APT40 is run by the Hainan department of the Chinese Ministry of State Security

intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/

intrusiontruth January 16, 2020

In our previous articles we identified a network of front companies for APT activity in Hainan and showed their links to Hainan University academic Gu Jian. Although it was difficult to find people who work for these companies we identified a number of individuals and concluded that this network of companies was actually APT40. One of the individuals we identified, Ding Xiaoyang, is the owner of a phone number used on job adverts under the name Mr Chen.

Ding Xiaoyang's role

When we started we weren't sure what Ding Xiaoyang's role was.

So we ran the numbers. How many Dings are there likely to be in Haikou, Hainan, and would it be possible to identify a specific Ding Xiaoyang among them?

- Current population of China: 1,419,627,903
- World Bank estimate of working age males: 511,625,426 (36.04%)
- Population of Haikou in Hainan: 1,517,400
- Estimate of working age males in Haikou: 546,862
- Number of common Chinese surnames: 100 ()
- How common is the surname Ding: 48th out of 100
- Arithmetic progression: $S_n = n/2 * (2a_1 + [n-1] * d) \Rightarrow S_{100} = 5,050$
- Proportion of Dings: 52 (100 – 48) out of 5,050
- Percentage chance of being a working age male called Ding: 1.04%
- How many Dings in Haikou: likely 5,687

5,687 Dings were too many to work through one by one. So we thought of a different way to find out which Ding was our Ding. Why not use a highly effective, international, and motivated network of contributors who could tell us exactly who he is and what he does…

As we saw previously, he is the owner of the telephone number being used on job adverts for the network of front companies for APT40.

Our contributors discovered that Ding Xiaoyang is also a Computer Science specialist who lives and works in Haikou.

We actually know quite a lot more about Ding Xiaoyang.

Our original blueprint for an APT in China requires: contract hackers and specialists, front companies, and an intelligence officer.

Front companies? Check. Specialists? Check. Intelligence officer? Ding Xiaoyang…

How did we do it?

Remember the (previously hacked and released) QQ information that be utilised to show APT17's use of reservoir dogs style codenames? Well…

QQ account 348504569 uses the name Wan Huo Yan Wan (卍火焰卍). Interesting? Not until you look into other names used by the same account. One is Ding Da Xia (丁大侠). Another is Ding Xiaoyang (丁晓阳). Let's hypothesise that this might be our Mr Ding and that he might be an intelligence officer in Hainan, China. Is there any evidence?

Let's look at what QQ user 348504569 was up to. Amongst other things, he was a member of QQ Group 92688210 which was called "内部文化活动交流" or "Exchange of internal cultural activities". The group was created on 18 September 2009 and had 25 members. It's description, "仅供内部成员文体休闲娱乐交", stated that it was for internal members only. But internal to what? A University perhaps? Or … a government institution?

One of our contributors examined all the members of this group to try to identify their affiliation. Imagine our surprise when we discovered an account that looked like it might belong to an intelligence officer!

Who is Mr Huang?

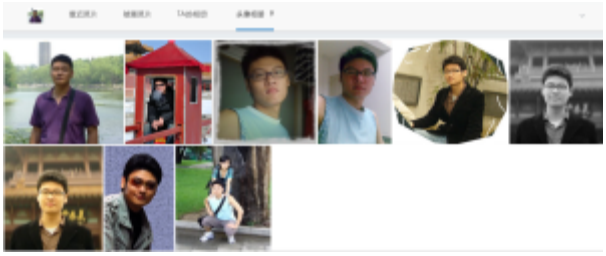
QQ account 249550138 was a member of the internal cultural exchange group. It variously used the name Huang Liangli (黄良利), Deng Dai (等待), Ge Li (哥利) and Lao Ban Liang Li (老班良利).

But somebody once said that a picture paints a thousand words. So here is a picture that we found online here and here.

Yes, that's an MSS uniform. The significance of number 461079 on his chest? 46 = Hainan.

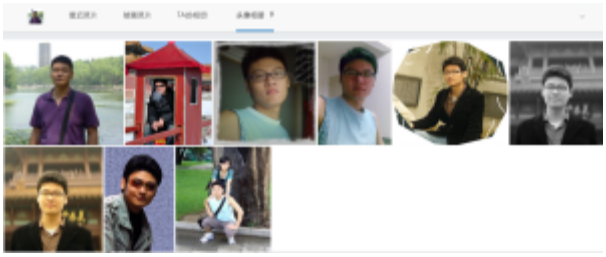
But that's not it…

We also found this RenRen profile for Ding Xiaoyang which contained a number of photos of the younger Mr Ding.



Ding Xiaoyang's profile photos on Renren

Ding Xiaoyang's Renren profile



Ding Xiaoyang's profile photos on Renren

Up until 2009 Ding Xiaoyang posted regularly on Renren, but his posts suddenly stopped. Why? Because he obtained a sensitive job working for the Chinese State. How do we know? Well, he said so:

08 05月 2009

写论文，真能把人搞崩溃啊！

状态 分享 回复(14)


申腾飞:
2009-05-08 22:58


张泰生: 确实。。
2009-05-08 23:16


李贤华: 呵呵，加油～过去了就好了～
2009-05-09 11:40


徐颖君: 同感
2009-05-09 14:47


丁晓阳: 回复李贤华: 过去了就好了？我都晕过去两次了，咋还没好呢?
2009-05-09 16:28


丁晓阳: 回复徐颖君: 工作？读研？哪里?
2009-05-09 16:29


李贤华: 回复丁晓阳: 哈哈，人生就是不断从一个火坑跳进另一个火坑，慢慢熬着吧～～～～
2009-05-09 17:44

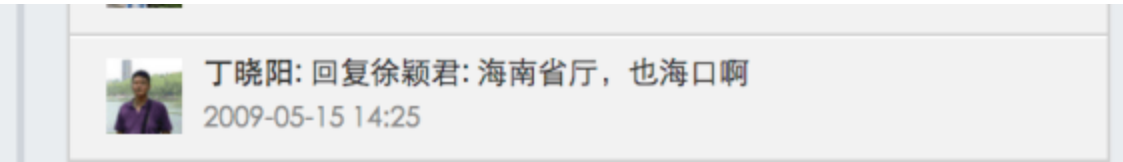

徐颖君: 回复丁晓阳: 工作啊 边检 你呢
2009-05-11 10:44


丁晓阳: 回复徐颖君: 差不多，公安
2009-05-11 12:07


徐颖君: 恩 在哪呢
2009-05-15 09:53


丁晓阳: 回复徐颖君: 在一个遥远偏僻的地方，海南。。。
2009-05-15 10:03


徐颖君: 呵呵 好的啊 我在广东 离得还算近 是海口公安局吗
2009-05-15 10:06



In 2009 in this post, Ding talked about his new job with the Ministry of Public Security (MPS) at the Hainan Provincial Department.

> Ding: Work? Studying? Where?
>
> Xu: Work, border inspection, how about you
>
> Ding: Almost, MPS
>
> Xu: Where is it?
>
> Ding: In a distant and remote place, Hainan. . .
>
> Xu: Hehe, okay. I'm close in Guangdong. Is it Haikou Public Security Bureau?
>
> Ding: Hainan Provincial Department, also Haikou

We haven't talked much about the Ministry of Public Security before. It is the Chinese national police force and it is commonly used as cover for … the MSS.

Hainan State Security Department

Our researchers are not the only team to find a link between APT40 and Chinese intelligence. Closely held commercial intelligence has also shown that APT40 is run by the Hainan department of the Chinese Ministry of State Security.

According this handy list of public toilets in Haikou, the Hainan State Security Department is based at No. 176 Nanhai Avenue, Xiuying District, Haikou, Hainan (海南省海口市秀英区南海大道176号).

It looks like this, note the hammer and sickle topiary, satellite dishes, and perimeter wall:


南海大道
蛋仔妈
金福路
金福路

Hainan State Security Department on Nanhai Avenue in Haikou

Conclusion

Either a Hainan intelligence officer has a side-hustle running a business empire of at least 13 “fast-growing, high-tech information security companies”, *and* that business empire has a side-hustle recruiting people with knowledge of the languages spoken in APT40 target countries coincidentally in the months preceding APT40 attacks in those countries, *and* on the same island that we know APT40 runs its operations.

Or, APT40 is run by Ding Xiaoyang, an intelligence officer at the Hainan State Security Department.

If it walks like a duck and quacks like a duck…

At this point, we are starting to think that we might not need to go to such lengths to investigate which part of the state is directing an APT.

We caught a re-run of the great TV show Blankety Blank the other day. We could have just played that instead of writing this blog.

- APT3 was known to be based in Guangdong and was the work of the Guangdong State Security Department
- APT10 was known to be based in Tianjin and was the work of the Tianjin State Security Bureau
- APT3 was known to be based in Jinan and was the work of the Jinan State Security Bureau
- APT40 was known to be based in Hainan and the work of was the _ _ _ _ _ _ State Security Department

Easy.