

# i春秋 流量分析 200分

原创

H9\_dawn 于 2020-04-11 16:57:40 发布 298 收藏

分类专栏: CTF 文章标签: web 安全

版权声明: 本文为博主原创文章, 遵循CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_43622442/article/details/105455160](https://blog.csdn.net/qq_43622442/article/details/105455160)

版权



CTF 专栏收录该内容

20 篇文章 2 订阅

订阅专栏

## i春秋 流量分析 200分

1. 下载源码发现, 比之前多了一个log文件, 肯定是有问题的:

|                 |                 |                    |        |
|-----------------|-----------------|--------------------|--------|
| password.pcapng | 2017/8/20 23:49 | Wireshark captu... | 546 KB |
| secret.log      | 2017/8/28 21:14 | 文本文档               | 21 KB  |

2. 直接用HxD打开log文件, 发现基本上看不懂, 这里有点奇怪:

```
20 00 00 00 E2 35 89 A9 9F EB 2A 04 13 05 01 02 00 ...â%öÿe*.....
30 01 00 00 00 01 CE 00 00 01 CE 00 00 00 01 00 00 .....î...î.....
40 00 00 00 E2 35 89 A9 A0 0B FF 02 02 20 C9 01 C5 ...â%ö .ÿ..É.Å
50 01 45 00 63 FF 7E 03 01 82 01 BF 01 00 11 00 73 .E.cÿ~...¿.....s
60 00 65 00 63 00 72 00 65 00 74 00 00 C3 00 00 01 .e.c.r.e.t..Å...
70 A3 49 01 A6 35 32 36 31 20 37 32 32 31 20 31 61 £I.¡5261 7221 1a
80 30 37 20 30 30 63 65 20 39 39 37 33 20 38 30 30 07 00ce 9973 800
90 30 20 30 64 30 30 20 30 30 30 0D 0A 30 30 30 0 0d00 0000..000
A0 30 20 30 30 30 20 37 35 38 65 20 65 65 39 35 0 0000 758e ee95
B0 20 64 31 33 64 20 62 38 32 38 20 38 36 37 65 20 dl3d b828 867e
C0 63 31 34 36 0D 0A 32 34 38 39 20 32 62 64 65 20 c146..2489 2bde
D0 38 64 65 39 20 63 62 61 31 20 61 34 64 66 20 35 8de9 cba1 a4df 5
E0 64 33 31 20 30 62 62 30 20 30 35 39 38 0D 0A 39 d31 0bb0 0598..9
F0 30 61 63 20 63 36 66 31 20 63 36 61 63 20 38 32 0ac c6f1 c6ac 82
00 63 30 20 65 32 33 39 20 34 31 61 61 20 33 63 34 c0 e239 41aa 3c4
10 33 20 31 61 31 36 0D 0A 30 64 32 37 20 61 30 64 3 1a16..0d27 a0d
20 32 20 66 63 35 34 20 32 63 61 35 20 37 35 66 33 2 fc54 2ca5 75f3
30 20 64 31 37 62 20 64 62 63 38 20 66 38 61 39 0D dl7b dbc8 f8a9.
40 0A 65 64 62 61 20 35 35 31 35 20 35 66 38 65 20 .edba 5515 5f8e
50 66 37 32 34 20 31 36 36 35 20 36 65 36 31 20 39 f724 1665 6e61 9
60 63 31 61 20 36 33 62 36 0D 0A 64 62 31 61 20 63 cla 63b6..db1a c
70 39 66 62 20 62 63 61 61 20 65 30 64 63 20 37 34 9fb bcaa e0dc 74
80 31 34 20 65 65 33 39 20 62 61 30 31 20 64 34 34 14 ee39 ba01 d44
90 65 0D 0A 62 64 36 33 20 32 35 65 33 20 38 64 35 e..bd63 25e3 8d5
A0 30 20 37 65 36 66 20 35 31 66 37 20 38 35 66 63 0 7e6f 51f7 85fc
B0 20 33 37 32 61 20 33 61 64 64 0D 0A 32 66 33 63 372a 3add..2f3c
C0 20 36 37 34 31 20 65 37 61 63 20 36 66 36 34 20 6741 https://blog.csdn.net/qq_43622442
```

3.我是想新建一个HxD复制进去的，结果发现每次都是复制的左侧的16进制，所以我先把右边的复制进一个txt文件：

```
5261 7221 1a07 00ce 9973 8000 0d00 0000
0000 0000 758e ee95 d13d b828 867e c146
2489 2bde 8de9 cba1 a4df 5d31 0bb0 0598
90ac c6f1 c6ac 82c0 e239 41aa 3c43 1a16
0d27 a0d2 fc54 2ca5 75f3 d17b dbc8 f8a9
edba 5515 5f8e f724 1665 6e61 9c1a 63b6
db1a c9fb bcaa e0dc 7414 ee39 ba01 d44e
bd63 25e3 8d50 7e6f 51f7 85fc 372a 3add
2f3c 6741 e7ac 6f64 e479 2439 758e ee95
d13d b828 32d0 48e0 2f32 9f08 e909 5a52
937e 526b
```



[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

4.然后再复制粘贴进HxD:

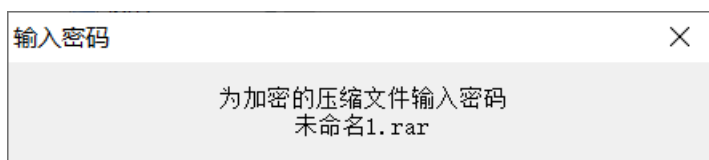
```
et(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 对应文本
0000 52 61 72 21 1A 07 00 CE 99 73 80 00 0D 00 00 00 Rar!...î™s€.....
0010 00 00 00 00 75 8E EE 95 D1 3D B8 28 86 7E C1 46 ....užī•Ñ=, (+~ÁF
0020 24 89 2B DE 8D E9 CB A1 A4 DF 5D 31 0B B0 05 98 $%+P.éË;#B]l.°.~
0030 90 AC C6 F1 C6 AC 82 C0 E2 39 41 AA 3C 43 1A 16 .~EñE~,Àá9A* <C..
0040 0D 27 A0 D2 FC 54 2C A5 75 F3 D1 7B DB C8 F8 A9 .' òùT,¥uóÑ(ŪÈø@
0050 ED BA 55 15 5F 8E F7 24 16 65 6E 61 9C 1A 63 B6 í°U. ž÷$.enæ.c¶
0060 DB 1A C9 FB BC AA E0 DC 74 14 EE 39 BA 01 D4 4E Ū.Éú4*àÛt.i9°.ŌN
0070 BD 63 25 E3 8D 50 7E 6F 51 F7 85 FC 37 2A 3A DD %c%ã.P~oQ÷...ú7*:Ý
0080 2F 3C 67 41 E7 AC 6F 64 E4 79 24 39 75 8E EE 95 /<gAç~odäy$9užī•
0090 D1 3D B8 28 32 D0 48 E0 2F 32 9F 08 E9 09 5A 52 Ñ=, (2ÐHà/2ÿ.é.ZR
00A0 93 7E 52 6B | ~Rk
```

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

5.看到了rar头，那么我们把这个数据包 文件->另存为：未命名1.rar

|  |                 |             |       |
|--|-----------------|-------------|-------|
|  secret.log | 2017/8/28 21:14 | 文本文档        | 21 KB |
|  未命名1.rar   | 2020/4/11 16:35 | WinRAR 压缩文件 | 1 KB  |

6.发现直接解压的话需要密码：







programming style based on the atomic parts of  
t characters to write and execute code.

ou can even run it on Node.js.

a script. Uncheck "eval source" to get back a

val Source

```

+[])+(!![]+[]) [!+[]+!+[]+!+[])+(!![]+[]) [+!+
+(!![]+[]) [+[]]+( [] (! []+[]) [+[]]+( [] []+[]
]+(!![]+[]) [+[]]+(!![]+[]) [!+[]+!+[]+!+[]]+
+(!![]+[]) [ (! []+[]) [+[]]+( [] []+[] [] [])] [+!+[]+
+[]]+(!![]+[]) [!+[]+!+[]+!+[]]+(!![]+[]) [+!+
]+(!![]+[] [ (! []+[]) [+[]]+( [] []+[] [] [])] [+!+
)] [+[]]+(!![]+[]) [!+[]+!+[]+!+[]]+(!![]+[])
]]) () [+!+[]+!+[]+!+[]]+(!![]+[]) [ (! []+[]) [+
+[]] [!+[]+!+[]]+(!![]+[]) [+[]]+(!![]+[]) [!+
+!+[]+[])] ()

```

[Run This](#)

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)

## 12.发现弹窗出现了密码，拿去解压得到flag:

flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
f1ag {C0nGr4t5_H4ck3r_Y0u_Ge7_Secr3t:})}
```

[https://blog.csdn.net/qq\\_43622442](https://blog.csdn.net/qq_43622442)