# NTFS文件隐写

原创

神林、 于 2019-11-07 22:19:10 发布 2473 收藏 1

分类专栏： CTF



本文链接：https://blog.csdn.net/qq_41079177/article/details/102964134






## NTFS文件隐写

### NTFS文件是什么

NTFS文件系统时windows NT内核系列操作系统支持的、专门为网络和磁盘配额的，文件加密等管理安全特性设计的磁盘格式。NTFS比FAT文件系统更加稳定，更能也更为强大。

NTFS数据流文件也被称为 Alternate data streams，简称ADS，是NTFS文件系统的一个特性之一，允许单独的数据流文件存在，同时也允许文件附着多个数据流，除了主文件流之外还允许许多非主文件流寄生在主文件流中，使用资源派生的方式来维持与文件的相关信息，并且这些寄生的数据流文件我们使用资源管理器无法看到。

### NTFS文件特性

ntfs文件在资源管理器中是无法被看到的，NTFS流文件一种是附着于寄主文件，一种是单独的数据流文件，编辑NTFS文件具有两种方法，一种是通过系统的自带命令，另外一种是通过工具。

### NTFS流文件的创建

#### 1.单独文件流

```
echo "this is a stream file" > :test1.txt
```

上面命令所创建的是单独的NTFS流文件，系统不可见的同时我们无法通过普通方法看到，此时有两种方法，一种是命令：

```
notepad :test1.txt //这个命令只有自己已经知道NTFS流文件名的时候使用，局限性很大，同时失败几率大
```

另外一种是利用工具：Ntfs Streams Editor（师傅们记得扶墙！）


阶面就是这个样子，会扫描你选中文件夹中的所有具有NTFS流的文件。

### 2.关联文件流

比如我的D:\QQdata\　中有一个test1.txt，这个时候我们可以使用命令来将test2.txt 这个NTFS文件流和test1.txt文件联合起来，具体命令：

```
echo "this is tow stream file" > test1.txt:test2.txt //此时我们就将数据写入了合并到test1.txt文件的test2.txt文件流中
```

此时用文件流扫描的时候就会被发现,同时我们可以进行编辑以及删除.

## NTFS流写入木马

### 1.鄙人木马技术较弱,so...之后学了再说