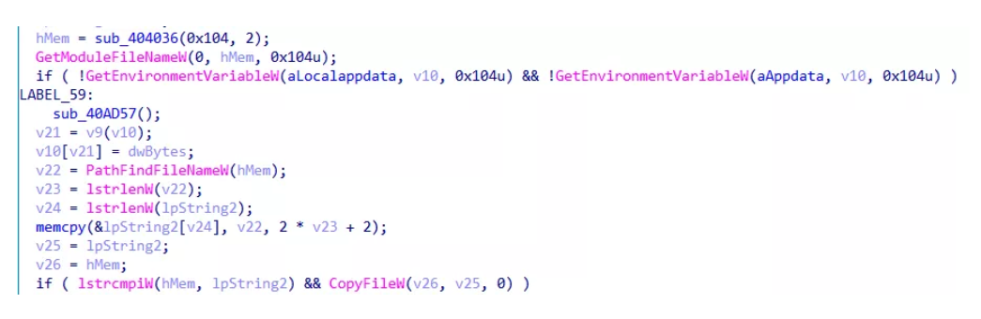
    Globelmposter恶意软件详细分析

**样本分析**

此次捕获到的Globelmposter家族新变种，经分析其代码结构与以往变种有很大变化，但其行为流程却具有鲜明的Globelmposter特点，且在攻击现场发现的样本母体被黑客命名为“5.1.exe”，因此也将此次发现的变种定义为Globelmposter 5.1变种。

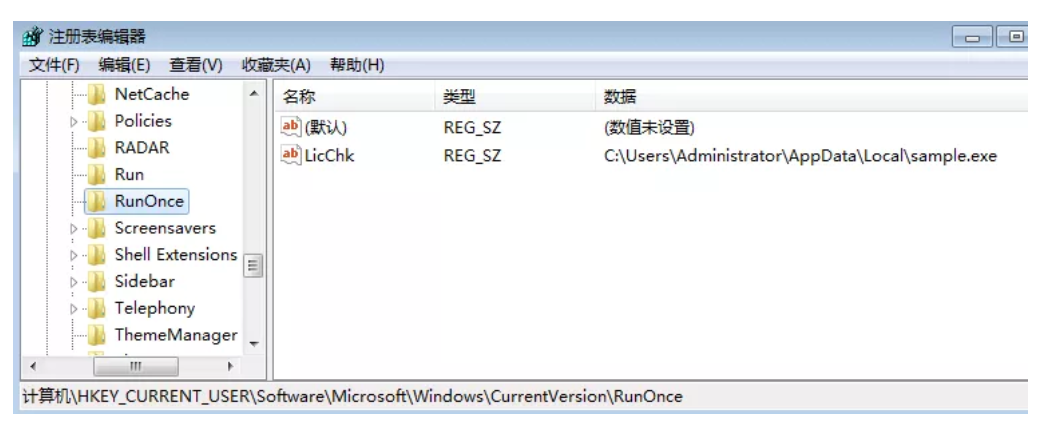
**行为分析**

运行后会将自身复制到%LOCALAPPDATA%或%APPDATA%目录：

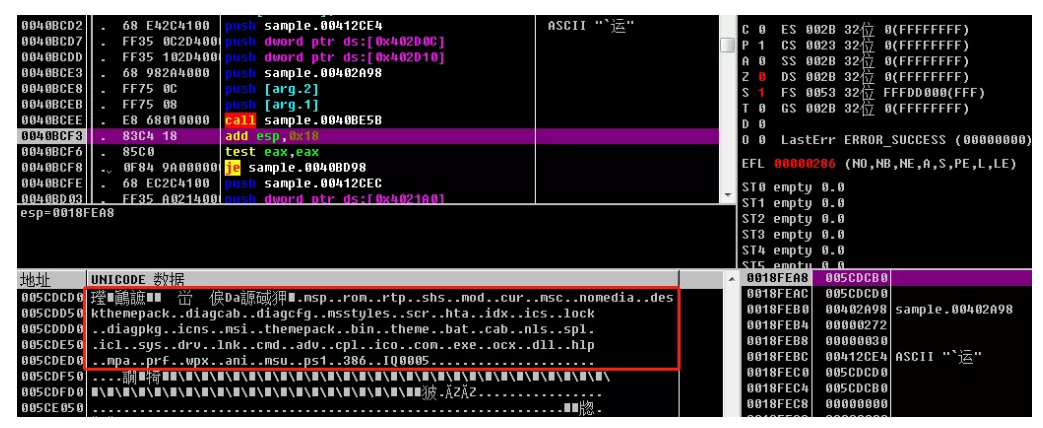


进行持久化操作，设置自启动项，注册表项为

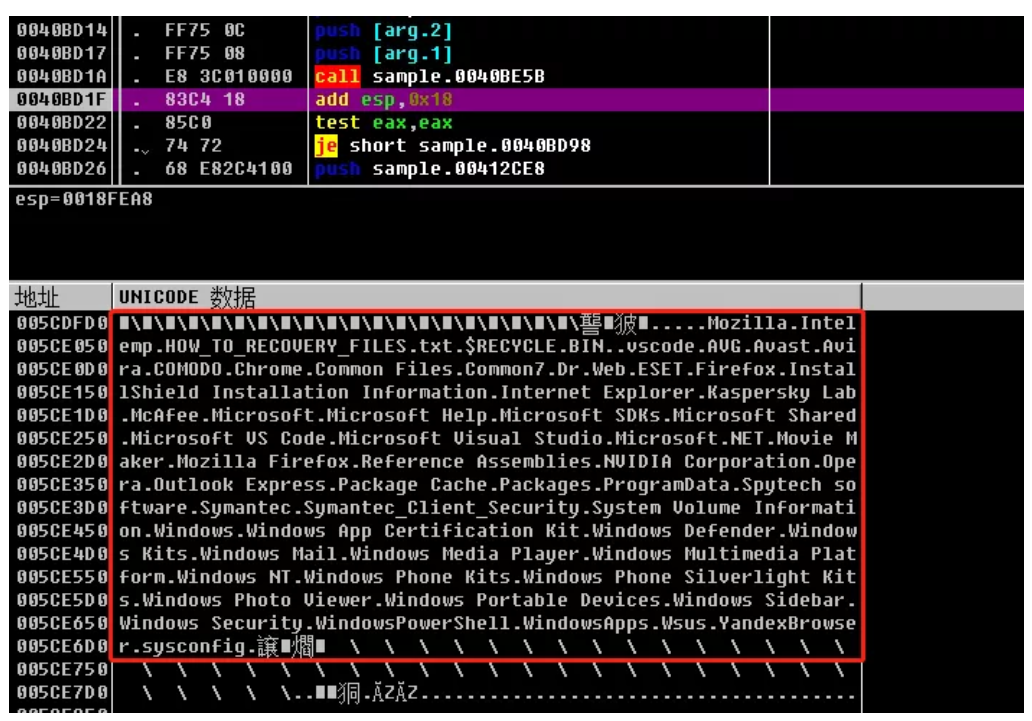
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\LicChk，实现开机自启动，如果在加密过程中主机关机，病毒在系统重启后能够自动运行并继续加密：



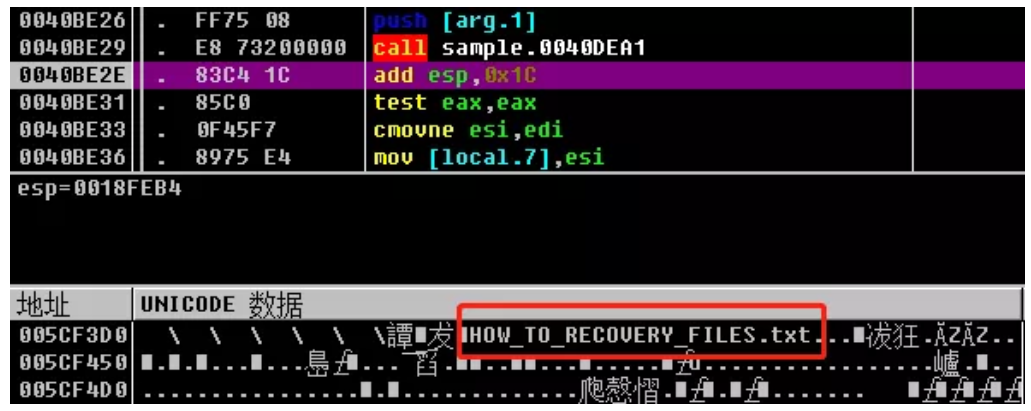
解密出豁免的文件后缀：



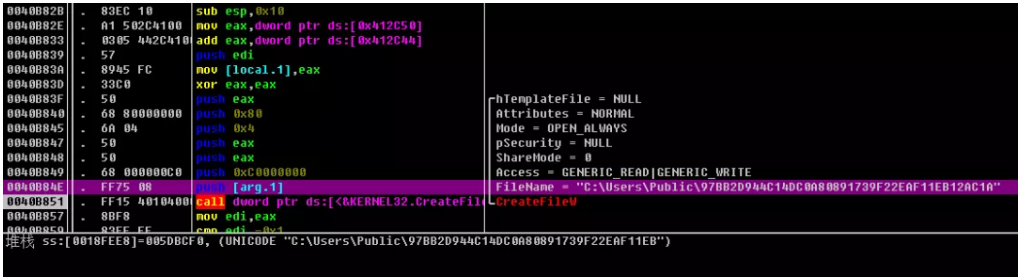
解密出豁免的文件及文件夹名：



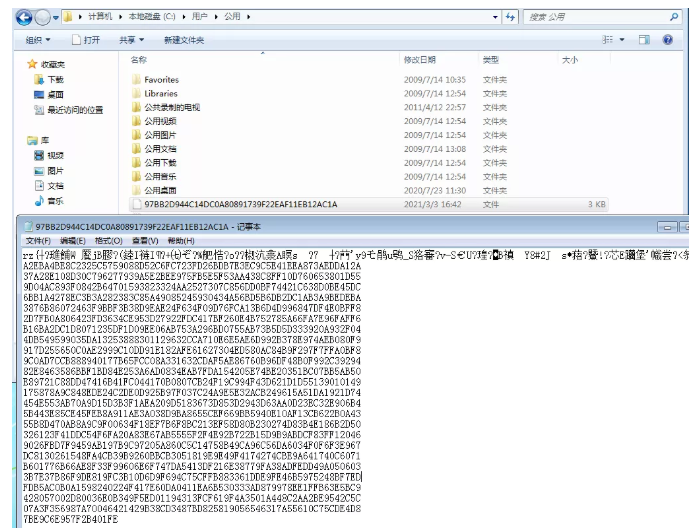
解密出勒索信息文件名：



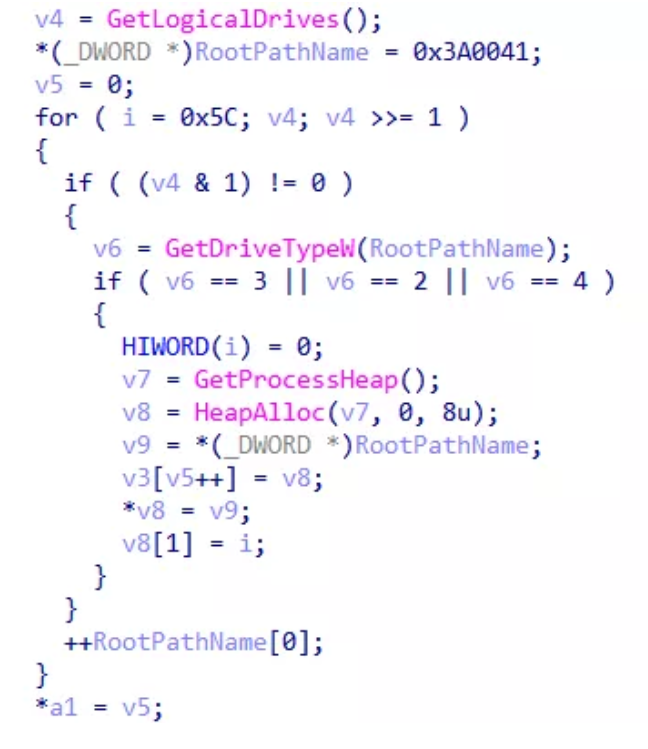
在C:\Users\Public目录写入ID文件：



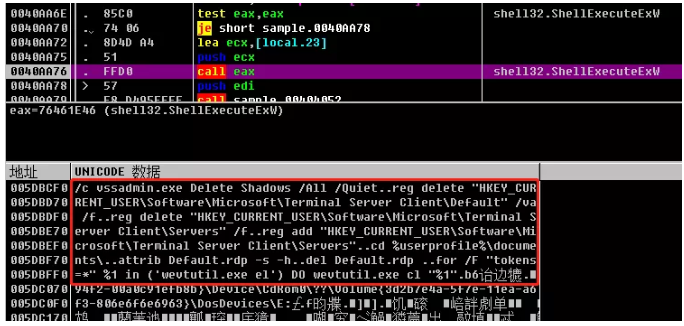
文件内容如下：



加密3种类型的磁盘：可移动磁盘，固定磁盘，网络磁盘。



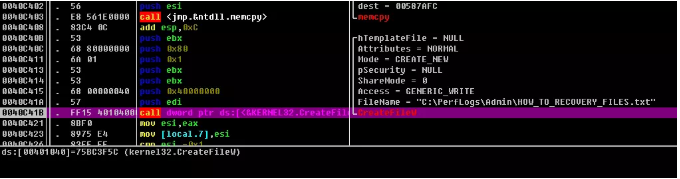
执行命令删除磁盘卷影，并删除注册表中“Terminal Server Client”中的键值，删除远程桌面连接信息文件default.rdp，还会通过wevtutil.exe cl的命令清除日志的相关信息：



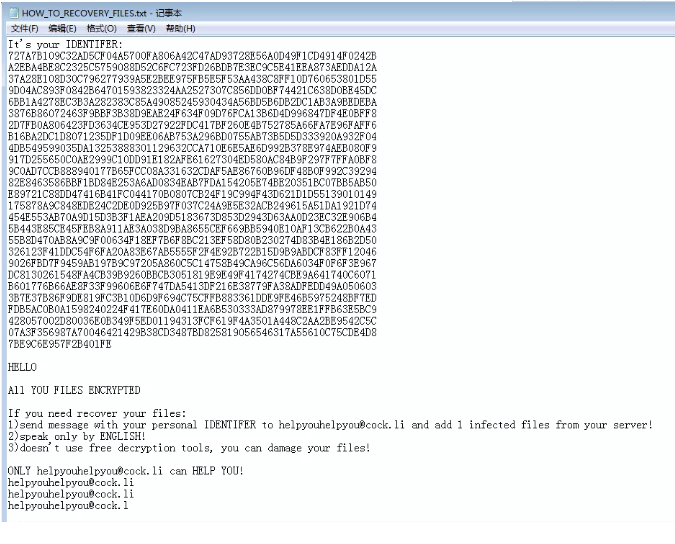
加密文件，加密后缀为”.IQ0005”：



写入勒索信息文件：



勒索信息内容如下：



勒索结束后病毒文件自删除：

