隐藏的木马文件

2021-01-25 | 2021-02-16 | 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 MO1N 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。

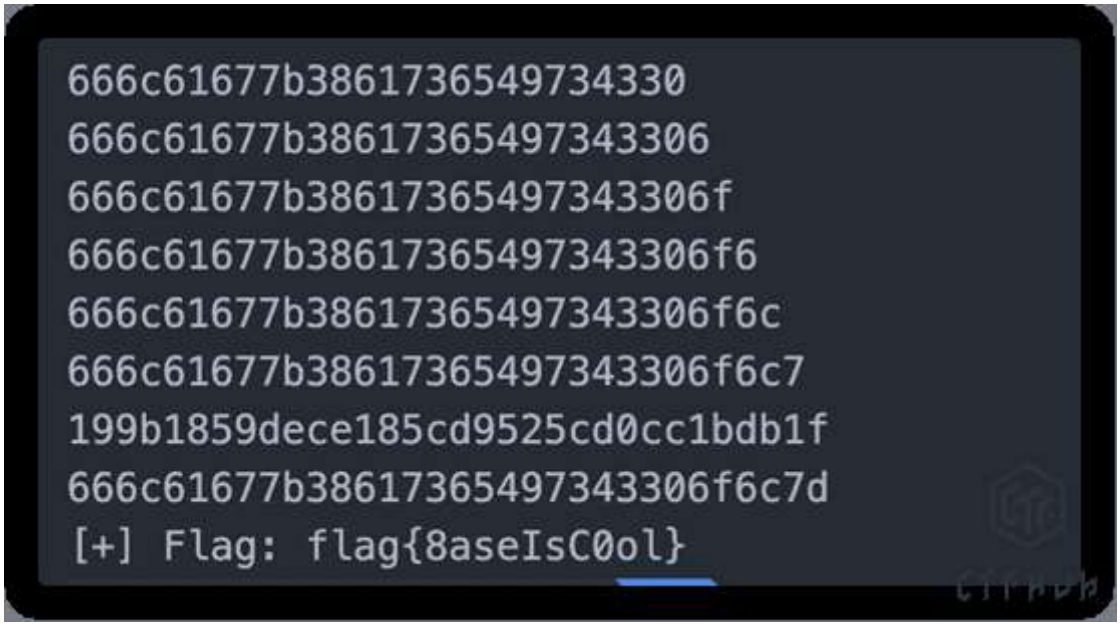
在解题过程中合理使用工具，因为题目中提到被植入木马病毒，并且所给出的都是些图片以及文本信息。那么合理使用一些ntfs流木马查杀的工具，如scanntfs，NtfsStreamsEditor2等，可以发现正常文件中异常的ntfs流。

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。

```
"bWFpbigpe2ludCBpLG5bXT12YVYtmveUAgHtecczrDpnBFPwQUVTyF4N==",
"ICAgICAgIDEpPDwoMTw8KDE+PjEpKSkrKCgxPDwxKTw8KDE8PDEpKSksKCgoMQp=",
"ICAgICAgIDw8ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAxKQq=",
"ICAgICAgIDw8ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAoMQp=",
"ICAgICAgIDw8MSk8PCgxPDwxKTw8ICAgICAgICAgKDE8PDEpKS0oKDE8PDEpPDwoCr==",
"ICAgIAkxPDwxKTw8KDE8PDEpKSsgICAgICAgICgoMTw8MSk8PCgxPDwoMT4+Ch==",
"ICAgICAgIDEpKSkrKDE8PCgxPj4xKSkpICAgICAgICAgICAgICAgICAgICAgICAgLAq=",
"ICAgICAgICgoKDE8PDEpPDwoMTw8MSkgICAgICAgICAgICAgICAgICAgICAgICA8PAo=",
"ICAgICAgICgxPDwxKTw8KDE8PDEpKS0oKDEgPDwxKTw8KDE8PDEpIDw8KDE8PCgxCl==",
"ICAgICAgID4+MSkpKS0oKDE8PDEpPDwoMTw8KDE+PjEpKSkpLCgoKDE8PDEpCp==",
"ICAgICAgIDw8KCAgICAxPDwgICAgICAgICAgICAgICAgICAgICAgICAgIDEpCt==",
"ICAgICAgIDw8KCAgICAxPDwgICAgICAgICAgICAgICAgICAgICAgICAgIDEpCu==",
"ICAgICAgIDw8KCAxPDwxKSktKCgxIDw8MSk8PCAoMSA8PDEpPDwoMSA8PAr=",
"ICAgICAgICgxPj4xKSkpLSgoMTw8MSk8PCgxPDwoMT4+MSkpKSksKCgoMTw8MSk8PAo=",
"ICAgICAgICgxPDwxKTw8KDE8PDEpPDwoMTw8MSkpLSgoMTw8MSk8PCgxPDwxKTw8KAr=",
"ICAgICAgICgxPDwxKTw8KDE8PDEpPDwoMT4+MSkpLCgoMTw8MSk8PCgxPj4xKSkpLAq=",
"ICAgICAgICgxPDwxKTw8KDE8PDEpPDwoMTw8MSkpLSgoMTw8MSk8PCgxPDwxKTw8Ch==",
"ICAgICAgICgxPDwoMT4+MSkpKS0oKCAgMTw8MSk8PCggICAgICAxPDwoMT4+Co==",
"ICAgICAgIDEpKSkpLCgoMTw8MSk8PCAgICAgICgxPDwxKSAgICAgICAgPDwoMTw8MSkpCl==",
"ICAgICAgICwoKCgxPDwxKTw8KDE8PCAgICAgIDEpPDwoICAgICAgIDE8PDEpPDwoMTw8MSkpLQ==",
"ICAgICAgICgoMTw8MSk8PCgxPDwxKSAgICAgKS0oMTw8KDE+PjEpICAgICAgICAgKSksKCgoCj==",
"ICAgICAgIDE8PDEpPDwoMTw8MSk8PCggICAgMTw8MSk8PCgxPDwxKSktICAgICgoMQp="
```

编写脚本对这些base64编码进行解密。得到flag。

```
1
2
```



Flag

```
1   flag{8aseIsC0ol}
```

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/a5JAcfnsnHeng3AZaYQnbm.html

Challenge # 2020 # 工业信息安全技能大赛 # 石家庄站

‹ MMS协议分析 ICS TRITON ›