Cologne, 22 August 2024

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 4: Offered products and i-Soon customers

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 4: Offered products and i-Soon customers

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]

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.

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),
- Affected countries and specific targets of i-Soon (part 3),
- **Offered products and i-Soon customers (part 4, this report).**

Following part 1 (organization and methods of i-Soon APT groups), part 2 (connections of i-Soon to the Chinese security apparatus) and part 3 (affected countries and specific targets of i-Soon), part 4 takes a closer look at products offered by i-Soon and potential customers.

2. Product lists

The i-Soon data leak includes information on:

- individual products and product versions,
- sales units,
- prices and
- comments with further information on the products offered by i-Soon (see Figure 1).

The products offered are divided into three categories: "Public Safety", "Blockchain Security" and "Enterprise Security". The majority of the products are listed in the category "Public Safety". In total, there are 22 products included – each priced on the basis of their expected service life, order quantity or priced as a bundle. The tools listed include analysis tools, obfuscation tools[4], and penetration testing tools[5]

4 Obfuscation tools are intended to hide the origin, direction and nature of an operation and thus are used by attackers to increase operational safety. They include tools for the anonymization of networks.

5 Penetration tests (or pentests) are authorized security tests of individual computers or networks that simulate a cyberattack. They involve the use of hacking tools and methods to penetrate a system in order to identify weaknesses and evaluate security measures.

for different operating systems and software manufacturers, sandbox systems[6] and monitoring software.

Figure 1: excerpt of a product list

For some of the listed tools there are user manuals or product descriptions. Products can either be commissioned individually, bought in sets or purchased as a one-year user license. Prices range from ¥ 30.000 to ¥ 800.000 (approx. € 3.500 to € 103.000).

A closer inspection of the tools provides an overview of i-Soon's capabilities but also sheds light on the perspective customer-base and those in the market for products and services of i-Soon. Some of the products in the "Public Safety" section are briefly presented below.

6 Sandbox systems are isolated (virtual) machines, which are used to run potentially unsafe software without causing damage.

2.1 Integrated Combat Platform

The “Integrated Combat Platform” is a software solution for cyber operations comprised of an internal and an external part. The internal part is used for administrative purposes, the external part is composed of offensive cyber tools (see Figures 2 and 3).

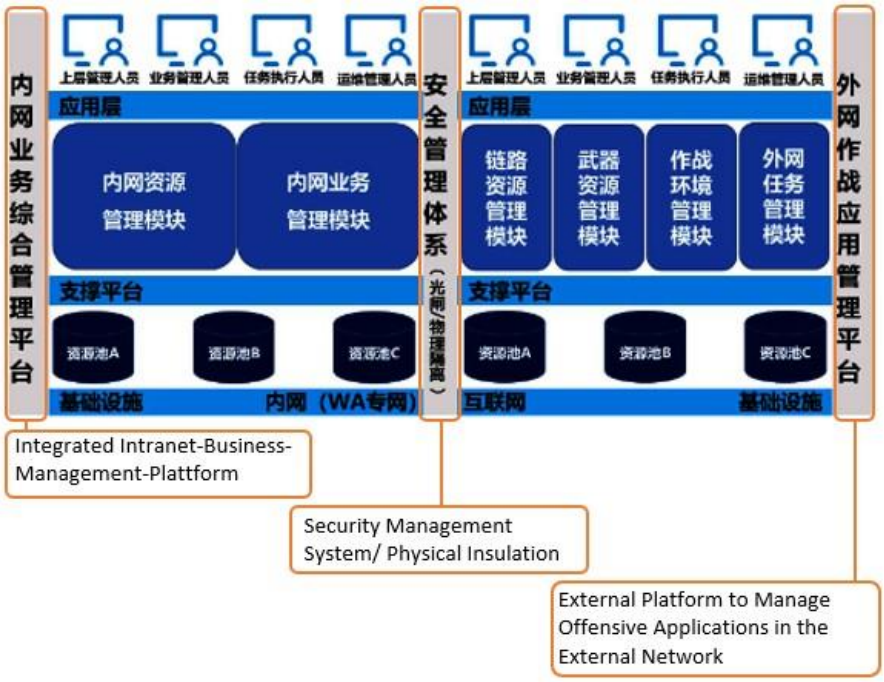


Figure 2: the “Integrated Combat Platform” (part 1)

Associated documents in the leak describe the software’s basic system architecture as well as its functions. Software features include usage management, maintenance and customization, testing environments, VPS[7] account management capabilities and external account management capabilities. Users are able to configure the applications according to their needs. The software is specifically designed to perform operations whilst hiding the user – providing a level of operational security. Furthermore, the software has a kill switch to automatically and irrevocably destroy itself. The “Integrated Combat Platform” enables large-scale cyber operations through its process optimization, resource distribution and planning and control capabilities.

7 A virtual private server (VPS) is a server that hosts all software and data necessary to run an application or web page. The term virtual points to the fact that only a portion of a server's underlying physical resources is used.

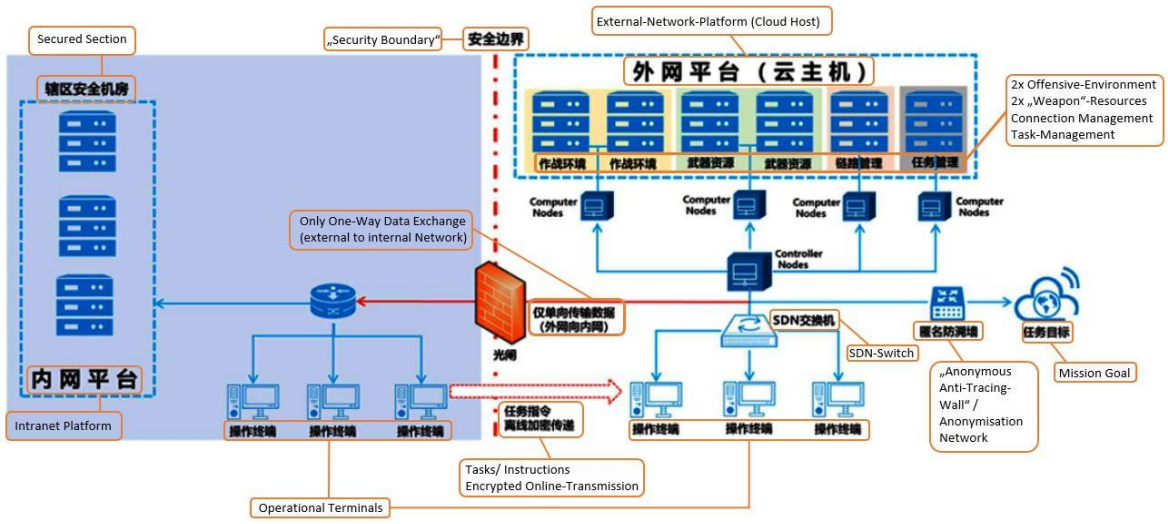


Figure 3: the "Integrated Combat Platform" (part 2)

2.2 Automated Penetration Testing Platform

The "Automated Penetration Testing Platform" is a modular and therefore versatile system. Basically, the product makes it possible to tailor skills precisely to a specific goal. If during a cyber operation certain functions are required, users can easily add missing functions to their toolset. Due to a high degree of automation, technically not-so savvy users should also be able to operate the platform (see Figure 4).

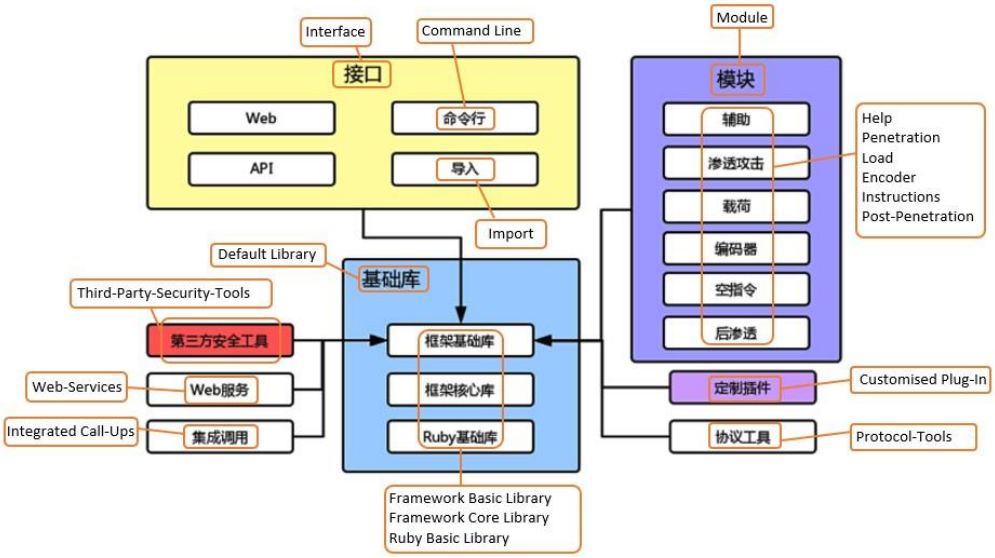
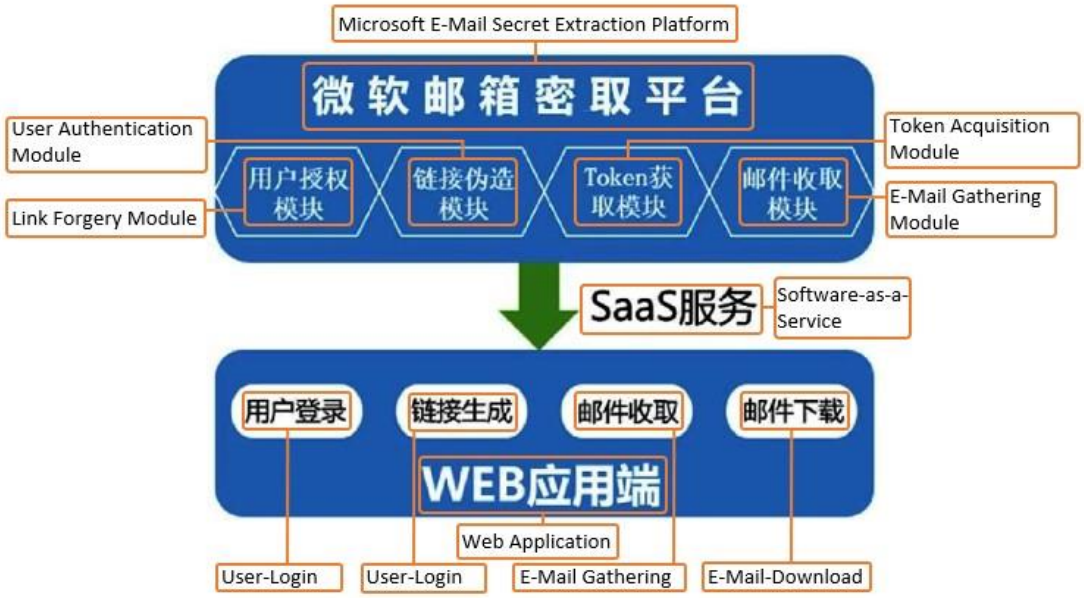


Figure 4

Penetration tests can be used against a large number of systems. The software in question is probably a dual-use tool: a product that can be used for legitimate as well as malicious purposes. The platform can almost certainly also be used as a tool for offensive cyber operations.

2.3 Microsoft Email Encryption Platform

The “Microsoft Email Encryption Platform” is advertised as being capable of compromising Microsoft email mailboxes and exfiltrating data. It is supposedly also capable of circumventing two-factor authentication and gaining access to accounts



without the victims’ knowledge (see Figure 5).

Figure 5: overview of the Microsoft Email Encryption Platform

The platform generates a phishing link that is sent to a victim. After clicking the link, the attacker automatically gains access to the person's Microsoft Outlook account. The documents state that the platform can be used by authorities to combat crime. In principle, however, there seems to be no restriction on the use of the tool, so that it can presumably also be used for offensive cyber operations.

2.4 Email Analysis Intelligence Decision Making Platform

The “Email Analysis Intelligence Decision Making Platform” is an advanced system to extract contents of email accounts and for the analysis of large data amounts. The tool is designed to automatically scan email attachments and create user relationship models based on email communication (see Figure 6).

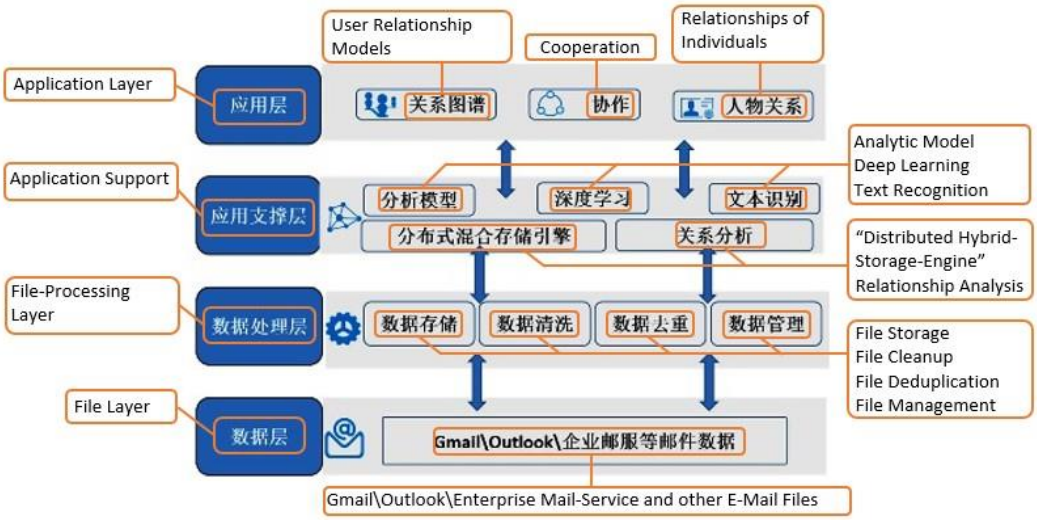


Figure 6: overview of the “Email Analysis Intelligence Decision Making Platform”

2.5 Anonymous Anti-Tracing Wall

The “Anonymous Anti-Tracing Wall” is an anonymization service with the added function of accessing the dark web.

The software provides four different modules: one for access to the internet, one for anonymization functions, one for connecting to other systems and one for accessing the dark web. The modules are offered as a package and sold under a usage license of at least one year. Next to the conventional access to the internet, the package enables the anonymization of activities similar to the TOR[8] browser

8 TOR is a network for anonymizing connection data that protects its users from the analysis of data traffic. Virtual Private Network (VPN) services also allow anonymous communication on the Internet. The TOR network conducts data via random servers provided by volunteers, while a VPN conducts data via a single server selected by the user.

or other VPN services. The user can freely choose between TOR or VPN-like methods for obfuscation purposes (see Figure 7).

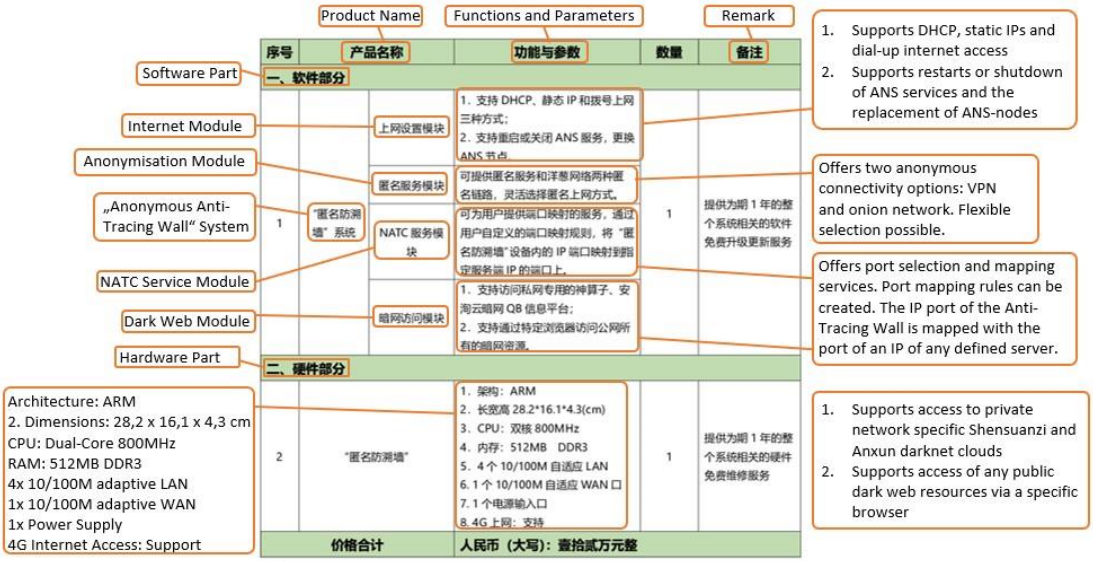


Figure 7: the “Anonymous Anti-Tracing Wall”

2.6 Individual (Soldier) Toolbox

The “Individual (Soldier) Toolbox” is a penetration testing solution that is distributed on a powerful laptop as a mobile tool (see Figure 8).

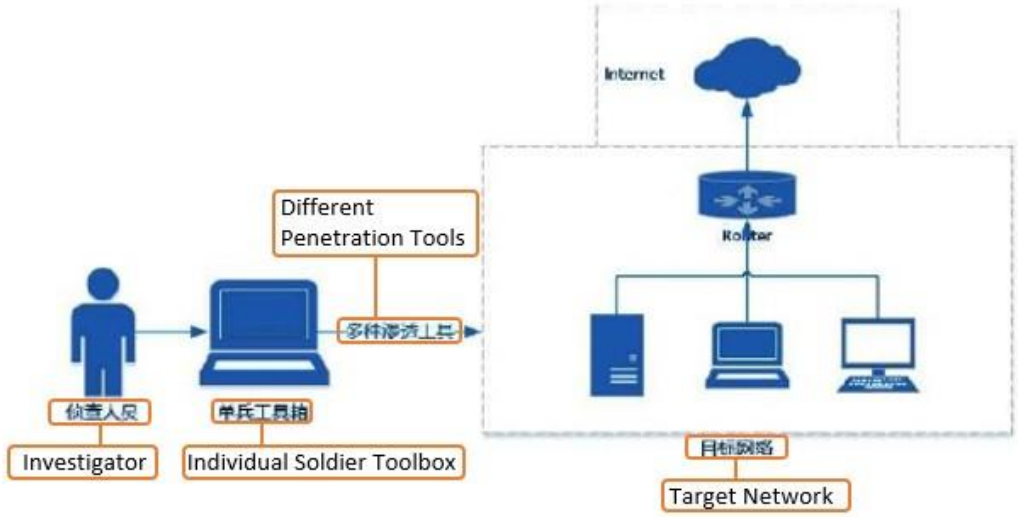


Figure 8: the “Individual (Soldier) Toolbox”

Many of the functions are generally used for penetration testing, but are also suitable for malicious activities. Some functions go beyond the general understanding

of what penetration testing tools should be capable of, which suggest a malicious purpose of the product. For example, the toolbox also has functions to capture and modify data packets, incorporates web shells for remote access and includes functions to actively exploit vulnerabilities.

2.7 Integrated Training Platform

The “Integrated Training Platform” is a tool to process large amounts of data. The platform can classify data efficiently, store it in a structured manner and make it more searchable (see Figure 9). With the tool, users are able to quickly find desired information.

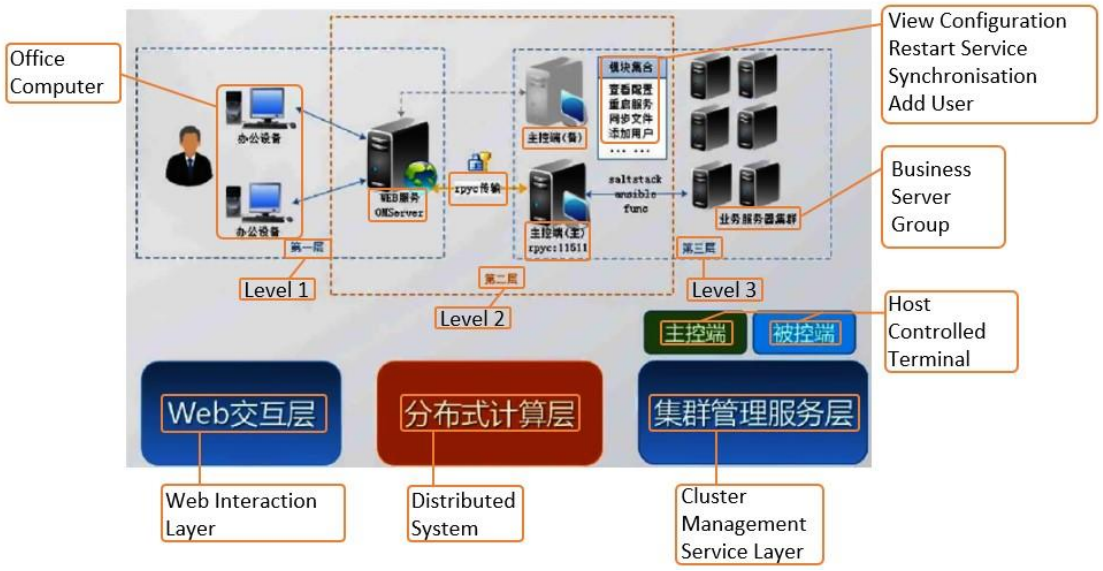


Figure 9: the “Integrated Training Platform”

The somewhat misleading name “training platform” is not supported by the description included in the leak. The documentation shows the primary function of processing large amounts of personal data. The product seems geared towards cybersecurity companies, whose day-to-day work consists of carrying out offensive and defensive cyber operations and follow-up analyses.

3. Contract books

The leaked data also contains information on i-Soon's contract books. With this, the target groups of the products and services offered by i-Soon can be traced. The company groups its consumer base into four categories:

- Public Security / **公安** (probably the Ministry of Public Security (MPS)[9] / **公安部**),
- Safety **安全** (probably the Ministry of State Security (MSS)[10] / **安全部**),
- Military (probably the People's Liberation Army of the PRC (PLA)),
- Enterprise (other private companies, often similar to i-Soon).

The contract books also hold information on contract titles and partners, end users, the date of contract fulfillment, purchase price and a brief summary of contractual obligations and services. The information supports the publicly known mode of operation, whereby the MSS – with the involvement of so-called contract hackers – carries out cyber operations against targets worldwide and sometimes uses anonymization networks for this purpose. This background helps to understand the contract titles listed in the data leak, for example:

- **"Network Technology Service Contract"** (a contract for technical network services, noted in the contract book as the acquisition of various email accounts),
- **"Technical Cooperation Agreement"** (probably means a hacking consignment),
- **"Overseas Data Inquiry"** (probably referring to cyber operations overseas),
- **"Data Purchase Contract"** (the acquisition of specific target data) and
- **"Anti-Tracing Sales Contract"** (anonymization networks for the concealment of cyber operations).

9 The MPS is responsible for public and political security in China. It is the superior authority of the police and also performs tasks in the field of counter-espionage.

10 Civil Intelligence and Secret Police. Responsible for foreign espionage, anti-espionage and political security.

4. Wide assortment of potent cyber tools and services

The evaluation of product lists and product manuals in the i-Soon-leaks shows the far-reaching arsenal of potent cyber tools of one single company. The products are catered towards bodies tasked with public safety and clearly aimed at security authorities in China. With the products and services on offer it is possible to carry out widespread cyber operations against foreign targets and governments.

The examples show i-Soon's continued efforts to consolidate or expand its market position. In order to be competitive and to be awarded government contracts, companies such as i-Soon are forced to constantly improve their products and price them competitively. The result is potential clients, such as government agencies, who profit from cheap tailor-made cyber tools.

An assessment of the product descriptions shows modularly designed hacking tools that can be variably combined with one another. In addition, they offer user interfaces that make the tools easily accessible and usable even for untrained users. The tools can be efficiently used against selected targets depending on desired objectives. The analysis also shows the danger arising from these tools. The number of affected countries and entities[11] proves that these tools are already being successfully used for worldwide campaigns.

It is apparent that an extensive industrialization of cyber espionage has already taken place in the Chinese cyber ecosystem. Here, a market has developed in which many providers offer their products to the public sector. This has led to government entities gaining access to potent cyber tools and has fostered an ongoing innovation process and steady professionalization of the Chinese cyber market.

The previous reporting on i-Soon exposes the organization and methods of its APT units (part 1), examines the links to the Chinese security apparatus (part 2) and covers affected countries and specific targets of i-Soon (part 3).

11 cf. "The i-Soon-Leaks, part 3: Affected countries and specific targets of i-Soon"

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