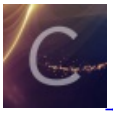
bugku-writeup-MISC-被勒索了

原创

dark2019 于 2021-07-07 10:50:30 发布 168 收藏 1
分类专栏： 信息安全 wp 文章标签： 杂项 ctf 火绒安全


信息安全 同时被 2 个专栏收录
53 篇文章 1 订阅
订阅专栏


wp
31 篇文章 0 订阅
订阅专栏

题目：被勒索了

工具：火绒安全

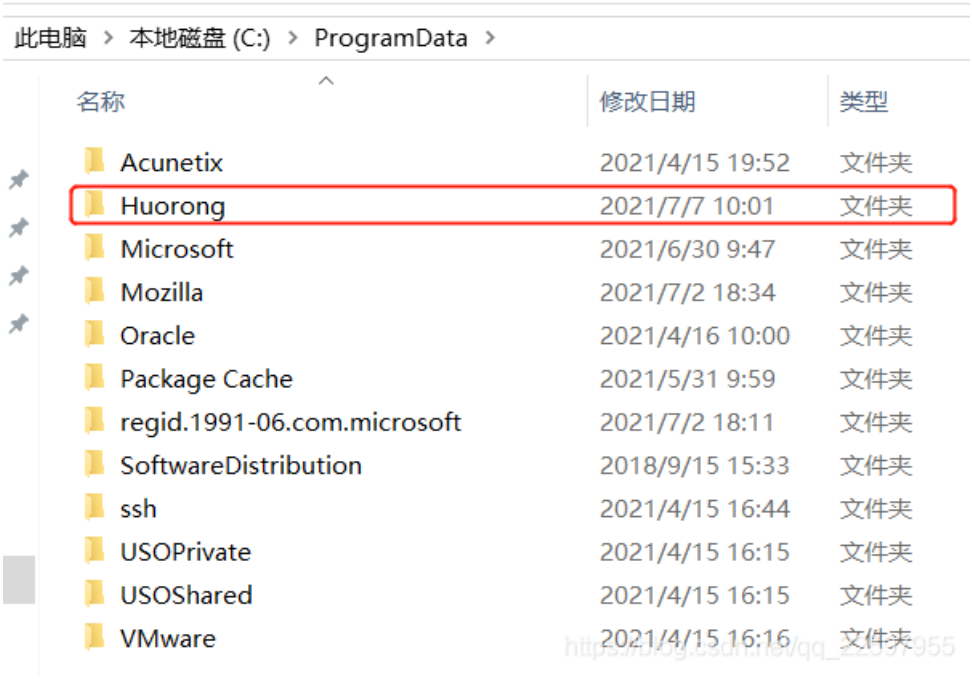
01—C:\ProgramData

写在前面

ProgramData文件夹是Vista引入的一个系统文件夹，保存了应用程序所需的数据，比如一些自定义的设置，或者缓存文件，都可能会存放在这里。

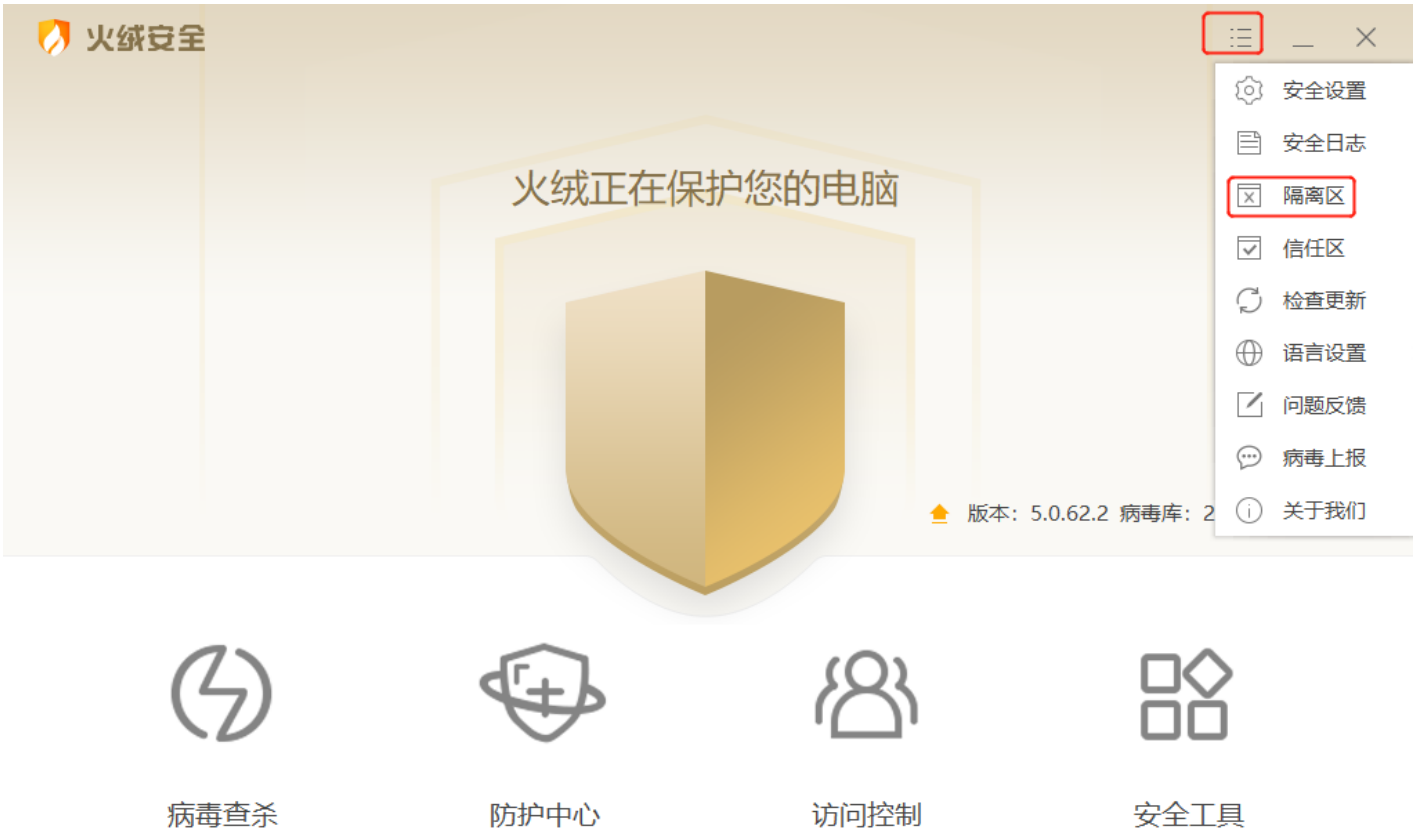
ProgramData是一个隐藏文件夹，如果你的资源管理器没有开启“显示隐藏文件夹”的话，它可能不会被显示出来，但是在地址栏输入“C:\ProgramData”还可以看到它的内容的。

火绒隔离区文件没有被加密，默认地址为C:\ProgramData。



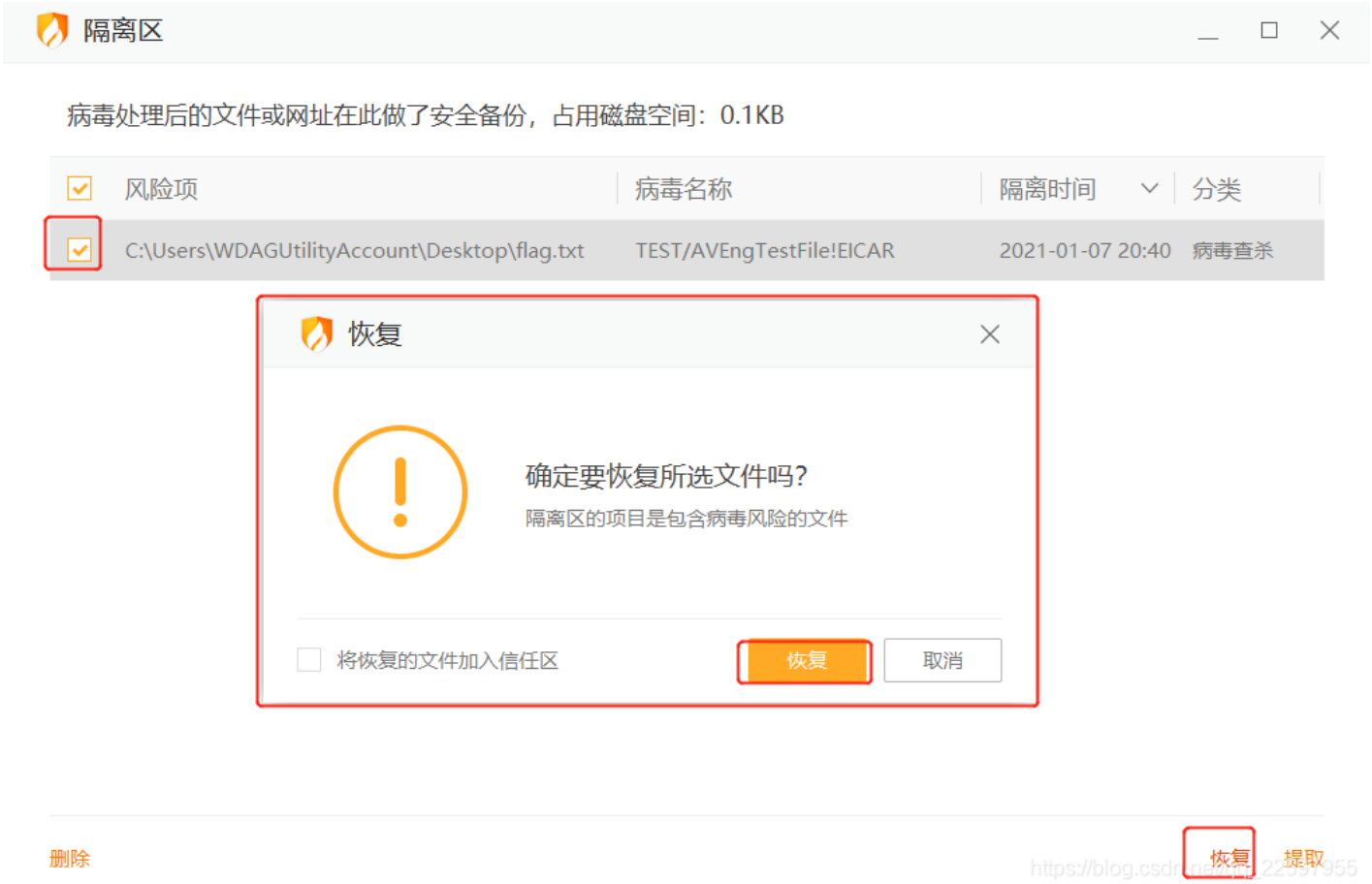
打开**C:\ProgramData**，直接键入，搜索不到，将题目中的附件火绒解压缩后放在**C:\ProgramData**下。

02—火绒安全



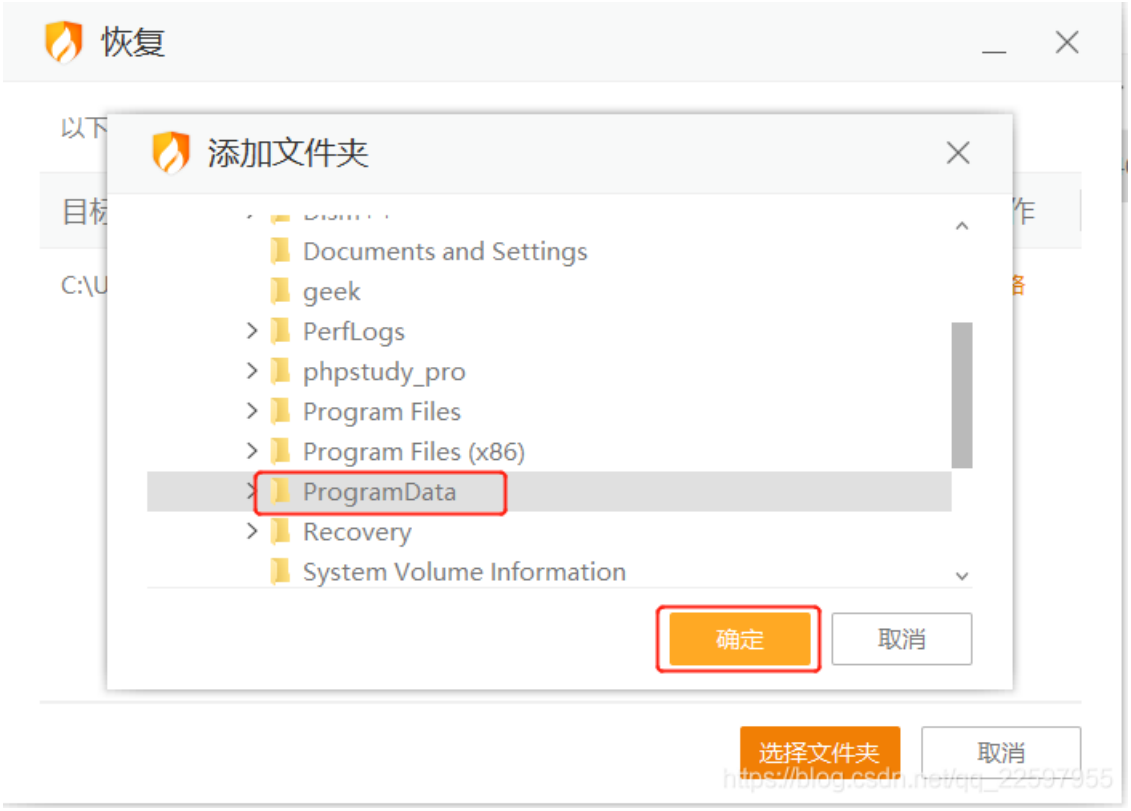
安装火绒安全软件，下载地址：https://www.huorong.cn/person5.html

选择菜单键-隔离区。



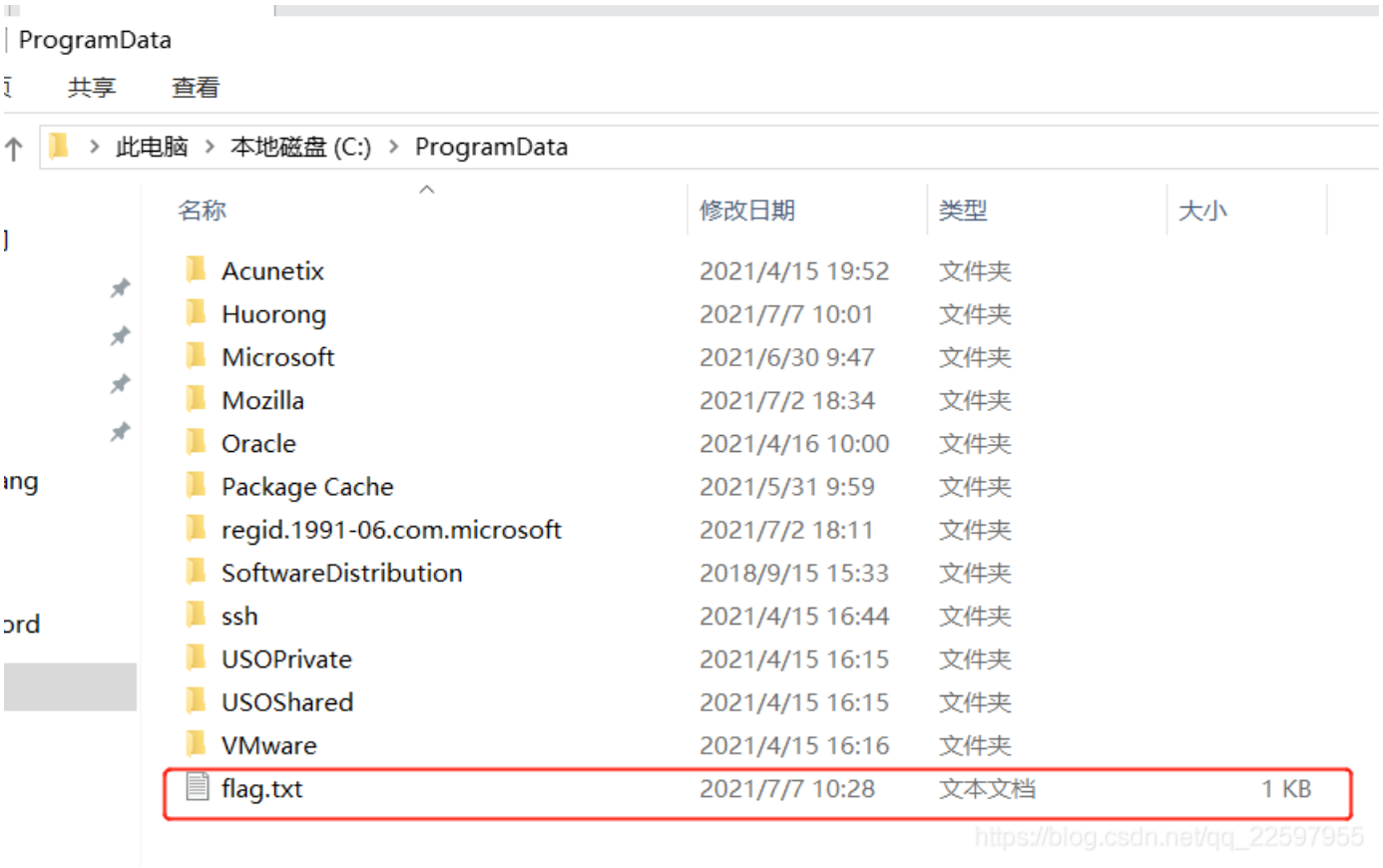
选中风险项-恢复。

恢复失败，选择文件夹。

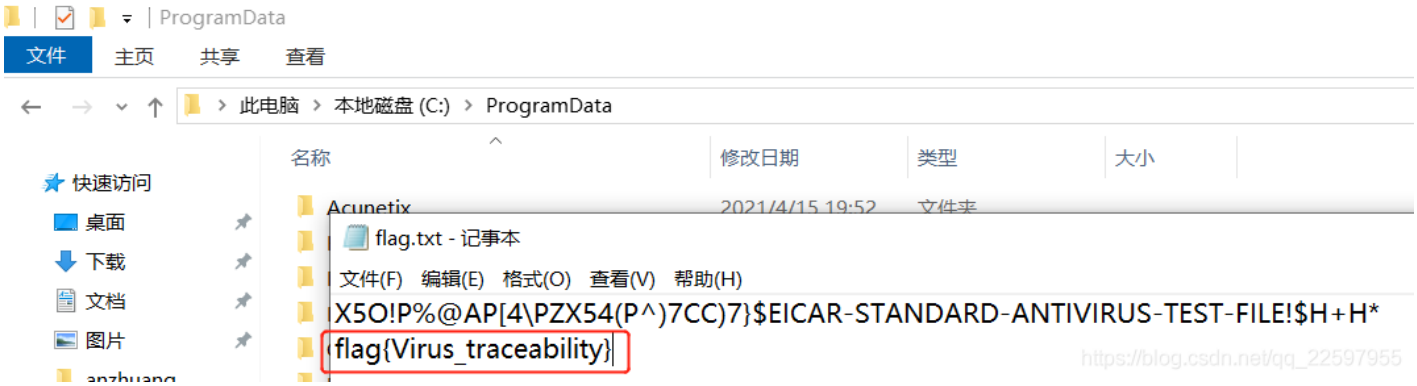


选择**C:\ProgramData**。

文件提取成功。



再次进入**C:\ProgramData**,发现新增了一个flag.txt文件。



打开flag.txt，得到flag。