

隐藏的木马文件

发表于 2021-01-25 更新于 2021-02-16 分类于 [Challenge](#) , [2020](#) , [工业信息安全技能大赛](#) , [石家庄站](#)
[Challenge | 2020 | 工业信息安全技能大赛 | 石家庄站 | 隐藏的木马文件](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自MOIN战队

题目描述

小明在工业生产现场的数控机床上发现了一个插着的U盘，u盘中都是些图片和文档，细心的小明总觉得这个文件好像有点异常，作为安全运营人员你能发现这个u盘中是否蕴藏着什么秘密呢？flag格式为：flag{}。——本题由恒安嘉新贡献

题目考点

- NTFS流隐写

解题思路

ntfs流隐写。NTFS文件系统支持给每个文件添加任意隐藏的数据，所以越来越多威胁采用这个特性隐藏自身。本题就是针对这个特性，对flag进行隐藏。

在解题过程中合理使用工具，因为题目中提到被植入木马病毒，并且所给出的都是些图片以及文本信息。那么合理使用一些ntfs流木马查杀的工具，如scanntfs，NtfsStreamsEditor2等，可以发现正常文件中异常的ntfs流。

□

查看或导出隐藏的信息进行分析，编写脚本对隐藏的信息进行解密。

□

编写脚本对这些base64编码进行解密。得到flag。

```
1
2
```

□

Flag

```
1 flag{8aseIsC0o1}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/石家庄站/a5JAcfsnHeng3AZaYQnbm.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge](#) [#2020](#) [#工业信息安全技能大赛](#) [#石家庄站](#)

[MMS协议分析](#)

[ICS TRITON](#)