Who is Mr Ding?

intrusiontruth.wordpress.com/2020/01/14/who-is-mr-ding

intrusiontruth January 14, 2020

We started by stating that Chinese APTs have a blueprint that us applied in multiple regions across China: contract hackers and specialists, front companies, and an intelligence officer. Applying this blueprint in Hainan, we surfaced inter-linked companies recruiting for people with hacking and specialist IT skills.

We have identified that Professor Gu Jian is connected to the front company Hainan Xiandun and supported some of their activities from his position at Hainan University. But his was more of a supporting role. Who was in charge?

Wang Tian, Manager Jiang, and Mr Chen

Job adverts for Hainan Tengyuan, Hainan Yili and Hainan Xiandun list Wang Tian (王天) and Manager Jiang (蒋经理) as contacts of the companies. We have been unable to identify much more about these individuals.

四、联系方式

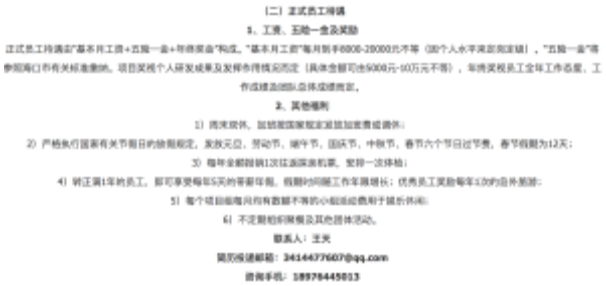
联系人：蒋经理

咨询电话：13208905740

简历投递邮箱：xiandunHR@yahoo.com

Hainan Xiandun – Manager Jiang

Hainan Tengyuan – Wang Tian



Hainan Yili – Wang Tian

Mr Chen

An advert on Sichuan University's website for a Penetration Test Engineer position at Hainan Xiandun lists 'Mr Chen' (陈先生) using 2918588955[at]qq.com and telephone number 13198985613 as the contact person.

Hainan Xiandun – Mr Chen

Mr Chen is seen on a number of job adverts for these Hainan front companies. While it's unclear who Mr Chen is, the website registrant for one of the front companies which we identified, Hainan Yanwu, is listed as a Mr Chen Yanwu (陈彦武).

```
Domain.............................. hnywco.net
  Creation Date..................... 2010-04-27  05:43:31

Registrant.......................... Chen Yanwu
  Registrant Address.............. 82th Haixiu Road
  Registrant Address.............. Haikou
  Registrant Address.............. 570126
  Registrant Address.............. HN
  Registrant Address.............. CN
  Registrant Email................ 445428688@qq.com
  Registrant Phone................ +86.89866781113
  Registrant Fax.................. +86.89866781113
```

Hainan Yanwu historical WHOIS

Are any of these contacts real people?

The number of contacts listed and the re-use of telephone numbers raised our suspicions. We started to think that perhaps some, or all, of these contact names were fictitious. We reached out to our trusted network of contributors and posed the question: who was the real owner of these telephone numbers and email addresses?

So, who is Mr Ding?

While researching the phone numbers from these companies, one of our contributors turned up this information linking phone number 15638338966 (you'll remember that from an earlier job advert for Hainan Xiandun, in the name Mr Chen) with a new e-mail address: dxy0015@163.com.

Relationship between 15638338966 and dxy0015@163.com

Why is that e-mail address important? Because this information, from a frequent flyer account, shows that dxy0015@163.com and the phone number belong not to a Mr Wang, or a Mr Jiang, or a Mr Chen, but to a Mr Ding Xiaoyang (丁晓阳), who is very much a real person.

Subject: 您已成功使用金鹏积分兑换奖励机票
From: "金鹏俱乐部" <ffp@vip.hainanairlines.com>
Date: 1/8/2019, 11:46 PM
To: DXY0015@163.COM

我的账户　获取积分　消费积分　活动专区　俱乐部新闻

尊敬的丁晓阳先生：

您已成功使用会员卡号6618400581中的23000消费积分兑换1-29 HU7659 海=武汉2-10 HU7660 武汉=海口奖励机票,您目前的帐户余额是54446.83积分。

如非您本人操作，请及时拨打会员热线950717咨询以保证账户安全。

金鹏俱乐部会员服务热线：950717
会员邮箱：ffp@hnair.com
金鹏俱乐部网站：ffp.hnair.com
海航24小时订票热线：95339

Ding Xiaoyang's name (丁晓阳) appears in this e-mail from Hainan airlines to dxy0015@163.com
We are extremely grateful to our contributor for their diligent work in finding this information. Our thanks also go out to Mr Ding for not changing his password after it had been leaked online.

In summary: in some cases the contacts for these front companies in Hainan may be aliases. Other than Hainan University academic Gu Jian, the only individual that we have been able to link to the adverts is the true owner of one of the telephone numbers: Hainan resident Ding Xiaoyang.

Is Ding the person in charge of these front companies? Does Ding have connections to the Chinese State? We know the answer, he knows the answer, do you?