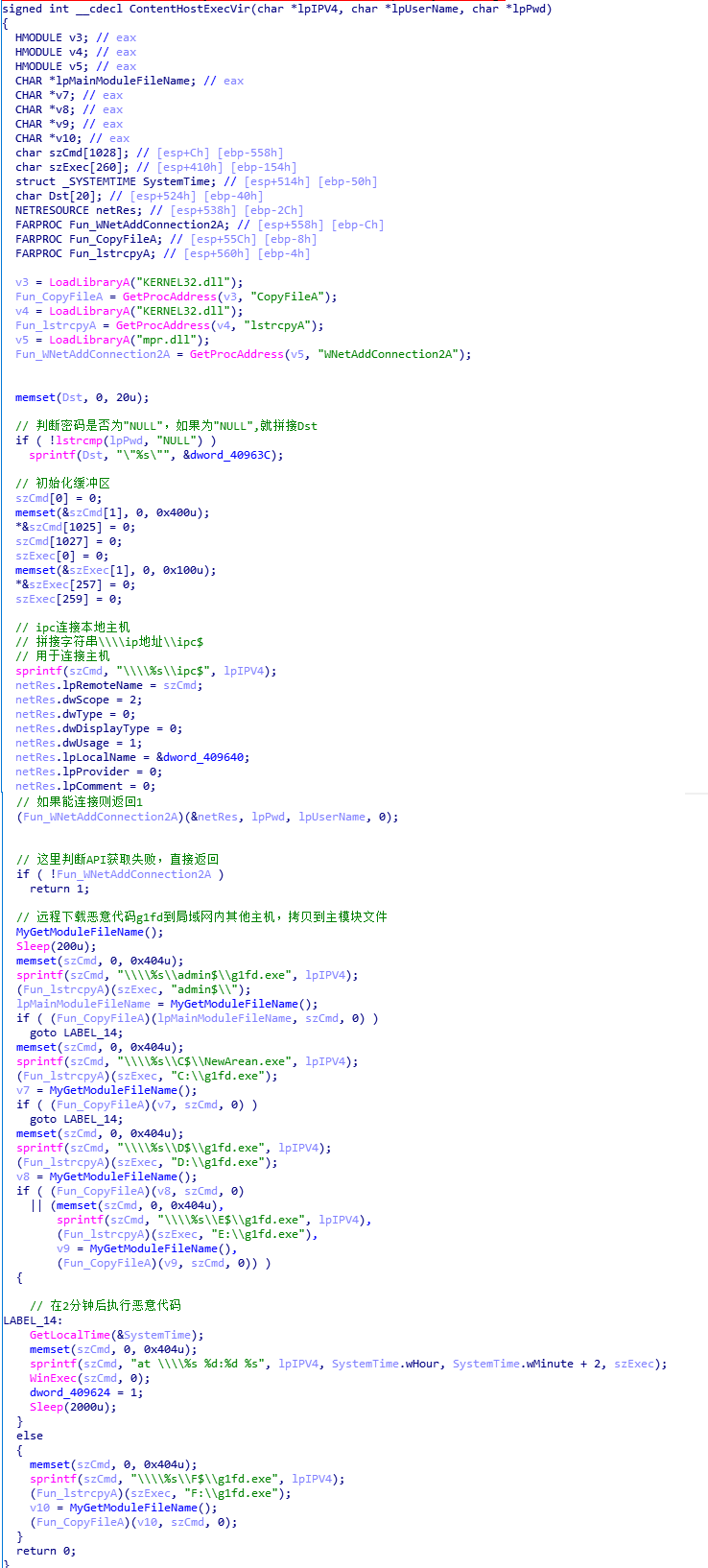
第三个服务器地址www.520123.xyz

第四个服务器地址被加密，"1NTUHRYRExYRExYREx3c0eQJChcRFUM="，解密后是[www.520520520.org:9426](http://www.520520520.org:9426)

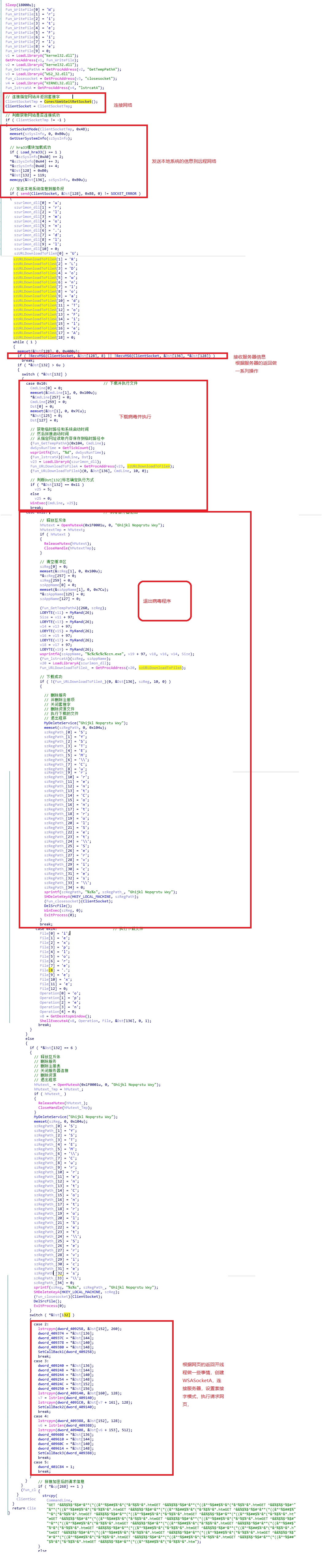
## 4.1 服务回调函数

### 4.1.1 ConcentHostDownExecVir线程回调



尝试连接局域网进程感染

### **4.1.2 DownVirAndExec和sub\_405241和sub\_40387C 以上函数执行功能基本一至**



### 4.1.3 枚举资源回调



### **4.1.4 更新资源函数**



## 4.2 CopyVirAndCreateVirServiceWriteReg函数



# **lpk.dll具体分析**

## 5.1 DllEntryPoint函数

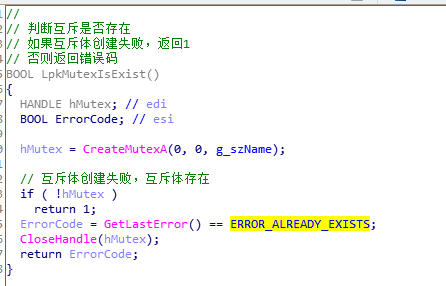


## **5.2 LpkLoadRes**



## **5.3 LpkExtensionIsTmp**

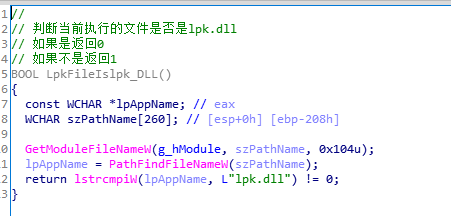
## **5.4 LpkMutexIsExist**



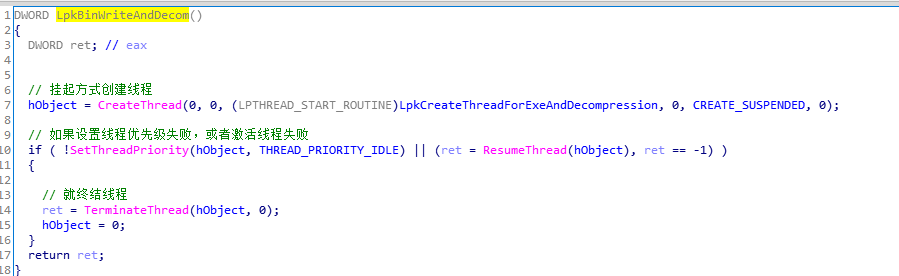
## **5.5 LpkCreateSrc0x66Process**



## **5.6 LpkFileIslpk\_DLL**



## **5.7 LpkBinWriteAndDecom**



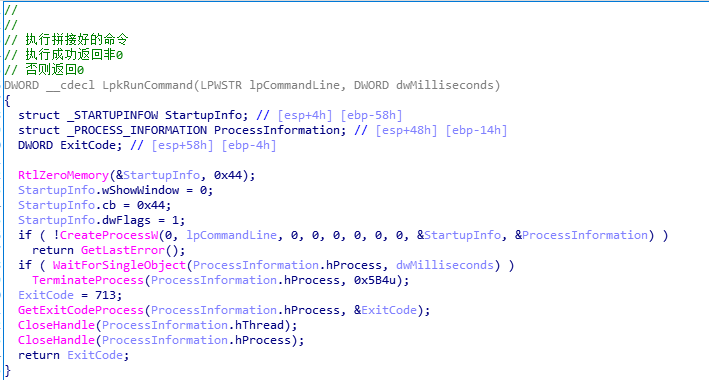
## **5.8 LpkCreateThreadForExeAndDecompression**



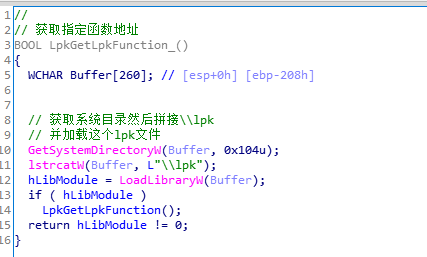
## 5.9 LplWriteExeAndDecompressionFile

## **5.10 LpkDecompressionFile**

## **5.11 LpkRunCommand**



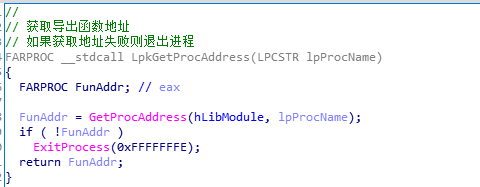
## **5.12 LpkGetLpkFunction\_**



## **5.13 LpkGetLpkFunction**



## **5.14 LpkGetProcAddress**



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。