# Two Birds, One STONE PANDA

crowdstrike.com/blog/two-birds-one-stone-panda

Adam Kozy

August 30, 2018

## Introduction

In April 2017, a previously unknown group calling itself IntrusionTruth began releasing blog posts detailing individuals believed to be associated with major Chinese intrusion campaigns. Although the group's exact motives remain unclear, its initial tranche of information exposed individuals connected to long-running GOTHIC PANDA (APT3) operations, culminating in a connection to the Chinese firm Boyusec (博御信息) and, ultimately, Chinese Ministry of State Security (MSS) entities in Guangzhou.

Recently, in July and August 2018, IntrusionTruth has returned with new reporting regarding actors with ties to historic STONE PANDA (APT10) activity and has ultimately associated them with the MSS Tianjin Bureau (天津市国家安全局). Though CrowdStrike® Falcon Intelligence™ is currently unable to confirm all of the details provided in these most recent posts with a high degree of confidence, several key pieces of information can be verified.

- Several of the named individuals have been active registering domains as recently as June 2018, and they responded to the IntrusionTruth blog posts by scrubbing their social media or by following IntrusionTruth's Twitter account.
- Named individuals ZHANG Shilong and GAO Qiang have significant connections to known Chinese hacking forums, and they have sourced tools currently in use by China-based cyber adversaries.
- ZHANG has registered several sites with overlapping registrant details that show both his affiliation with several physical technology firm addresses as well as his residence in Tianjin.
- Named firm Huaying Haitai has been connected to a Chinese Ministry of Industry and Information Technology (MIIT) sponsored attack and defense competition; this is similar to GOTHIC PANDA's ties to an active defense lab sponsored by China Information Technology Evaluation Center (CNITSEC).
- Huaying Haitai has previously hired Chinese students with Japanese language skills; this is significant, as STONE PANDA has engaged in several campaigns targeting Japanese firms.
- The MSS Tianjin Bureau is confirmed to be located at the described address, not far from many of the registrant addresses listed by ZHANG as well the firms GAO was likely recruiting for.

More details that may further illuminate these findings and provide a higher confidence in connecting STONE PANDA to the MSS Tianjin Bureau are likely to emerge.

## Background

Throughout May 2017, using a variety of historical information and open-source intelligence (OSINT), IntrusionTruth released several blog posts identifying several individuals connected to Boyusec. Though CrowdStrike's Threat Intelligence team had suspected GOTHIC PANDA was an MSS contractor for several years, the IntrusionTruth posts and subsequent research by RecordedFuture into MSS ties to the China Information Technology Evaluation Center (CNITSEC/中国信息安全测评中心) corroborated additional details from various sources and provided a higher degree of confidence. Confidence in these findings was further boosted when the U.S. Department of Justice named Boyusec and several of the described individuals in an indictment, and detailed GOTHIC PANDA tactics, techniques, and procedures (TTPs) in detail.

CrowdStrike Falcon Intelligence was able to independently verify the majority of this information and concluded that not only is CNITSEC associated with the MSS, but its former director WU Shizhong (吴世忠) was simultaneously dual-hatted as the director of the MSS Technology/13th Bureau (国家安全部科技局局长)[1] [2] [3], implying that the MSS plays a crucial role in China's code review of foreign products and is now able to cherry pick high-value vulnerabilities from its own capable domestic bug hunting teams. CNITSEC's role in code review for foreign entities has led to its access to Microsoft's source code dating back to 2003 and the use by KRYPTONITE PANDA of a high-value vulnerability (CVE-2018-0802), discovered by Chinese firm Qihoo 360, a month before it was publicly revealed.

WU Shizhong Presenting on the "Digital Silk Road" at the Second Wuzhen World Internet Conference in 2015

As research into the IntrusionTruth leads on STONE PANDA continues, Falcon Intelligence has already observed some consistencies with known MSS operations.

## Sinking Like a STONE

### GAO Qiang (高/郜 强)

Many of the personal details for GAO were scrubbed shortly after IntrusionTruth's post introducing him went live, including his Tencent QQ account. The blog connects him to the moniker *fisherxp* via an initial spear-phishing campaign from 2010 previously attributed to STONE PANDA. Multiple sites with profile pictures appear to show the owner of the *fisherxp* accounts, though this has yet to be independently confirmed as GAO. *Fisherxp*'s QQ shows his alternate username as **肥猪** or "big porker". IntrusionTruth later links GAO to several documented Uber rides to the MSS Tianjin Bureau's office address where both his first name, Qiang/**强**, and **猪** are used by the app to identify him and tie him to the QQ number 420192. CrowdStrike cannot confirm the validity of these Uber receipts at this time.


fisherxp

However, *fisherxp*'s account on popular Chinese technology forum 51CTO is still active and shows that he has downloaded not only the open-source *DarkComet* RAT and numerous password cracking tools, but more importantly, several favorite tools used by a plethora of known Chinese cyber adversaries including *Gh0st RAT 3.6*, *zxarps* (an ARP-spoofing tool by legacy hacker LZX), and *lcx.exe* (a port-forwarding tool by legacy hacker LCX)[4].

### ZHANG Shilong (张世龙)

ZHANG was originally introduced by IntrusionTruth as a reciprocal follower of *fisherxp*'s Twitter account via his own @baobeilong account. *Baobeilong* (**宝贝龙**/"Baby Dragon") also maintained a GitHub account that had forked both the *Quasar* and *Trochilus* RATs, two open-source tools historically used by STONE PANDA, but the account has since been scrubbed. This information was verified by CrowdStrike before being removed completely. Falcon Intelligence recently independently conducted detailed analysis of the *RedLeaves* malware used to target numerous Japanese defense groups and found it was directly sourced from Trochilus code, but it has undergone several evolutions and contains prefixes suggesting it could also be used to target Russia and the DPRK. There is no conclusive evidence at this time that RedLeaves is solely attributed to STONE PANDA.

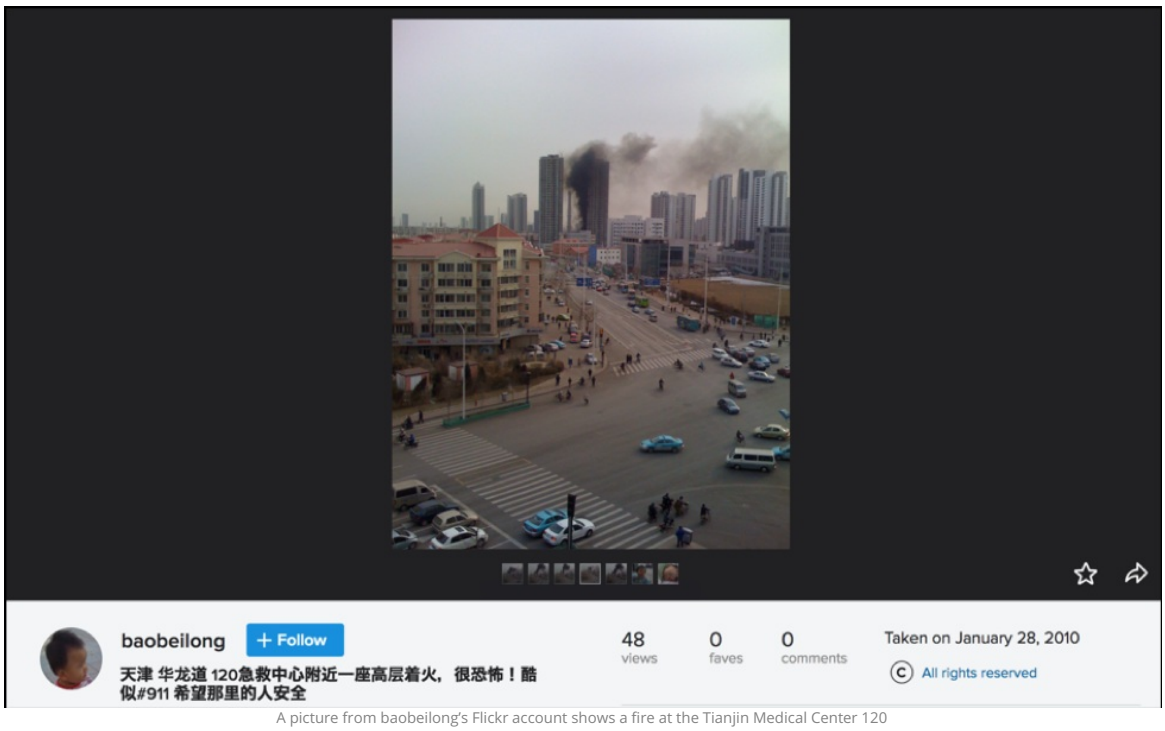

*Baobeilong* did maintain a Flickr account with numerous pictures that proved key in identifying his location later, similar to how *cpyy*'s photos helped identify his affiliation to the People's Liberation Army (PLA) in CrowdStrike's PUTTER PANDA report.

IntrusionTruth then drew connections from *baobeilong*'s other online accounts to registrant details for *xiaohong[.]org*, which dated back to 2007 and revealed ZHANG's full name—ZHANG Shilong. From there, a trail of overlapping registrant details reveals ZHANG's hanzi characters for his name (**张世龙**), likely one of his personal home addresses, potential work addresses and several email addresses:

- long@xiaohong[.]org
- baobei@xiaohong[.]org

- atreexp@yahoo[.]com.cn
- robin4700@foxmail[.]com
- eshilong@vip.qq[.]com

Specifically tracing registrant details from atreexp → robin4700 → eshilong shows that ZHANG was active registering sites as recently as June 5, 2018, including a personal blog where his picture and name features prominently along with several technology-related blog posts.

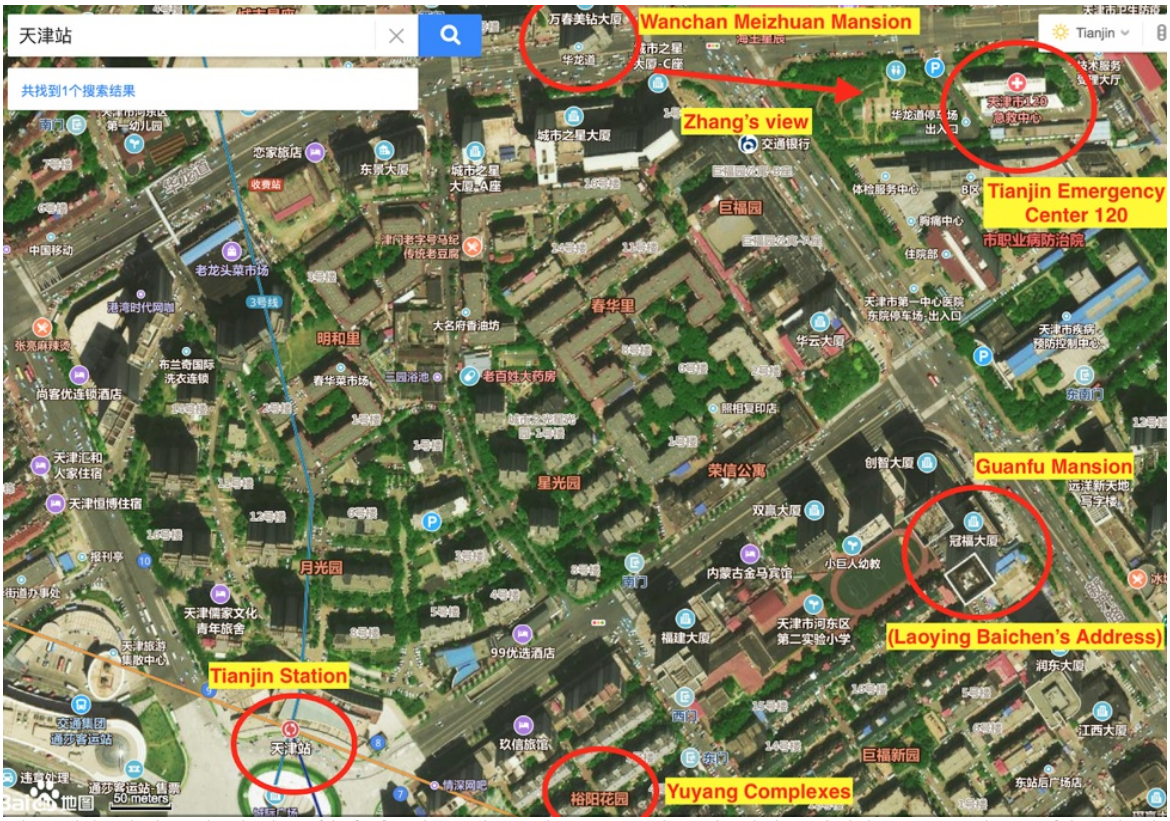



A picture from baobeilong's Flickr account shows a fire at the Tianjin Medical Center 120

## Laoying Baichen Instruments

The original blog post on GAO lists his contact information in recruitment postings for two separate companies, one of which is Laoying Baichen Instruments (characters unknown at the time of this writing). No records could be found for such a firm, however, IntrusionTruth lists the address associated with it as Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin (**天津市河东区新开路46号冠福大厦** 1102).

During the course of investigating Laoying and the Guanfu mansion, Falcon Intelligence noticed that the Guanfu Mansion is also the registered address of a firm called Tianjin Henglide Technology Co., Ltd. (**恒利德天津科技有限公司**), which is listed as one of only a few "review centers" certified by CNITSEC in Tianjin[5]. Laoying and Henglide are listed as being on different floors, however having a CNITSEC review center in the same building is noteworthy given CNITSEC's connection to MSS and previous linkage to Boyusec/GOTHIC PANDA.



Zhang is believed to have taken the photo of the fire from the Wanchan Meizhuan Mansion. This is relatively close to both the Yuyang Complex (one of Zhang's listed registrant addresses) and the Guanfu Mansion, Laoying Baichen's listed address.

## Tianjin Huaying Haitai Science and Technology Development Company

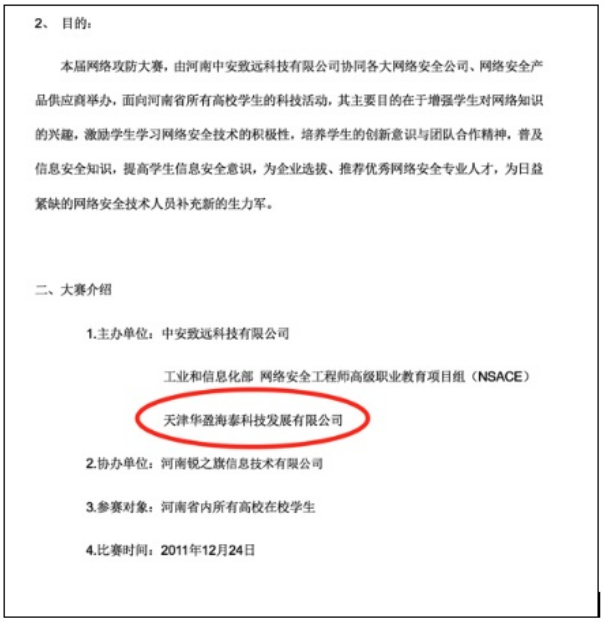
The other firm GAO appears to have been recruiting for is Huaying Haitai (**天津华盈海泰科技发展有限公司**). As the IntrusionTruth blog post mentions, it is a registered firm with two listed representatives, Fang Ting (**方亭**) and Sun Lei (**孙杰**), and a listed address of 1906 Fuyu Mansion (**天津市河西区解放南路中段西侧富裕大厦**1-1906).

Searches for more information on Huaying Haitai turned up two interesting government documents. One is a recruitment Excel sheet detailing recent graduates, their majors and their new employers and addresses. Huaying Haitai is listed as having hired a recently graduated female student from Nankai University in 2013 who majored in Japanese. This is interesting considering STONE PANDA's extensive targeting of Japanese defense firms after this time period, but it is by no means conclusive evidence that the firm is connected to STONE PANDA.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 975 | 外国语学院 | 日语 | 091004 | 张驰 | 女 | 公主岭市西公主大街170号 | 136100 | 公主岭市人力资源和社会保障局 | 曾佳 | 0434-6203688 |
| 976 | 外国语学院 | 日语 | 091004 | 刘丹 | 女 | 四平市铁西区中央西路7-8马路四平市人力资源市场5楼 | 136000 | 四平市人才服务中心 | | 0434-3226591 |
| 977 | 外国语学院 | 日语 | 091004 | 徐丹 | 女 | 吉林省集安市人力资源和社会保障局鸭江路3001号 | 134200 | 吉林省集安市人力资源和社会保障局 | | 0435-6229275 |
| 978 | 外国语学院 | 日语 | 091004 | 张嘉 | 女 | 吉林省桦树市人才中心收 桦西大街 | 130400 | 吉林省桦树市社会保险局 | | 0431-83656393 |
| 979 | 外国语学院 | 日语 | 091004 | 吴笛 | 女 | 天津市河西区珠江道华夏津典菜市场门口 | 300000 | 天津华盈海泰科技发展有限公司 | 张生 | 18622393464 |
| 980 | 外国语学院 | 日语 | 091004 | 韩旭 | 女 | 吉林市昌邑区辽北路166号吉林市人才服务中心档案室 | 132000 | 吉林市人才服务中心 | 档案室 | 0432-62507903 |
| 981 | 外国语学院 | 日语 | 091004 | 姜研 | 女 | 吉林省长春市双阳区西双阳大街599号人力资源社会保障局 | 130600 | 吉林省长春市双阳区人力资源社会保障局 | 刘静 | 0431-84222370 |
| 982 | 外国语学院 | 日语 | 091004 | 姜玲 | 女 | 河北省沧州市孟村回族自治县人力资源和社会保障局 | 061400 | 孟村回族自治县人力资源和社会保障局 | 人才市场中心 | 0317-6724305 |
| 983 | 外国语学院 | 日语 | 091004 | 曹琪 | 女 | 哈尔滨市道里区地段街10号 | 150010 | 哈尔滨市人力资源与社会保障局 | 档案室 | 0451-4006660581 |

The second government document lists Huaying Haitai as the co-organizer of a Network Security Attack and Defense competition with the Ministry of Industry and Information Technology's (MIIT) national training entity, NSACE[6]. It was open for all students of Henan Province.

NSACE appears to be a national education body that teaches network information security, including offensive activity [7]. This information is particularly interesting given Boyusec's previous work at CNITSEC's Guangdong subsidiary setting up a joint active defense lab[8]. It suggests that these technology firms act as both shell companies and recruitment grounds for potential MSS use in cyber operations.



2、 目的：

本届网络攻防大赛，由河南中安致远科技有限公司协同各大网络安全公司、网络安全产品供应商举办，面向河南省所有高校学生的科技活动，其主要目的在于增强学生对网络知识的兴趣，激励学生学习网络安全技术的积极性，培养学生的创新意识与团队合作精神，普及信息安全知识，提高学生信息安全意识，为企业选拔、推荐优秀网络安全专业人才，为日益紧缺的网络安全技术人员补充新的生力军。

二、大赛介绍

1.主办单位：中安致远科技有限公司

工业和信息化部 网络安全工程师高级职业教育项目组（NSACE）

天津华盈海泰科技发展有限公司

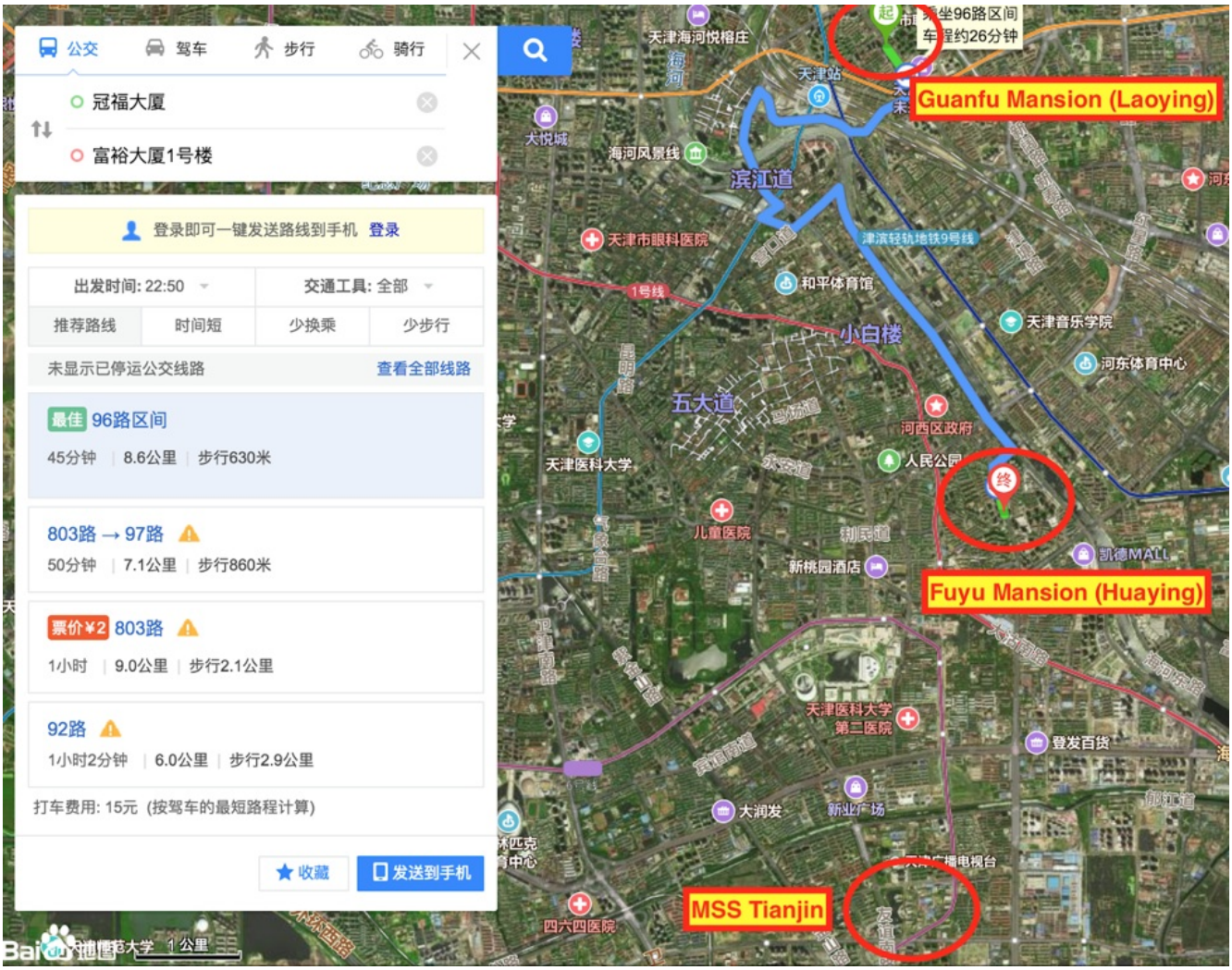
2.协办单位：河南锐之旗信息技术有限公司

3.参赛对象：河南省内所有高校在校学生

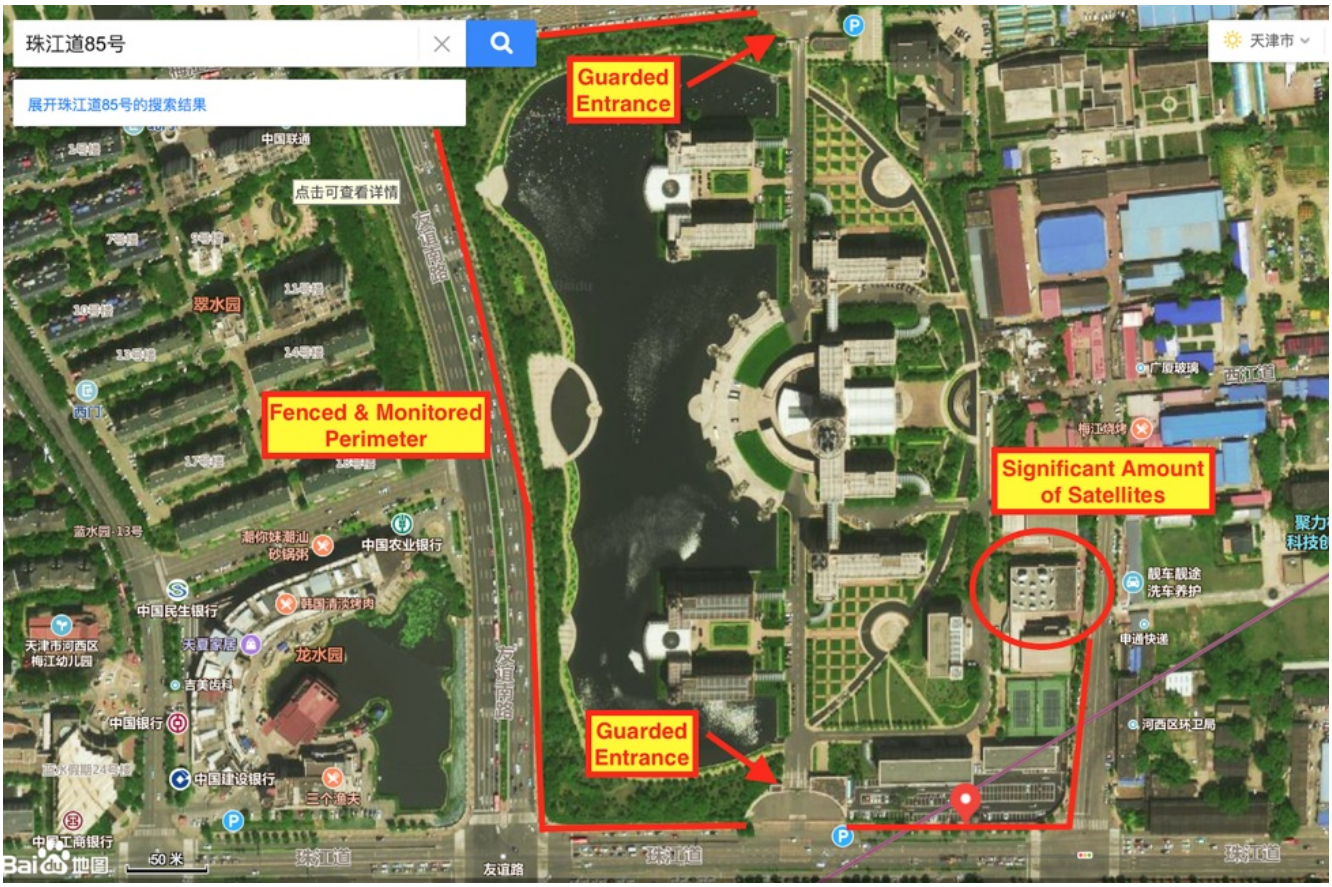
4.比赛时间：2011年12月24日

## MSS Tianjin Bureau

The most recent IntrusionTruth post assesses that GAO's Uber rides frequently took him from Huaying's address at the Fuyu Mansion to 85 Zhujiang Road (**珠江道85号**).



When observed closely, the compound is a striking one complete with towers, a fenced perimeter with surveillance cameras, guarded entrances, and a building with a significant number of satellite dishes.




There are no markers on the building and no government listed address; however, it is apparently difficult for locals to determine where the Tianjin Bureau's location is as well. There are several Baidu questions asking what transportation routes are best to get to that specific address. Three separate ones specifically mention the 85 Zhujiang Road address as the headquarters for the MSS's Tianjin Bureau and the difficulty in finding its location[9] [10] [11].


As with most cyber-enabled operations, satellite arrays are often indicative of installations with significant signals intelligence (SIGINT) capabilities. The Tianjin Bureau appears to have the potential for such capabilities, housing several large arrays that appear to have existed since at least January 2004.

Barely visible satellite dishes from the street view of 85 Zhujiang Road outside the compound

## Conclusion

There are still significant intelligence gaps that prevent Falcon Intelligence from making an assessment about STONE PANDA's potential connections to the MSS Tianjin Bureau with a high degree of confidence. However, additional information is likely to materialize either directly from IntrusionTruth or from other firms in the infosec community who are undoubtedly looking at this material as well and may have unique insight of their own. Ultimately, IntrusionTruth's prior releases on GOTHIC PANDA proved accurate and led to a U.S. Department of Justice indictment resulting in the dismantling of Boyusec. From their latest post, which contains GAO's Uber receipts, it is clear the group's information likely goes beyond merely available OSINT data.

It cannot be ignored that there are striking similarities between the entities associated with GOTHIC PANDA and the actors and firms mentioned in the blogs about STONE PANDA. In addition, FalconIntelligence notes that following the late 2015 Sino-U.S. brief cyber detente, much of the responsibility for western cyber intrusion operations was handed to the MSS as the PLA underwent an extensive reform that is still currently underway, and which is consolidating its military cyber forces under the Strategic Support Force.

Though the detente saw an initial drop in Chinese intrusion activity, it has steadily been increasing over the past several years, with a majority of the intrusions into western firms being conducted by suspected contractors. These adversaries are tracked by CrowdStrike as GOTHIC PANDA, STONE PANDA, WICKED PANDA, JUDGMENT PANDA, and KRYPTONITE PANDA. Many of these adversaries have begun targeting supply chain and upstream providers to establish a potential platform for future operations and enable the collection of larger sets of data.

While the APT1, PUTTER PANDA, and Operation CameraShy reports all exposed PLA units at a time when Chinese military hacking against western firms was rampant, the attention has now swung toward identifying MSS contractors. The exposure of STONE PANDA as an MSS contractor would be another blow to China's current cyber operations given STONE PANDA's prolific targeting of a variety of sectors, and may prompt an additional U.S. investigation at a tenuous time for Sino-U.S. relations during an ongoing trade war. However, it is important to note that such public revelations often force these actors to cease operations, improve their operational security (OPSEC), and then return stronger than before. As such, CrowdStrike Falcon Intelligence assesses that although Boyusec may have shuttered, elements of GOTHIC PANDA are likely to still be active. The same is likely to be true for STONE PANDA following a period of silence.

The activities of STONE PANDA impact entities in the Aerospace & Defense, Government, Healthcare, Technology, Telecommunications Services of several nations.

*For more information on how to incorporate intelligence on threat actors like STONE PANDA into your security strategy, please visit the Falcon Intelligence product page.*

### Footnotes

1. http://kjbz.mca.gov[.]cn/article/mzbzhzcwj/201106/20110600157934.shtml
2. http://bjgwql[.]com/a/hezuojiaoliu/2011/0422/288.htm
3. http://alumni.ecnu.edu[.]cn/s/328/t/528/3b/02/info80642.htm
4. http://down.51cto[.]com/424761/down/1/
5. http://www.djbh[.]net/webdev/web/LevelTestOrgAction.do?p=nlbdLv3&id=402885cb35d11a540135d168e41e000c
6. http://rjzyjsxy.zzia.edu[.]cn/picture/article/25/27/01/6c8b24a143f9959a85301d4527f0/801f81cf-8f30-4aa4-8428-7f9d4e778e76.doc
7. http://www.yingjiesheng[.]com/job-001-607-536.html
8. https://www.recordedfuture.com/chinese-mss-behind-apt3/
9. https://zhidao.baidu[.]com/question/1046720364336588899.html?fr=iks&word=%CC%EC%BD%F2%CA%D0%D6%E9%BD%AD%B5%C085%BA%C5%CA%C7%CA%B2%C3%B4%B5%A5%CE%BB%C2%EF&ie=gbk
10. https://zhidao.baidu[.]com/question/146035392.html?fr=iks&word=%CC%EC%BD%F2%CA%D0%D6%E9%BD%AD%B5%C085%BA%C5%CA%C7%CA%B2%C3%B4%B5%A5%CE%BB%C2%EF&ie=gbk
11. https://zhidao.baidu[.]com/question/223614321.html?fr=iks&word=%CC%EC%BD%F2%CA%D0%D6%E9%BD%AD%B5%C085%BA%C5%CA%C7%CA%B2%C3%B4%B5%A5%CE%BB%C2%EF&ie=gbk