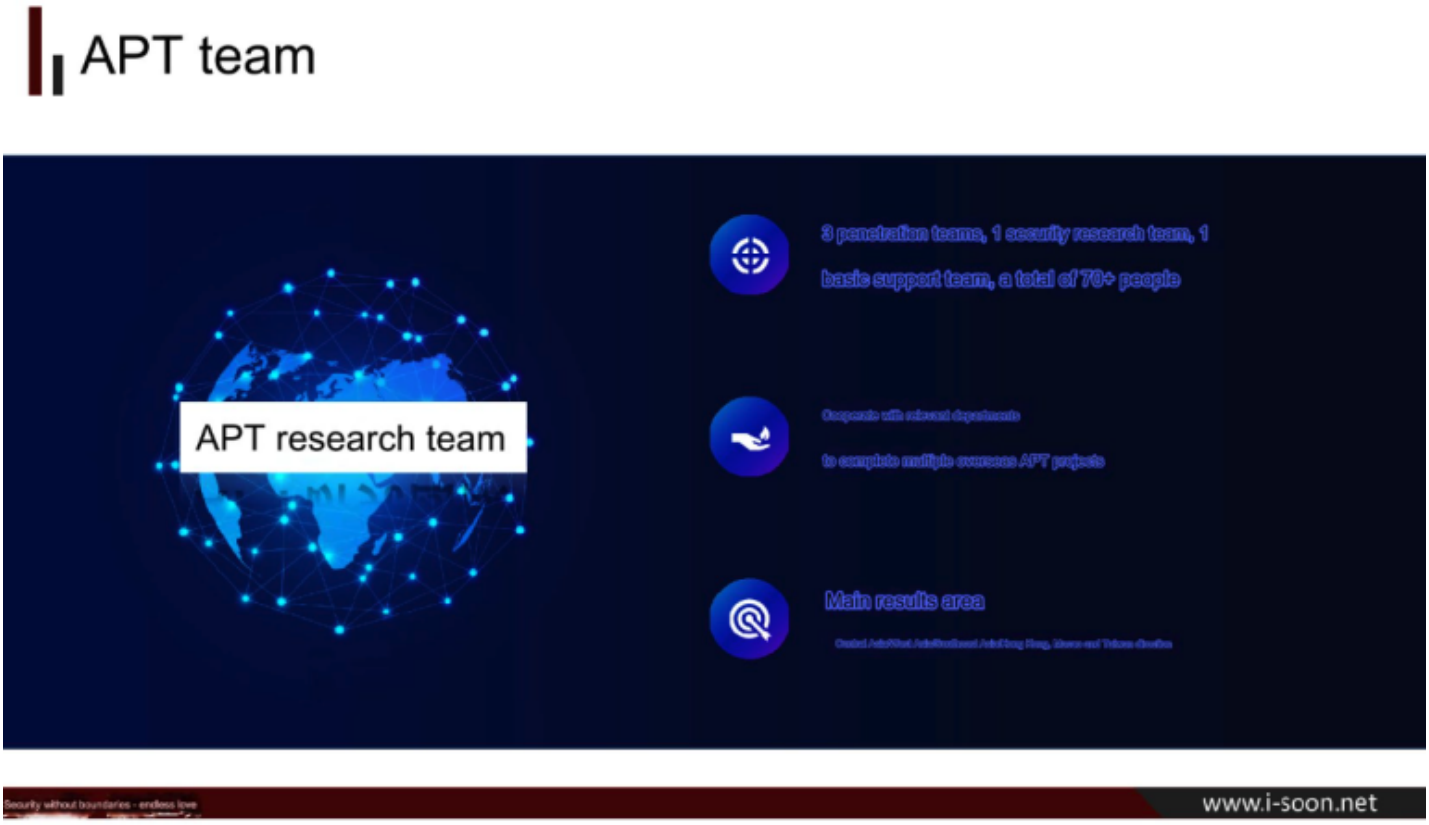
New Leak Shows Business Side of China's APT Menace

A new data leak that appears to have come from one of China's top private cybersecurity firms provides a rare glimpse into the commercial side of China's many state-sponsored hacking groups. Experts say the leak illustrates how Chinese government agencies increasingly are contracting out foreign espionage campaigns to the nation's burgeoning and highly competitive cybersecurity industry.



A marketing slide deck promoting i-SOON's Advanced Persistent Threat (APT) capabilities.

A large cache of more than 500 documents published to GitHub last week indicate the records come from **i-SOON**, a technology company headquartered in Shanghai that is perhaps best known for providing cybersecurity training courses throughout China. But the leaked documents, which include candid employee chat conversations and images, show a less public side of i-SOON, one that frequently initiates and sustains cyberespionage campaigns commissioned by various Chinese government agencies.

The leaked documents suggest i-SOON employees were responsible for a raft of cyber intrusions over many years, infiltrating government systems in the United Kingdom and countries throughout Asia. Although the cache does not include raw data stolen from cyber espionage targets, it features numerous documents listing the level of access gained and the types of data exposed in each intrusion.

Security experts who reviewed the leaked data say they believe the information is legitimate, and that i-SOON works closely with China's Ministry of Public Security and the military. In 2021, the Sichuan provincial

government named i-SOON as one of “the top 30 information security companies.”

“The leak provides some of the most concrete details seen publicly to date, revealing the maturing nature of China’s cyber espionage ecosystem,” said **Dakota Cary**, a China-focused consultant at the security firm **SentinelOne**. “It shows explicitly how government targeting requirements drive a competitive marketplace of independent contractor hackers-for-hire.”

Mei Danowski is a former intelligence analyst and China expert who now writes about her research in a Substack publication called Natto Thoughts. Danowski said i-SOON has achieved the highest secrecy classification that a non-state-owned company can receive, which qualifies the company to conduct classified research and development related to state security.

i-SOON’s “business services” webpage states that the company’s offerings include public security, anti-fraud, blockchain forensics, enterprise security solutions, and training. Danowski said that in 2013, i-SOON established a department for research on developing new APT network penetration methods.

APT stands for Advanced Persistent Threat, a term that generally refers to state-sponsored hacking groups. Indeed, among the documents apparently leaked from i-SOON is a sales pitch slide boldly highlighting the hacking prowess of the company’s “APT research team” (see screenshot above).

i-SOON CEO Wu Haibo, in 2011. Image: nattothoughts.substack.com.

The leaked documents included a lengthy chat conversation between the company’s founders, who repeatedly discuss flagging sales and the need to secure more employees and government contracts. Danowski said the CEO of i-SOON, **Wu Haibo** (“Shutdown” in the leaked chats) is a well-known first-generation red hacker or “Honker,” and an early member of Green Army — the very first Chinese hacktivist group founded in 1997. Mr. Haibo has not yet responded to a request for comment.

In October 2023, Danowski detailed how i-SOON became embroiled in a software development contract dispute when it was sued by a competing Chinese cybersecurity company called **Chengdu 404**. In September 2021, the **U.S. Department of Justice** unsealed indictments against multiple Chengdu 404 employees,

charging that the company was a facade that hid more than a decade's worth of cyber intrusions attributed to a threat actor group known as "APT 41."

Danowski said the existence of this legal dispute suggests that Chengdu 404 and i-SOON have or at one time had a business relationship, and that one company likely served as a subcontractor to the other.

"From what they chat about we can see this is a very competitive industry, where companies in this space are constantly poaching each others' employees and tools," Danowski said. "The infosec industry is always trying to distinguish [the work] of one APT group from another. But that's getting harder to do."

It remains unclear if i-SOON's work has earned it a unique APT designation. But **Will Thomas**, a cyber threat intelligence researcher at Equinix, found an Internet address in the leaked data that corresponds to a domain flagged in a 2019 Citizen Lab report about one-click mobile phone exploits that were being used to target groups in Tibet. The 2019 report referred to the threat actor behind those attacks as an APT group called **Poison Carp.**

Several images and chat records in the data leak suggest i-SOON's clients periodically gave the company a list of targets they wanted to infiltrate, but sometimes employees confused the instructions. One screenshot shows a conversation in which an employee tells his boss they've just hacked one of the universities on their latest list, only to be told that the victim in question was not actually listed as a desired target.

The leaked chats show i-SOON continuously tried to recruit new talent by hosting a series of hacking competitions across China. It also performed charity work, and sought to engage employees and sustain morale with various team-building events.

However, the chats include multiple conversations between employees commiserating over long hours and low pay. The overall tone of the discussions indicates employee morale was quite low and that the workplace environment was fairly toxic. In several of the conversations, i-SOON employees openly discuss with their bosses how much money they just lost gambling online with their mobile phones while at work.

Danowski believes the i-SOON data was probably leaked by one of those disgruntled employees.

"This was released the first working day after the Chinese New Year," Danowski said. "Definitely whoever did this planned it, because you can't get all this information all at once."

SentinelOne's Cary said he came to the same conclusion, noting that the Protonmail account tied to the GitHub profile that published the records was registered a month before the leak, on January 15, 2024.

China's much vaunted Great Firewall not only lets the government control and limit what citizens can access online, but this distributed spying apparatus allows authorities to block data on Chinese citizens and companies from ever leaving the country.

As a result, China enjoys a remarkable information asymmetry vis-a-vis virtually all other industrialized nations. Which is why this apparent data leak from i-SOON is such a rare find for Western security researchers.

"I was so excited to see this," Cary said. "Every day I hope for data leaks coming out of China."

That information asymmetry is at the heart of the Chinese government's cyberwarfare goals, according to a 2023 analysis by **Margin Research** performed on behalf of the **Defense Advanced Research Projects Agency** (DARPA).

“In the area of cyberwarfare, the western governments see cyberspace as a ‘fifth domain’ of warfare,” the Margin study observed. “The Chinese, however, look at cyberspace in the broader context of information space. The ultimate objective is, not ‘control’ of cyberspace, but control of information, a vision that dominates China’s cyber operations.”

The National Cybersecurity Strategy issued by the White House last year singles out China as the biggest cyber threat to U.S. interests. While the United States government does contract certain aspects of its cyber operations to companies in the private sector, it does not follow China’s example in promoting the wholesale theft of state and corporate secrets for the commercial benefit of its own private industries.

Dave Aitel, a co-author of the Margin Research report and former computer scientist at the **U.S. National Security Agency**, said it’s nice to see that Chinese cybersecurity firms have to deal with all of the same contracting headaches facing U.S. companies seeking work with the federal government.

“This leak just shows there’s layers of contractors all the way down,” Aitel said. “It’s pretty fun to see the Chinese version of it.”