The Pangu Team—iOS Jailbreak and Vulnerability Research Giant: A Member of i-SOON's Exploit-Sharing Network


nattothoughts.substack.com/p/the-pangu-teamios-jailbreak-and-vulnerability

Share this post


Natto Thoughts

The Pangu Team—iOS Jailbreak and Vulnerability Research Giant: A Member of i-SOON's Exploit-Sharing Network

Copy link

Facebook

Email

Notes

More

This week marks the one-year anniversary of the i-SOON leaks1—files, chat logs, and images exposing the company's eight-year espionage effort targeting at least 20 foreign governments for China's government agencies. Since then, threat intelligence reports, U.S. indictments and sanctions have uncovered additional contractors linked to Chinese state-sponsored operations, such as Integrity Tech (北京永信至诚科技有限公司) and Sichuan Silence (四川无声信息技术), covered by the Natto Team in reports 1, 2, and 3. All these firms appeared in the i-SOON leaks at some point, revealing a tightly connected network of business partners, competitors, clients, and exploit brokers.

Other actors, such as the Pangu Team (盘古团队) (Pangu), were also mentioned in the leaks. Known as one of China's top white-hat hacker groups specializing in mobile system and application security, Pangu has gained global recognition since 2014 for its groundbreaking iOS jailbreaks2—downloaded tens of millions of times—and its performance in hacking competitions like PwnFest and the Tianfu Cup.3

The Pangu Team logo and its flagship product, Jailbreaks—software tools that exploit system vulnerabilities to remove restrictions on Apple devices, allowing users to install unauthorized apps and customize iOS beyond Apple's limitations. Source: hxxps://en.9.pangu[.]io/tv_help_en.html (Note: The Natto Team is not able to verify the legitimacy of the website source or whether the Pangu Team operates the website.)

Previous analyses revealed i-SOON sought Pangu's expertise in designing technical challenges for its flagship event, the Anxun Cup. Further examination of the leaks reveals a more intricate relationship between Pangu and i-SOON, extending beyond informal discussions about hacking contests.

Share

Who is “TB”?

In a previous analysis, the Natto Team highlighted that i-SOON has closer ties to Qi An Xin (奇安信) than to any other company, likely due to Qi An Xin’s 13% stake in i-SOON. A review of two years' worth of chat logs between i-SOON’s CEO, Wu Haibo (aka Shutd0wn), and COO, Chen Cheng (aka lengmo)—spanning August 2020 to August 2022—showed that Qi An Xin was the most frequently mentioned company in their exchanges, appearing 100 times. Further scrutiny has shown that two names dominated discussions related to Qi An Xin:

He Chunlin (何春林/老何), Vice President of Qi An Xin, mentioned 28 times, and **“TB”** or **“Tibi”** (提笔) mentioned 46 times—nearly twenty more times. While He Chunlin was primarily referenced in the context of partnerships, training, and market strategy, TB came up in more technical discussions.

While TB’s full name never appears in the logs, multiple references clarify his affiliation and identity. For instance, in August 2020, i-SOON executives arranged to meet TB at "Pangu, Shanghai." In another exchange, i-SOON’s COO hesitated about drinking with TB, commenting on the lack of women, to which the CEO joked, "The Pangu girls are really no good." Further open-source research revealed TB is the alias of Han Zhengguang (韩争光), the founder and leader of the Pangu Team.

An incomplete group photo of the core members of the Pangu team, from left to right: OGC557 (Li Xiaojun), windknown (Xu Hao), TB (Han Zhengguang), DM (Chen Xiaobo), INT80 (Wang Tielei).

Source: Anquanke

In 2021, The Pangu Lab formally merged with Qi An Xin, forming Qi An Pangu Lab Technology (北京奇安盘古实验室科技有限公司). This merger integrated Pangu's expertise into Qi An Xin's big data, cyberattack and defense research, and anti-fraud operations. Today, Han serves as Vice President of Qi An Xin while remaining head of Pangu Team.

Han Zhengguang (TB) has emerged as Qi An Xin's key point of contact for Shutdown, i-SOON's CEO, reinforcing a long-standing connection that dates back to China's early hacking scene. In the 2000s, both were core members of 0x557, one of China's most influential hacking groups at the time, whose members later played a pivotal role in shaping the country's vulnerability research ecosystem, including Pangu. The i-SOON leaks reveal that their discussions spanned Qi An Xin's investments in i-SOON, training programs, going out for drinks together, as well as vulnerability acquisition, with at least one exchange suggesting TB's potential interest in exploitation.

TB Sought NoSugar Tech's QQ Vulnerability

Zhang Ruidong (张瑞冬), aka "Only_guest" or "onlyguest," founded NoSugar Tech (成都无糖信息技术有限公司) in 2017 after working at Sichuan Silence, a firm sanctioned by the U.S. in late 2024 for compromising tens of thousands of firewalls worldwide. While NoSugar Tech claims to be a cybersecurity firm focused on combating online fraud and cybercrime, the i-SOON leaks suggest it was also deeply involved in trading vulnerabilities, acting as a supplier to entities like i-SOON and, potentially, Pangu.

In August 2020, TB expressed interest in acquiring a vulnerability in the QQ4 platform offered for sale by NoSugar Tech. Shutdown, i-SOON's CEO, remarked, "Tibi just asked me about this vulnerability, so I guess they want to use it." Lengmo, i-SOON's COO, responded, "Tell Tibi to ask Zhang Ruidong—he knows him anyway." This implies that the Pangu team head was personally acquainted with NoSugar's "onlyguest."

This chat suggests that TB was not just a passive observer in vulnerability transactions—he was reaching out to Shutdown for intelligence on acquiring vulnerabilities.

Later in the same conversation about the QQ vulnerability, lengmo, i-SOON's COO, describes how a member of their team recently discovered a vulnerability in a gambling customer service system. They also successfully used a phishing method to compromise customer service systems. He boasted, "The [phishing method] success rate is quite high—we've successfully done this several times lately." He also noted that i-SOON excelled at phishing, prompting Shutdown to take a jab at TB: "Tibi's team is always just copying other people's methods." By criticizing TB's team for a lack of originality, this statement strongly suggests that they, too, engage in compromise operations through phishing.

"Tibi's team" likely refers to the Pangu team. While Pangu is today part of Qi An Xin, raising the possibility that the reference points to another team within the company, the merger was not finalized until 2021—one year after these chat logs. More importantly, Pangu has continued to operate under its own branding as Qi'an Pangu, with TB as its CEO.

Phishing for "Spinach"

The discussion around the QQ vulnerability implies a domestic use case. QQ's user base is primarily in China, limiting its viability for targeting foreign entities. Instead, it is far more likely to be used for operations against domestic targets. The likely motive: cybercrime investigations. NoSugar Tech, the seller of the QQ vulnerability, specializes in fighting cybercrime, and has collaborated with China's Ministry of Public Security (MPS) on cybercrime enforcement since its founding in 2017.

In the chat logs, lengmo suggests that the QQ vulnerability for sale by NoSugar Tech may not be useful to i-SOON, to which Shutdown responded: "He [TB] and Zhao Jinlong think this vulnerability is highly valuable." Zhao Jinlong (赵晋龙) is the Director of Qi An Xin's Cybercrime Research Center (奇安信集团涉网犯罪研究中心), which oversees cybercrime

intelligence, security research, and supports China's law enforcement operations. Shutdown then added: "They [TB and Zhao] used this before, mainly to target customer service computers in 'spinach' operations."[The Chinese words for "gambling" (博彩, bócǎi) and "spinach" (菠菜, bōcài) are homophones.5] Shortly after the conversation, lengmo also mentioned targeting a gambling platform, as highlighted in the previous section.

These leaked conversations, dated August 2020, coincided with China's crackdown on illicit online gambling that year. In 2020, the MPS launched a nationwide operation to dismantle these activities, resulting by December 2020 in the shutdown of over 2,260 gambling platforms, 980 illegal technical teams, 1,160 gambling promotion platforms, and 1,960 underground banking and illegal payment networks, leading to more than 3,500 cases solved and over 75,000 arrests, according to China News Service (CNS). In 2021, Amendment 11 to the Criminal Law further tightened enforcement measures by officially criminalizing cross-border gambling.

The interest in the QQ vulnerability likely stems from the QQ platform's longstanding role in facilitating illicit online gambling activities. As early as 2007, The Wall Street Journal reported that Tencent's QQ Coins, a form of online play money, were being used to circumvent gambling restrictions, and since then, QQ has remained a key platform for large-scale underground transactions. In 2021, law enforcement operations uncovered a major QQ-based gambling network with over 5 million yuan (approx. US $700,000) in transactions.

The extent of TB and Zhao Jinlong's collaboration in this context is unclear, but the appearance of their names together likely indicates close pre-merger cooperation to tackle cybercrime—an effort that continues today. At the 2024 "New Cybercrime Investigation and Combating Seminar" hosted by Jiangsu Police Institute (江苏警官学院) and organized by Qi An Xin, Li Rongze (李榕泽), head of Qi An Pangu's Offensive and Defensive Expert Department (奇安盘古攻防专家部负责人), detailed how the team investigates and combats cybercrime. He used **gambling cases** as an example and explained the process of tracking criminal activity, from deploying **phishing links** to conducting target infiltration and **gathering intelligence on suspects**.

Li Rongze (李榕泽), head of Qi An Pangu's Offensive and Defensive Expert Department at the 2024 New Cybercrime Investigation and Combating Seminar. Source: Qi An Xin

Pangu's Place in China's Exploit Flow

Following the 2021 edition of the Tianfu Cup (天府杯),6 i-SOON's leaders discussed their expectations for receiving proof-of-concept (POC) for exploiting vulnerabilities from the event. Their conversation pointed to a structured system: vulnerabilities found at the competition are first collected by the Ministry of Public Security (MPS), then assigned to specific provincial and local MPS offices, and finally passed to contractors who carry out offensive tasks. A similar process is likely in place for vulnerabilities submitted to the Ministry of State Security (MSS).

On October 26, 2021, i-SOON's Shutdown and lengmo discussed the usability of vulnerabilities provided to the MPS by Tianfu Cup contestants. Lengmo explains his understanding of how provincial and local departments [of the MPS] use vulnerabilities in general,7 and speculates that the vulnerabilities provided to the MPS by hacking competition contestants are "probably just half-finished products." Shutdown agrees, adding that he explicitly asked TB about this, who confirmed that only a POC [proof of concept] is available. Shutdown then notes the difficulty of converting POCs for vulnerabilities in Apple's iOS mobile phone operating system into fully weaponized exploits. This suggests he was

possibly specifically interested in obtaining the vulnerabilities exploited by the Pangu Team at the 2021 Tianfu Cup. That year, Pangu successfully executed a remote jailbreak of an iPhone 13 Pro running iOS 15 using a single-click exploit embedded in a specially crafted link, winning the competition's highest single reward of USD $300,000.

Qi An Pangu achieved second place at the 2021 Tianfu Cup. Source: HACKREAD

i-SOON's CEO's attempt to access the iOS vulnerabilities or POC, and TB's likely proximity to them as Pangu's leader, suggests that despite their close contact and business ties, TB was seemingly unable to provide the highly sought-after vulnerability to his friend and business partner (whether freely or for a price). If accurate, this reinforces the institutionalized distribution process whereby the MPS (and MSS) acts as the central gatekeeper, controlling access to high-value vulnerabilities exploited at hacking contests, and determining their allocation to different actors, such as private contractors.

Within this vulnerability distribution system, companies like i-SOON, Integrity Tech, and Sichuan Silence serve distinct roles from Pangu. Despite variations in their structures—differing employee backgrounds and core business areas—these firms share similar operational models. To survive and thrive, they adapt by restructuring, diversifying services, and collaborating—sharing tools, expertise, and sometimes even personnel. Unlike these firms, Pangu focuses heavily on vulnerability research and takes on a more strategic position, setting it apart in fundamental ways.

Pangu's Strategic Role in China's Cyber Ecosystem

As part of Qi An Xin, Pangu belongs to an exclusive group of state-backed or quasi-state-owned cybersecurity firms, alongside 360 Group (数字安全集团), Venustech (启明星辰), NSFocus (绿盟科技), and TopSec (天融信). Qi An Xin is one of China's largest cybersecurity companies, supplying products and services to over 90% of China's central government departments, state-owned enterprises, and major banks. It is deeply integrated with Chinese intelligence and military services and operates its own Cybersecurity Military-Civil Fusion Innovation Center. Additionally, it is a known top-tier vulnerability supplier to the MSS.

Within this structure, Pangu is a premier vulnerability research entity, renowned for its iOS jailbreaks, successes at PwnFest and the Tianfu Cup, and contributions to Apple's bug bounty program. Since 2015, Pangu has hosted MOSEC in Shanghai, an event dedicated to advancing mobile security research and facilitating knowledge exchange among security professionals.

In 2022, Pangu, like parent company Qi An Xin, expanded its efforts to include cyber threat intelligence supporting China's information operations accusing Western countries of offensive cyber activity. That year, Pangu released a report exposing a decade-old exploit linked to the Telescreen (Bvp47) backdoor, which they attributed to Equation, a hacking group tied to the U.S. National Security Agency (NSA). In an interview with China's state-run Global Times, Pangu leader Han (TB) detailed the backdoor's technical complexity, reach, and scope. In 2023, Pangu Lab claimed to have identified six members of the "Against The West" hacking group, alleging that they were connected to or sponsored by Western nation-states, though it provided no evidence to support these claims.

Cover of Qi An Pangu's 2022 Bvp47 report. Source: Pangu Lab

Elite Vulnerability Researchers vs. Frontline Exploiters

Findings from ETH Zurich's Center for Security Studies (CSS) report "From Vegas to Chengdu" **broadly** categorized Chinese hackers into two groups:

1. **Elite vulnerability researchers** – These hackers, often Pwn2Own and Tianfu Cup winners, are linked to Level 1 Technical Support Units (TSUs), which supply the most vulnerabilities to China's Ministry of State Security (MSS). They refine their skills through global competitions and bug bounty programs, primarily targeting Western systems. While their research bolsters China's cyber capabilities, direct links to state-sponsored operations against foreign targets are rare.

2. **Government-contracted hackers** – These hackers focus on operational tasks for state-sponsored operations rather than original vulnerability research on Western products. Exposed by Intrusion Truth and U.S. indictments, they typically do not compete in high-profile exploit contests or contribute significantly to bug bounty programs.

The Pangu Team fits squarely into the first category. Nonetheless, the chat logs analyzed in this article reveal the intricate and often fluid relationships within China's cyber ecosystem, which operates less in strict silos and more as interconnected, tight-knit networks. This article revealed three key aspects of the Pangu leader's relationship with i-SOON and his broader role within China's cyber ecosystem:

- TB's close ties with i-SOON's CEO, rooted in their shared background as patriotic hackers and his role as Qi An Xin's primary liaison;
- TB's interest in acquiring vulnerabilities and alleged involvement in compromise operations—likely in support of cybercrime enforcement efforts—operating within the same exploit network as cyberespionage-linked i-SOON;
- Further reinforcement that high-value vulnerabilities—such as those showcased at events like the Tianfu Cup—likely flow first to government agencies under China's centralized vulnerability distribution system before reaching contractors.

Thanks for reading Natto Thoughts! Your paid subscription supports access for all and serves as a token of appreciation for the efforts of the Natto Team. We encourage you to subscribe and share Natto Thoughts with others who can benefit from our insights.

1
Natto Thoughts analysis of the i-SOON leaks can be found here, here and here.

2
Pangu's jailbreaking was quite impressive due to the substantial complexities built into the operating system. iOS security is essentially stratified into three layers: the application layer, the system layer, and the kernel layer, each having progressively greater permissions. To execute a successful jailbreak, one must attain kernel permissions, which in turn necessitates overcoming all the other security layers. Jailbreaks thus require the exploitation of numerous vulnerabilities that work in concert to reach the kernel.

3
More details on the Pangu Team's organizational structure and performance in prominent hacking contests can be found in the CSS/ETH Cyberdefense Report "From Vegas to Chengdu" (section 6).

4
QQ is a Chinese instant messaging platform developed by Tencent, offering chat, gaming, and social networking features. While it was once widely used, its relevance has declined, having been largely overshadowed by Weixin (its overseas version is called WeChat).

5

While 赌博 (dǔbó), or 博彩 (bócǎi) which is mainly used in Taiwan, is the general term for gambling in Chinese, **菠菜 (bōcài)**—which literally translates to “spinach,” is a Chinese homophone of 博彩 (bócǎi) and appears to be used as slang for gambling in hacker and underground communities.

6
The Tianfu Cup is one of China’s premier exploit hacking competitions, comparable to Pwn2Own. It rewards participants for uncovering vulnerabilities in widely used software and hardware products. Established in November 2018, the event is held in Chengdu, Sichuan province.

7
Winnona Bernsen’s analysis of the i-SOON leaks identified three key findings regarding the vulnerability pipeline to government agencies enabled by the Tianfu Cup. First, the Chinese Ministry of Public Security (MPS) gains access to exploits discovered by private companies during the competition. Second, when Tianfu Cup submissions do not include full exploit chains, the MPS distributes proof-of-concept vulnerabilities to private firms like i-SOON, which further develop them into working exploits. Third, provincial MPS departments collaborate with city and prefecture-level authorities to target their intended systems. Separately, Harfang Lab’s analysis concluded that leaked discussions around the Tianfu Cup suggest an institutional process in which vulnerabilities discovered during the event are collected by the MPS, distributed to individual provinces for their cyber operations, and eventually passed down to contractors who conduct some operations on behalf of these provinces. For further insights into the relationship between contractors and MPS offices at the national, provincial, and local levels, see Natto Thoughts analyses 1, 2, and 3.

No posts