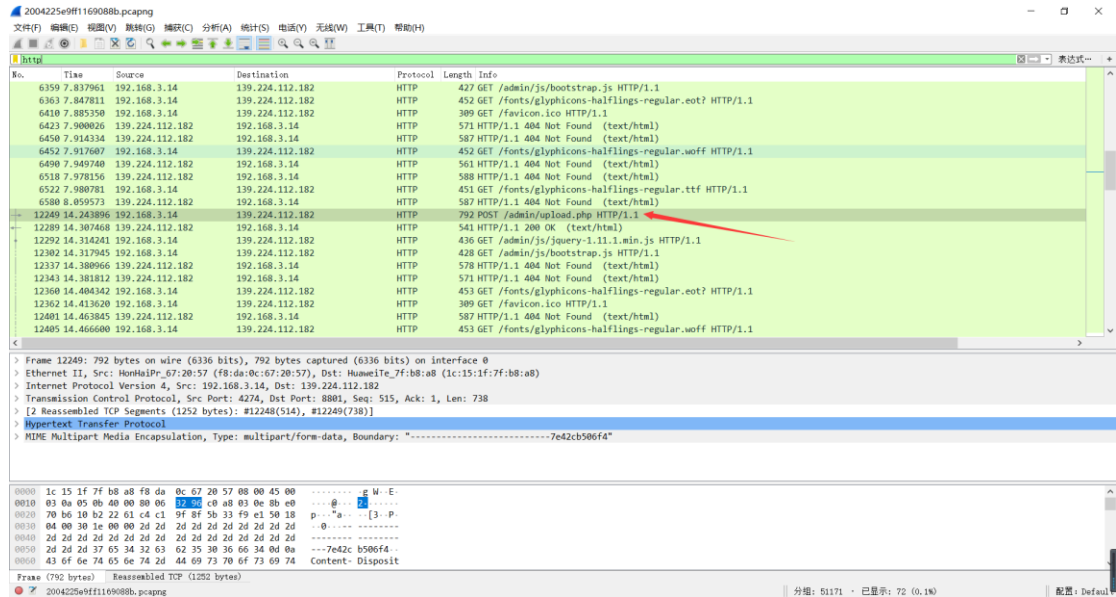


AWDshell Writeup

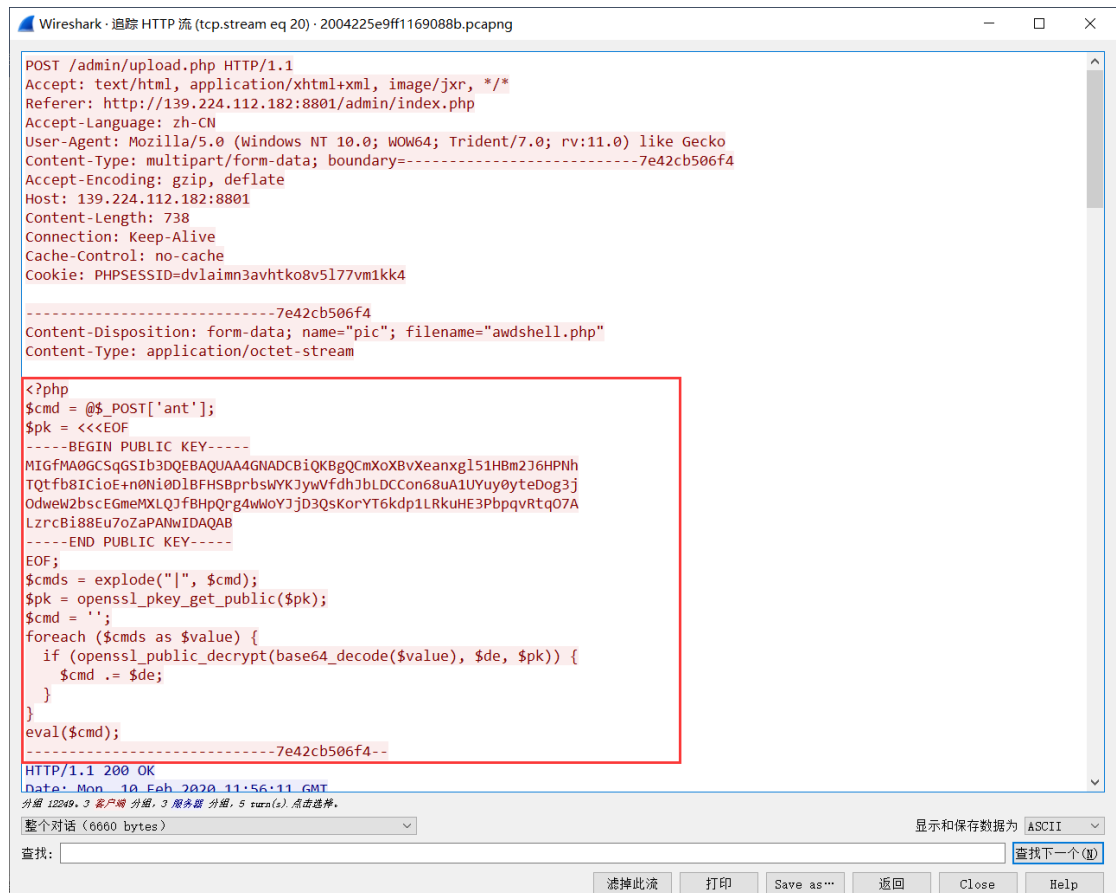
Nepnep@1cePeak

根据题目描述是一个 shell 🐞，之后在大量的 udp 混淆流量中追踪 HTTP，发现 upload.php



追踪 HTTP 流

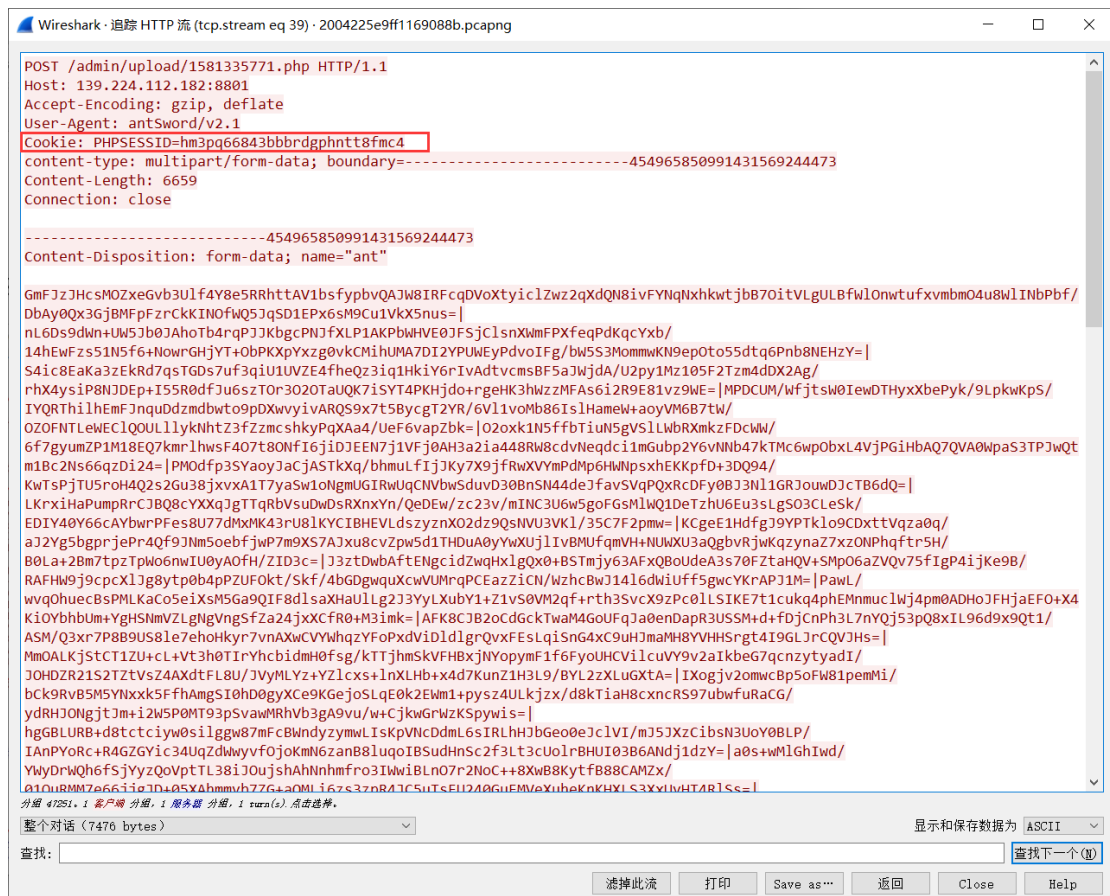
一个用蚁剑来连接的 RSA 🐞



追踪其中一个木马传输的流量

拿到 session

hm3pq66843bbbrdgphntt8fmc4



破解密文

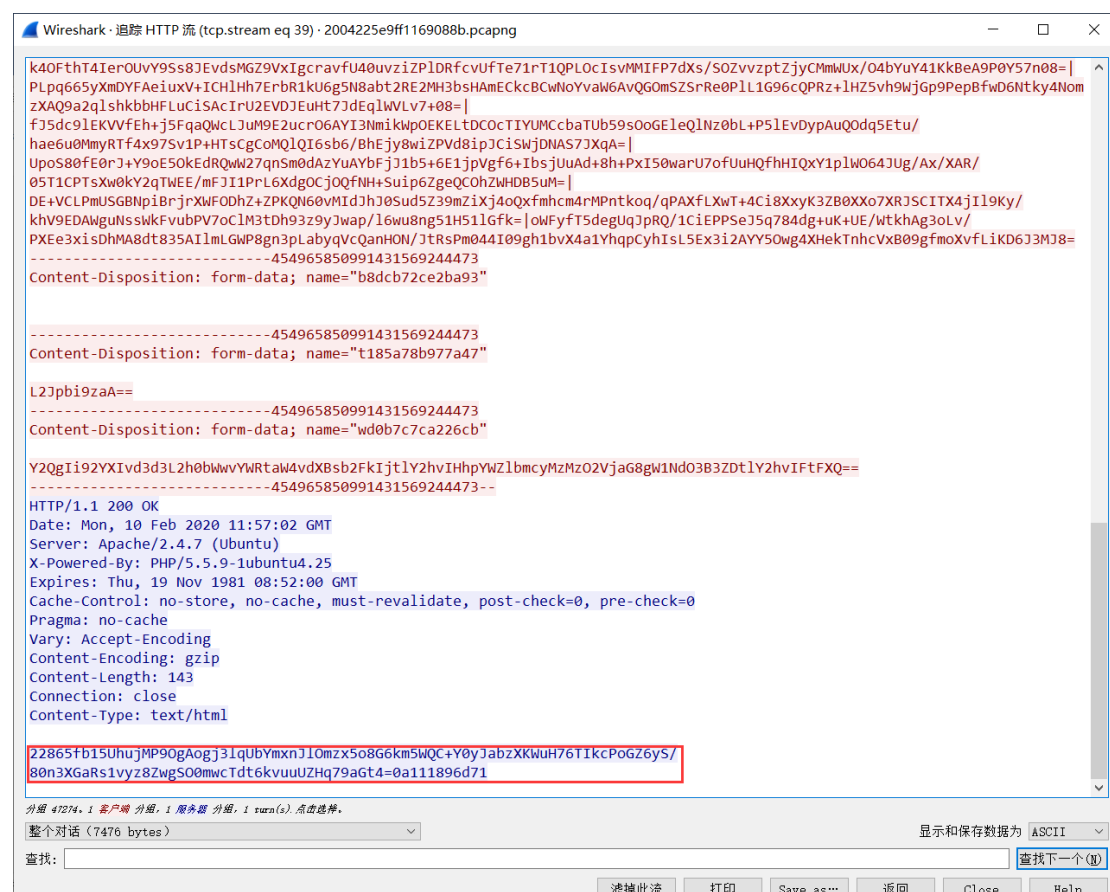
我们可以利用上传的 rsa 木马的公钥进行解密

[illegible]

解密后返回一串 php 代码

```
@ini_set("display_errors", "0");
@set_time_limit(0);
function asenc($out){
    @session_start();
    $key=@substr(str_pad(session_id(),16,'a'),0,16);
    return @base64_encode(openssl_encrypt(base64_encode($out), 'AES-128-ECB', $key, OPENSSL_RAW_DATA));
};;
function asoutput(){
    $output=ob_get_contents();
    ob_end_clean();
    echo "22865fb15";
    echo @asenc($output);
    echo "0a111896d71";
    ob_start();
    try{$p=base64_decode($_POST["t185a78b977a47"]);
    $s=base64_decode($_POST["wd0b7c7ca226cb"]);
    $envstr=@base64_decode($_POST["b8dcb72ce2ba93"]);
    $d=dirname($_SERVER["SCRIPT_FILENAME"]);
```

观察发现流量采用 AES-128-ECB 加密，key 取 session 的前 16 位，同时继续读代码发现流量前后都有垃圾字符（坏



AES 解密+base64 解密

AES 解密网站 <https://oktools.net/aes>

22865fb15UhujMP9OgAogj3lqUbYmxnJlOmzx5o8G6km5WQC+Y0yJabzXKWuH76TlkcPoGZ
6yS/80n3XGaRs1vyz8ZwgSO0mwcTdt6kvuuUZHq79aGt4=0a111896d71

AES加密/解密

eG1hZmVuZzIzMzMKW1NdCi92YXIvd3d3L2h0bWwvYWRtaW4vdXBsb2FkC1tFXQo=

模式 ECB 填充 Pkcs7 偏移量 ECB模式不需要 密文编码 Base64
密钥 hm3pq66843bbbrdg 加密 解密 清空

UhujMP9OgAogj3lqUbYmxnJlOmzx5o8G6km5WQC+Y0yJabzXKWuH76TlkcPoGZ6yS/80n3XGaRs1vyz8ZwgSO0mwcTdt6kvuuUZHq79aGt4

base编码

base16、base32、base64

eG1hZmVuZzIzMzMKW1NdCi92YXIvd3d3L2h0bWwvYWRtaW4vdXBsb2FkC1tFXQo=

编码 base64 字符集 utf8(unicode编码)

编码

解码

xiaofeng2333
[S]
/var/www/html/admin/upload
[E]

夏风师傅 tqI (happymisc)

芜湖~刚才追踪的最后一个流量没有发现 flag，按照以上方法逐个查找，倒数第二个有 flag

```
@ini_set("display_errors", "0");
@set_time_limit(0);
function asenc($out){
    @session_start();
    $key=@substr(str_pad(session_id(),16,'a'),0,16);
    return @base64_encode(openssl_encrypt(base64_encode($out), 'AES-128-ECB', $key, OPENSSL_RAW_DATA));
};
function asoutput(){
    $output=ob_get_contents();ob_end_clean();
    echo "f3c7239848e0";
    echo @asenc($output);
    echo "05fda2646c";
}
ob_start();
try{$p=base64_decode($_POST["t185a78b977a47"]);
    $s=base64_decode($_POST["wd0b7c7ca226cb"]);
```

f3c7239848e0+L8pc9pJEhqPQ1cmL18eJXX9QGADkKnp8A1j7s4oX2Qo8YJNGNTbuaXu+Ofy
nYgRewqyflj/Wrg0rgKj/cRdO4zJMmfLfyFVB4pBRYeTetM0G/w/Px6+xl/WPIRrx/+MvK6eQyPr
+xDqTX82AqiGrOYDwN94/vuGcLS7NAXhty4=05fda2646c

AES 解密

AES加密/解密

Wm14aFozczJNbUU0WW1RM09HUTRabUkxWVRBMFpHRm1NVFUzT1dJME9EUmtPV0U0T0gwPVtTXQovdmFyL3d3dy9odG1sL2FkbW1uL3VwbG9hZApbRVOK

模式

ECB

填充

Pkcs7

偏移量

ECB模式不需要

密文编码

Base64

密钥

hm3pq66843bbbrdg

↓ 加密

↑ 解密

清空

+L8pc9pJEhqPQ1cmL18eJXX9QGADkKnp8A1j7s4oX2Qo8YJNGNTbuaXu+OfynYgRewqyFLj/Wrg0rgKj/cRd04zJMmFLfyFVB4pBRyETetM0G/w/Px6+xl/WP1Rrx/+MvK6eQyPr+xDqTX82Aq1Gr0YDwN94/vuGcLS7NAxhty4=

base16、base32、base64

Wm14aFozczJNbUU0WW1RM09HUTRabUkxWVRBMFpHRm1NVFUzT1dJME9EUmtPV0U0T0gwPVtTXQovdmFyL3d3dy9odG1sL2FkbW1uL3VwbG9hZApbRVOK

编码

base64

字符集

utf8(unicode编码)

编 码

解 码

ZmxhZ3s2MmE4YmQ3OGQ4ZmI1YTA0ZGF1MTU3OWI0ODRkOWE4OH0=[S]
/var/www/html/admin/upload
[E]

ZmxhZ3s2MmE4YmQ3OGQ4ZmI1YTA0ZGF1MTU3OWI0ODRkOWE4OH0=

再次进行 base64 解密

base16、base32、base64

ZmxhZ3s2MmE4YmQ3OGQ4ZmI1YTA0ZGF1MTU3OWI0ODRkOWE4OH0=

编码

base64

字符集

utf8(unicode编码)

编 码

解 码

flag {62a8bd78d8fb5a04dab1579b484d9a88}

成功拿到 flag

flag {62a8bd78d8fb5a04dab1579b484d9a88}