Who is Mr Zhang?

intrusiontruth.wordpress.com/2018/08/06/who-is-mr-zhang/

intrusiontruth August 6, 2018

Gao Qiang and Zheng Yanbin weren't working alone. In this article we identify another member of the group.

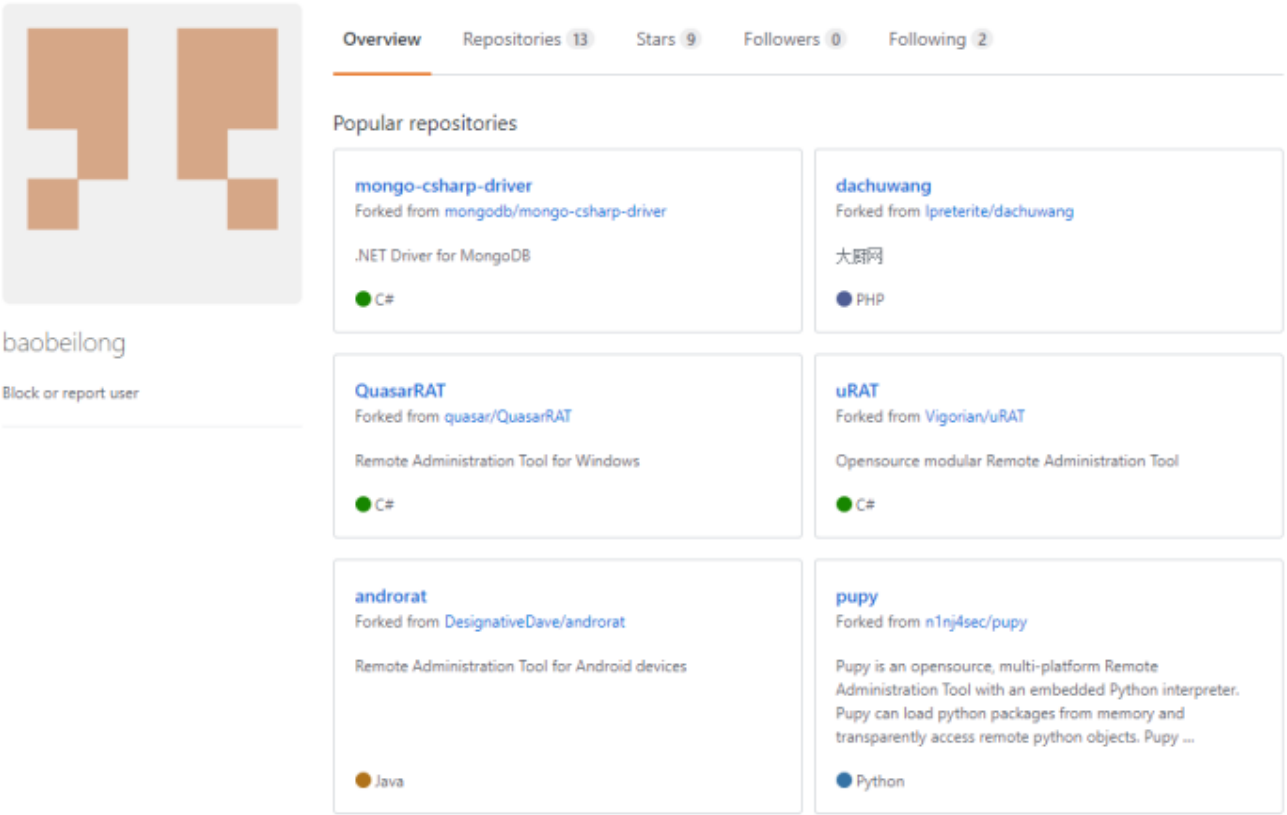
fisherxp to baobeilong

Inspection of @fisherxp's Twitter account shows that he follows 259 people and has 16 followers. One particularly interesting account, @baobeilong, both follows @fisherxp and is followed by it.

baobeilong's Twitter account

baobeilong's interest in APT10 tools

'baobeilong' also has a GitHub account that shows a strong interest in Remote Access Trojans (RATs) including QuasarRAT and Trochilus, which baobeilong forked in 2015. JPCert reported in 2017 that Trochilus was used by APT10 as the basis for the RedLeaves malware. QuasarRAT was also used by APT10, as described in the FireEye blog post APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat.



baobeilong's GitHub account

Location in Tianjin

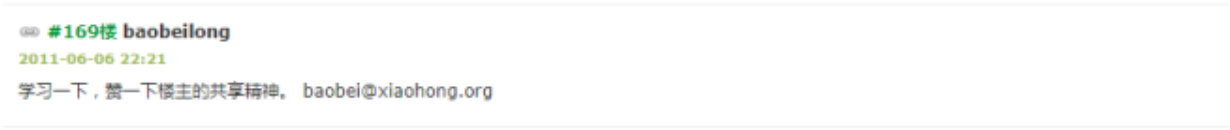
‘baobeilong’ has a Flickr profile including photos of family and a fire on Hualong Road in Tianjin.

Photo of a fire in Tianjin uploaded by baobeilong to Flickr

Analysis by this blog leads us to conclude that the photo of the fire may have been taken from the Wanchun Meizuan Mansion building on the corner of Hualong Road and Xinkai Road in Tianjin from one of the floors occupied by flats. Readers will remember Xinkai Road as the address of the Laoying Baichen Instruments Equipment Co, associated with Gao Qiang in our previous article.

baobeilong to xiaohong[.]org

‘baobeilong’ also has a fanfou.com account where the user provides a website address – xiaohong[.]org. A Chinese language blog also contains a posting using the e-mail address baobei[at]xiaohong.org, helping to confirm the connection between ‘baobei[long]’ and the xiaohong[.]org domain.



A user named baobeilong posting an e-mail address using the xiaohong[.]org domain**xiaohong[.]org to Zhang Shilong**

In 2007, the registration details for xiaohong[.]org were Zhang Shilong, Hedong, Yuyang Road No 121, Tianjin. He provided +8613116037711 as his phone number and the e-mail address atreexp[at]yahoo.com.cn.

The registration details were later updated on 08/07/2008 to include fax number +865925163169 and then on 01/06/2016 to add phone number +8615122188031. The e-mail address was changed at the same time to robin4700[at]foxmail.com.

Zhang Shilong to atreex[.]cn

Reverse WHOIS registration information for Zhang's e-mail address atreexp[at]yahoo.com.cn shows that it was also associated with the domain atreex[.]cn. The Wayback Machine shows that this domain hosted a Chinese language blog relating to hacking and IT security topics between 2006 and 2007.

atreex[.]cn to fisherx[.]com

Completing the circle back to Gao Qiang / fisherxp, an article in 2006 on the atreex[.]cn blog provided a link to fisherx[.]com.

Link to fisherx[.]com on a 2006 copy of atreex[.]cnThis domain, which bears a striking resemblance to Gao Qiang's "fisherxp", was registered to an address in 'Tian Jing' with postcode 300011. The same postcode as the Laoying Baichen Instruments Equipment Co, associated with Gao Qiang (see previous article).

Zhang Shilong's reaction to Cloud Hopper report

The domain xiaohong[.]org is particularly interesting because on 12/04/2017, the domain registration information was updated to 'Domain Protection Services', making it effectively anonymous. That date is significant – it was the week after the Cloud Hopper report on APT10 was released by PwC and BAE Systems.

In summary, APT10 hacker Gao Qiang of Tianjin, China has multiple connections to Zhang Shilong, another Chinese hacker from Tianjin. Zhang Shilong has independent links to APT10 tools and made an attempt to protect his identity immediately after the 2017 Cloud Hopper report.