东华杯-Misc250-面具-writeup(zip伪加密)

原创

C

misc 专栏收录该内容

4篇文章0订阅

订阅专栏

三步:提取-分析-解密

第一步:提取

压缩包加密有一种伪加密的方法,首先我们需要先了解一下zip文件的格式信息。

一个 ZIP 文件由三个部分组成:

压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

其中:

压缩源文件目录区:

50 4B 01 02: 目录中文件文件头标记(0x02014b50)

3F 00: 压缩使用的 pkware 版本

14 00: 解压文件所需 pkware 版本

00 00: 全局方式位标记(有无加密,这个更改这里进行伪加密,改为09 00打开就会提示有密码了)

08 00: 压缩方式

我们用010editor打开压缩包,搜索14 00 09 00,发现果然存在

| 🌛 010 Editor - C:\Users\win7\De | esktop\1.zip | | | | | |
|----------------------------------|-------------------------------------------------------------|----------------------------------------|----------------|----------------------------|---------------------------------|---------------|
| <u>File Edit Search View For</u> | mat Scr <u>i</u> pts Temp <u>l</u> ates <u>T</u> ools | <u>W</u> indow <u>H</u> elp | | | | |
| i 🗅 + 📂 + 🔚 🖨 🎒 🍅 | 🎒 i % 🗈 🔒 😡 🛯 🖉 | 🕂 🦻 🌛 😓 🗛 📐 Her | R T T T | 🔲 🖻 📣 🗶 🔽 🍕 | | 50 |
| Workspace & X | 1. zip 📓 Startup 🛋 | | | | | |
| 😂 Open Files 🔷 | ▼ Edit As: Hex ▼ Run Script | 🔻 – Run Template: ZIPTemplate.bt 🤻 | r Þ | | | - |
| C:\Users\win7\\1.zip | 0 1 2 3 4 5 | 6789ABCD | E F 01234567 | 9ABCDEF | | |
| 🥫 E:\ctf工具\Template1.bt | 2:5840h: BD C5 FF C7 C4 FI | F 83 FF 8B F1 7F 6F F1 FF | 90 F8 ₩AÿÇAÿfÿ | n.oñÿ.ø | | |
| 📂 Favorite Files 🛛 😑 | 2:5860h: FE EF 2D FE 9F 25 | 5 FE 7F F8 BF 18 FF F7 16 | FF CF bi-bY%b. | 2-2 <u>2</u> 1 87.V÷.VI | | |
| 🔗 Recent Files | 2:5870h: 13 FF 3F FD 5F 80 | C FF 7B 8B FF 17 89 FF 5F | FE 2F .ÿ?ý_Œÿ{ | ÿ.‰ÿ_þ/ | | |
| C:\Users\\flag.zip | 2:5880h: C6 FF BD C5 FF C | B C4 FF 6F FF 17 E3 FF DE | E2 FF Æÿ₩ÅÿËÄÿ | oÿ.ãÿÞâÿ | | |
| C:\\C4n_u_find_m3_DB | 2:5890h: 55 E2 FF 8F FF 8 | B F1 7F 6F F1 FF 3A F1 FF | D7 FF Uâÿ.ÿ<ñ. | oñÿ:ñÿ×ÿ | | |
| C:\\C4n_u_find_m3_DB | 2:58A0h: C5 F8 BF B7 F8 / | 0 00 00 00 00 00 00 00 00 00 | 95 FE AØ2 Ø. Ø | /сурив >р | | |
| C:\Users\win7\\2.zip | 2:58C0h: 00 00 00 00 00 00 | 0 00 00 00 00 00 90 F1 07 | 50 4B | ñ.PK | | |
| C:\Users\\flag.bf | 2:58D0h: 01 02 3F 00 14 00 | 0 09 00 08 00 6C 87 42 49 | 56 A1 | l‡BIV; | | |
| C:\Users\\题目.png | 2:58E0h: A2 02 A7 58 02 00 | 0 00 00 30 00 09 00 24 00 | 00 00 ¢.§X | \$ | | |
| C:\Users\\svega.mp3 + | 2:58F0h: 00 00 00 00 20 00 | 0 00 00 00 00 00 00 66 6C | 61 67 | flag | | |
| 🞯 Files 💋 Explorer 🔹 🕨 | 2:5910h: 00 B8 22 67 44 88 | B 1C D2 01 70 51 53 E0 85 | 1C D2 "gDc.Ò | pOSàÒ | | |
| Inspector 🗗 🗙 | 2:5920h: 01 70 51 53 E0 8 | 5 1C D2 01 <mark>50 4B 05 06 00</mark> | 00 00 .pQSàÒ | PK | | |
| Type Value ^ | 2:5930h: 00 01 00 01 00 5 | B 00 00 00 CE 58 02 00 (00 | 00)[| .îx() | | |
| Signed Byte 20 | | | | | | |
| Unsigned Byte 20 | | | | | | |
| Signed Short 20 | | | | | | |
| Signed Int 589844 | | | | | | * |
| Unsigned Int 589844 | Template Results - ZIPTemplate.bt | | | | | × |
| Unsigned Int64 975817452 | Name | Value Start | Size Col | or Comm | ent | |
| Float 8.265475e-40 | Struct ZIPFILERECORD record struct ZIPDIPENTRY disEctory | flag.vmdk Oh | 258CEh Fg: 1 | ig: | | |
| Double -6.4698448 + | Struct ZIPENDLOCATOR endLocator | 25929h | 16h Fg: 1 | ig: | | |
| 🛃 Auto 🔚 Variables 🧗 🕩 | | | | | | |
| Output | | | | | | 8 × |
| Address | | Value | | | | |
| Found 1 occurrences of '14 | 00 09 00'. | | | | | |
| 258D4h 14 00 09 0 | 00 | | | | | |
| | | | | | | |
| I Dutnut S Find S Find i | n Rilon 💿 Compose 🗔 History | an 🔽 Chaolerum 🕞 Progore | | | | |
| Found 1 occurrences of '14 00 00 | | am Citecksum Cm 110Cess | | C+ | rt: 153812 [258D/b] Sel- 4 [4b] | S 🕁 👌 🔹 🧶 🗮 🖉 |
| | | | | 3(4) | 1. 155512 [256541] Sel. 4 [41] | |

第二步:分析

很明显,这是一个磁盘取证分析环节,先下载安装好磁盘取证工具AccessData FTK

Imager(http://download.csdn.net/download/streetmilk/5238752),或者其他工具也行。直接打开,可以发现两个文件:

| <u></u> | | | | |
|---------------------------------------------------|-----------------------------------|-----------------|---------------|---------------------|
| 🔍 AccessData FTK Imager 3.1.2.0 | | | | e f |
| <u>File View M</u> ode <u>H</u> elp | | | | |
| 🗛 🎪 🗞 🚖 🚘 🖨 🖬 🗧 🚛 🛥 📼 🚥 | 🖻 🥄 🗋 🖹 🖻 🐱 😹 🖹 🥊 | | | |
| Evidence Tree × | File List | • | | × |
| ⊟- 💁 flag. vmdk | Name Siz | e Type | Date Modified | |
| Partition 1 [9MB] | \$BadClus |) Regular File | 2016/10/2 8: | |
| 日 『 新加壱 [MTFS] | \$Bitmap | L Regular File | 2016/10/2 8: | |
| [mallocated space] | \$Boot | 8 Regular File | 2016/10/2 8: | |
| [orphan] | \$130 | 1 NTFS Index A | 2016/10/2 8: | |
| | LogFile 2,04 | 8 Regular File | 2016/10/2 8: | |
| | SMFT 25 | 5 Regular File | 2016/10/2 8: | |
| | SMFTMirr | 1 Regular File | 2016/10/2 8: | |
| | Secure \$ | L Regular File | 2016/10/2 8: | _ |
| | \$TXF_DATA | L NTFS Logged | 2016/10/2 8: | = |
| | UpCase 12 | 3 Regular File | 2016/10/2 8: | |
| | \$Volume |) Regular File | 2016/10/2 8: | |
| | X key_part_one.txt | L Regular File | 2016/10/2 8: | |
| | Key_part_two.txt | 3 Regular File | 2016/10/2 8: | |
| | P | | | ÷ |
| | | | | * |
| Custom Content Sources × | +++++ [->+++ +<]>+ +++ < +++++ + | +.+ +++++ .‹+++ | | |
| Evidence:File System Path File Options | <1><+++ [->++ +<1>+ +< | +++ .<+++ +[->- | | |
| | +++++<]>++++ +++. < +++++ [-> | -<] >+++ | .<+++ [-><]>< | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| New Edit Remove Remove All Create Image | | | | |
| Properties Hex Value Int Custom Conte | | | | - |
| flag.vmdk/Partition 1 [9MB]/新加卷 [NTFS]/[root]/key | /_part_one.txt | | | - 乞 🕈 🌙 🦻 🎍 📟 🐁 🕇 🗡 |

| AssessData ETK Imager 2120 | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| AccessData FIX Imager 5.1.2.0 | | |
| <u>File view M</u> ode <u>H</u> elp | | |
| 🕼 🎎 🗣 🗠 🚘 🖾 🛏 🖬 🚑 🚑 🚍 🚥 | | 52 |
| Evidence Tree × | File List | |
| Comparison of the system | Name Size Type Date Modified \$BadClus 0 Regular File 2016/10/2 8: \$Stimap 1 Regular File 2016/10/2 8: \$Stoot 8 Regular File 2016/10/2 8: \$Stoot 8 Regular File 2016/10/2 8: \$Stoot 4 NTFS Index A 2016/10/2 8: \$StoofFile 2,048 Regular File 2016/10/2 8: \$MFT 256 Regular File 2016/10/2 8: \$MFT 4 Regular File 2016/10/2 8: \$Stype 1 Regular File 2016/10/2 8: \$Stype 1 Regular File 2016/10/2 8: \$Stype 128 Regular File 2016/10/2 8: \$Stolume 0 Regular File 2016/10/2 8: \$Stolume 0 Regular File 2016/10/2 8: \$Wext cast two tot 1 Regular File 2016/10/2 8: | A |
| | | - |
| | [| |
| Custom Content Sources × | Ock. Ock. Ock. Ock. Ock. Ock. Ock. Ock. | |
| Evidence:File System Path File Options | Ock. Ock. Ock. Ock! Ock! Ock! Ock! Ock. Ock? Ock. Ock. Ock. Ock. Ock. Ock. Ock. Ock. | = |
| Properties Hex Value Int Custom Conte | I are | |
| flag.vmdk/Partition 1 [9MB]/新加卷 [NTFS]/[root]/key | y_part_two.txt | |

第三步: 解密 可以看到两个文件里面的内容为brainfuck跟Ook编码,直接在线解密即可得到结果

https://www.splitbrain.org/services/o