Bundesamt für Verfassungsschutz

Cologne, 01 August 2024

BfV CYBER INSIGHT

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 1: Organization and methods of i-Soon APT units

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 1: Organization and methods of i-Soon APT units

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, this report),**
- Connections of i-Soon to the Chinese security apparatus (part 2),
- Affected countries and specific targets of i-Soon (part 3),
- Offered products and i-Soon customers (part 4).

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.

2. The company

According to media reports, i-Soon was founded in 2010 and is headquartered in Shanghai. It has offices in 32 other provinces, cities and autonomous regions in China.[4] The description on the company‘s homepage portrays i-Soon as a cyber security company, that is tasked with defending cyber-attacks against the Chinese government and ensuring the security of customer networks. The company founder is reportedly a former member of the Green Corps – a part of China's “patriotic” hacker scene. Over the years, members of the scene have formed a comprehensive network of cybersecurity firms that also work on behalf of Chinese security services and government institutions.

3. Organization and methods

The data sets uploaded to GitHub include a presentation on i-Soon's capabilities and services. This gives a rare insight into the organization itself and the relationship with the cybersecurity company's customer base. Among other things, the presentation promotes company-organised APT units, which are capable of carrying out several simultaneous cyber campaigns overseas for their clients. Accordingly, the teams supposedly consist of more than 70 people, organized in three groups: a “security research team”, three “penetration teams” and a “basic support team" (see Figure 1).

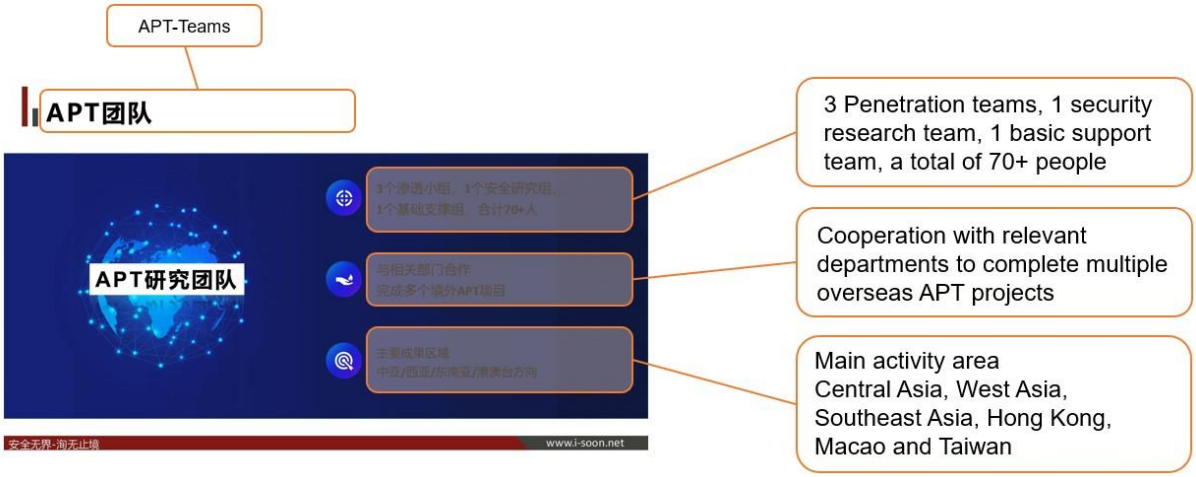

Figure 1: i-Soon APT-teams

4 Cf. "Ist das Chinas Snowden-Moment?“ of 23.02.2024, in: www .spiegel.de; last visited on 28.06.2024.

The terms chosen point towards a highly specialized and professional process for carrying out cyber-attacks. The “security research team” is probably tasked with reconnaissance work beforehand. The three “penetration teams” can then use this information for a targeted approach. The teams are prepared to infiltrate the security systems of their selected targets and to carry out previously defined objectives and exfiltrate desired information. The "basic support team" presumably deals with all other technical issues that occur during an operation.

In addition to organizational demarcations, i-Soon categorizes the capabilities of its APT unit into three service areas:

- “target penetration services”,
- “battle support services” and
- “intelligence services”.

Possible targets of the “target penetration services” are listed as networks of government organizations and authorities, including their intranet networks. Also, the procurement of file server permissions and login information of overseas government personnel (see Figure 2) is mentioned. In addition to the government sector, i-Soon also advertises “processing” the telecommunications sector as well as energy, transportation and medical networks (some of which are critical infrastructure).

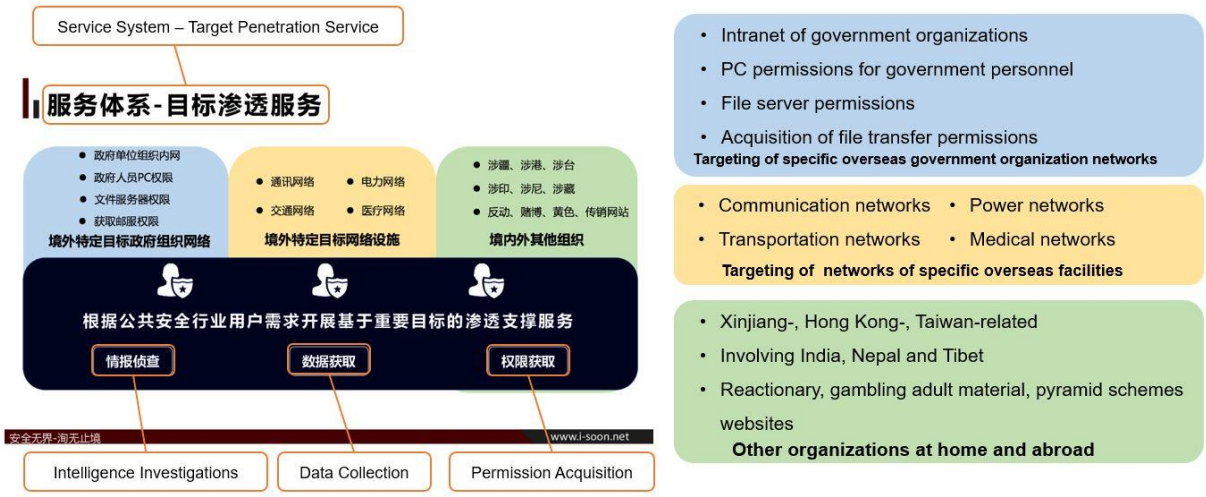

Figure 2: services on offer

The services offered by i-Soon coincide with the alleged interests of state-controlled Chinese cyber-actors. These include gaining access to information on foreign, security and economic policy through the intrusion of networks of governmental organizations.

In addition to the listed services, the published data also provides details on how i-Soon internally prepares hacking campaigns (see Figure 3):

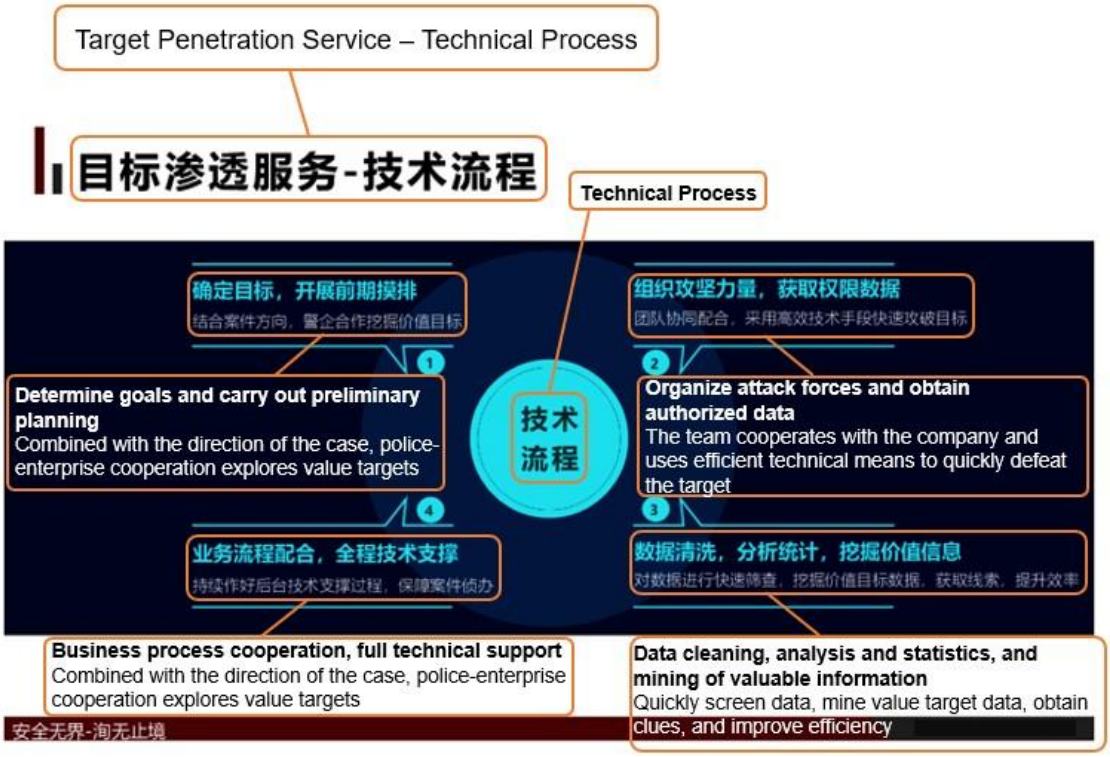

Figure 3: process of a i-Soon hacking campaign (technical process)

- The first step describes the target selection and the definition of goals based on customer specifications. If the targets are of high-quality and well-secured, i-Soon will provide its clients with necessary insider knowledge, for example the targets' IT security standards. Based on the information and possible attack vectors identified, i-Soon will then prepare a preliminary deployment plan.
- In the second step, i-Soon assembles the APT teams in a demand-oriented manner. The toolset is then chosen or specifically developed. This dynamic and demand-oriented approach suggests that i-Soon is capable of developing and combining different techniques, tactics and procedures (TTPs) in order to achieve maximum efficiency.

- The third step takes place in the target systems themselves: the outlined data is acquired and, if necessary, further useful information is identified.
- The fourth step comprises of backend support for the client. This may include further technical assistance as well as other unspecified support in regard to the further case handling.

The described methods are confirmed by the lists of products and services, contract books, cyber operations and target entities contained in the leaked data. Among other things, these lists include client-set targets (cf. Figure 4), toolsets offered by i-Soon, the status of respective cyber operations as well as information on the company's target achievements.

Figure 4: contractual provisions

4. i-Soon and the Chinese cyber ecosystem

By evaluating the text files contained in the leaked data, further insight into the functioning of the company can be gained. The chat protocols provide a glimpse of i-Soon's business-oriented participation in Chinas highly professional cyber ecosystem.[5] They show that i-Soon not only acts on behalf of its cooperation partners, but that the company conducts cyber operations on its own initiative or at least goes beyond contractually agreed guidelines by gathering further data within an ongoing cyber-operation –

5 Cyber ecosystem describes the involvement of various sectors in state-based cyber espionage activities. These include entities in education and research, services and product development, which support Chinese intelligence services with their respective portfolio. Cooperation can take place either on a voluntary basis or can be enforced in accordance with existing statutory regulations.

presumably in order to later sell the surplus information to other clients for profit. The transcripts contain, among other things, a conversation about information generated by i-Soon concerning the NATO Secretary General. Clients were offered an excerpt of data for purchase, but they signaled disinterest.

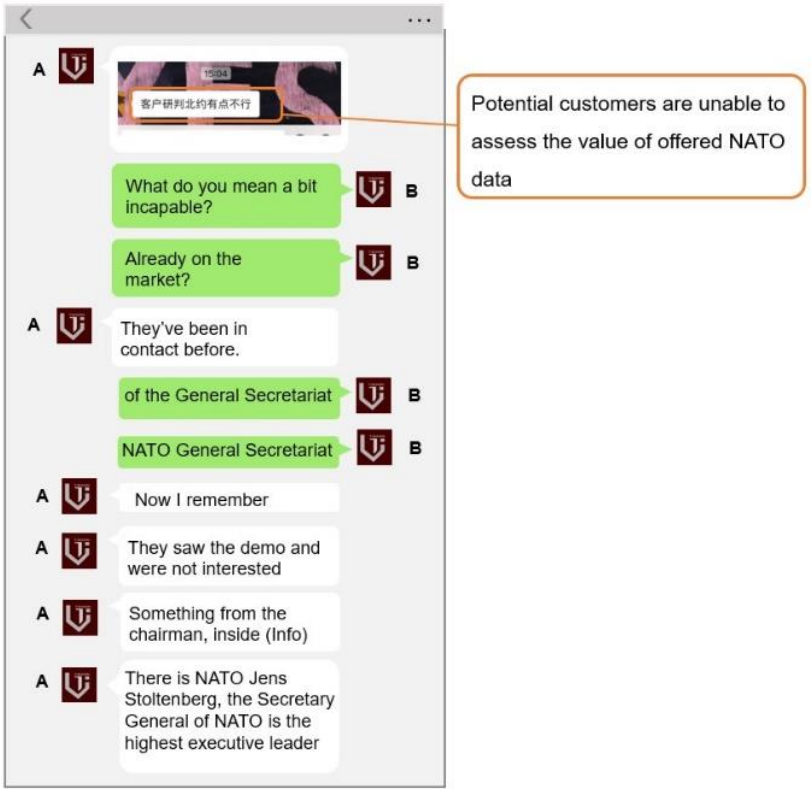

Figure 5: chat dealing with allegedly stolen NATO data

Furthermore, i-Soon seems involved in the procurement of login data on the black market, presumably to execute client contracts with the acquired information. One concrete example refers to a discussion about the increased cost for access data to computer networks of the Federal Bureau of Investigation (FBI).

Figure 6: chat concerning FBI credentials

On the basis of the evaluated chat protocols, a highly contested cyber market is pictured: the wages of the employees are low and stagnant, the business competition is described as intense and it is difficult to find a market for exploited data. Also, there are problems finding qualified staff. Attempts are made to attract young talent through the cooperation with local universities as well as through appearances and participation in Chinese cybersecurity competitions.

5. Insight into the Chinese cyber landscape

In their entirety, the leaked data provides a unique insight into the complex structure and scale of China's cyber ecosystem. Although i-Soon is only a single, medium-sized company within an established and flourishing industry in China, it is still able to conduct numerous operations simultaneously with its APT units. In this regard, the technical level of the outfit and to what extent the industry as a whole operates can only be assumed. Companies, like i-Soon, partly maintain numerous other subcontractors, which in turn are specialized in specific fields of work such as software development, hardware development, infrastructure deployment, malware development and APT services.

However, what the i-Soon-leaks also show is an unregulated market, in which individual actors can apparently act without control. One first measure taken by the Chinese government in response to the data leak was to extend the current legal statutes: now data concerning government contracts is classified as a state secret.

In the further course of reporting on the i-Soon-leaks, BfV examines the links to the Chinese security apparatus (part 2), reports on known targets and attack vectors of the APT-like units of i-Soon (part 3) and focusses 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