

一道关于chm设计ctf钓鱼的一些思考

转载

[weixin_30820077](#) 于 2017-06-09 10:14:00 发布 63 收藏


原文链接: <http://www.cnblogs.com/adisli777/p/6970637.html>

版权

版权声明: 本文为博主的原创文章, 未经博主同意不得转载

题目: flag就是文件指向的地址

文件:

 内网渗透.CHM 2017/3/9 16:17 编译的 HTML 帮... 1,858 KB

作为一名web狗的出题人, 这道ctf有点意思不是在于因为它难, 而是相对于一些代码审计以及一些杂项题来说, 它只是很好玩。

首先, 我们看到题目是一个chm文件。chm文件在钓鱼中比较常见的。比如很久以前的那些动作片种子, 下载回来总会有个chm文件的图片简介在文件目录下, 那些充满诱惑的FBI warning, 以及当你点击xxxavi.chm的时候。

相对于pdf绑马以及之前比较新Word漏洞CVE-2017-0199。它是我所知在win下伪装的比较好的一个。可以参考ping: [CHM渗透: 从入门到“入狱”](#)

writeup普及: CHM (Compiled Help Manual) 即“已编译的帮助文件”。它是微软新一代的帮助文件格式, 利用HTML作原文, 把帮助内容以类似数据库的形式编译储存。CHM支持Javas cript、VBs cript、ActiveX、Java Applet、Flash、

常见图形文件(GIF、JPEG、PNG)、音频视频文件(MID、WAV、AVI)等等, 并可以通过URL与Internet联系在一起。因为使用方便, 形式多样也被采用作为电子书的格式。以及下图



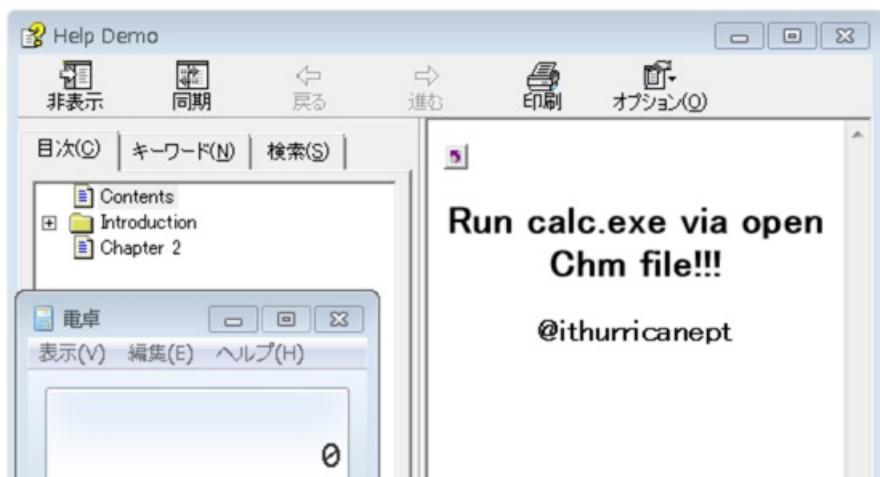
powertool
@ithurricanept

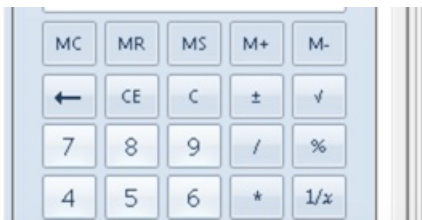


 Follow

Run calc.exe via open Chm file, no UAC warning and no av detects! Sample :

[mega.co.nz/#!tRkkFLwY!vww ...](http://mega.co.nz/#!tRkkFLwY!vww...)





根据这些知识，以及题目所问的，找出文件指向的地址即是后门连接的服务器就是flag。根据后门连接一般采用TCP或者DNS。这里根据自己pc的ip。

```
以太网适配器 以太网 2:
    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::ddc6:7f5:25b9:4e11%21
    IPv4 地址 . . . . . : 172.16.9.213
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 172.16.9.254
```

筛选tcp或者dns过滤大部分流量出来
ip.addr == 172.16.9.213 and tcp

以及一些标志符：

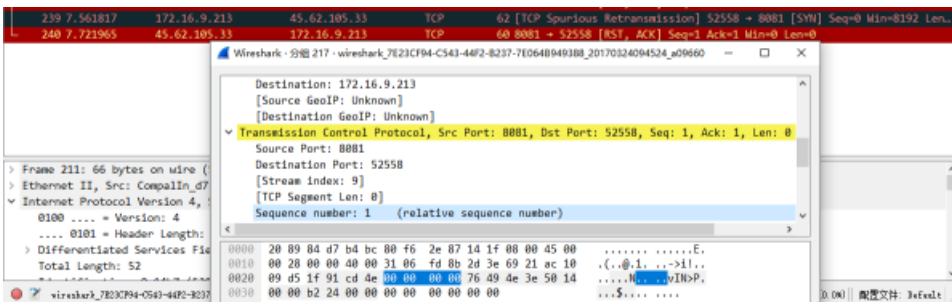
- SYN表示建立连接，
- FIN表示关闭连接，
- ACK表示响应，
- PSH表示有 DATA数据传输，
- RST表示连接重置。

No.	Time	Source	Destination	Protocol	Length	Info
230	6.877974	218.84.244.44	172.16.9.213	TCP	60	80 → 52559 [FIN, ACK] Seq=374 Ack=990 Win=17152 Len=0
231	6.878095	172.16.9.213	218.84.244.44	TCP	54	52559 → 80 [ACK] Seq=990 Ack=375 Win=65280 Len=0
232	6.878240	172.16.9.213	218.84.244.44	TCP	54	52559 → 80 [FIN, ACK] Seq=990 Ack=375 Win=65280 Len=0
233	6.892242	172.16.9.213	45.62.105.33	TCP	66	[TCP Spurious Retransmission] 52558 → 8081 [SYN] Seq=0 Win=819...
234	6.955555	Giga-Byt_f1:3b:61	Broadcast	ARP	60	Who has 172.16.9.6? Tell 172.16.9.94
235	6.975520	218.84.244.44	172.16.9.213	TCP	60	80 → 52559 [ACK] Seq=375 Ack=991 Win=17152 Len=0
236	7.045714	45.62.105.33	172.16.9.213	TCP	60	8081 → 52558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
237	7.297441	192.168.8.209	224.11.11.11	IGMPv2	60	Membership Report group 224.11.11.11
238	7.318456	172.16.9.132	172.16.9.255	NBNS	92	Name query NB WPAD<00>
239	7.561817	172.16.9.213	45.62.105.33	TCP	62	[TCP Spurious Retransmission] 52558 → 8081 [SYN] Seq=0 Win=819...
240	7.721965	45.62.105.33	172.16.9.213	TCP	60	8081 → 52558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
241	7.754211	172.16.9.130	172.16.9.255	UDP	1482	63991 → 1689 Len=1440
242	7.778039	172.16.9.111	255.255.255.255	UDP	1482	61694 → 1689 Len=1440

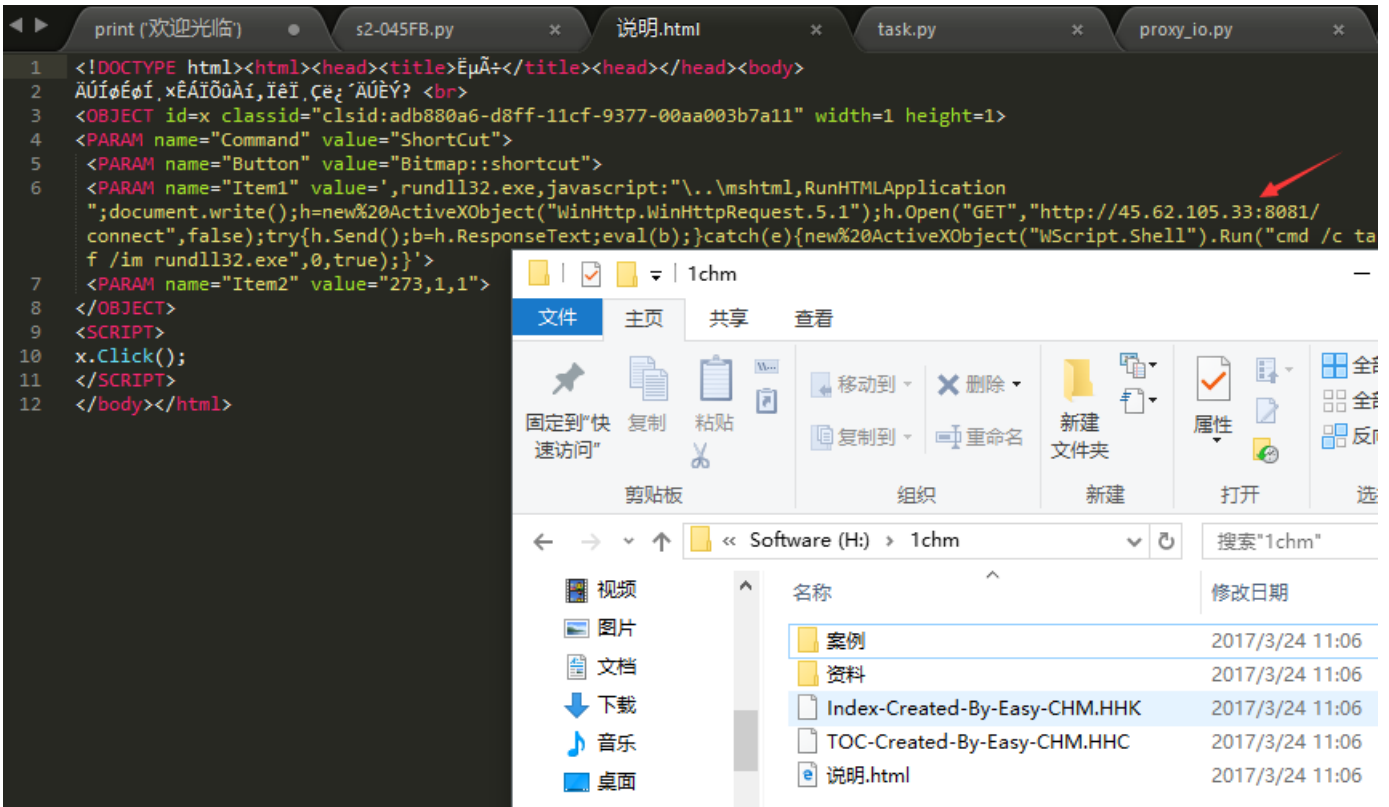
可以发现xxx.xxx.xxx.xxx在与本机进行tcp的通信，根据两个tcp的两个标识RST ack。可以发现文件在与服务器进行通信。这里flow下这些tcp流，确定文件指向的后门服务器地址。

这里cobalt strike 的teamservice没有开启，但是可以确定在双方在“串通”进行尝试握手。

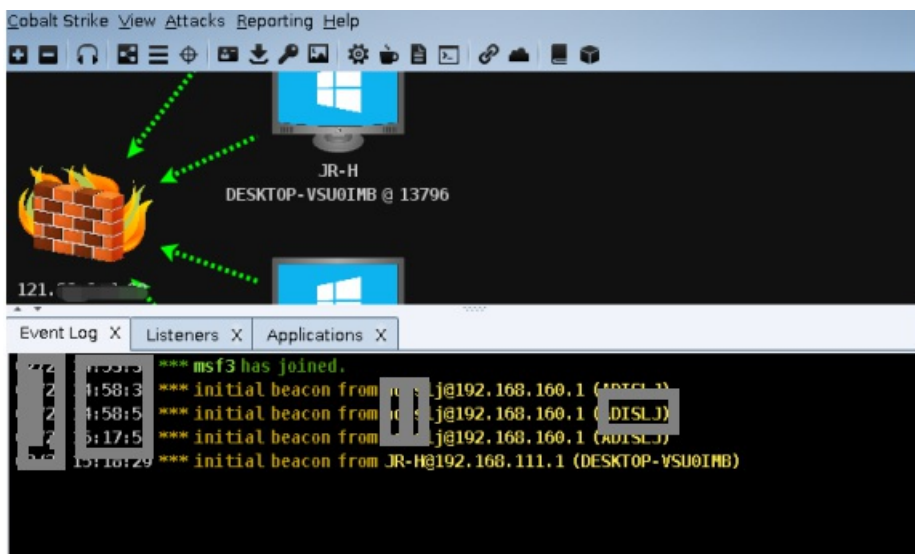
No.	Time	Source	Destination	Protocol	Length	Info
211	6.235251	172.16.9.213	45.62.105.33	TCP	66	52558 → 8081 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
217	6.388080	45.62.105.33	172.16.9.213	TCP	60	8081 → 52558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
233	6.892242	172.16.9.213	45.62.105.33	TCP	66	[TCP Spurious Retransmission] 52558 → 8081 [SYN] Seq=0 Win=8192 Len=0
236	7.045714	45.62.105.33	172.16.9.213	TCP	60	8081 → 52558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



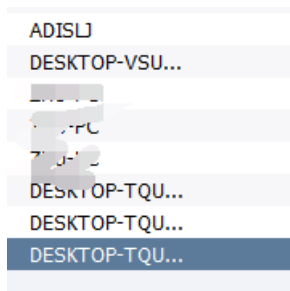
另一种方法溯源 chm是可以反编译为html的。使用windows自带的hh.exe 则可进行反编译。hh -decompile h:\1chmF\1.chm 【1.chm是内网渗透.chm，这里改了一下名字】



很典型的利用了chm exec 调用js，能做到免杀市面上很多杀毒软件，这里随便用了个测试截图



这里记录一次被黑与反杀的一个过程。



限号第一次发在土司上了。好久都没写博客，只好把笔记带上



分享一个我制作的免杀样本 链接: <http://pan.baidu.com/s/1jH6mid4> 密码: 2qpa

一只在安全道路上慢跑的菜鸡

转载于: <https://www.cnblogs.com/adislj777/p/6970637.html>