More on Huaying Haitai and Laoying Baichaun, the companies associated with APT10. Is there a state connection?

intrusiontruth.wordpress.com/2018/08/09/was-apt10-the-work-of-individuals-a-company-or-the-state/

intrusiontruth August 9, 2018

In the absence of more concrete proof, the 2017 Cloud Hopper report on APT10 relied on timing analysis to make the connection to China. Compile times of executable files and registration times of domains all pointed to work undertaken between 9am and 5pm Beijing time.

If Zheng Yanbin, Gao Qiang and Zhang Shilong were working between 9am and 5pm and managed to orchestrate one of the largest Cyber attacks on western infrastructure of all time, it follows that any company for whom they were working would probably have been involved in the operation.

Laoying Baichaun Instruments Equipment Co Ltd

The first company identified in our article on Gao Qiang was Laoying Baichaun Instruments Equipment Co Ltd. It was associated with fisherxp via his name, phone number and the postcode registered to fisherx[.]com, and less conclusively to Zhang Shilong via the photo he took from a building nearby on Xinkai Road. The company has offices in Tianjin and appears to still operate, making sales online.

Xinkai Road, the home of Laoying Baichaun Instruments Equipment Co Ltd

Tianjin Huaying Haitai Science and Technology Development Co Ltd

The second company identified was the Tianjin Huaying Haitai Science and Technology Development Co Ltd (天津华盈海泰科技发展有限公司). It was associated with fisherxp via a job advert placed in his name. Huaying Haitai has an entry in several online Chinese company registration databases.

Alibaba Enterprise entry for Huaying Haitai

Fang Ting, Sun Jie and Feng Tao

The entries name two shareholders – Fang Ting (方亭), who owns 70% of the company, and Sun Jie (孙杰) who owns 30%.

Shareholder information for Tianjin Huaying Haitai from 1688.com

Another individual named Feng Tao is also associated with the company, listed as a manager in some databases.

The company is headquartered in Tianjin at the Fuyu Plaza building on Jiefang South Road in the Hexi district (天津市河西区解放南路中段西侧富裕大厦1-1906).

Company information online shows that the company has previously had a website – huayinghaitai[.]com – though there is no trace of it ever having had any content

The site shown above includes a company profile that loosely translates as:

> Haitai Technology Development Co., Ltd. is a high-tech company dedicated to network security construction and network security product development. The company's technical team is a senior engineer with extensive network security experience overseas. Enthusiasm and superb technology contribute to China's cyber security and contribute to the world's cyber security. We also welcome enthusiastic young people to join my team and career.

WHOIS registration information for the huayinghaitai[.]com domain shows that the domain is registered to zhangduker[at]gmail.com with the phone number +86 022 88269292. Other domains associated with the same e-mail address bear the name Zhang Du, including:

- 8haowaimai.cn
- 8haowaimai.com.cn
- appforge.cn
- appforge.com.cn
- bahaowaimai.cn
- bahaowaimai.com.cn
- bahaozhizunwaimai.cn
- bahaozhizunwaimai.com.cn
- daodewang.cn
- dns-up.org
- gujian.net.cn
- huayinghaitai.com
- iecho.cn
- iecho.com.cn
- linuxhome.com.cn
- linuxhome.org.cn
- lvxinghome.com
- zhizunwaimai.cn
- zhizunwaimai.com.cn

Association with the state?

Having identified two companies at one time connected to at least one APT10 hacker, the question remains – were they hacking on behalf of the Chinese state? Huaying Haitai is a small company with two shareholders and, for a Cyber security company, a very small web presence. The situation bears more than a striking resemblance to Boyusec, a company used as cover for APT3 activity by the Chinese Ministry of State Security.

This blog believes that it has proof of links between the APT10 actors named in our research and the Chinese state, but our analysts are keen to corroborate it before publishing. **If you are a Cyber Threat Intelligence analyst and have information that could help us confirm the link between Zheng Yanbin, Gao Qiang, Zhang Shilong, Laoying Baichaun or Huaying Haitai and the Chinese state, please contact us.**