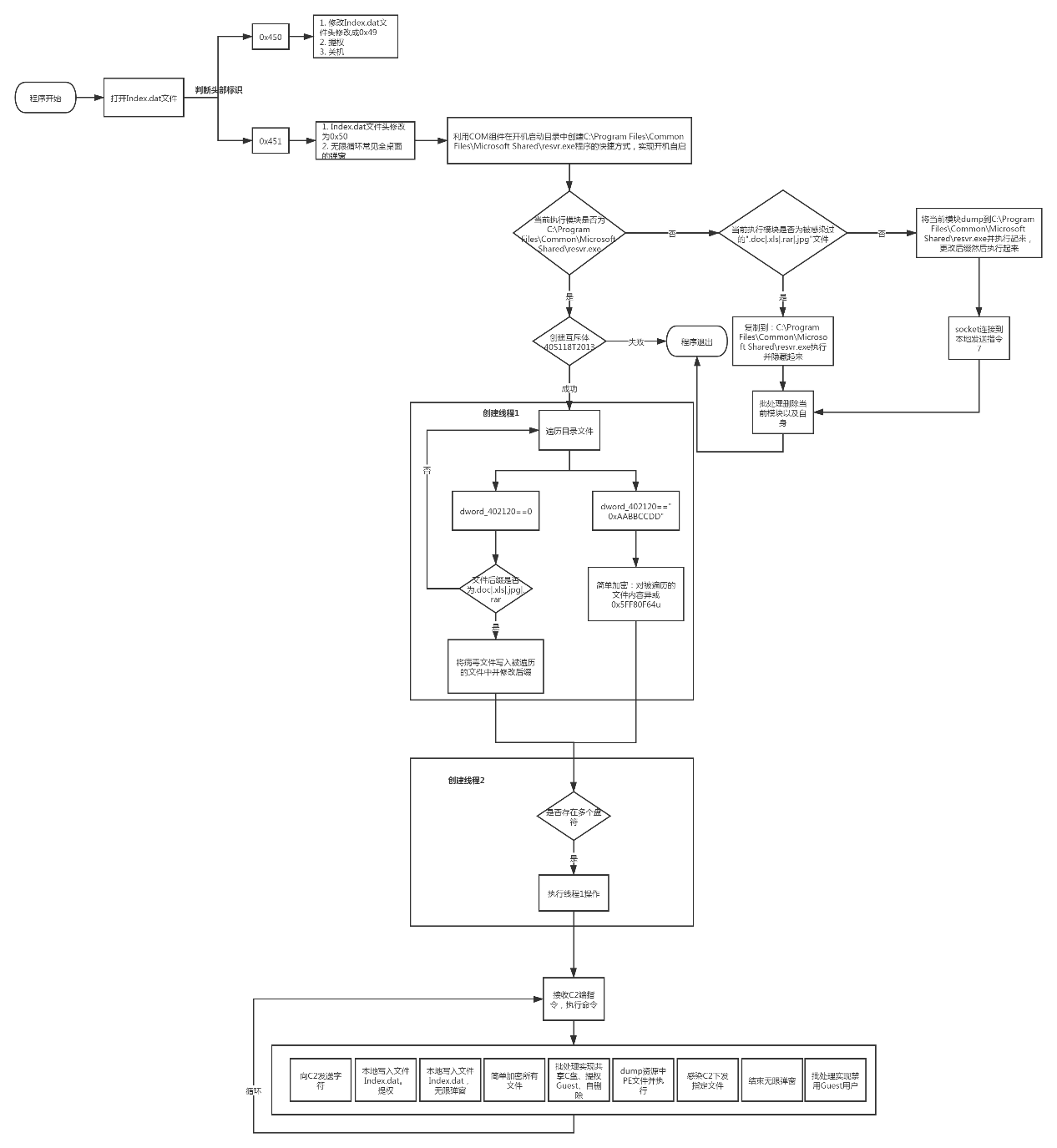
# 1、概述

本片报告为一起老感染型病毒的分析报告。病毒主体分为两个模块，所有功能都在病毒母体模块中，主要遍历盘符将指定后缀的文件感染成病毒文件，然后监听本地等待C2回连发送特定指令进行加密、提权、命令执行、执行资源中PE文件等，并且由于他会设置文件隐藏属性以及子删除操作，所以程序运行后在资源管理器中看不见该样本。

# 2、病毒软件概览

|  |  |
| --- | --- |
| MD5 | 5E63F3294520B7C07EB4DA38A2BEA301 |
| 文件名 | resvr.exe |
| 描述 | 水印标签系统 |
| 数字签名 | 无 |
| 时间戳 | 2007-07-05 11:52:54 |
| 病毒类型 | 感染|后门 |
| 壳类型 | 未加壳 |
| 保护手段 | 无 |
| 感染文件类型 | .doc|.xls|.rar|.jpg |
| 加密文件类型 | 所有文件格式 |
| 加密算法 | 异或0x5FF80F64 |
| VT首次上传时间 | 2015-03-10 23:07:19 |
| VT检测结果 | 54/65 |

## 2.1 病毒行为概况

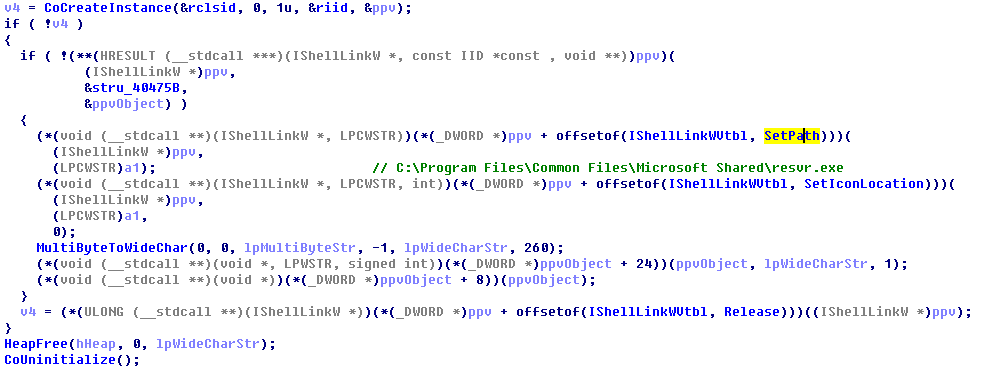


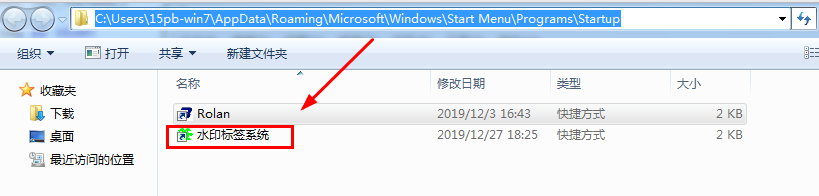
# 3、病毒样本分析

## 3.1 母体病毒行为分析

**在开机自起目录创建快捷方式实现开机启动**

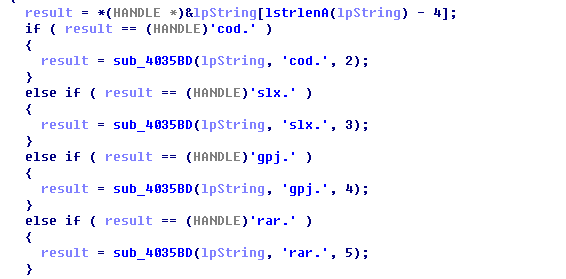
利用COM组件在开机启动目录中创建快捷方式"C:\Users\15pb-win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\水印标签系统.lnk"，实现开机启动C:\Program Files\Common Files\Microsoft Shared\resvr.exe程序





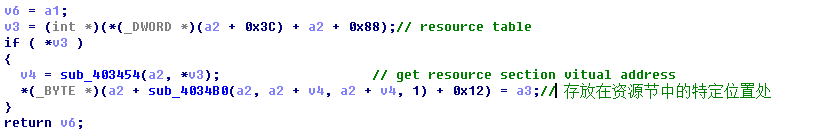
**感染文件**

如果当前执行的模块是C:\Program Files\Common\Microsoft Shared\resvr.exe：睡眠1s，然后创建互斥体"40S118T2013"，成功后执行遍历桌面、其他盘符以及其子目录所有文件，如果全局变量dword\_402120为0并且文件后缀为”.doc|.xls|.jpg|.rar”，将该文件和resvr.exe内容映射进内存空间



将保存这种特定文件长度的地址替换掉内存中0x11111111（前2000字节数据中）后面四字节数据(0xFFFFFFFF)进行存放，标记该文件是被感染过的文件

将保存这种特定文件后缀的地址替换掉内存中0x222222222e（前2000字节数据中）后面3字节数据进行存放，存放原始文件后缀



随后将修改好的内存数据前面PE文件部分重新写回被遍历的文件中，并且将文件后缀改成exe，如果出现同名则在原本后缀后面加上".exe"



实现成果

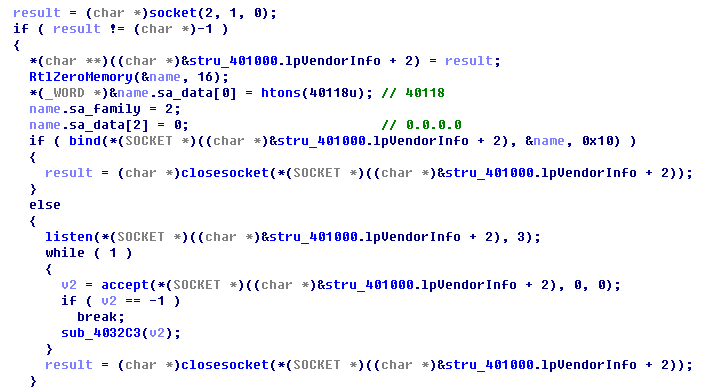


**后门**

接收C2服务器的指令执行相应操作，需要满足接收的命令为二进制数据，不能输入ASCII字符(指令7除外)，前4字节是命令，4-8字节是传入数据长度，后面跟着的就是传入的数据

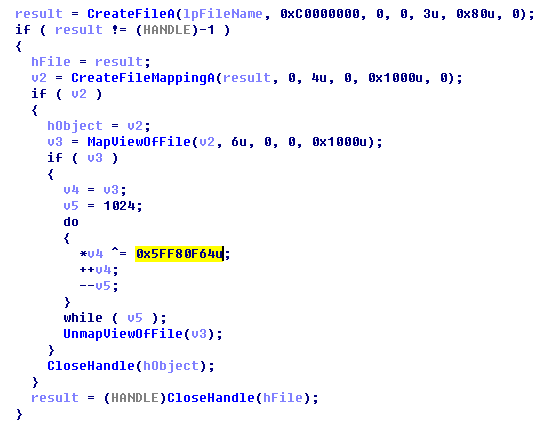


监听受害者机器上所有网卡的40118端口来实现这个后门



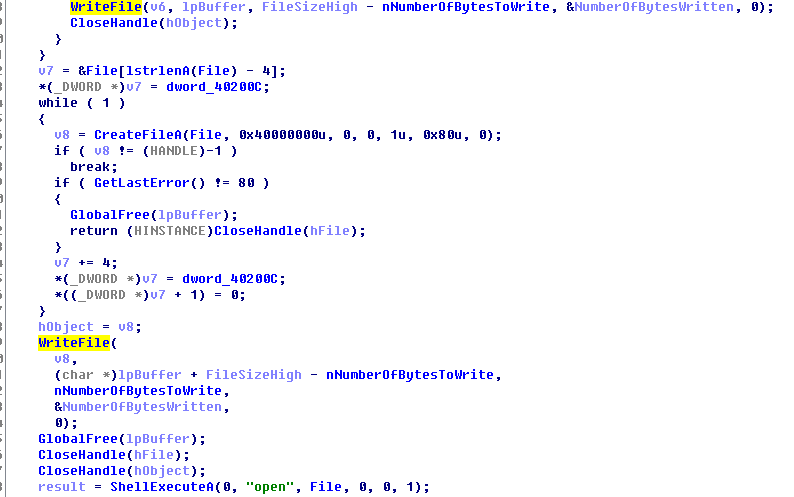
**加密文件**

本地接收到0x455指令后，全局变量设置为dword\_402120="0xAABBCCDD"时，将遍历盘符将所有文件映射进内存将其内容全部异或0x5FF80F64u进行简单加密

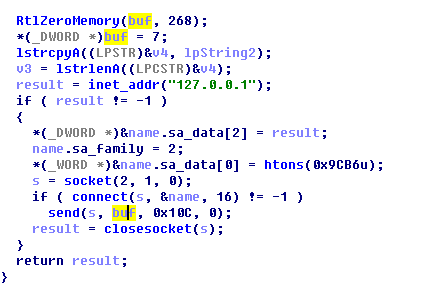


## 3.2 感染文件行为分析

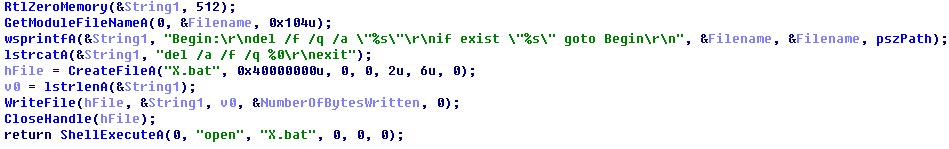
当前执行的进程模块不是C:\Program Files\Common\Microsoft Shared\resvr.exe，并且是被感染过的".doc|.xls|.rar|.jpg"文件时：将被感染的文件复制到"C:\Program Files\Common\Microsoft Shared\resvr.exe"并且设置为系统文件并隐藏属并执行起来



socket连接到本地发送指令7，但由于没有传入指定文件参数所以未能感染任何文件



自删除以及删除当前执行模块的可执行文件

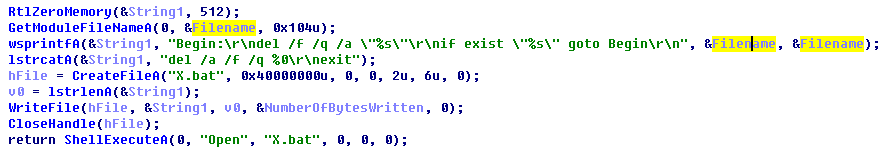


## 3.3 衍生物样本分析

|  |  |
| --- | --- |
| MD5 | E5BCC51B80BA1D91CB7179FB7A58FED7 |
| 文件名 | Message.exe |
| 来源 | 病毒母体resvr.exe的资源中 |
| 数字签名 | 无 |
| 时间戳 | 1999-04-24 22:00:55 |
| 病毒类型 | 感染|后门 |
| 壳类型 | 未加壳 |
| 保护手段 | 无 |
| VT首次上传时间 | 2014-10-22 14:21:46 |
| VT检测结果 | 30/71 |

**自删除**

批处理删除当前模块pe文件和自身



弹窗后成程序消失



# 4、防护意见

安装正版正规杀毒软件即可免受该病毒侵扰