


Who is Mr An, and was he working for APT10?

 intrusiontruth.wordpress.com/2018/08/31/who-is-mr-an-and-was-he-working-for-apt10/

intrusiontruth

August 31, 2018



On August 15th 2018 this blog revealed a connection between APT10 and the Tianjin bureau of the Chinese Ministry of State Security (MSS). But the story doesn't stop with that revelation; analysts working with this blog have continued to investigate every lead provided to us. One such lead has helped us to identify another individual in China connected to APT10. The trail starts with a domain name first published in [FireEye's Poison Ivy Report](#) as a MenuPass (APT10) affiliated domain.

chromeenter[.]com

The domain chromeenter[.]com appears in the FireEye report as a domain associated with the MenuPass malware.

We can see the connection between the happyyongzi password and menuPass by observing the following connections:

- The sample e6ca06e9b000933567a8604300094a85 connected to the domain sh.chromeenter.com with the password happyyongzi.
- The domain sh.chromeenter.com previously resolved to the IP 60.2.148.167.
- The domain jj.mysecondarydns.com also resolved to 60.2.148.167.

- The sample 4e84b1448cf96fabe88c623b222057c4 connected to jj.mysecondarydns.com with the password menuPass.

The password of fishplay can be linked to menuPass by observing the following relationships:

- The sample 494e65cf21ad559fccf3dacdd69acc94 connected to mongoles.3322.org with the password fishplay.

FireEye PoisonIvy Report showing chromeenter[.]com as a MenuPass domain. The domain and subdomains also appeared in early versions of Annex A (Indicators of Compromise) of the PwC Operation Cloud Hopper report and it is listed on Alien Vault as a sink-holed domain.

chaindungeons[.]com
chibashiri[.]com
chromeenter[.]com
cia.ezua[.]com
cia.toh[.]info

chromeenter[.]com in Version 1 of the PwC Operation Cloud Hopper report **Tianjin Tiaoyiye Technology Co Ltd**

Domain registration information for chromeenter[.]com shows that it was registered in April 2010 to Hogate Technology Co Limited. Although much of the registration information remained the same when the domain was updated in April 2012, the registrant company was changed to Tianjin Tiaoyiye Technology Co Limited and the registration e-mail address was updated to gbaike[at]gmail.com. The domain became WHOIS protected in late June 2013 just prior to being repossessed by GoDaddy and named in the FireEye report.

gbaike[at]gmail.com

The registration e-mail address used from 2012 leads to a number of other domains, many of which are connected to Tianjin, China, the home of APT10. Domains registered by gbaike[at]gmail.com include:

- jixiaotuangou[.]com
- shgongxingbc[.]com
- tjguge[.]com

- tjqiming[.]com
- tjttjx[.]com
- web1680[.]com
- w1680[.]com

The domain [jiaxiaotuangou\[.\]com](http://jiaxiaotuangou[.]com) was registered to an individual named An Zhiqiang and was also associated with the Tianjin Tiaoyiye Technology Development Co Ltd (天津天骄易业科技发展有限公司) in registration data. Chinese characters for the company were identified at hhlyny.com and give a slightly different name of Tianjin *Tianjiaoyiye* Technology Development Co Ltd.

网站综合查询

网站综合信息 www.jiaxiaotuangou.com		网站头文件(HTTP Header)
标题:	天津驾校团购 - 天津驾校超优惠-团购报名真给力	HTTP/1.1 200 OK 服务器: nginx/1.2.7 访问时间: 2014年04月17日 06:13:25 类型: text/html; charset=UTF-8 文件大小: 7655 连接: keep-alive 语言环境: PHP/5.3.28 设置Cookie: PHPSESSID=lbghj4s1lug9nuk691mr1 过期时间: 1981年11月19日 16:52:00 缓存控制: no-store, 不缓存, 必须更新, post-che 其他指令: 不缓存 设置Cookie: referer=http%3A%2F%2Fwww.jiaxia 网站编码: UTF-8
关键字:	驾校团购 驾校 驾校团购 学车团购	
描述:	驾校团购, 驾校团购是一种全新的驾校报名学车优惠系统。学员团购驾校优惠券到指定驾校报名, 即省100到500元, 省了就是赚了。已经有1368名学员参加天津驾校团购活动!	
域名信息	域名年龄: 7年1个月4天 注册日期: 2011年07月27日 到期时间: 2014年07月27日 邮箱: abuse 电话: +86.1082151122 注册商: BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN	
服务器空间	IP: 125.39.151.27 同IP网站13个 详情 地址: 天津市 联通	
备案信息	备案号: 津ICP备11002861号 审核时间: 2014-04-22 详情 主办单位: 天津天骄易业科技发展有限公司 性质: 企业 网站名: 首页网址:	

同IP网站(同服务器)

Registration information for [jiaxiaotuangou\[.\]com](http://jiaxiaotuangou[.]com) showing the company name The company entry on Zhaopin (a Chinese online recruitment services website) provides additional data related to the company including a link to the company website at [tjwangdian\[.\]com](http://tjwangdian[.]com).

天津天骄易业科技发展有限公司

公司性质: 民营

公司规模: 20-99人

公司网站: <http://www.tjwangdian.com>

公司行业: 互联网/电子商务

公司地址: 天津市南开区白堤路236号生物医学工程研究院内3号楼3层305, 科贸大厦站下

[查看公司地图](#)

公司介绍

天津天骄易业科技发展有限公司

天骄网络 (www.tjwangdian.com) 公司是专业从事电子商务服务的高科技公司。公司坚持“高瞻远瞩, 锐意进取, 努力打造全新的品牌”的创业理念, 本着“客户至上、服务第一, 诚信合作、互利互惠”的服务宗旨, 为广大企业全力打造全新的电子商务平台, 为商家搭建更加专业, 优质, 高效的电子商务网站。

您还可以

[查看公司地图](#)

[查看该公司的职位](#)

Zhaopin entry for 天津天骄易业科技发展有限公司 showing company domain name
The Zhaopin entry also provides a summary of the business activities of the company that translates roughly as:

Tianjiao Network is an e-commerce website construction company with rich experience, professional technology and excellent team. The company focuses on e-commerce website development and network operations, including: e-commerce website construction, B2C website construction, independent online shop construction, mall website construction, industry website construction, portal construction, brand website construction and post-maintenance. From pre-market research, website positioning, website construction and implementation, network promotion, website operation, and even later online customer service and customer relationship management, we have experienced planning team, professional website design team and dedicated customers. The service team consistently adheres to the spirit of “no best, only better!” to create a real profit platform for the company, strengthen the competitiveness of the company, and obtain greater success value!

Finally the [entry for Tianjin Tiaoyiye on Liepin](#) (China's largest recruitment website) provides Chinese characters for An Zhiqiang (安志强).

天津天娇易业科技发展有限公司 关注 111人关注

五险一金 带薪年假 员工福利

我要编辑

公司信息 | 招聘信息 | 评论

公司介绍 编辑

天娇易业是一家拥有丰富经验、专业技术、优秀团队的电子商务公司。公司专注于电子商务网站开发和网络运营，其中涉及：电子商务网站建设、B2C网站建设、独立网店建设、商城网站建设、行业网站建设、门户网站建设、品牌网站建设到后期维护等。

[注册](#) | [登录](#) 查看更有人气公司>>

点击展开更多详情

工商信息

企业类型：有限责任公司	法人：安志强
注册资本：30万元	注册时间：2010-09-08
注册地址：南开区白堤路236号院内3号楼三层305	
组织机构代码：559492640	统一信用代码：911201045594926401
经营状态：存续	登记机关：天津市南开区市场和质量监督管...

投递查看

78% 简历查看率

2天 简历查看用时

企业信息

公司名称：天津天娇易业科技发展有限公司

公司行业：互联网/移动互联网/电子商务

公司规模：51-100人

公司地址：天津

推荐职位

Liepin entry for 天津天娇易业科技发展有限公司 showing 安志强's name @gbaike

Armed with a name (安志强), a handle (gbaike), a location (Tianjin) and a company (天津天娇易业科技发展有限公司) a number of new sources of material on the individual can be discovered, including Twitter account @gbaike. The account is in the name 安志强, bears the handle @gbaike and has its location set as Tianjin. The account also refers to marketing in its profile image – this matches the description of the company from Zhaopin.

Home Moments Search Twitter Have an account? Log in

链接的力量
构建
商业

o2o营销 互联网+ 微信营销 自媒体营销 互联网思维

Tweets 15 Following 60 Followers 11 Likes 10 Follow

安志强
@gbaike
15年SEO老兵
@ Tianjin
Joined August 2013

Tweets Tweets & replies

安志强 @gbaike · May 25
我是小强我用小强

安志强 @gbaike · May 25
只因在群里说了句真话，然后就被推出了。

New to Twitter?
Sign up now to get your own personalised timeline!
Sign up

You may also like · Refresh

@gbaike's Twitter account

