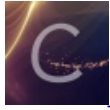


# 杂项--你知道他是谁吗?

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](#)



[安全技术](#) 专栏收录该内容

95 篇文章 9 订阅  
订阅专栏

- 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](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

HxD - [C:\新建文件夹\NF2\20140328144416-985375150.jpg:flag]

文件(F) 编辑(E) 搜索(S) 查看(V) 分析(A) 附加(O) 窗口(W) 关于(A)

16 ANSI 十六进制

20140328144416-985375150.jpg:flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	31	2E	3C	5A	57	41	58	4A	47	44	4C	55	42	56	49	51
00000010	48	4B	59	50	4E	54	43	52	4D	4F	53	46	45	20	3C	0D
00000020	0A	32	2E	3C	4B	50	42	45	4C	4E	41	43	5A	44	54	52
00000030	58	4D	4A	51	4F	59	48	47	56	53	46	55	57	49	20	3C
00000040	0D	0A	33	2E	3C	42	44	4D	41	49	5A	56	52	4E	53	4A
00000050	55	57	46	48	54	45	51	47	59	58	50	4C	4F	43	4B	20
00000060	3C	0D	0A	34	2E	3C	52	50	4C	4E	44	56	48	47	46	43
00000070	55	4B	54	45	42	53	58	51	59	49	5A	4D	4A	57	41	4F
00000080	20	3C	0D	0A	35	2E	3C	49	48	46	52	4C	41	42	45	55
00000090	4F	54	53	47	4A	56	44	4B	43	50	4D	4E	5A	51	57	58
000000A0	59	20	3C	0D	0A	36	2E	3C	41	4D	4B	47	48	49	57	50
000000B0	4E	59	43	4A	42	46	5A	44	52	55	53	4C	4F	51	58	56
000000C0	45	54	20	3C	0D	0A	37	2E	3C	47	57	54	48	53	50	59
000000D0	42	58	49	5A	55	4C	56	4B	4D	52	41	46	44	43	45	4F
000000E0	4E	4A	51	20	3C	0D	0A	38	2E	3C	4E	4F	5A	55	54	57
000000F0	44	43	56	52	4A	4C	58	4B	49	53	45	46	41	50	4D	59
00000100	47	48	42	51	20	3C	0D	0A	39	2E	3C	51	57	41	54	44
00000110	53	52	46	48	45	4E	59	56	55	42	4D	43	4F	49	4B	5A
00000120	47	4A	58	50	4C	20	3C	0D	0A	31	30	2E	3C	57	41	42
00000130	4D	43	58	50	4C	54	44	53	52	4A	51	5A	47	4F	49	4B
00000140	46	48	45	4E	59	56	55	20	3C	0D	0A	31	31	2E	3C	58
00000150	50	4C	54	44	41	4F	49	4B	46	5A	47	48	45	4E	59	53
00000160	52	55	42	4D	43	51	57	56	4A	20	3C	0D	0A	31	32	2E
00000170	3C	54	44	53	57	41	59	58	50	4C	56	55	42	4F	49	4B
00000180	5A	47	4A	52	46	48	45	4E	4D	43	51	20	3C	0D	0A	31
00000190	33	2E	3C	42	4D	43	53	52	46	48	4C	54	44	45	4E	51
000001A0	57	41	4F	58	50	59	56	55	49	4B	5A	47	4A	20	3C	0D
000001B0	0A	31	34	2E	3C	58	50	48	4B	5A	47	4A	54	44	53	45
000001C0	4E	59	56	55	42	4D	4C	41	4F	49	52	46	43	51	57	20
000001D0	3C	0D	0A	0D	0A	C3	DC	D4	BF	A3	BA	31	2C	32	2C	35
000001E0	2C	37	2C	39	2C	31	31	2C	31	34	2C	33	2C	34	2C	36
000001F0	2C	38	2C	31	30	2C	31	32	2C	31	33	0D	0A	0D	0A	C3
00000200	DC	CE	C4	A3	BA	42	51	4B	55	54	50	56	44	4B	59	55
00000210	51	56	55													

```

1.<ZWAXJGDLUBVIQ
HKYPNTPCRMOSFE <
.2.<KPBELNACZDTR
XMJQOYHGVSFUWI <
..3.<BDMAIZVRNSJ
UWFHTEQGYXPLOCK
<..4.<RPLNDVHGFC
UKTEBSXQYIZMJWAO
<..5.<IHFRLABEU
OTSGJVDKCPMNZQWX
Y <..6.<AMKGHIWP
NYCJBFZDRUSLOQXV
ET <..7.<GWTSPY
BXIZULVKMRAFDCOE
NJQ <..8.<NOZUTW
DCVRJLXKISEFAPMY
GHBQ <..9.<QWATD
SRFHENYVUBMCOIKZ
GJXPL <..10.<WAB
MCXPLTDSRJQZGOIK
FHENYVU <..11.<X
PLTDAOIKFZGHENYS
RUBMCQWVJ <..12.
<TDSWAYXPLVUBOIK
ZGJRFHENMCQ <..1
3.<BMCSRFLTDENQ
WAOXPYVUIKZGJ <
.14.<XPHKZGJTDSE
NYVUBMLAOIRFCQW
<...ÛÔç¹,2,5
,7,9,11,14,3,4,6
,8,10,12,13...Û
ÛÏÄºBQKUTPVDKYU
QVU

```

6、直接另存为txt文件，打开，如下图所示

20140328144416-985375150 - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

1.<ZWAXJGDLUBVIQHKYPNTPCRMOSFE <
2.<KPBELNACZDTRXMJQOYHGVSFUWI <
3.<BDMAIZVRNSJUFHTEQGYXPLOCK <
4.<RPLNDVHGFCUKTEBSXQYIZMJWAO <
5.<IHFRLABEUOTSGJVDKCPMNZQWXY <
6.<AMKGHIWPNYCJBFZDRUSLOQXVET <
7.<GWTSPYBXIZULVKMRAFDCOEONJQ <
8.<NOZUTWDCVRJLXKISEFAPMYGHBQ <
9.<QWATDSRFHENYVUBMCOIKZGJXPL <
10.<WABMCXPLTDSRJQZGOIKFHENYVU <
11.<XPLTDAOIKFZGHENYSRUBMCQWVJ <
12.<TDSWAYXPLVUBOIKZGJRFHENMCQ <
13.<BMCSRFLTDENQWAOXPYVUIKZGJ <
14.<XPHKZGJTDSENYVUBMLAOIRFCQW <

```

密钥: 1,2,5,7,9,11,14,3,4,6,8,10,12,13

密文: BQKUTPVDKYUQVU

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.<ZWAXJGDLUBUIQHKYPNTCRMOSFE <
2.<KPBELNACZDTRXMJQOYHGUSFUWI <
5.<IHFRLABEUOTSGJUDKCPMNZQWXY <
7.<GWTHSPYBXIZULUMRAFDCEONJQ <
9.<QWATDSRFHENYVUBMCOIKZGJXPL <
11.<XPLTDAOIKFZGHENYSRUBMCQWUJ <
14.<XPHKZGJTDSENYUUBMLAOIRFCQW <
3.<BDMAIZVRNSJUWFHTEQGYXPLOCK <
4.<RPLNDVHGFCUKTEBSXQYIZMJWAO <
6.<AMKGHIWPNYCBFZDRUSLOQXUET <
8.<NOZUTWDCVRJLXKISEFAPMYGHBQ <
10.<WABMCXPLTDSRJQZGOIKFHENYUU <
12.<TDSWAYXPLUUBOIKZGJRFHENMCQ <
13.<BMCSRFLTDENQWAOXPYUUIKZGJ <

```

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）

密文: BQKUTPVDKYUQVU

```

1.<VIQHKYPNTCRMOSFEZWAXJGDLUB <
2.<OYHGVSFUWIKPBEINACZDTRXMJQ <
5.<CPMNZQWXYIHFRLABEUOTSGJVDK <
7.<LVKMRADFCEONJQGWTHSPYBXIZU <
9.<DSRFHENYVUBMCOIKZGJXPLQWAT <
11.<LTDAOIKFZGHENYSRUBMCQWVJXP <
14.<UBMLAOIRFCQWXFKZGJTDSENYV <
3.<MAIZVRNSJUWFHTEQGYXPLOCKED <
4.<TEBSXQYIZMJWAOPLNDVHGFCUK <
6.<CJBFZDRUSLOQXUETAMKGHIWPNY <
8.<TWDCVRJLXKISEFAPMYGHBQNOZU <
10.<ZGOIKFHENYVUWABMCXPLTDSRJQ <
12.<UBOIKZGJRFHENMCQTDSWAYXPLV <
13.<IKZGJBMCSRFLTDENQWAOXPYVU <

```

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](http://www.cnblogs.com/Chesky/p/ALTERNATE_DATA_STREAMS.html)

## ##目录

####一、NTFS交换数据流（ADS）简介

####二、ADS应用

写入隐藏文件（文本\图像\可执行文件）

ADS在Windows平台下的利用——写入后门

ADS在Web中的利用——Get shell（待完成）

####三、NTFS交换数据流在CTF中的应用——查看ADS内容

####四、清除ADS

## ##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

```
E:\ADStest>dir
驱动器 E 中的卷没有标签。
卷的序列号是 0005-128F

E:\ADStest 的目录

2016/11/15  00:40    <DIR>          .
2016/11/15  00:40    <DIR>          ..
2016/11/15  00:40                9 001.txt
               1 个文件             9 字节
               2 个目录 140,988,084,224 可用字
```

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*/
```

```
E:\ADStest>echo "Baolimo" > 001.txt:hidden.txt
E:\ADStest>dir
驱动器 E 中的卷没有标签。
卷的序列号是 0005-128F

E:\ADStest 的目录

2016/11/15  00:40    <DIR>          .
2016/11/15  00:40    <DIR>          ..
2016/11/15  00:44                9 001.txt
               1 个文件             9 字节
               2 个目录 140,988,084,224 可用字节
```

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
*/
```

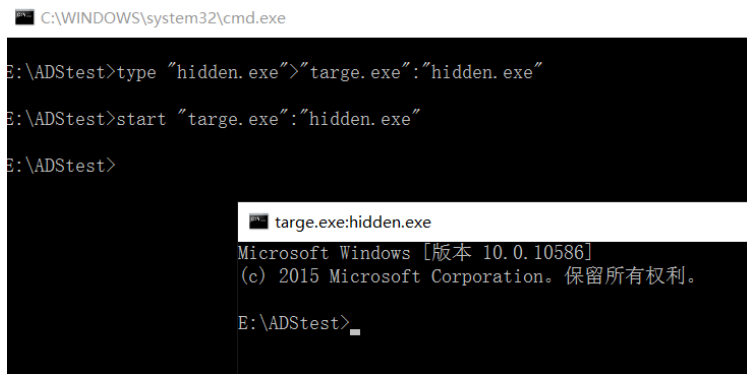
### 2、向ADS中写入图像/音频/可执行文件

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。



```
C:\WINDOWS\system32\cmd.exe
E:\ADStest>type "hidden.exe">"targe.exe":"hidden.exe"
E:\ADStest>start "targe.exe":"hidden.exe"
E:\ADStest>
```

```
targe.exe:hidden.exe
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation。保留所有权利。
E:\ADStest>
```

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 weeeeeee"

-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。

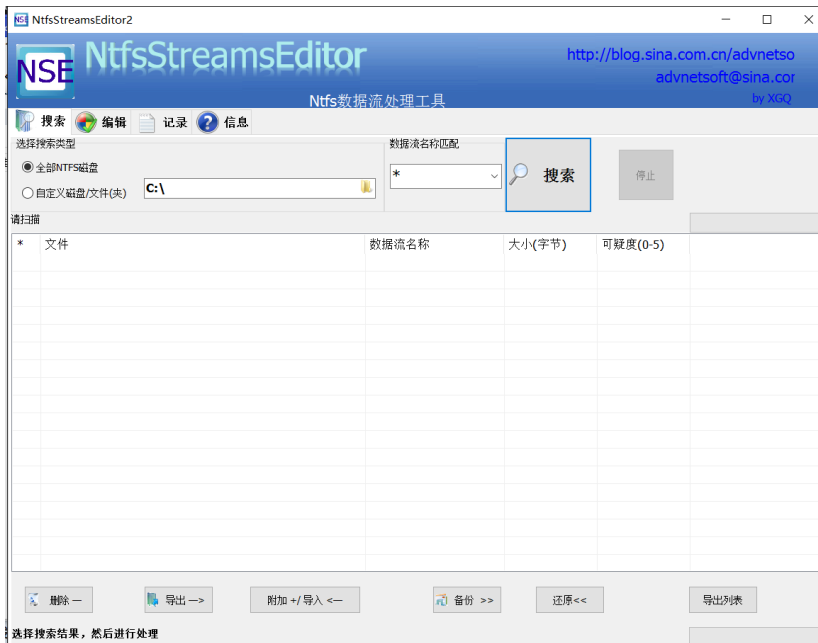
\*\*最好不要使用CMD命令（notepad）查看，这些命令对ADS的支持不是很好。

## 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/1sITJwMp>

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*/
```

```
C:\WINDOWS\system32\cmd.exe
E:\ADStest>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 E:\ADStest\ with subdirectories

  size  ADS in file
-----
      7  E:\ADStest\001.txt:test002.txt
 821760  E:\ADStest\targe.exe:hidden.exe

821767 bytes in 2 ADS listed
```

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
```

```
E:\ADStest>notepad.exe 001.txt:test002.txt
E: 001.txt:test002.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
helloha
```

#### ####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>
```

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

usage: streams.exe [-s] [-d] <file or directory>
-s      Recurse subdirectories
-d      Delete streams
```

```
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。