找到那个他

原创先锋情报站 酒仙桥六号部队
2020-12-24原文

这是 **酒仙桥六号部队** 的第 **135** 篇文章。
全文共计2132个字，预计阅读时长7分钟。

前情

随着攻防演练不断的演化，溯源也成为其必不可少的环节。溯源其实也是个庞大的分支，下面主要针对攻防演练，来聊聊溯源。一起来找到那个他。

整体思路

攻防场景下的攻击溯源，首先要了解溯源的思路，其次对攻击进行发现，然后对攻击进行追踪溯源，最后撰写溯源报告。发现攻击主要通过网络安全设备、态势感知、蜜罐等设备对攻击进行发现。追踪溯源主要通过对IP地址、域名等情报进行分析，对攻击机进行反向渗透以及对邮箱、手机号、账号等信息进行社工排查，最终完整还原攻击链条，溯源到黑客的虚拟身份、真实身份溯源到攻击队员，反控攻击方主机。

大多数情况下IP地址会作为溯源的初始信息。首先应尽可能地在现场部署设备的日志中检索，获取一些跟IP地址相关联的信息，如：网站/系统的注册账号、注册手机号、注册邮箱、关联域名等信息，从而提高溯源的成功率。

案例一

攻击者通过代码执行的方式进行命令执行探测，并且发送大量种类繁多的攻击向量；我方安全团队发现攻击后，果断处置执行封堵IP操作。并组织溯源。

目前掌握的攻击者信息只有IP，通过IP反查，未获取有用信息。接下来尝试对攻击ip进行反向渗透。通过使用端口扫描工具进行IP反制，发现该IP打开了80、3306与3389端口。

80端口：默认为web服务端口，可通过web网站查找攻击者相关信息，也可通过常规web漏洞获取权限，进一步查找攻击者。

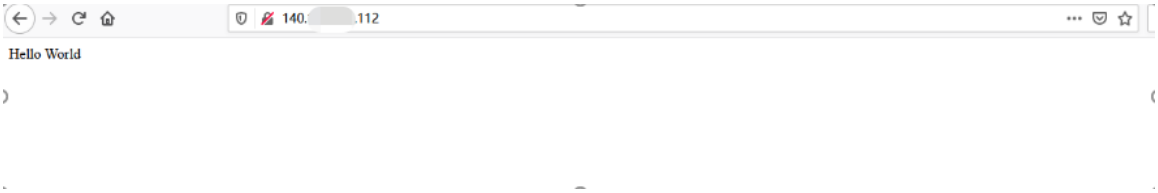
3306端口：默认为MySql数据库端口，可尝试弱口令扫描。进而获取更多信息。

3389端口：默认Windows远程桌面端口，可尝试弱口令扫描，CVE漏洞扫描。

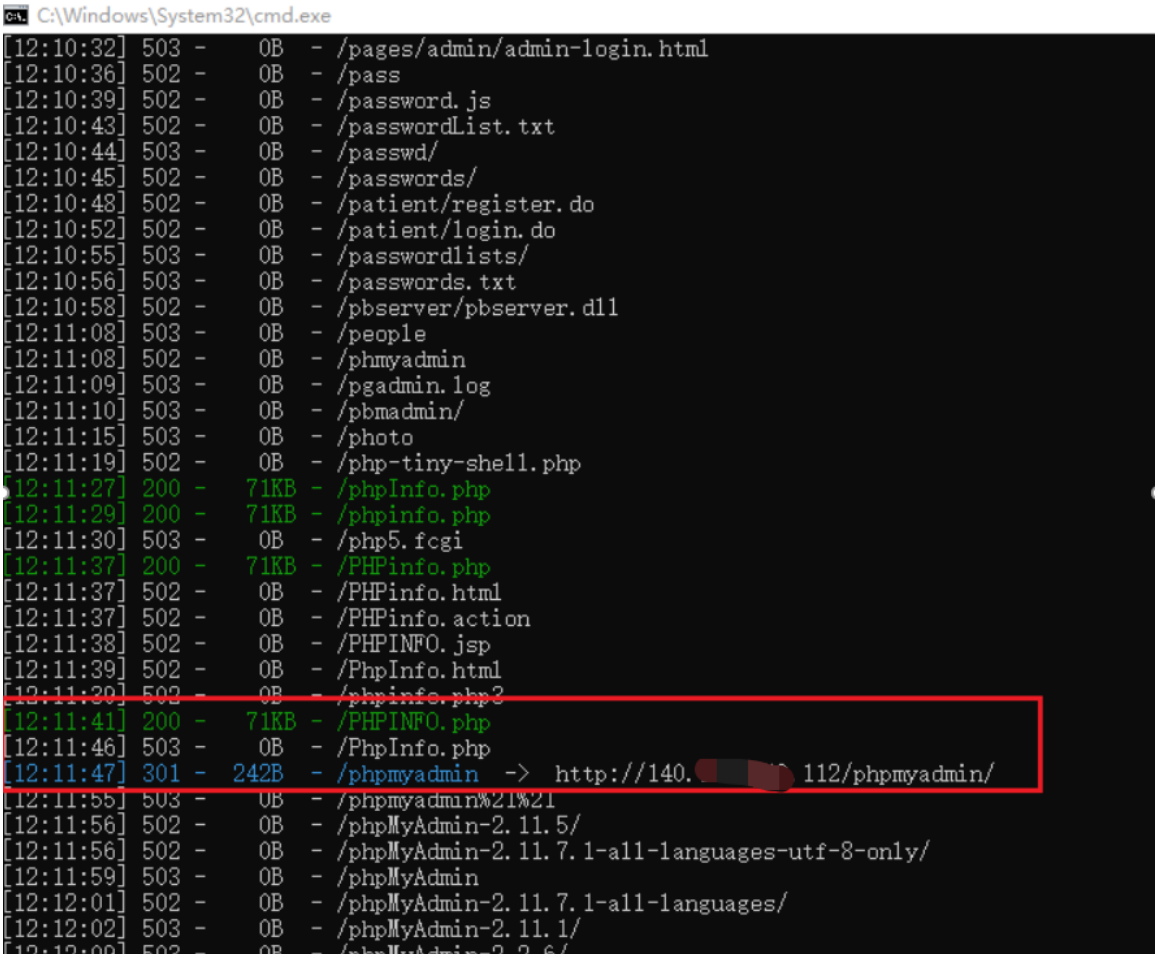
```
root@kali:~# nmap -sV --open 140.      .112
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-15 02:31 EDT
Nmap scan report for 140.      .112
Host is up (1.1s latency).
Not shown: 982 closed ports, 5 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PHP/5.4
.45)
110/tcp   open  tcpwrapped
135/tcp   open  msrpc?
139/tcp   open  netbios-ssn?
3306/tcp  open  mysql        MySQL 5.5.53
3389/tcp  open  ssl?         Microsoft SChannel TLS
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
2 services unrecognized despite returning data. If you know the service/version,
```

先使用浏览器访问该ip地址80端口对应的web服务，发现该页面为很简单的hello

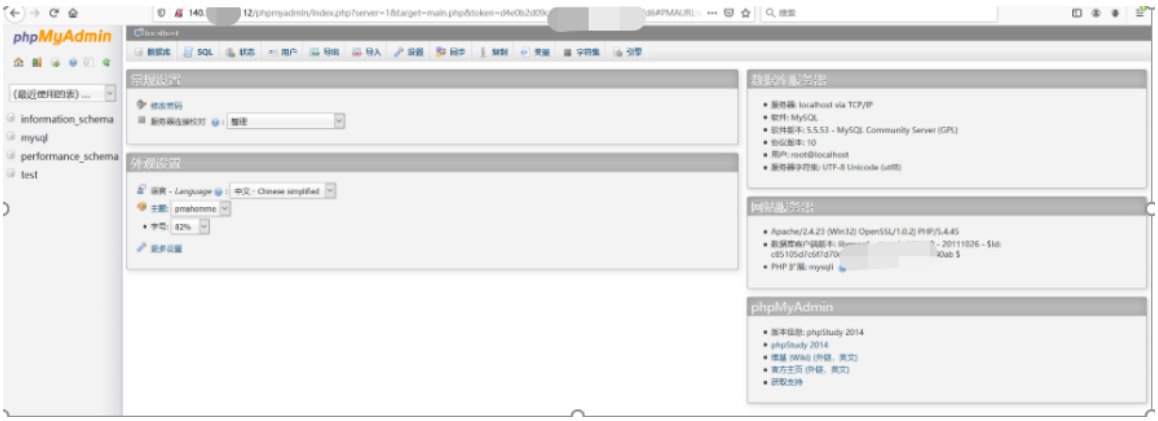
world页面。根据经验，此页面为默认页面，也就意味着扫描web路径会有惊喜。



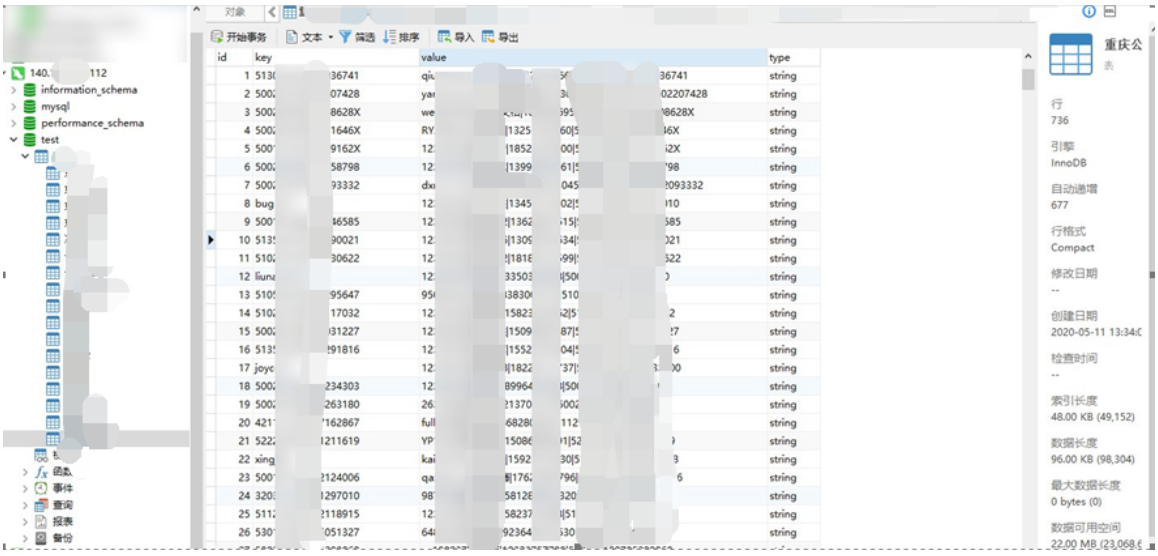
通过使用dirsearch工具扫描web目录，果然发现该网站存在phpMyAdmin目录和phpinfo文件。



PhpMyAdmin是一个开源的通过web管理MySQL的工具。存在弱口令漏洞和sql注入登陆漏洞。使用默认密码root/root尝试登录，发现可以登录系统，查看mysql数据库信息，如下图所示：

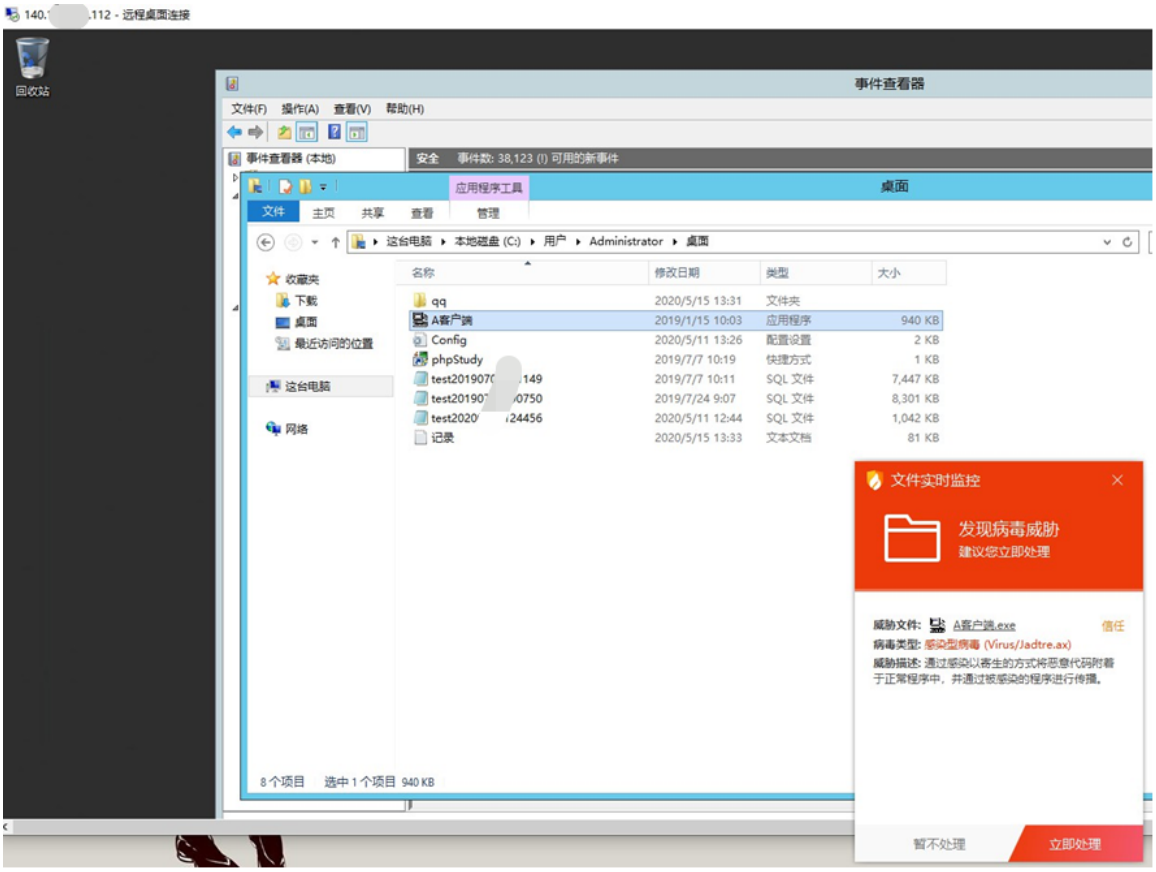


查看到该users表存在root帐号密码，尝试使用Navicat登录其数据库test，发现其中存在大量用户名、手机号、身份账号信息，故确定其为黑产使用的收集信息服务器，如下图所示：



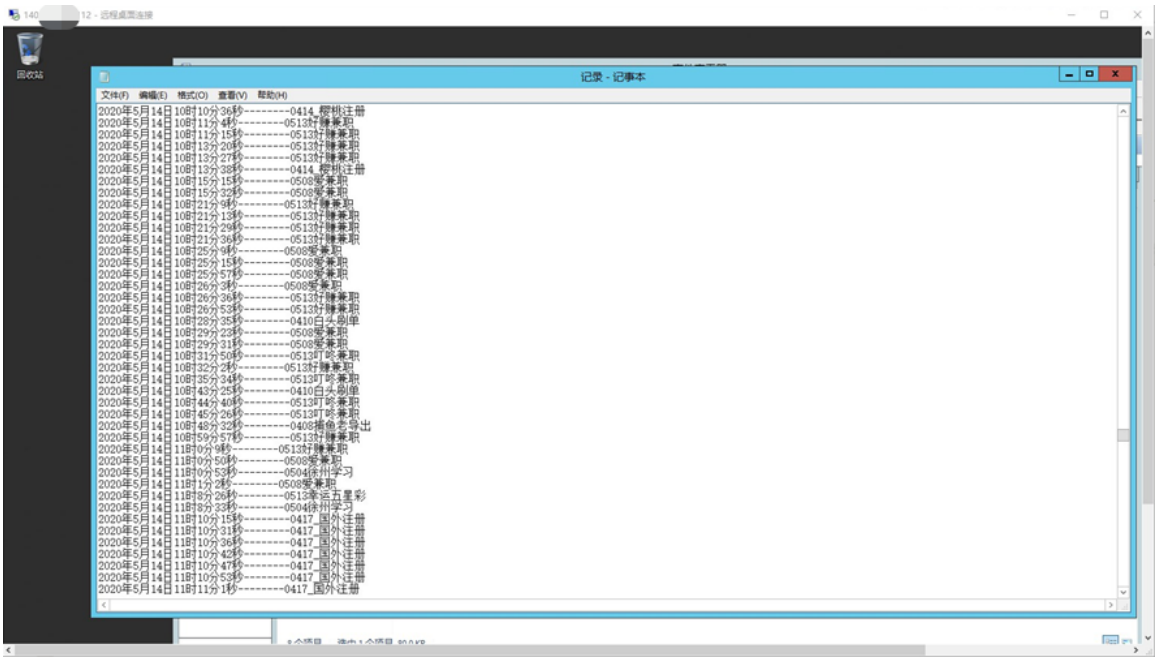
登陆了PhpMyAdmin的后台，大部分情况下都是可以拿到webshell。通过写日志的方式，顺利获取webshell，接着添加系统用户，提升至管理员权限。前面已探测出系统开启了远程桌面端口，至此，可以直接登陆系统。

通过mstsc登陆攻击者服务器，一般会先到攻击者用户目录下的几个文件夹中查找信息。先看下桌面，在该IP地址桌面发现黑产工具。是一个批量感染服务器的后门程序。

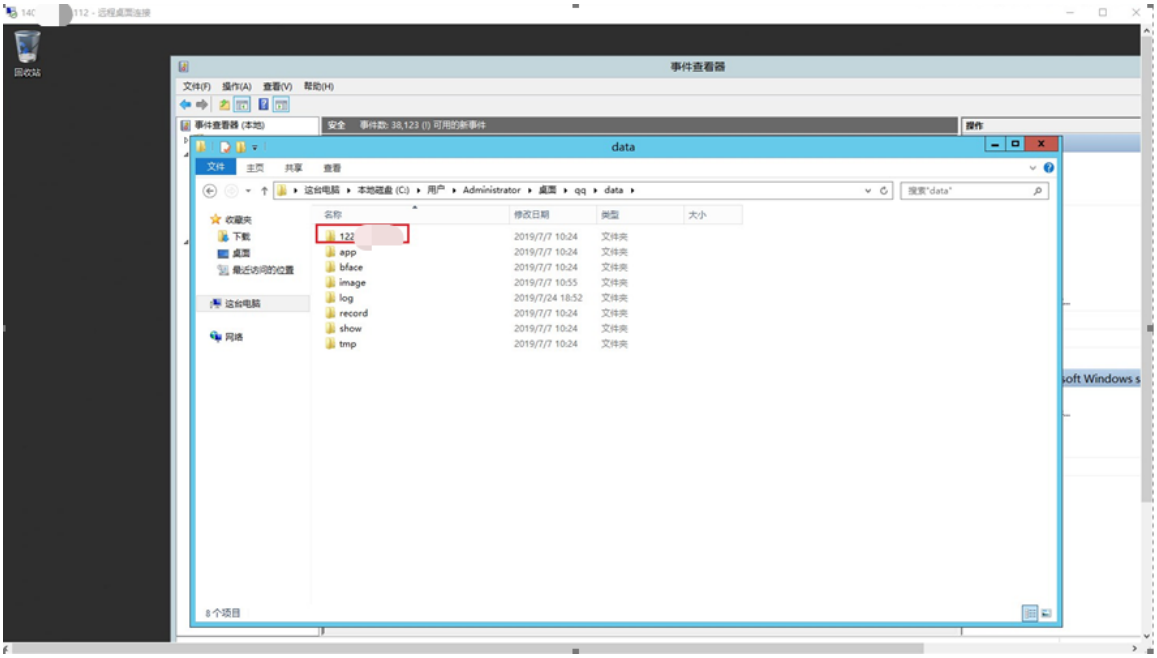


同时桌面还有大量存量黑产数据，该文件可以直接导入数据库。

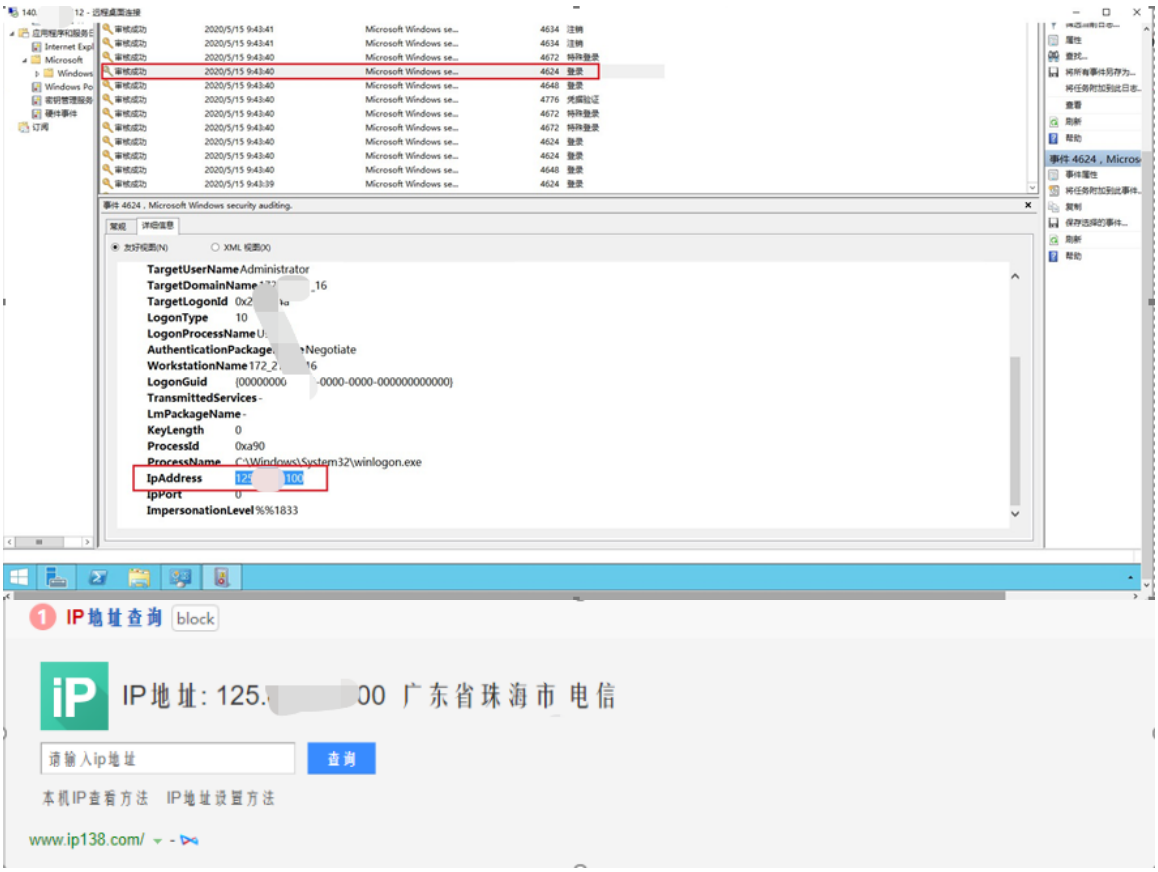
还在该IP地址桌面发现其攻击事件及时间线，看情况，该攻击者搞了不少站。



桌面还看到安装有QQ程序，QQ登陆一次后，会默认保存QQ信息，直接以QQ号单独新建文件夹。该IP地址上面发现黑产人员QQ。



既然是vps服务器，攻击者肯定也要远程登陆，通过查看登录日志，发现黑产活动地区为广东省珠海市。



点到才为止。

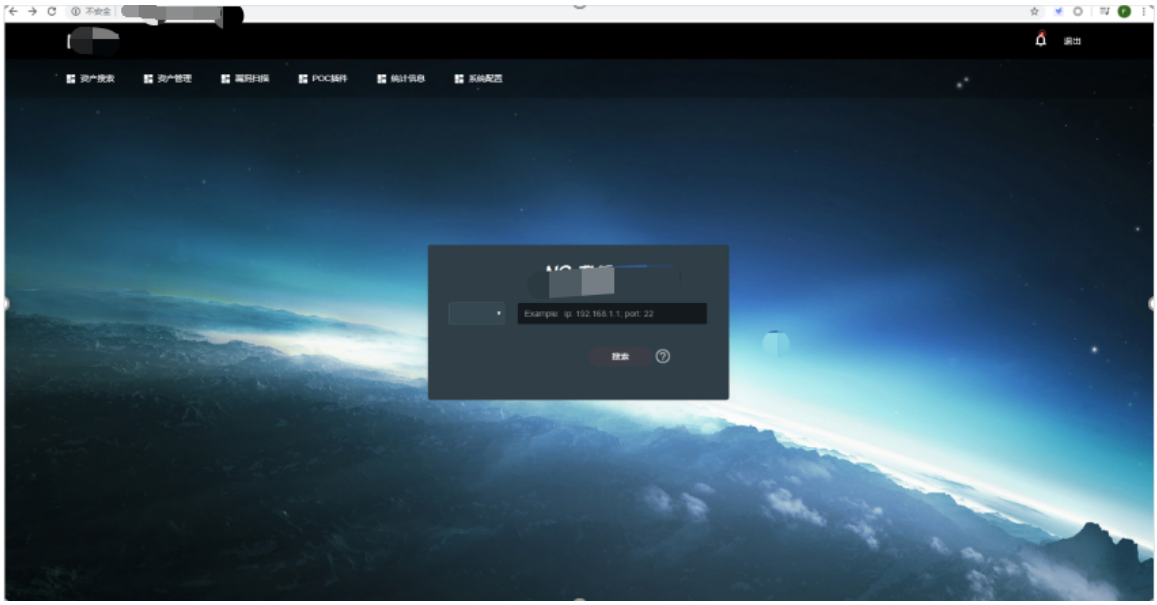
最后确认其身份为黑产身份的信息收集服务器。形成溯源报告，上报至组织方。

说好的溯源至攻击方人员那？怎么净搞黑产了？

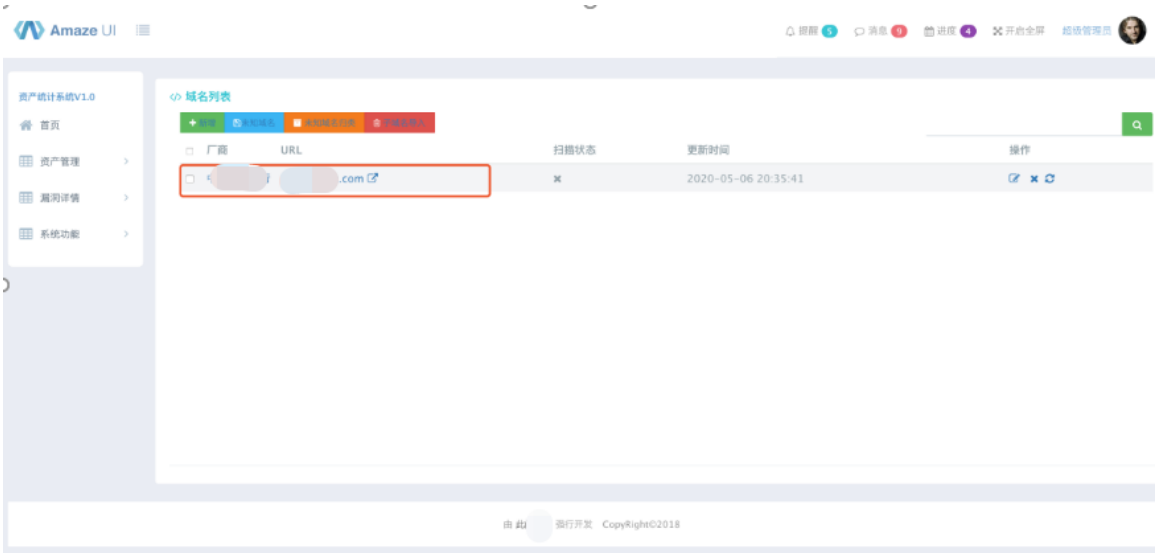
案例二

通过监控设备，获取攻击IP：182.xxx.xxx.xxx。

根据攻击IP【182.xxx.xxx.xxx】于18888端口发现攻击者网络扫描器。

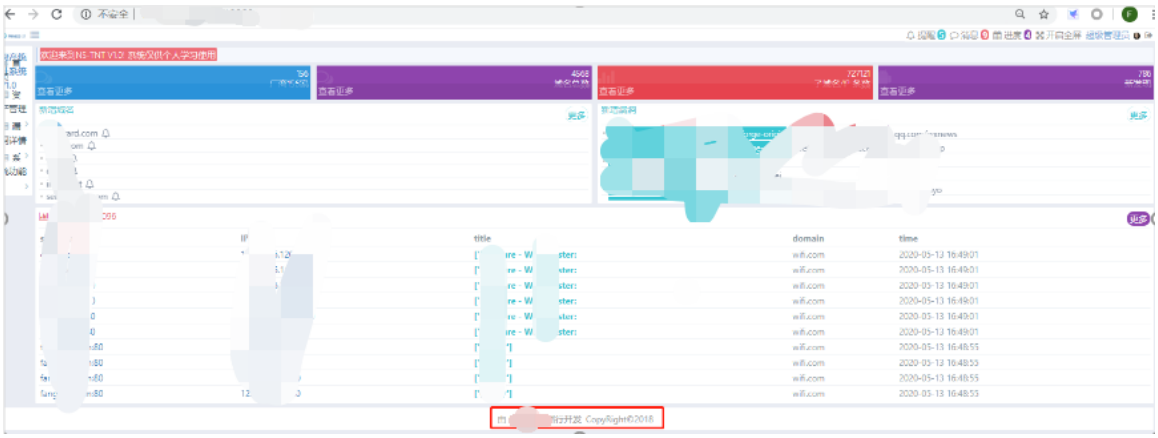


经过一番查找，在扫描目标列表中发现针对我方系统的扫描任务。由此确认其为攻击队人员，扫描设备不设密码，直接互联网访问，这也太不小心了。

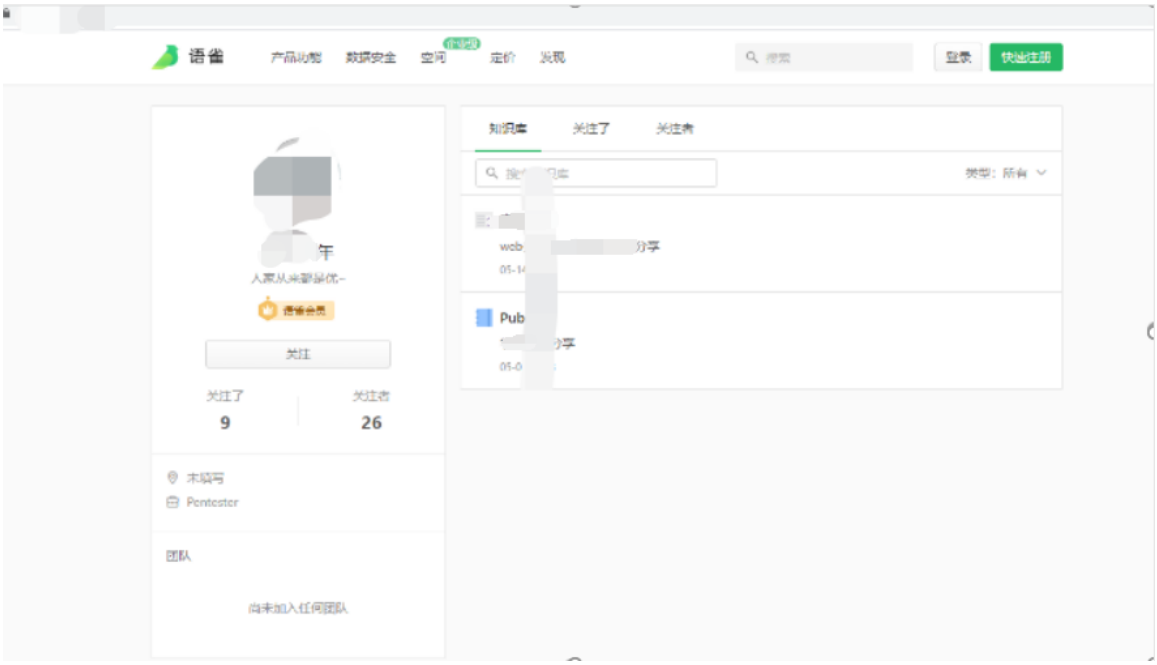


扫描器看着眼生，然后根据扫描器的各种特征，到互联网上搜索，均未发现类似此页面开源框架扫描器的相关描述和下载连接。既然不是公开扫描器，那么找到开发者，是不是就找到了使用者？

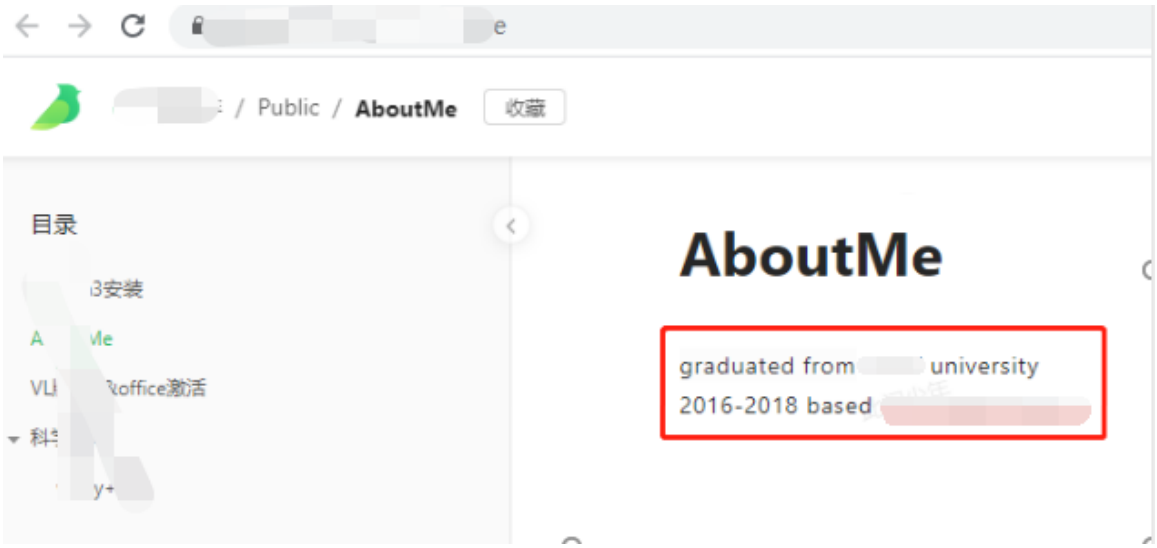
网页下方中间，一般会携带版权信息，查看开发者信息。



直接跳转至开发者个人博客，博客没什么文章，可能是刚入行的时候建的博客。一般刚开始都会在自我介绍处留下自己的相关信息。



查看博客中自我介绍，果然不出意料。XX交大毕业，2016-2018就职于XX科技。



显然信息不够多，仍需进一步探索。安全从业者有一个特点，都会给自己起一个ID，它是你网络中的名字。不管是英文、中文、一串毫无意义的字符串。无论是论坛、微信、QQ、圈子、文章，都会有它的陪伴。所以，接下来的思路就瞬间清晰了。根据微信群关系与QQ群关系查找，确认其为活跃的安全从业者：

微信是一个比较私密的聊天软件，一般不会泄露很多信息。QQ就不一样了，QQ空间、QQ贴吧等等，都是可以直接查看的。查找关注的贴吧，发现关注了XX交大，进一步确认其信息的真实度。最后通过脉脉，找到真实姓名XXX：

最后，获得攻击方人员信息：姓名：XXXX学校：XXXX公司：XXXX微信：XXXXQQ：XXXX。

小结

通过以上几个案例，技术方面确实平平无奇。溯源，说白了就是一个信息收集的过程。最终，通过抽丝剥茧，找到了那个他。

精选留言

用户设置不下载评论