2018年金融业ctf竞赛 backdoor 流量数据分析writeup

原创

qq_42773814 于 2018-08-08 11:25:37 发布 2451 收藏 3
文章标签： 金融业 ctf流量数据分析 文件头

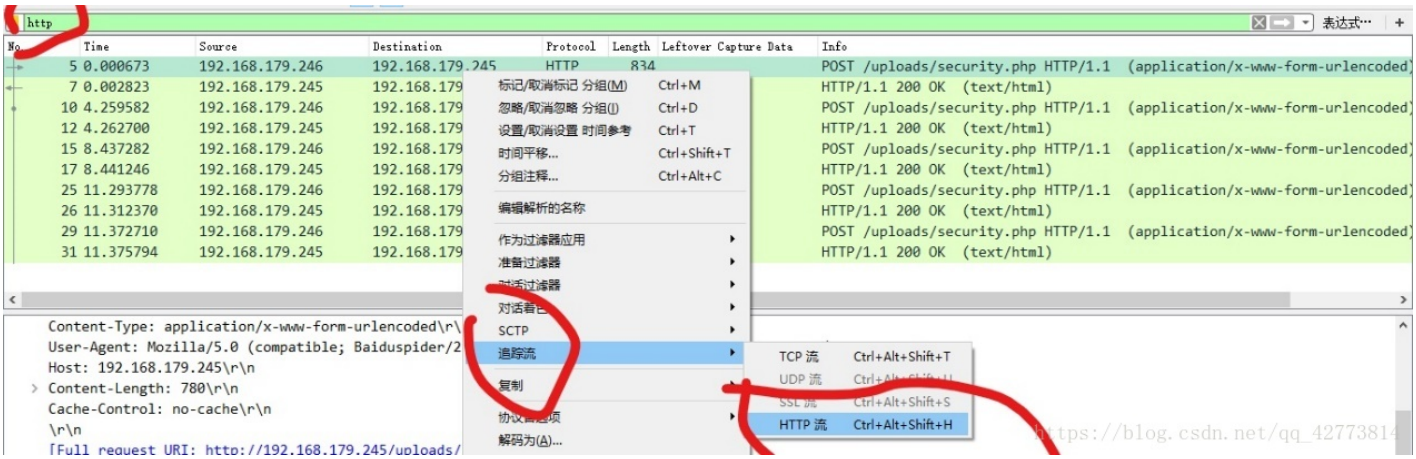
本文链接：https://blog.csdn.net/qq_42773814/article/details/81504812

Backdoor

flag：flag{b3c4r3fortheChinaChopperFHGJKUI^U%}

解题过程：

利用wireshark打开文件，过滤http报文，任意选择一个报文右键选择追踪流->http流



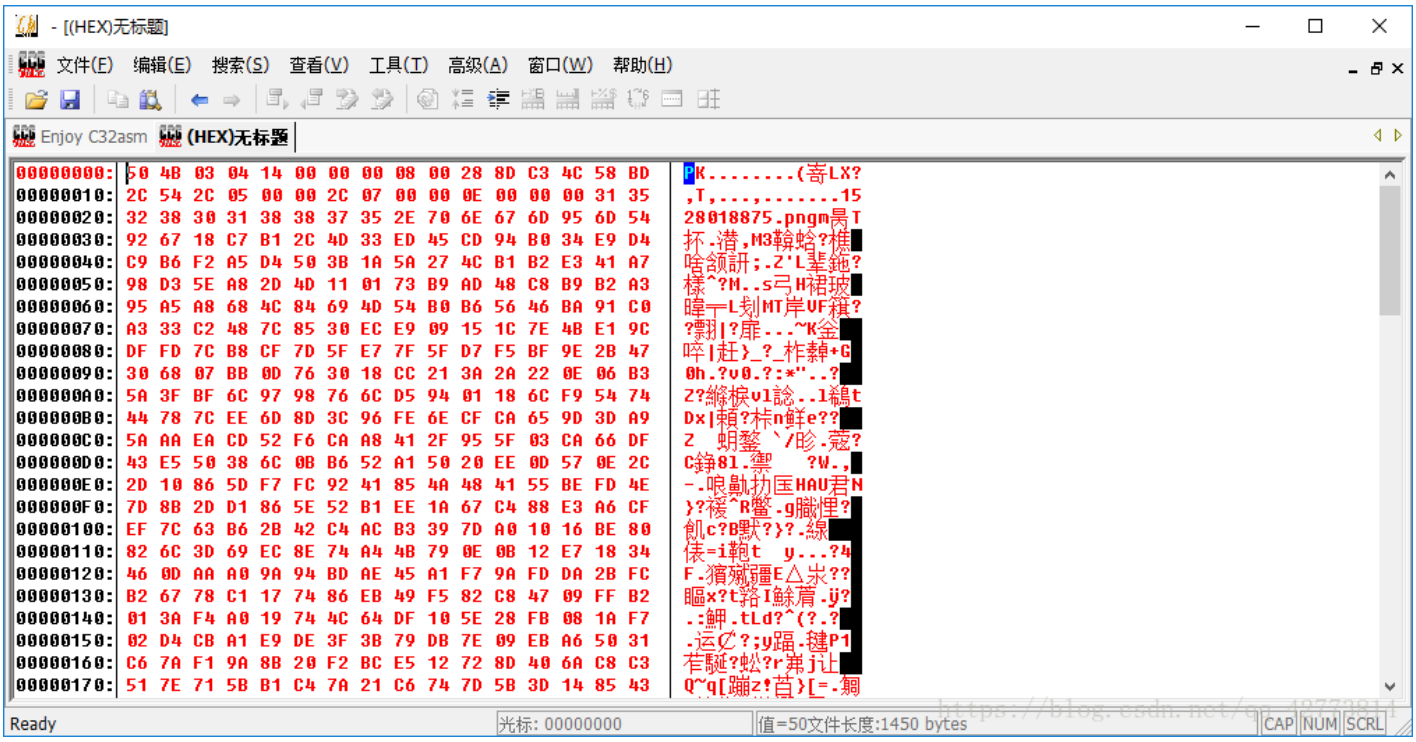
追踪流里面包含大量16进制代码，观察前几位发现它是zip压缩文件的文件头

将z1后面的参数复制下来

```
JGJ1Zj0iIjtmb3IoJGk9MDskaTxzdHJsZW4oJGMpOyRpKz0yKSRidWYuPXVybGRlY29kZSgnJScuc3Vic3RyKCRjLCRpLDIpKTtlY2hvKEB
md3JpdGUoZm9wZW4oJGY
\");"));&z1=504B0304140000000800288DC34C58BD2C542C0500002C0700000E0000003135323830313838373527E706E676D956D5
4926718C7B12C4D33ED45CD94B034E9D4C9B6F2A5D4503B1A5A274CB1B2E341A798D35EA82D4D110173B9AD48C8B9B2A395A5A8684C
84694D54B0B65646BA91C0A333C2487C8530ECE909151C7E4BE19CDFFD7CB8CF7D5FE77F5FD7F5BF9E2B47306807BB0D763018CC213
A2A220E06B35A3FBF6C9798766CD59401186CF9547444787CEE6D8D3C96FE6ECFCA659D3DA95AAAEACD52F6CAA8412F955F03CA66DF
43E550386C0BB652A15020EE0D570E2C2D10865DF7FC9241854A484155BEFD4E7D8B2DD1865E52B1EE1A67C488E3A6CFEF7C63B62B4
2C4ACB3397DA01016BE80826C3D69EC8E74A44B790E0B12E71834460DAAA09A94BDAE45A1F79AFDDA2BFCB26778C1177486EB49F582
C84709FFB2013AF4A019744C64DF105E28FB081AF702D4CBA1E9DE3F3B79DB7E09EBA65031C67AF19A8B20F2BCE512728D406AC8C35
17E715BB1C47A21C6747D5B3D1485436BB5D1C06903E7A499DA79C1E341AFC01BC5CAEDB0987297FC727AAD667D58EFF8B16755BD20
E22DC36DC5E6454157BD5050B31FE5A3F1F0A5B9D3EFAA00A36D779493E74226897FF6F45FED7210A3CBE4817B0BE8FBE4871D66843
47385C3E5A3819A0139878BD9F8208F999071F7B593A187E4FF5B98074E76CDDAAA7021525D4E07A18F3B95A363F54EB400B58EC1C4
22EECD51508422EF4C5F982413197BA7752C425FEC34BB8C490BE671722288711E09860A78A286E5D8F9FEDC2D1F33DD5F411B220D4
C71570F6A06CA1BD9EE5E7A07AC40A9D35CEF07ED5E636DBB90663F71657E7155639F7A384FC4F42AC54D069F5295C624BA6E5A1CB8
C9971AE3125D7635F1090D08E19F3124C1C7491A48EA1A40F74D6C2FF1DD3F99B4E89D366D42DA3E35C38E078FD4545BA919E379C9F
A6AA516ECF8548AB868A1CE28B87424AF98572F49F2E864A6DECFFF1E82C4EB7D84FD7452266549B1B5D979192776DD71F7719A33DC
DEFE703781DE782299B3B5BC1D48739C9978699694264AB17270CEF1624D6B92CF1BE83F253864BF0BDF62ACF599469B1F3E7FFE473
5B8DCEFA9306403157BA18AFC1439F93105098181E00411699E448FDB9B667A367E02D02DD426B5D879DCA083E63EB7D975CF01F1BF
86A69A9BEB876164A9212CE8FDD1D0632D99100496E7F6B636E283479103C21093B70A16798B3F2B8FDDDCFE2660DAC1F92DD74AE20
FBA55CEA623735A2A4A3C17B97DDEF046371EBCAE3CA0E30057D21C72D44FFFEAA0BC2F351D61AE3ABE6274A7545452BA654C799271
F01160DF7D088E76F1C0A5E8EA6A684EED65161C9E193C0556631427EA1A2BCE5C6E8E6F3F4EE690D79A47668B14A5D211BA08F3FE3
961DBF300693D64D344E500379990146DEEDEF959C3F636A4093F0F64C94E61C1563C2E8527D60FA13E18ACDA2F99F78989866F9F63
F8145606F931132F9DB853DD909CA2CB559263A05D96B28763BB07C03FF66749329F3D7000FF0E021847C99A354F045D96065FABEF7
EB420437BA14322E08C71F3C54087242BE4C96A8B4527E13ECCF6D69276F867CB76DEDD7104D1C9CCA18F5F31572C53696BBA5EE0B9
4654FF2CD334CAB01F72E61ECB62C49A3D9C8794223A72127FA0D076718FE8A038ACB66415B8ED6CEF4F9A0CA1E96A1A6FAB826974B
E65A9ECF7F8F42C1C79D9601B5F7AA63C24E153C62582EEA552E9BED642774F822A2DF9305985FCE7FAD96DD181FE32E28868F52170
8B93851E1129929B0FF1EBB93D436BFFA05C256011350691E021BEC4FC91A6890A044EB9F86B8C465FB8CD3046F697A215303EBB66B
D7AD15CA80C3DF2AAC88243E7952176AF6B886B2408969BFE82B0E8484C44E3FE6F0AFF07504B0102140014000000080028 8DC34C58
BD2C542C0500002C0700000E0000000000000000000200000000000000031353238303138383752E706E67504B0506000000000100
1003C000000580500000000HTTP/1.1 200 OK
```

以16进制形式粘贴到C32asm工具里

（文件->新建十六进制文件，新建后中间的内容框内含有内容，此时我们应先删除其内容。删除后，编辑->特别粘贴，选择“ASCII Hex”->确定，保存为zip文件）



通过文件头可观察到该文件为zip压缩文件保存后可将其改成扩展名为zip文件

打开压缩包可以看到里面包含一张图片

1528018875.png

打开图片是一个二维码

扫描二维码即可得到flag

附：常见文件文件头

FFD8FFFE00, .JPEG;.JPE;.JPG, "JPGGraphic File"

FFD8FFE000, .JPEG;.JPE;.JPG, "JPGGraphic File"

474946383961, .gif, "GIF 89A"

474946383761, .gif, "GIF 87A"

424D, .bmp, "Windows Bitmap"

4D5A,.exe;.com;.386;.ax;.acm;.sys;.dll;.drv;.flt;.fon;.ocx;.scr;.lrc;.vxd;

.cpl;.x32, "Executable File"

504B0304, .zip, "Zip Compressed"

3A42617365, .cnt, ""

D0CF11E0A1B11AE1,.doc;.xls;.xlt;.ppt;.apr, "MS Compound Document v1 or Lotus Approach APRfile"

0100000058000000, .emf, ""

03000000C466C456, .evt, ""

3F5F0300, .gid;.hlp;.lhp, "Windows HelpFile"

1F8B08, .gz, "GZ Compressed File"

28546869732066696C65, .hqx, ""

0000010000, .ico, "Icon File"

4C000000011402, .lnk, "Windows LinkFile"

25504446, .pdf, "Adobe PDF File"

5245474544495434, .reg, ""

7B5C727466,.rtf, "Rich Text Format File"

lh, .lzh, "Lz compression file"

MThd, .mid, ""

0A050108, .pcx, ""

25215053, .eps, "Adobe EPS File"

2112, .ain, "AIN Archive File"

1A02, .arc, "ARC/PKPAK Compressed 1"

1A03, .arc, "ARC/PKPAK Compressed 2"

1A04, .arc, "ARC/PKPAK Compressed 3"

1A08, .arc, "ARC/PKPAK Compressed 4"

1A09, .arc, "ARC/PKPAK Compressed 5"

60EA, .arj, "ARJ Compressed"

41564920, .avi, "Audio Video Interleave(AVI)"

425A68, .bz;.bz2, "Bzip Archive"

49536328, .cab, "Cabinet File"

4C01, .obj, "Compiled Object Module"

303730373037, .tar;.cpio, "CPIO ArchiveFile"

4352555348, .cru;.crush, "CRUSH ArchiveFile"

3ADE68B1, .dcx, "DCX Graphic File"

1F8B, .gz;.tar;.tgz, "Gzip ArchiveFile"

91334846, .hap, "HAP Archive File"

3C68746D6C3E,.htm;.html, "HyperText Markup Language 1"

3C48544D4C3E,.htm;.html, "HyperText Markup Language 2"

3C21444F4354, .htm;.html, "HyperText MarkupLanguage 3"

100, .ico, "ICON File"

5F27A889, .jar, "JAR Archive File"

2D6C68352D,.lha, "LHA Compressed"

20006040600, .wk1;.wks, "Lotus 123 v1 Worksheet"

00001A0007800100, .fm3, "Lotus 123 v3 FMTfile"

00001A0000100400, .wk3, "Lotus 123 v3Worksheet"

20006800200, .fmt, "Lotus 123 v4 FMTfile"

00001A0002100400, .wk4, "Lotus 123 v5"

5B7665725D, .ami, "Lotus Ami Pro"

300000041505052, .adx, "Lotus ApproachADX file"

1A0000030000, .nsf;.ntf, "Lotus NotesDatabase/Template"

4D47582069747064, .ds4, "MicrografixDesigner 4"

4D534346, .cab, "Microsoft CAB FileFormat"

4D546864, .mid, "Midi Audio File"

000001B3, .mpg;.mpeg, "MPEG Movie"

09020600000001000B9045C00, .xls, "MS Excel v2"

0904060000001000F6055C00, .xls, "MS Excel v4"

7FFE340A,.doc, "MS Word"

1234567890FF, .doc, "MS Word 6.0"

31BE000000AB0000, .doc, "MS Word forDOS 6.0"

1A00000300001100, .nsf, "NotesDatabase"

7E424B00, .psp, "PaintShop Pro Image File"

504B0304, .zip, "PKZIP Compressed"

89504E470D0A, .png, "PNG Image File"

6D646174, .mov, "QuickTime Movie"

6D646174, .qt, "Quicktime MovieFile"

52617221, .rar, "RAR Archive File"

2E7261FD, .ra;.ram, "Real AudioFile"

EDABEEDB, .rpm, "RPM Archive File"

2E736E64, .au, "SoundMachine AudioFile"

53495421, .sit, "Stuffit v1 ArchiveFile"

53747566664974, .sit, "Stuffit v5Archive File"

1F9D, .z, "TAR Compressed ArchiveFile"

49492A, .tif;.tiff, "TIFF (Intel)"

4D4D2A,.tif;.tiff, "TIFF (Motorola)"

554641, .ufa, "UFA Archive File"

57415645666D74, .wav, "Wave Files"

D7CDC69A,.wmf, "Windows Meta File"

4C000000, .lnk, "Windows Shortcut (LinkFile)"

504B3030504B0304, .zip, "WINZIPCompressed"

FF575047, .wpg, "WordPerfectGraphics"

FF575043, .wp, "WordPerfect v5 orv6"

3C3F786D6C,.xml, "XML Document"

FFFE3C0052004F004F00540053005400550042004200, .xml, "XML Document(ROOTSTUB)"

3C21454E54495459, .dtd, "XML DTD"

5A4F4F20, .zoo, "ZOO Archive File"