Bundesamt für Verfassungsschutz

Cologne, 08 August 2024

BfV CYBER INSIGHT

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 2: Connections of i-Soon to the Chinese security apparatus

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 2: Connections of i-Soon to the Chinese security apparatus

Table of Contents

1. Introduction

On February 16th 2024 a data set was leaked on the GitHub[1] developer platform that provides a rare insight into China's methods of conducting hacking operations worldwide. The internal documents show the extent of cooperation between the Chinese cybersecurity company i-Soon and the Chinese government and intelligence services. In four consecutive reports BfV examines the leak in detail and describes the level of industrialization of cyber espionage activities by privately organized companies, who carry out cyber-attacks for state entities.

The leak includes over 570 files, images, and chat messages in Chinese, including:

- a presentation on the skills and services of i-Soon,
- lists of employees, product information/services, contract books and information on cyber operations and target entities,
- screenshots of presumably captured data and
- log files of compromised telecommunications service providers in Asia.

The leaked documents do not contain any indication of affected entities in Germany, however, the analysis offers an insight into the inner workings of private hacker companies and providers of malicious software and their close ties to the Chinese state. It also lays bare how APT[2] groups operate and how government agencies leverage them.[3]

The BfV's evaluation of the leaked data is presented in a total of four reports, which are structured as follows:

- Organization and methods of i-Soon APT units (part 1),
- **Connections of i-Soon to the Chinese security apparatus (part 2, this report),**
- Affected countries and specific targets of i-Soon (part 3),

1 GitHub is an online software development and version management service for software projects.

2 Advanced Persistent Threats (APT) denotes complex and targeted threats that target one or a specific group of victims. They are usually comprised of resource-intensive, government-controlled cyber-attacker groups. The attacks themselves are often elaborately prepared by the attackers, are sophisticated ("advanced") and can continue over a long period of time ("persistent").

3 For illustration purposes, various screenshots from the leak were translated and included in this report.

- Offered products and i-Soon customers (part 4).

Following part 1 (organization and methods of i-Soon APT groups), part 2 is dedicated to the connections of i-Soon to the Chinese security apparatus.

2. i-Soon's involvement in national vulnerability mining

The leaked files contain a company presentation on the capabilities and services of i-Soon and shows its ties to the Chinese state apparatus. For example, the company advertises its participation in national vulnerability mining[4] and in this context also contributes to the "China National Vulnerability Database" (CNNVD).

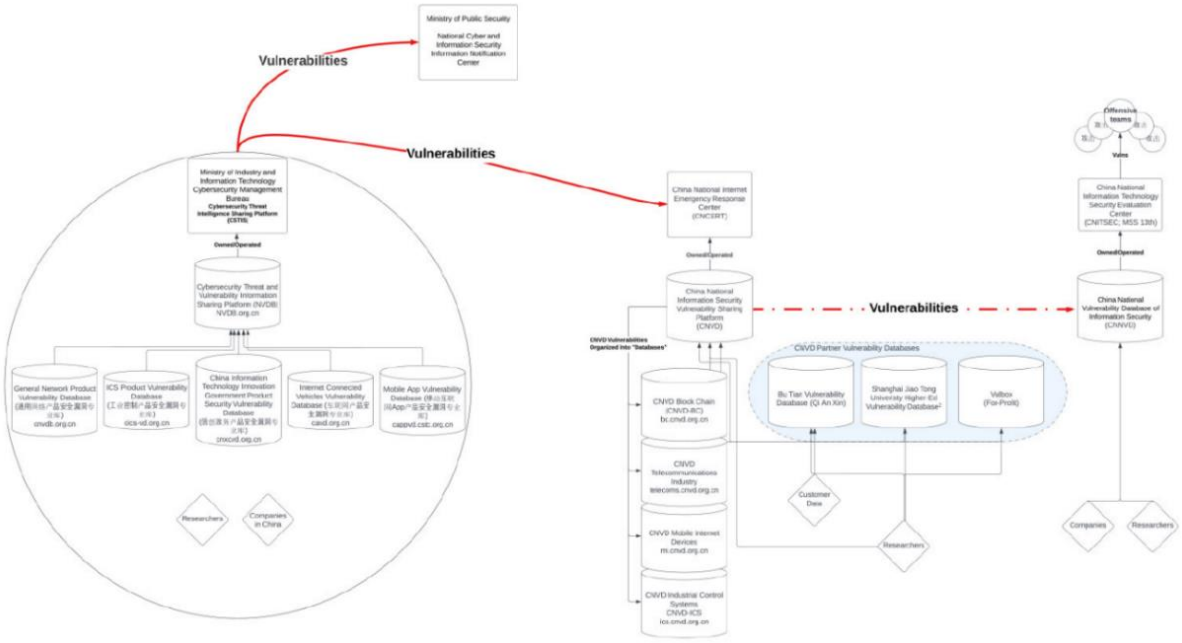

Figure 1: vulnerability mining[5]

In July 2021 the Chinese government introduced binding regulations and structures to institutionalize vulnerability mining. This ensures a wide-ranging collection of information by government agencies. All companies operating in China are legally obliged to report identified vulnerabilities within 48 hours via specified reporting channels. The

4 Vulnerability mining refers to the (targeted) collection and availability of vulnerabilities in software and similar products.

5 Representation from Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Source: CNNVD Handbook)

information is merged into various databases, to which all relevant agencies of the Chinese security apparatus have access (see Figure 1). It is strictly prohibited to otherwise disclose the security vulnerability.

The CNNVD database is operated by the China National Information Technology Security Evaluation Center (CNITSEC)[6] and the information is made available to (offensive) cyber actors.

Companies such as i-Soon need to apply to become a technical supporter of CNNVD. After qualifying, candidates are then assigned to one of three levels – depending on size and skills (see Figure 2).

CNNVD Initial Application Requirements for Businesses Applying to be Technical Support Units

Category	Level 1	Level 2	Level 3
Responsbility for Security Services, Vulnerability Capability Team	The company's main business segment is information/cyber security. The business also maintains software vulnerability discovery and analysis capabilities, as well as incident response capabilities.		
	The vulnerability analysis and discovery team exceeds 20 people. The team's work is prolific.	The vulnerability analysis and discovery team exceeds 10 people. The team's work is good.	The vulnerability analysis and discovery team exceeds 5 people. The team's work is acceptable.
Technical Capabilities	The business has scientific research, engineering capabilities, and services related to cybersecurity.		
Submission of Novel Vulnerabilities	The company submits at least 20 "common" (通用型) novel vulnerabilities, from which at least 3 are considered "critical risk."	The company submits at least 15 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 3 "common" (通用型) novel vulnerabilities.
Vulnerability Early Warning Support	The business provides no fewer than 5 *critical* alerts.	The business provides no fewer than 5 alerts.	The business provides no fewer than 3 alerts.

Figure 2: application criteria for companies wanting to join CNNVD[7]

6 The China Information Technical Security Evaluation Center (CNITSEC) was founded in 1997 and is according to its own statements an integral part of China's information security system. In particular, these are the analysis of software monitoring units and the evaluation, assessment and certification of software code, products related to IT security and actors in the Chinese cyber space.

7 Representation from Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Source: CNNVD Handbook)

The partnership levels differ based on the number and quality of vulnerabilities submitted. Level 1 denotes the premium level.

If an enterprise was successful in its application in accordance with the above criteria, annual follow-up criteria must be met (see Figure 3).

CNNVD Annual Requirements for Technical Support Units

Category	Level 1	Level 2	Level 3
Data Coordination	Information submitted to the annual CNNVD Work Report is accurate and complete.		
Business Coordination	Coordination with the CNNVD is smooth and the business's attitude is energetic. There has never been an instance when the business point of contact is inaccessible or when an email has gone unanswered for too long.		
Annual Submission of Novel Vulnerabilities	The company submits at least 35 "common" (通用型) novel vulnerabilities, from which at least 5 are considered "critical risk."	The company submits at least 25 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 5 "common" (通用型) novel vulnerabilities.
Annual Vulnerability Early Warning Support	The business provides new fewer than 10 *critical* alerts.	The business provides no fewer than 10 alerts.	The business provides no fewer than 5 alerts.
Other Support	Enthusiatically respond to CNNVD requests related to vulnerability technology evaluation and judgement, technical seminars, data anaylsis support, and special event-based vulnerability support.		

Figure 3: annual requirements for CNNVD support units[8]

According to the company presentation in the leak, i-Soon is noted as a level 3 partner and must therefore supply at least five new “ordinary” (i.e. non-critical) vulnerabilities each year as well as fulfill all other overarching requirements. These include requests from CNNVD to participating corporations such as i-Soon that the company's technical support units must realize. Requests cover the full range of vulnerabilities evaluation

8 Representation from Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities (Source: CNNVD Handbook)

and assessment, technical seminars and data analysis, and specific event-based support in the context of vulnerability exploitation.[9]

3. i-Soon's training institute and certifications

i-Soon provides services for cyber operations and also trains people itself for their implementation at the so-called Anxun College. The leaked materials show that more than 3.000 students are trained at Anxun College each year. Participants include students from other institutions, members of other companies, state institutions or public security institutions. The college was established in line with the state's requirement to improve cybersecurity capabilities. The teaching program includes offline material for self-study, remote teaching, personalized lessons and participation in organized competitions. These competitions are an important source of young talent for i-Soon but the data also shows that other competitions are scouted to acquire new employees. Additionally, the company presentation shows that i-Soon also promotes numerous certifications (see Figure 4).

Figure 4: certifications specified by i-Soon

- Level-2 certificate for classified information for weapons and equipment (meaning digital services/products) and research and development units,
- Level-1 qualification for National Information Security Services,
- National qualification for information security services with the ability to handle information security emergencies at level 3,

9 see Atlantic Council (2023): Sleight of hand: How China weaponizes software vulnerabilities.

- Level-3 certification for National Information Security Services by CNITSEC,
- Technical partnership with CNNVD Level-3 (see chapter 2),
- Registration as a professional training center for information security for attack and defense.

These certifications allow the execution of classified assignments or cooperation formats such as the provision of certain software products or the execution of special hacking operations and thus form the (certified) basis for a cooperation with government agencies.

4. Personnel links to the Chinese state and the national hacking scene

A leaked list of “employees for confidential content” also indicates links between i-Soon and the Chinese state apparatus (see Figure 5). In addition to the names of employees, it also provides an insight into the structure of the individual workspaces of the company. Confidential information is therefore dealt with in the following divisions:

- information management,
- sales and pre-sales,
- technical services,
- safety evaluation,
- administration,
- confidentiality office,
- finance,
- security division,
- human resources,
- software development and
- operation and maintenance.

List of confidential personnel

Name	gender	nationality	Birthplace	Confidential positions	Position	Classification level	political status	major
[redacted]	male	Chinese	Yancheng	Legal Person/General Manager/Team Leader	Legal Person/General Manager/Team Leader	important	the masses	Electronic information engineering
[redacted]	male	Chinese	Huangyan, Zhejiang	Confidentiality Director Fu Team Leader	Confidentiality Director Fu Team Leader	important	the masses	Calculation software technology and application
[redacted]	male	Chinese	Guang'an, Sichuan	Classified Computer Security Auditor	Head of Information Management Department	important	member	Calculation technology
[redacted]	male	Chinese	Ji'an, Jiangxi	Pre-sales engineer	Pre-sales engineer	generally	the masses	Logistics management
[redacted]	male	Chinese	Xingtai, Hebei	Director of Technical Services Department	Director of Technical Services Department and Manager of Government and Enterprise Division	generally	the masses	Calculation technology
[redacted]	male	Chinese	Dazhou, Sichuan	Safety evaluation engineer	Safety evaluation engineer	generally	party member	network engineering
[redacted]	female	Chinese	Zigong, Sichuan	Director of Confidentiality Office	Administration Manager and Director of the Confidentiality Office	important	the masses	international trade
[redacted]	female	Chinese	Chongqing Rongchang	Sales Assistant	Sales Assistant	important	member	English
[redacted]	female	Chinese	Chengdu, Sichuan	finance professional	finance professional	generally	the masses	Accounting
[redacted]	male	Chinese	Chengdu, Sichuan	Security Division Director	Security Division Director	generally	the masses	computer information management
[redacted]	female	Chinese	Chengdu, Sichuan	Human Resources Manager	human resources manager	generally	party member	e-commerce
[redacted]	female	Chinese	Chengdu, Sichuan	Confidentiality Administrator	Confidentiality Administrator	important	the masses	Tourism management
[redacted]	male	Chinese	Mianyang, Sichuan	Software Development Manager	Software Development Manager	important	member	/
[redacted]	male	Chinese	Chengdu, Sichuan	Software Development Engineer	Software Development Engineer	generally	the masses	Multimedia design and production
[redacted]	male	Chinese	Neijiang, Sichuan	Classified Computer Security Administrator	Operation and Maintenance Engineer	important	member	Mechanical equipment Co., Ltd., manufacturing and automation

Figure 5: list of "confidential personnel"[10]

The list also indicates that contacts or families "overseas" must be reported and retained by the company. For the staff listed, this column is uniformly blank, which could indicate that contacts or families overseas are an exclusion criterion for employees working in the confidential area of the company. The list also includes information if a person is a member of the Chinese Communist Party (CCP) and which classification level they have within the company.

In addition, the analysis of the text files contained in the data leak provides extensive information on connections between competing cybersecurity companies. For instance, next to the alias "shutd0wn" of the i-Soon founder, other names appear in chat logs that show overlaps with otherwise well-known APT groups or former members of the patriotic hacking scene. Many of these former members have set up similar cybersecurity companies that provide services to Chinese services.

5. "Limitless" supply in a competitive market

The i-Soon data leak provides important insights into the complex structure and reach of China's cyber ecosystem. Information gained from the i-Soon-leaks is likely to be

10 Illustration shortened; in addition, names were blacked out.

transferable to other companies operating within a thriving industry. The analysis reveals how professional and complex the system works but also shows an industry built on competition. i-Soon advertises its capabilities on the company's homepage with the slogan "security is limitless". The successful application of i-Soon for participating in the CNNVD and the pursuit of other certifications/quality seals demonstrate a strong commitment in gaining a strategic advantage over competing companies.

Government agencies in China benefit from an industry that has developed its own dynamics and operates in accordance to market economy principles. State entities can pick and choose from a range of competing companies offering diverse services and technical expertise in a growing economic sector.

Customers or clients of cyber products and services, such as those offered by i-Soon, no longer have to recruit specialized personnel independently or invest large amounts in product development. Also, they do not have to consider operational security aspects themselves. This outsourcing in cyberspace leads to an increased professionalization of state controlled cyber campaigns and in particular makes it more difficult for cyber defense agencies to trace specific actors. The attribution of individual cyber operations within this highly complex system is increasingly challenging.

After exposing the organization and methods of i-Soon APT units (part 1) and showing i-Soon's links to the Chinese security apparatus (part 2), the further course of reporting on the i-Soon-leaks will focus on known targets and attack vectors of i-Soon's APT-like units (part 3) and report on clients and products of i-Soon (part 4).

Publication information

Published by
Bundesamt für Verfassungsschutz
Abteilung 4
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 792-2600

Image credits
cover: BfV, ai-generated

Date of Information
July 2024