

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_22597955/article/details/118540874

版权



[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

被勒索了

MISC

已解决

分数: 20

金币: 3

题目作者: [Tokeii](#)

一血: [犬来八荒](#)

一血奖励: 3金币

解决: 157

提示: 格式: flag{}

描述: 题主遇到真实事件改编 全盘所有文件都被加密了, 检查文件的时候发现了火绒的数据目录没有被加密, 不知道能不能发现什么线索

其他: [↓Huorong.zip](#)

请输入flag

提交

https://blog.csdn.net/qq_22597955

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。

此电脑 > 本地磁盘 (C:) > ProgramData >

名称	修改日期	类型
Acunetix	2021/4/15 19:52	文件夹
Huorong	2021/7/7 10:01	文件夹
Microsoft	2021/6/30 9:47	文件夹
Mozilla	2021/7/2 18:34	文件夹
Oracle	2021/4/16 10:00	文件夹
Package Cache	2021/5/31 9:59	文件夹
regid.1991-06.com.microsoft	2021/7/2 18:11	文件夹
SoftwareDistribution	2018/9/15 15:33	文件夹
ssh	2021/4/15 16:44	文件夹
USOPrivate	2021/4/15 16:15	文件夹
USOShared	2021/4/15 16:15	文件夹
VMware	2021/4/15 16:16	文件夹

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



https://blog.csdn.net/qq_22597955

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。

病毒处理后的文件或网址在此做了安全备份，占用磁盘空间：0.1KB

<input checked="" type="checkbox"/> 风险项	病毒名称	隔离时间	分类
<input checked="" type="checkbox"/>	C:\Users\WDAGUtilityAccount\Desktop\flag.txt	TEST/AVEngTestFile!EICAR	2021-01-07 20:40 病毒查杀



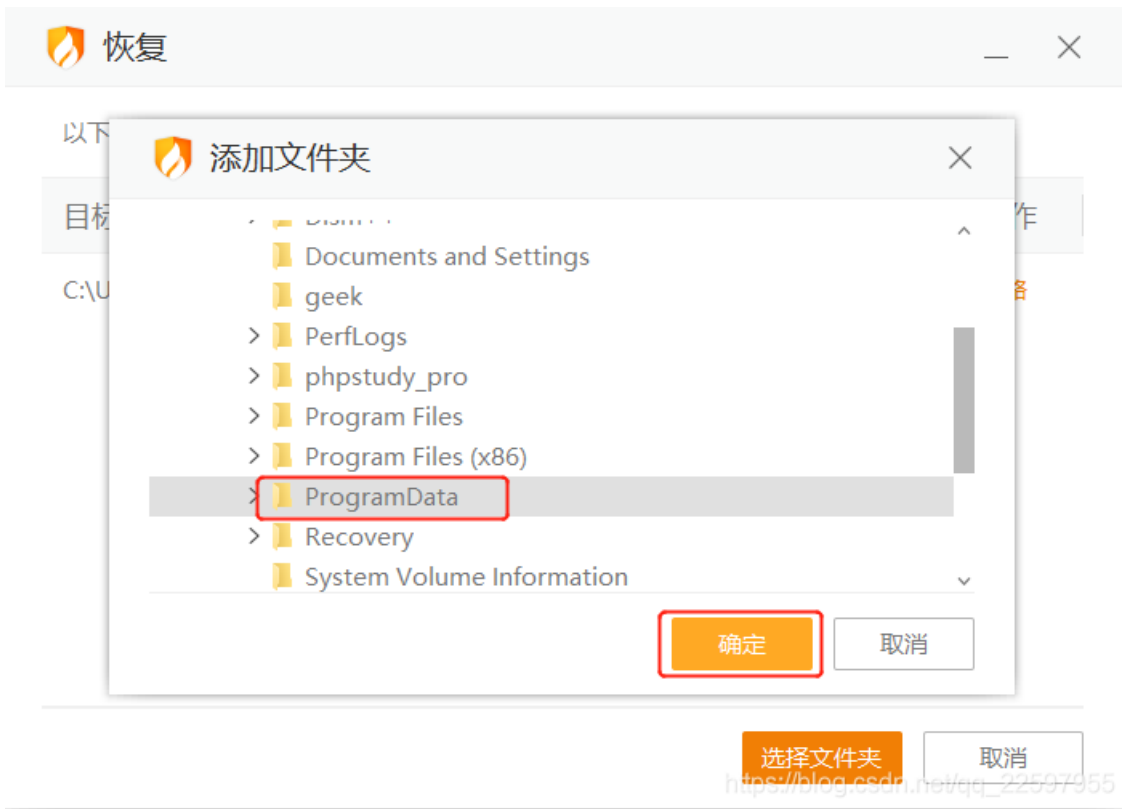
删除

https://blog.csdn.net/qj_22597955 恢复 提取

选中风险项-恢复。



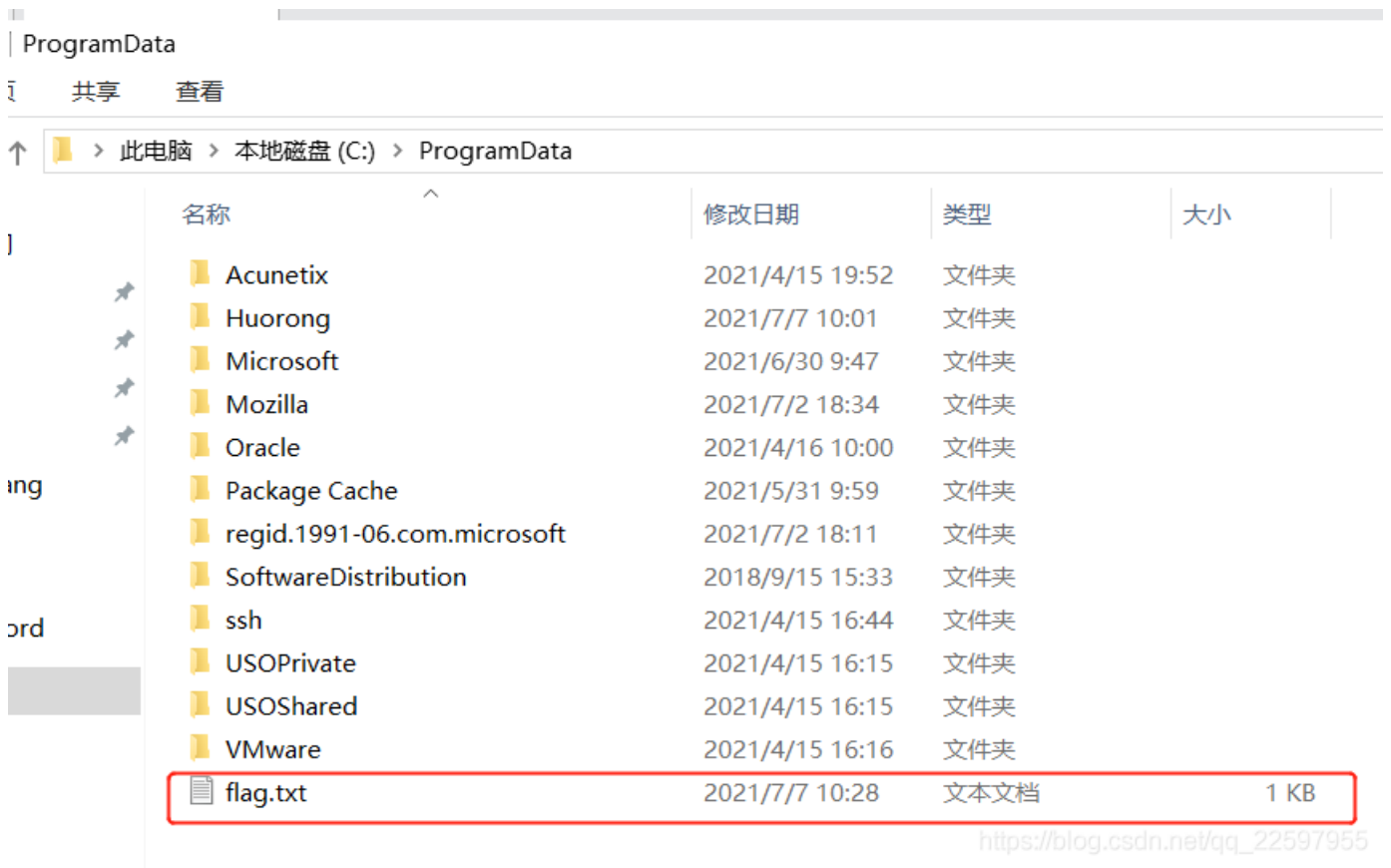
恢复失败，选择文件夹。



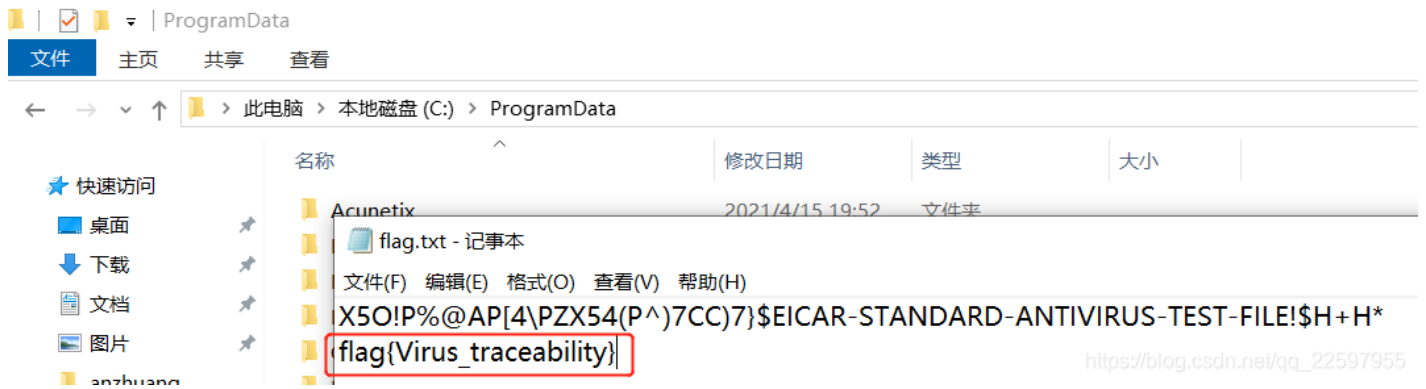
选择C:\ProgramData。



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。