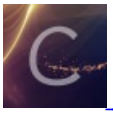
杂项--你知道他是谁吗？

转载

Wh0ale 于 2018-05-06 16:55:24 发布 471 收藏 1
分类专栏： 安全技术 文章标签： 杂项



1、根据提示windows、winrar考虑到NTFS交换数据流，原理参考文章【http://www.cnblogs.com/Chesky/p/ALTERNATE_DATA_STREAMS.html】

2、在windows XP虚拟机下进行操作，使用winrar解压文件

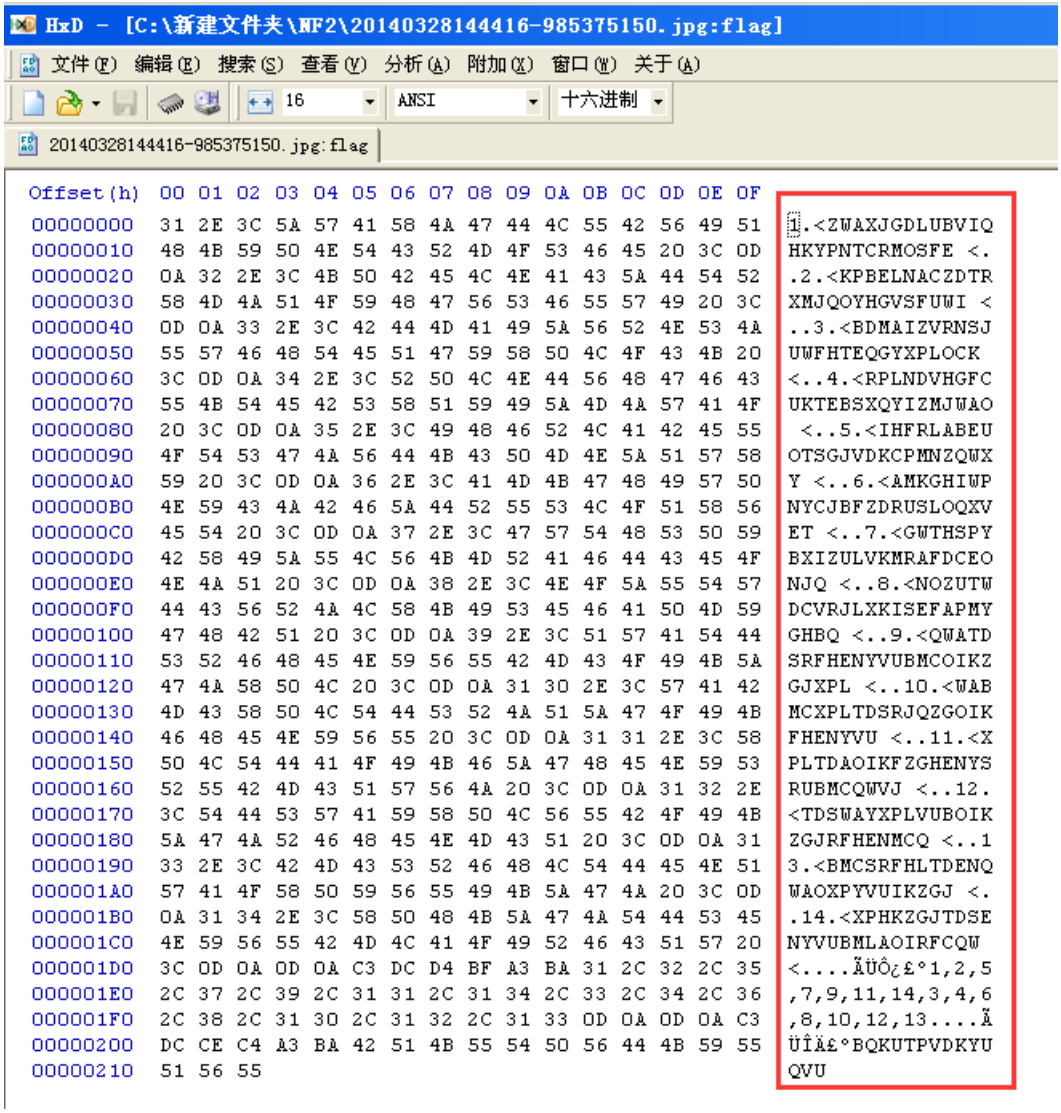
3、使用lads.exe查看解压后的文件是否隐含数据流，从结果来看，解压后的jpg文件隐含了数据，文件为flag

```
C:\新建文件夹\NF2>lads.exe /s

LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\新建文件夹\NF2\ with subdirectories

      size  ADS in file
----------  ------------------------------
       531  C:\新建文件夹\NF2\20140328144416-985375150.jpg:flag
         0  C:\新建文件夹\NF2\Thumbs.db:encryptable

       531 bytes in 2 ADS listed

C:\新建文件夹\NF2>
```

4、如何提取jpg文件中隐含的文件？使用HxD，在jpg文件同目录下，dos窗口中输入以下命令

```
C:\新建文件夹\NF2>hxd.exe 20140328144416-985375150.jpg:flag

C:\新建文件夹\NF2>
```

5、命令输入后，弹出HxD图形窗口，右侧红色框中的信息就是我们需要的内容；使用步骤4的命令打开文件，与运行图形界面下打开HxD再打开jpg文件，所看到的界面是完全不同的



6、直接另存为txt文件，打开，如下图所示

7、此为杰弗逊转轮加密，解密过程如下，首先还原转轮的原来顺序，即按照密钥顺序，重新排列14个转轮，重新排列后如下图所示

```
 1.<ZWAXJGDLUBVIQHKYPNTCRMOSFE <
 2.<KPBELNACZDTRXMJQOYHGVSFUWI <
 5.<IHFRLABEUOTSGJVDKCPMNZQWXY <
 7.<GWTHSPYBXIZULVKMRAFDCEONJQ <
 9.<QWATDSRFHENYVUBMCOIKZGJXPL <
11.<XPLTDAOIKFZGHENYSRUBMCQWVJ <
14.<XPHKZGJTDSENYVUBMLAOIRFCQW <
 3.<BDMAIZVRNSJUWFHTEQGYXPLOCK <
 4.<RPLNDVHGFCUKTEBSXQYIZMJWAO <
 6.<AMKGHIWPNYCJBFZDRUSLOQXVET <
 8.<NOZUTWDCVRJLXKISEFAPMYGHBQ <
10.<WABMCXPLTDSRJQZGOIKFHENYVU <
12.<TDSWAYXPLVUBOIKZGJRFHENMCQ <
13.<BMCSRFHLTDENQWAOXPYVUIKZGJ <
```

8、下一步调整每一个转轮，使得密文【BQKUTPVDKYUQVU】出现在同一个位置，（每一个转轮上的数据是可以循环移动的）

9、完成以上转动后，就可以发现有一列字母为可读明文

转自：http://www.shiyanbar.com/ctf/writeup/4971

转自：http://www.cnblogs.com/Chesky/p/ALTERNATE_DATA_STREAMS.html

##目录

##Content

####一、NTFS交换数据流（ADS）简介

在NTFS文件系统中存在着NTFS交换数据流（Alternate Data Streams，简称ADS），这是NTFS磁盘格式的特性之一。每一个文件，都有着主文件流和非主文件流，主文件流能够直接看到；而非主文件流寄宿于主文件流中，无法直接读取，这个非主文件流就是NTFS交换数据流。

ADS的作用在于，它允许一个文件携带着附加的信息。例如，IE浏览器下载文件时，会向文件添加一个数据流，标记该文件来源于外部，即带有风险，那么，在用户打开文件时，就会弹出文件警告提示。再如，在网址收藏中，也会附加一个favicon数据流以存放网站图标。

ADS也被用于一些恶意文件隐藏自身,作为后门。

####二、ADS应用

**最好在管理员模式下操作（需要文件的写权限）

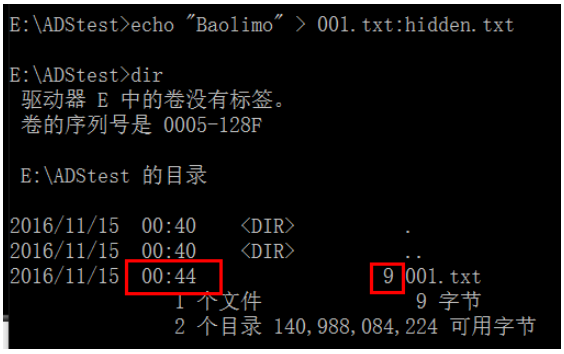
**格式为　宿主文件:关联的数据流文件

1.向ADS中写入文本文件

首先需要创建一个文本文件，这里的测试文件是001.txt

然后向这个文件写入ADS

```
echo "Baolimo" > 001.txt:hidden.txt
/*echo "隐藏内容" >宿主文件：关联文件*/
```



可以看到，文件字节没有改变，但是时间改动了。

还可以使用type命令，将已经存在的文件附加上去。

```
type "test002.txt" > "001.txt":"test002.txt"
/*type "要隐藏的附加文件">"宿主文件":"要隐藏的附加文件"
最好使用引号括起来，否则会引起误解
*/
```

2、向ADS中写入图像/音频/可执行文件

类似于写入文本文件，可以使用如下命令：

```
type "hidden.jpg" > "targe.jpg":"hidden.jpg"
type "hidden.mp4" > "targe.jpg":"hidden.mp4"
type "hidden.exe">>"targe.txt":"hidden.exe"
type "hidden.exe">>"targe.exe":"hidden.exe"
```

3.在Windows平台下使用ADS构造后门

在Windows XP中，可执行文件可以隐藏并且被执行。但是，微软已经发现了这个问题并进行了修复，目前在Windows Vista及后续系统中已经无法直接运行ADS中的可执行文件了。

我们可以使用mklink命令来建立一个链接，但必须要管理员权限才能完成。

```
mklink D:\moha.exe "hidden.txt":moha.exe
```

这里有一个在普通用户权限下也可操作的方法，使用Powershell的脚本。

项目地址

这个脚本只有两个参数：

Arguments “BadFunction -Lhost 192.168.1.11 -LPort 3333 -Payload weeeeee”

-URL即payload，-Arguments是Payload所需要的参数。

这个后门被运行后，会在注册表下

HKCU:\Software\Microsoft\Windows\CurrentVersion\Run中建立一个键值为update的键，注册表的键值调用wscript.exe来执行隐藏的VBS。执行完毕后，VBS脚本会解析执行在AppData目录下的payload（当然，是隐藏的）。

具体内容参考作者的文章。

在Windows10下，这个方法已经意义不大了，WD会对该脚本进行查杀。不过也可以考虑Winrar自解压文件，但是这个方法……呃……

从目前公开的资料来看，对ADS的利用主要集中于Web方面，但是我暂时不打算发展这方向的，这一块以后写一写。

4.Getshell（待完成）

####三、NTFS交换数据流在CTF中的应用——查看ADS内容

**如果文件原本是在压缩包内的，这时使用除WinRAR以外的软件进行提取会造成数据流丢失。所以务必使用WinRar进行文件解压。

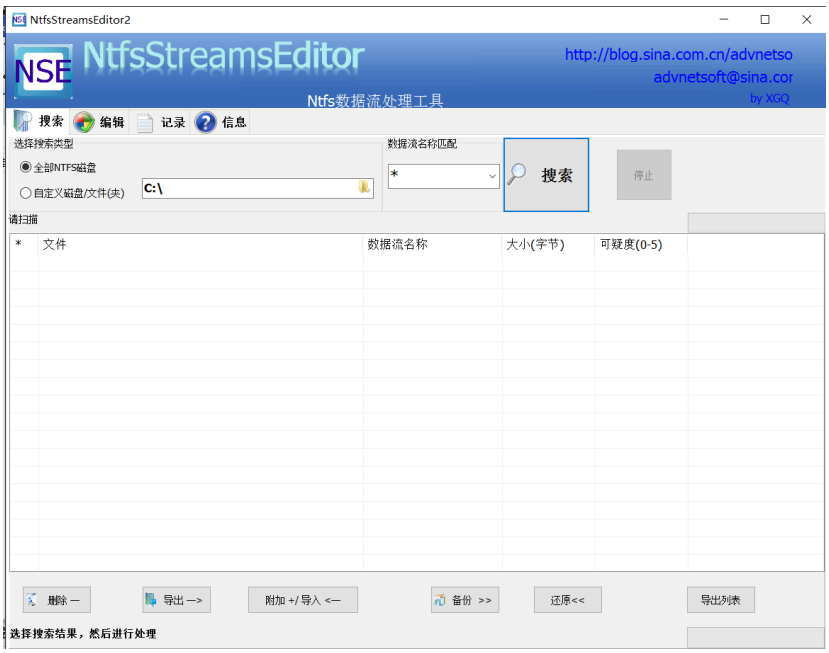
**最好不使用CMD命令（notepad）查看，这些命令对ADS的支持不是很好。

1.使用工具查看

使用工具查看是最快捷方便的方法了，可以使用NTFS Streams Info这个软件进行查看，但似乎是收费的。

地址：https://ntfs-streams-info.en.softonic.com/

在做CTF题时，我用的是Ntfs Streams Editor这个软件。



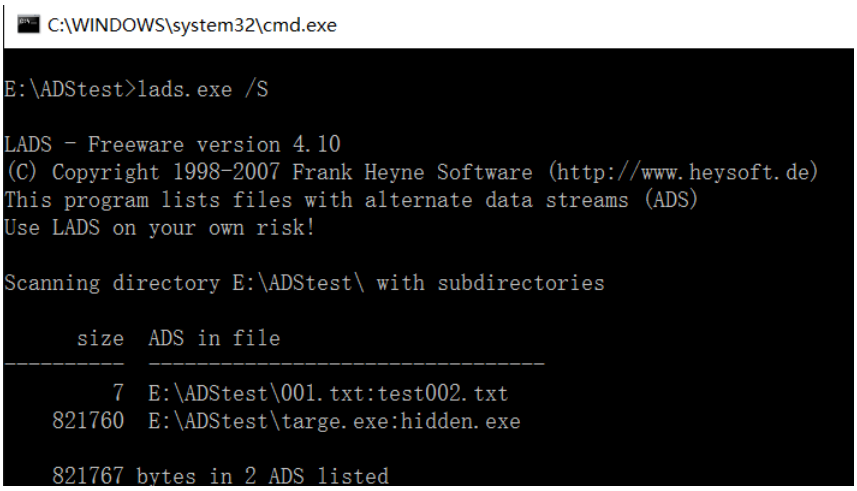
网盘下载：http://pan.baidu.com/s/1c2zbNaC

2.使用labs

网盘下载：http://pan.baidu.com/s/1slTJwMp

将labs.exe放入需要检测的文件的所在目录下。

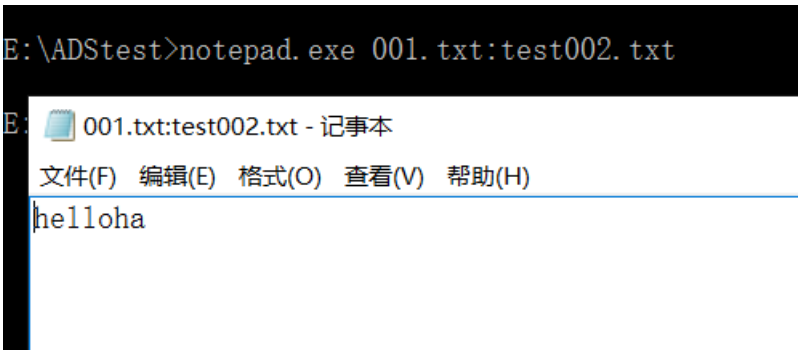
```
lads.exe File /S
/*这条命令会检测File这个目录下所有文件的隐藏流文件*/
lads.exe /S
/*检测根目录下的隐藏流文件*/
```



可以清楚地看到001.txt有着一个ADS：test002.txt。

知道了Hidden的文件，就可以进行查看了。

```
notepad.exe test.txt:hidden.txt
mspaint.exe test.txt:hidden.jpg
```

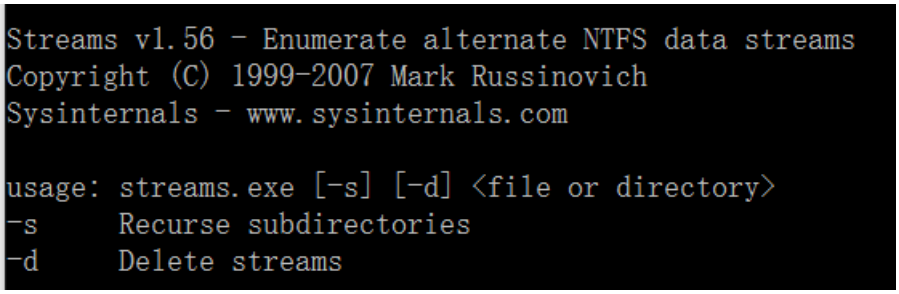


####四、清除ADS

这里可以采用之前的Ntfs Streams Editor这个软件直接删除ADS文件。

也可以用streams.exe进行清除。

```
streams.exe -d <File>
```



```
E:\ADStest>streams.exe -d E:\ADStest\001.txt

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

E:\ADStest\001.txt:
   Deleted :test002.txt:$DATA
```

若出现 Error deleting，说明这个进程还在运行，需要先结束该进程再进行删除操作。