

# 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 Baichuan 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](#).

The screenshot displays the company profile for Tianjin Huaying Haitai Science and Technology Development Co Ltd on the Alibaba Enterprise platform. The page is organized into sections: 'Basic Information' (基本信息) and 'Overall Information Overview' (综合信息概况).

**Basic Information:**

- 企业名称: 天津华盈海泰科技发展有限公司
- 统一社会信用代码: 911201036974473116
- 工商注册号: 120103000126096
- 经营状态: 在营 (开业)
- 企业机构类型: 有限责任公司
- 成立日期: 2010-01-08
- 法定代表人: 方享
- 营业期限: 2010-01-08 - 2030-01-07
- 注册资本 (万元): 100.0000
- 注册资本币种: 人民币元
- 登记机关: 天津市河西区市场和质量技术监督局
- 最后年检年度: 2015
- 地址: 天津市河西区解放南路中段西侧富袖大厦1-1906
- 经营范围: 计算机软件技术开发、咨询、服务、转让; 商务信息咨询; 会议服务; 机械设备 (小轿车除外)、五金交电、化工产品 (危险化学品及易制毒品除外)、金属材料、电子产品、建筑材料、计算机软硬件及耗材、文具用品、办公设备批发兼零售。 (依法须经批准的项目, 经相关部门批准后方可开展经营活动)

**Overall Information Overview:**

- 阿里巴巴平台经营店铺: 该企业暂未激活
- 失信信息: 无
- 工商变更记录: 无
- 是否深度认证: 否

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%.

The screenshot shows a corporate information page with two main sections: '主要管理人员' (Main Management Personnel) and '企业股东信息' (Company Shareholder Information). The management section lists Fang Ting as Executive Director and Sun Jie as Supervisor. The shareholder section lists Fang Ting as the 70% shareholder and Sun Jie as the 30% shareholder, both with investment dates of 2010-01-08 and investments in RMB.

| 主要管理人员     |          |
|------------|----------|
| 方亭<br>执行董事 | 孙杰<br>监事 |

  

| 企业股东信息  |   |
|---|---|
| <b>方亭</b><br>出资日期: 2010-01-08<br>出资方式: 货币<br>出资比例: 70.00% | <b>孙杰</b><br>出资日期: 2010-01-08<br>出资方式: 货币<br>出资比例: 30.00% |

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 screenshot shows the recruitment page for Tianjin Huaying Haitai Technology Development Co., Ltd. on the Zhanqi (赶集网) website. The page includes a search bar, navigation tabs for '公司简介' (Company Introduction) and '在招职位' (Open Positions), and a '基本信息' (Basic Information) section.

**天津华盈海泰科技发展有限公司**

公司简介 | 在招职位

更多企业招聘信息

**基本信息**

|                      |   |
|----------------------|---|
| 公司名称: 天津华盈海泰科技发展有限公司 | 公司规模: 20-99人  |
| 公司行业: 计算机网络通信        | 公司网站: <a href="http://www.huayinghaitai.com">http://www.huayinghaitai.com</a> |
| 公司类型: 民营             |   |

公司简介: 海泰科技发展有限公司是一家致力于网络安全建设、网络安全施工、网络安全产品开发的科技公司, 公司技术团队都是在海外有着丰富网络安全经验的高级工程师, 凭着满腔热忱和高超的技术为中国网络安全能开身世界网络安全贡献力量, 同时也欢迎有热情的年轻人加入我的团队和事业中来。

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.**