APT10 was managed by the Tianjin bureau of the Chinese Ministry of State Security

By intrusiontruth

Published: 2018-08-15 · Archived: 2026-04-05 16:49:37 UTC

In previous posts, Intrusion Truth showed that the Cloud Hopper / APT10 hackers that attacked thousands of global clients of Managed Service Providers (MSPs) in 2016 were based in Tianjin, China.

We identified Zheng Yanbin, Gao Qiang and Zhang Shilong as three actors responsible. We associated them with the Huaying Haitai Science and Technology Development Co Ltd (天津华盈海泰科技发展有限公司) and Laoying Baichen Instruments Equipment Co Ltd in Tianjin China. But we haven’t yet explained who was masterminding or controlling the attacks.

In the course of our investigation over the last year, we engaged with several Cyber Threat Intelligence analysts who provided both raw data and analysis to our team. Amongst the data provided to us recently was evidence that Gao Qiang has been working with the Chinese state. The key piece of data was an Uber journey.

Journeys to 85 Zhujiang Road

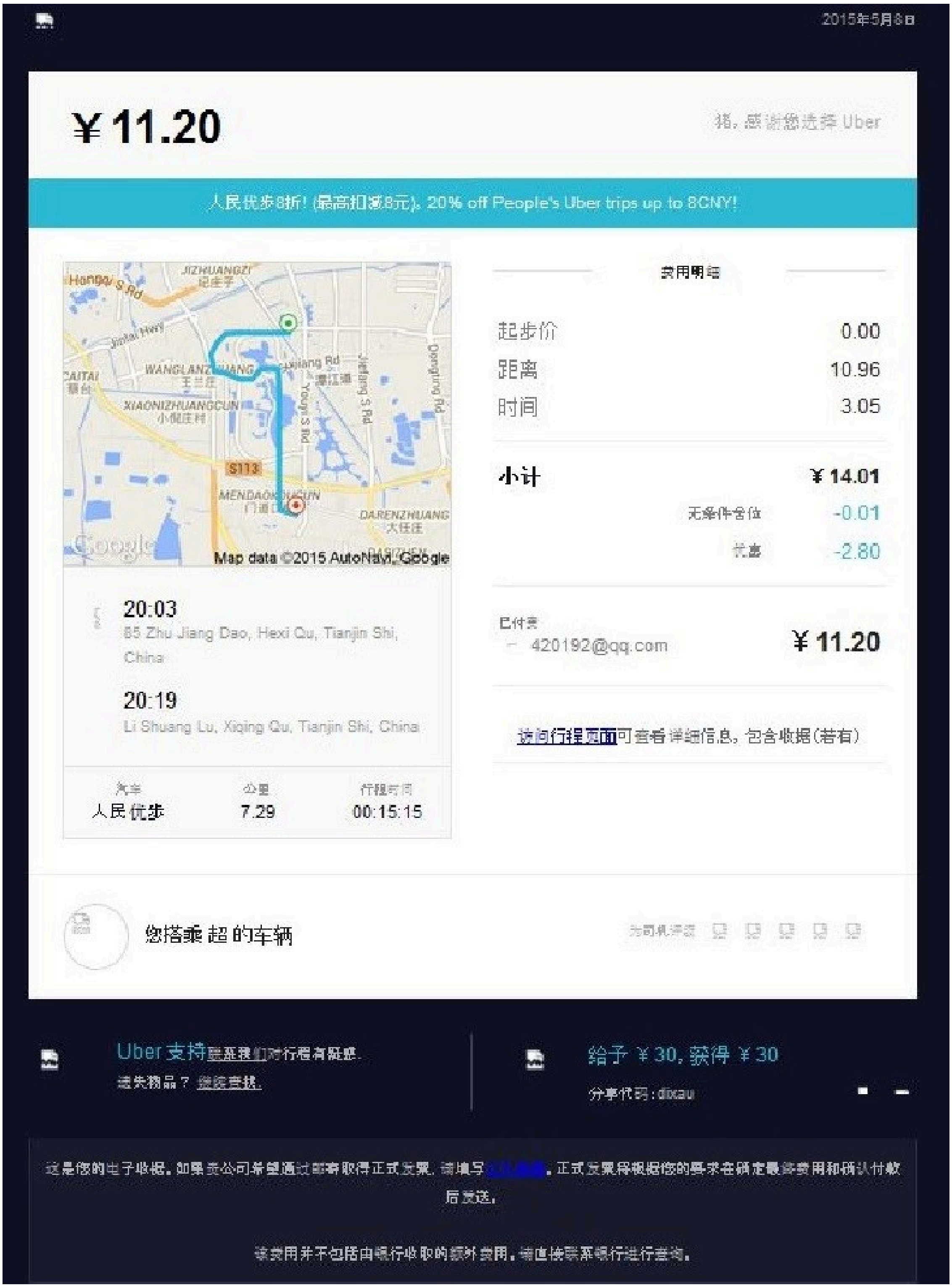
强's travel from work at Huaying Haitai to Xiqing District.

This image, which was provided by an analyst who prefers not to be named publicly (but whose identity we have independently verified), shows an Uber receipt addressed to a user called 'Qiang' (强) and bears the e-mail address 420192[at]qq.com, an account that we believe to be used by APT10 actor Gao Qiang.

The receipt shows travel at the end of the working day between 384 Jiefang South Road (解放南路) – immediately outside the Fuyu Mansion address of Huaying Haitai – and a destination in what appears to be a residential area of the Xiqing District of Tianjin just south of the Waihuan River. We have blacked out the exact street number in the image. This map shows the location of the start of the journey, outside the Fuyu Mansion buildings.

The collection address outside the Fuyu Mansion Buildings, home of Huaying Haitai

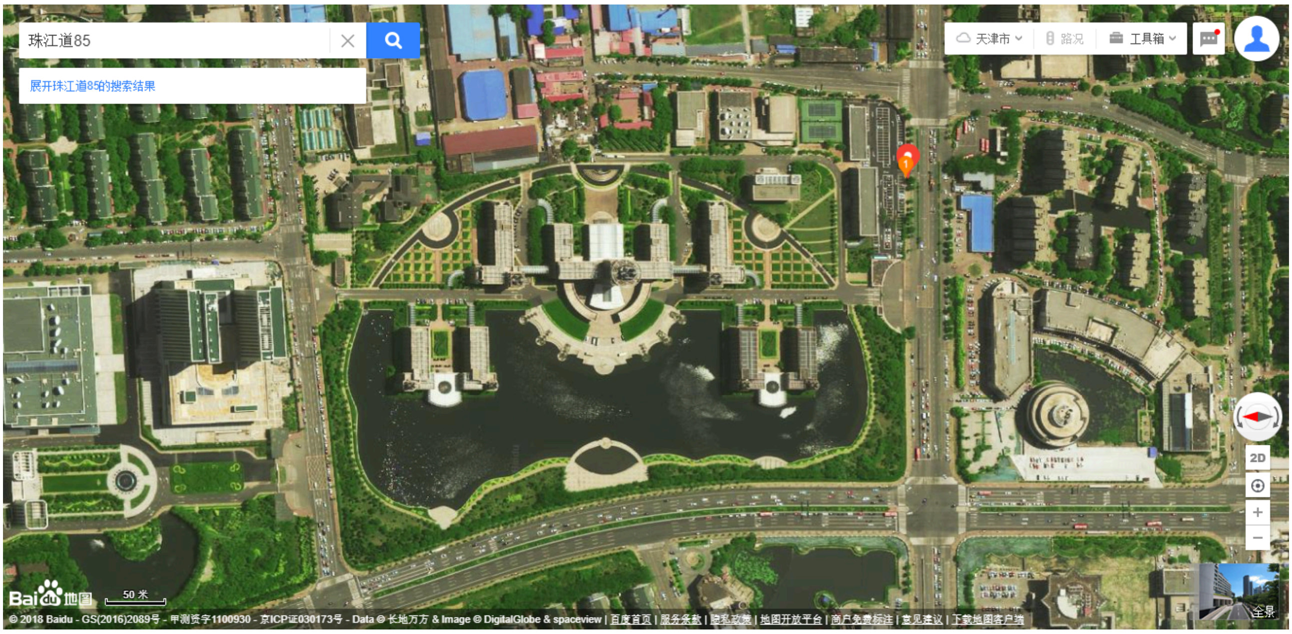
This second Uber receipt, provided by the same analyst, shows further travel by the same user, though here he uses the name 'Pig' (猪). This could be some attempt to disguise the nature of the journey, though readers will note the same QQ e-mail address is used.



猪's travel between Xiqing District and 85 Zhujiang Road

In this case the journey is between the same residential area in the Xiqing District and a large complex at 85 Zhujiang Road (珠江道), Tianjin.

According to the rest of the data revised by analysts working for this blog, this was one of a number of journeys made by the user to/from the same complex on Zhujiang Road.



Tianjin State Security Bureau

85 Zhujiang Road is an [important address in Tianjin]() – it is the headquarters of the Tianjin State Security Bureau (天津市国家安全局), a regional arm of the Ministry of State Security (MSS). MSS is the same Chinese Intelligence Service that was [tasking APT3 via a cover company managed by its office in Guangdong]().

The large complex visited by Gao Qiang at 85 Zhujiang Road, Tianjin

This looks like what it is – an exact copy of the APT3 model. This was a large scale infiltration of western infrastructure conducted by a team of Chinese citizens working for a small company with links to the Chinese Intelligence Service, MSS. It is the second time that this blog has proven a link between a damaging APT group and the Chinese state (and it certainly won't be the last).

The conclusion?

Either:

someone with the *same name* as an apparent APT10 hacker,

travelled from the *same building* as an APT10 associated company, and

met frequently with the Ministry of State Security in Tianjin.

Or:

APT10 was the work of the Chinese Ministry of State Security.

Discover more from Intrusion Truth

Subscribe to get the latest posts sent to your email.

Post navigation
