

BRNO • 09 DECEMBER 2025  
SITUATIONAL REPORTLEAK OF INTERNAL INFORMATION FROM THE CHINESE  
COMPANY I-S00N (安洵信息), INCLUDING SCREENSHOTS OF  
INTERNAL DOCUMENTS OF A CZECH INSTITUTION

## SUMMARY

- On Monday, 19 February 2024, internal data of the Chinese company I-S00N (安洵信息, An-xūn xin-si), which offered and developed offensive cyber tools for Chinese state authorities, was published. Currently available information points not only to the specifics of these tools but also to a large number of victims against whom they have been used in recent years.
- Among the leaked data, there is also a screenshot of several Czech documents, very likely (75–85%) internal documents belonging to a Czech institution. Other victims include government institutions, telecommunications companies, universities, healthcare facilities, think tanks, or human rights organizations from more than 20 countries, such as the United Kingdom, France, Turkey, and various Asian and African states.
- The cybersecurity community is gradually attributing I-S00N's activities to already known threat actors. I-S00N's operations overlap with several Chinese state-sponsored groups, and there is a real possibility (25–50%) that the company cooperated with multiple actors, with the most prominent connection being with the APT41 group. Analyses conducted before the data leak noted links between I-S00N and actors APT41 and RedHotel, which was at one time even confused with APT41.

**NOTICE:** The information and conclusions contained in this analysis are based on publicly available information and information obtained from NÚKIB's activities at the time of publication. This is a cybersecurity analysis from the perspective of the NÚKIB based on information available to it.

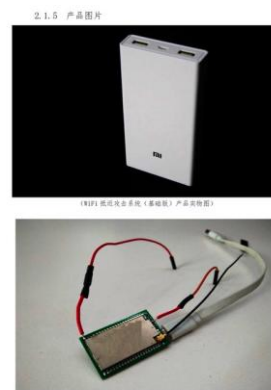
According to leaked information on GitHub, I-S00N developed offensive cyber tools, including hardware for penetration testing, commissioned by Chinese state institutions.<sup>1</sup> Recipients included various local offices of the Chinese Ministry of Public Security (MPS), Ministry of State Security (MSS), and the People's Liberation Army (PLA).<sup>2</sup> It is likely (55–70%) that these tools were also used by other institutions.

THE TOOLS DEVELOPED BY I-S00N WERE  
PRIMARILY INTENDED FOR ESPIONAGE

According to information contained in the leaked documents, the primary source of income for the company I-S00N was renting out offensive cyberattacks aimed at espionage. The company also developed software and hardware for espionage activities, such as various spyware variants capable of collecting sensitive data, remote access tools (RAT), and software for creating phishing emails or malicious

documents. Hardware includes surveillance devices, such as a device disguised as a power bank, intended to compromise Wi-Fi networks, intercept communications, and send them back to attackers (Fig. 1).

Fig. 1: Hardware intended for surveillance purposes



Source: sentinelone.com

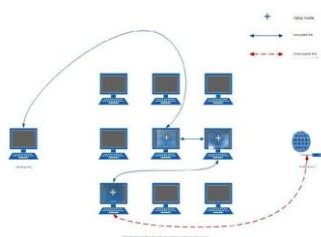
**Marketing documents and product manuals indicate that I-S00N has tools that can be used against Western targets.** This includes a program capable of compromising accounts on the social network X (formerly Twitter), even with multi-factor authentication (MFA), advertised as a tool for monitoring dissidents. The program can be distributed via a forensic link (URL) and, **after gaining access, can collect IP addresses and their locations.**<sup>3</sup>

Another tool is a platform for mass email analysis, allowing the acquisition of incoming and outgoing mail, contacts, and other email data, with automatic translation from any language.<sup>4</sup> **Both tools were used by the MPS.**<sup>5</sup>

I-S00N also developed anonymization devices, primarily for espionage abroad, capable of masking both IP and physical addresses (Fig. 2). There is a growing use of anonymization networks for reconnaissance, exploitation, or C2 (Command and Control) by Chinese APT groups to hinder attribution or detection in victim networks. Some of these tools are shared within centralization efforts, either via “quartermasters” or as commercial services.

Some tools targeted Chinese and other Asian victims, being adapted for local applications like WeChat, Weibo, or Baidu.

**Obr. 2: Sample from the I-S00N company manual illustrating an anonymization network diagram**



Source: github.com

## LEAKED DOCUMENTS INCLUDE FILES FROM A CZECH INSTITUTION

Leaked documents show that I-S00N penetrated networks of organizations in at least 20 countries, including the Czech Republic (Annex 1).<sup>6</sup>

Conversations and screenshots also mention the compromise of NATO and its Secretary General Jens Stoltenberg (Annex 1). However, these claims cannot be independently verified. It is unclear whether the

attackers compromised NATO's network directly or exfiltrated documents related to NATO.

Other targets in the leaked documents include organizations in France, the UK, Turkey, India, South Korea, Thailand, the Philippines, Guinea, and Djibouti.

Non-governmental targets included human rights organizations such as Amnesty International, Human Rights Watch, think tanks like RAND, Chatham House, and the International Institute for Strategic Studies, as well as telecom providers like Roshan (Afghanistan) and Kcell (Kazakhstan), for which I-S00N even developed a piece of software.<sup>7</sup> Leaked documents also contain call detail records and location-based services data stolen from telecom operators' systems. **It is likely (55–70%) that this data was stolen for surveillance, as long-term access would allow precise monitoring of user locations.**<sup>8</sup>

## I-S00N HAS OPENLY COOPERATED WITH GOVERNMENT INSTITUTIONS FOR SEVERAL YEARS, EXEMPLIFYING PUBLIC-PRIVATE PARTNERSHIP IN CHINA

From the information in the leaked materials, clients include Chinese state institutions, especially local MPS offices, MSS, and PLA. **Open sources show that I-S00N has long cooperated with the MPS.** In 2019, I-S00N became a certified supplier of technology, tools, and equipment for the Cybersecurity and Defense Office under the MPS. In 2020, it obtained a second-class secrecy qualification for companies engaged in weapons and equipment research and production, the highest level of secrecy a non-state-owned company can achieve. **I-S00N can thus conduct secret research and development related to state security.**<sup>9</sup>

The company also participated in a crackdown on gambling companies led by the MPS since 2021, cooperating on 1,500 cases with police forces that year.<sup>10</sup> In a series of campaigns targeting the gambling industry, several APT groups operated covertly, the most prominent activity being attributed to APT10, Bronze Starlight, and APT41.

As evident from open sources, I-S00N was also involved in the Belt and Road Initiative, providing big data analysis tools and software and hardware.<sup>11</sup> This matches the selection of victims, which overlaps with the Belt and Road Initiative.<sup>12</sup> There is therefore

a possibility that I-S00N was also involved in espionage within the mentioned initiative.

**The company's CEO, Wu Hai-ba, is close to offensive cyber operations, being part of the first generation of hacktivists.** Under the alias "shutdown," was Wu active in both Honker Union and Green Army, two groups dedicated to patriotic hacking.<sup>13</sup> Under the nickname "shutd0wn," Wu appears in leaked document conversations. **In 2013, I-S00N established a department for researching penetration methods used by APT groups.** The company also collaborates with universities and organizes its own hacking competition, the Anxun Bei (I-S00N Cup), very likely (75–85%) serving as a talent recruitment tool.

#### Box 1: Public-Private Partnership

A characteristic of the Chinese hacker ecosystem is the partnership between the private and public sectors, where state institutions cooperate with companies. Cyber espionage activities are state-directed, but aspects may be carried out by private company employees. This is due to financial motivation and a legislative environment requiring companies and individuals to participate in intelligence activities, as well as the fact that all significant companies in China have ties to the Communist Party, either through personnel or institutional party cells.

### I-S00N WAS ALSO INVOLVED IN ESPIONAGE CONCERNING DOMESTIC ISSUES OF THE PRC, PRIMARILY RELATED TO THE INTEGRATION OF TAIWAN, HONG KONG, OR ETHNIC MINORITIES

Leaked documents describe the situation in Hong Kong in 2022, such as the arrest of Cardinal Joseph Zen, a critic of Beijing, and documents about John Lee, then incoming city administrator. Hong Kong universities were also targeted.

In the case of Taiwan, one of the objectives was to obtain a database containing maps of the Taiwanese road network and 3D models of buildings in all cities.<sup>14</sup> **This data represents a significant source of information necessary for planning an invasion of the island.**<sup>15</sup>

I-S00N was also involved in monitoring ethnic minorities in PRC. **In 2021, it was shortlisted for a cybersecurity project for the public security office in Aksu, Xinjiang.**<sup>16</sup>

### POSSIBLE CONNECTION BETWEEN I-S00N AND CHINESE ACTOR APT41

Based on leaked documents, cybersecurity researchers are attributing I-S00N's activities to various threat actors. **The most prominent connection is with APT41 and other groups around cluster Winnti (Annex 1).** Shared tools include PlugX, Shadowpad, and Treadstone.<sup>17</sup> There is also likely cooperation with Chengdu 404, which previously worked with APT41 as a contractor. In 2020, three Chengdu 404 employees were indicted by the US Department of Justice for participating in a global cyber offensive campaign attributed to APT41.<sup>18</sup>

**There is a real possibility (25–50%) that these two companies competed for government contracts for cyber espionage.**<sup>19</sup> Evidence of at least commercial competition between Chengdu 404 and I-S00N is their legal dispute over intellectual property related to software development, which took place in 2023.

Attribution to other actors was based on indicators of compromise (IoCs), such as IP addresses present in leaked documents or overlapping campaign targets, with one IP address also linked to APT41 (Annex 2).

Victimology overlaps with the Chinese APT group RedHotel (Earth Lusca), which shares some targets with APT41 but is a separate actor. Common targets include gambling companies, government institutions in East Asian countries, Hong Kong democratic organizations, and educational institutions in Taiwan.

### LEAKED INFORMATION OFFERS UNIQUE INSIGHT INTO CHINESE GOVERNMENT CYBER CONTRACTORS

I-S00N and its state ties were already under scrutiny before the data leak, but the leaked documents provide unique insight into the internal workings of state-linked contractors. **There is a real possibility (25–50%) that contractors conduct their own operations and try to sell stolen documents, including on the black market, very likely (75–85%) for financial gain (Annex 1).**

There is a real possibility (25–50%) that Chinese state institutions will tighten cooperation rules with contractors after this incident, but it is almost certain (90–100%) that they will continue to cooperate with private companies due to the high level of existing cooperation and the benefits of these relationships.

**Other evidence suggests a rather uncoordinated, competitive market for offensive tools and services in China, where clients issue contracts for which contractors compete.** Contractors, however, may also collaborate with each other, and there is a real possibility (25–50%) that they cooperate on a single project. It is also highly likely (75–85%) that contractors routinely hire external resources, both in the form of companies and individuals.<sup>20</sup>

**The diversity of victims indicates that the historical targeting of threat actors working with contractors may not always be relevant for deducing future targets.**<sup>21</sup>

## ANNEX 1: SCREENSHOTS AND LEAKED CONVERSATIONS

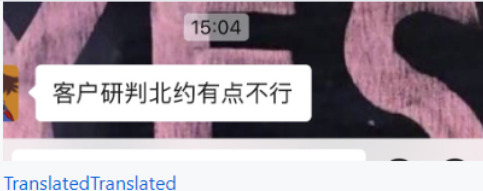
Screenshots referencing the compromise of documents related to NATO.

2022-07-06 03:16:48	wxid_jcnxegjccqi441	wxid_7p054rmzkhqf21	Did you give me the wrong one yesterday? The customer saw that it was all in English, like NATO or something like that
2022-07-06 03:17:12< /td>	wxid_7p054rmzkhqf21	wxid_jcnxegjccqi441	Indeed, there was a mistake, it was NATO yesterday

```

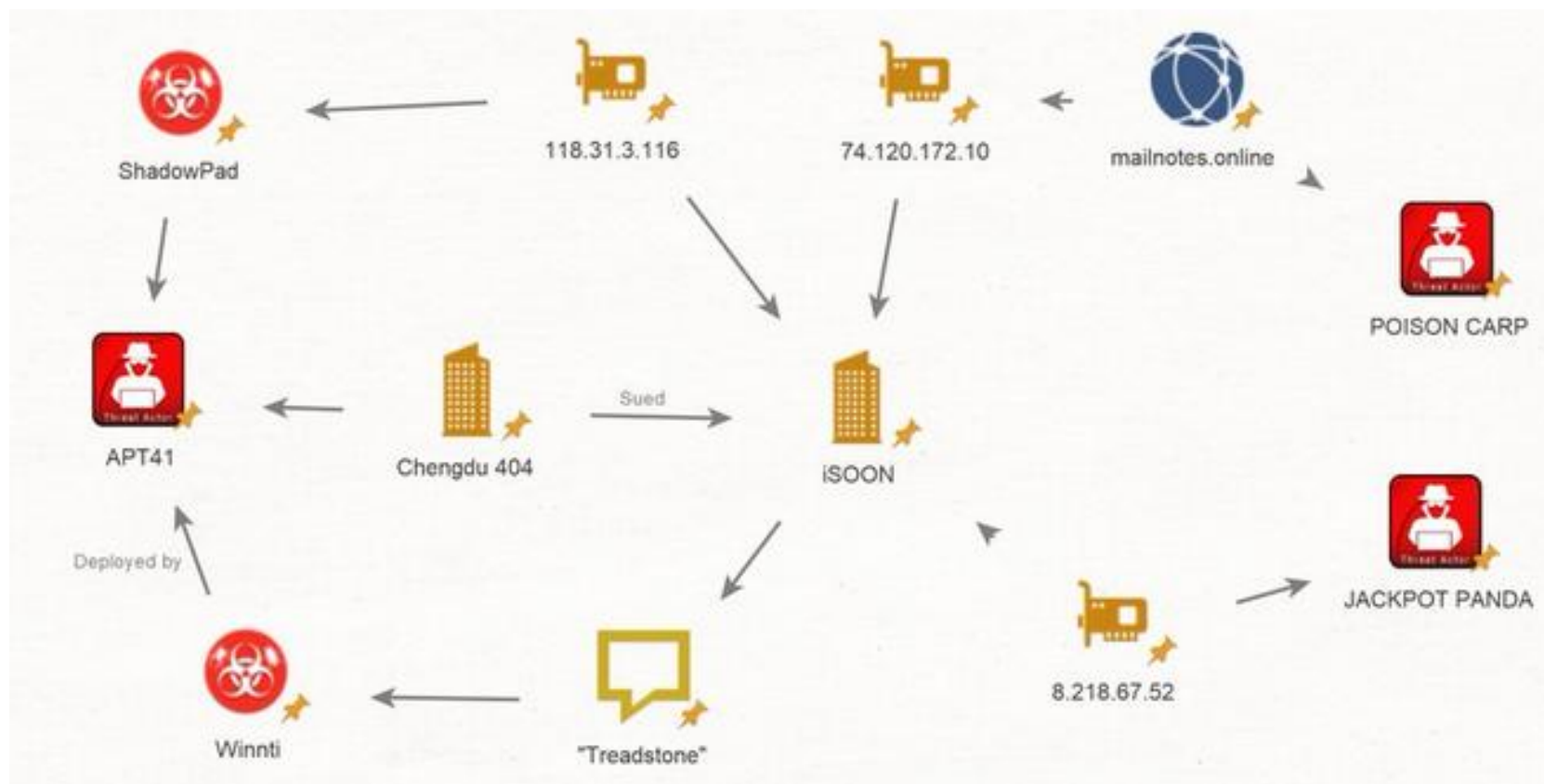
kali@kali: ~/Documents
File Actions Edit View Help
(kali@kali)-[~/Documents]
$ unzip -l JYC.zip
Archive:  JYC.zip
  Length   Date      Time    Name
-----
0         2022-07-04 01:50   nato-0621/
178       2022-07-04 01:50   __MACOSX/._nato-0621
480702   2022-07-04 01:48   nato-0621/NATO-1.png
234      2022-07-04 01:48   __MACOSX/nato-0621/._NATO-1.png
2628418  2022-07-04 01:48   nato-0621/NATO-2.jpg
234      2022-07-04 01:48   __MACOSX/nato-0621/._NATO-2.jpg
-----
3109766                               6 files
  
```

**Conversation record concerning the compromise of documents mentioning NATO Secretary General Jens Stoltenberg. The discussion also sheds light on the functioning of the so-called hackers-for-hire system.**

2022-05-10 07:05:27	wxid_5390224027312	wxid_wh6x59w70y3r22	
2022-05-10 07:05:40	wxid_wh6x59w70y3r22	wxid_5390224027312	What does it mean to be a little bad
2022-05-10 07:05:42	wxid_wh6x59w70y3r22	wxid_5390224027312	[crying]
2022-05-10 07:05:56	wxid_wh6x59w70y3r22	wxid_5390224027312	Is it on the market?
2022-05-10 07:06:44	wxid_5390224027312	wxid_wh6x59w70y3r22	They have been in contact before
2022-05-10 07:07:02	wxid_wh6x59w70y3r22	wxid_5390224027312	General Secretariat
2022-05-10 07:07:05	wxid_wh6x59w70y3r22	wxid_5390224027312	NATO General Secretariat
2022-05-10 07:07:12	wxid_5390224027312	wxid_wh6x59w70y3r22	Now I know it again
2022-05-10 07:07:20	wxid_5390224027312	wxid_wh6x59w70y3r22	They saw the demo and were not interested
2022-05-10 07:07:28	wxid_wh6x59w70y3r22	wxid_5390224027312	[Pinch]
2022-05-10 07:07:47	wxid_wh6x59w70y3r22	wxid_5390224027312	There are things from their chairman
2022-05-10 07:07:49	wxid_wh6x59w70y3r22	wxid_5390224027312	Inside
2022-05-10 07:08:41	wxid_wh6x59w70y3r22	wxid_5390224027312	With NATO Secretary General Jens Stoltenberg
2022-05-10 07:08:49	wxid_wh6x59w70y3r22	wxid_5390224027312	The Secretary-General of NATO is the highest administrative leader
2022-05-10 07:09:08	wxid_5390224027312	wxid_wh6x59w70y3r22	
2022-05-10 07:09:11	wxid_5390224027312	wxid_wh6x59w70y3r22	So
2022-05-10 07:09:21	wxid_5390224027312	wxid_wh6x59w70y3r22	It's not that you think it's valuable, others will think it's valuable

## ANNEX 2: INDICATORS OF COMPROMISE AND LINKS TO OTHER CHINESE THREAT ACTORS

Based on data from leaked materials, the company I-SOON is connected to at least three APT groups. The first is the cluster around the Winnti group, which includes APT41, followed by Poison Carp and Jackpot Panda.





**I-SOON LEAK****Indicators of Compromise (IOCs)**

No	IP	Domain	Country	Region	City	ISP	ASN	Description
1	118.31.3.116		China	Zhejiang	Hangzhou	Hangzhou Alibaba Advertising Co.,Ltd.	37963	C2 IP for SecuritySystemv5 Windows RAT aka ShadowPad <a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
3	74.120.172.10	74.120.172.10.16clouds.com	United States	California	Los Angeles	IT7NET	25820	mailnotes[.]online -> POISON CARP APT <a href="https://github.com/I-SOON/I-SOON/blob/main/0/23.md">https://github.com/I-SOON/I-SOON/blob/main/0/23.md</a>
4	8.218.67.52		Hong Kong		Hong Kong	Alibaba US Technology Co., Ltd.	45102	Jackpot Panda or Iron Tiger <a href="https://github.com/I-SOON/I-SOON/blob/main/0/36.md">https://github.com/I-SOON/I-SOON/blob/main/0/36.md</a>
5	171.88.143.37		China			Chinanet	4134	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
6	1.192.194.162		China			Luoyang, Henan Province, P.R.China.	137687	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
7	101.219.17.111		India					<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
8	221.13.74.218		China	Guizhou	Guiyang	CHINA UNICOM China169 Backbone	4837	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
9	171.88.142.148		China			Chinanet	4134	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
10	171.88.143.72		China			Chinanet	4134	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>
11	66.98.127.105	66.98.127.105.16clouds.com	United States	California	Los Angeles	IT7NET	25820	<a href="https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md">https://github.com/I-SOON/I-SOON/blob/main/0/9fe6b262-9944-417d-a0c4-9f2de1de2994.md</a>



## SOURCES

- <sup>1</sup> Cary, D., Milenkovski, A. 2024 Unmasking I-Soon | The Leak That Revealed China's Cyber Operations. <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations>
- <sup>2</sup> Ibid.
- <sup>3</sup> BushidoToken. 2024. Lessons from the iSOON Leaks. <https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html>
- <sup>4</sup> BushidoToken. 2024. Lessons from the iSOON Leaks. <https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html>
- <sup>5</sup> Ibid.
- <sup>6</sup> Cary, D., Milenkovski, A. 2024 Unmasking I-Soon | The Leak That Revealed China's Cyber Operations. <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations>
- <sup>7</sup> Dingtalk. 2024. 上海安洵信息技术有限公司. <https://dingtalk.com/qidian/company/1180716015092461056>, Github. 2024. I-SOON. [https://raw.githubusercontent.com/mttaggart/I-SOON/main/0/01cdc26f-e773-4ad7-8808-d04abf16aae7\\_2\\_0.png](https://raw.githubusercontent.com/mttaggart/I-SOON/main/0/01cdc26f-e773-4ad7-8808-d04abf16aae7_2_0.png)
- <sup>8</sup> BushidoToken. 2024. Lessons from the iSOON Leaks. <https://blog.bushidotoken.net/2024/02/lessons-from-isoon-leaks.html>
- <sup>9</sup> Ibid.
- <sup>10</sup> Yin, Z. 2022. 「安洵信息」：聚焦实战能力建设，构建数字安全体系. <https://36kr.com/p/1937498250594690>
- <sup>11</sup> Freebuf. 021. 上海安洵信息技术有限公司. <https://web.archive.org/web/20210224224228/https://company.freebuf.com/company/%E4%B8%8A%E6%B5%B7%E5%AE%89%E6%B4%B5%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8>
- <sup>12</sup> Krstinovska, A. 2022. Chinese Influence in North Macedonia. <https://cepa.org/comprehensive-reports/chinese-influence-in-north-macedonia/>
- <sup>13</sup> Natto team. 2023. i-SOON: Another Company in the APT41 Network. <https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41>
- <sup>14</sup> Github. 2024. I-SOON. [https://raw.githubusercontent.com/mttaggart/I-SOON/main/0/01cdc26f-e773-4ad7-8808-d04abf16aae7\\_2\\_0.png](https://raw.githubusercontent.com/mttaggart/I-SOON/main/0/01cdc26f-e773-4ad7-8808-d04abf16aae7_2_0.png)
- <sup>15</sup> Mozur, P., Bradsher, K., Liu, J., Krolik, A. 2024. Leaked Files Show the Secret World of China's Hackers for Hire. <https://www.nytimes.com/2024/02/22/business/china-leaked-files.html>
- <sup>16</sup> Natto team. 2023. i-SOON: Another Company in the APT41 Network. <https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41>
- <sup>17</sup> Vicens, A. 2024. Leaked documents show how firm supports Chinese hacking operations. <https://cyberscoop.com/isoon-chinese-apt-contractor-leak>
- <sup>18</sup> U.S. Department of Justice. 2020. Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>
- <sup>19</sup> Natto team. 2023. i-SOON: Another Company in the APT41 Network. <https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41>
- <sup>20</sup> Github. 2024. I-SOON. <https://raw.githubusercontent.com/mttaggart/I-SOON/main/0/1-en.md>
- <sup>21</sup> Cary, D., Milenkovski, A. 2024 Unmasking I-Soon | The Leak That Revealed China's Cyber Operations. <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations>

## TERMS OF USE OF INFORMATION

The use of the information provided shall be in accordance with the [Traffic Light Protocol](#) methodology. The information is marked with a flag that specifies the conditions of use of the information. The following flags are set, indicating the nature of the information and the conditions of use:

Colour	Conditions of use
<b>Red</b> <b>TLP:RED</b>	The information may not be provided to any person other than the person to whom the information was addressed unless other persons to whom such information may be provided are specifically identified. Where the recipient considers it important to disclose the information to other bodies, this may be done only with the consent of the originator of the information.
<b>Orange</b> <b>TLP:AMBER+STRICT</b>	The information may only be shared within the recipient's organisation, and only to persons who meet the need-to-know and whose information is relevant to resolving the problem or threat identified in the information.
<b>Orange</b> <b>TLP:AMBER</b>	Information may be shared within the recipient organisation and to its partners, and only to persons who meet the need-to-know and whose information is relevant to resolving the problem or threat identified in the information.
<b>Green</b> <b>TLP:GREEN</b>	Information may be shared within the beneficiary's organisation and, where appropriate, with other partners of the beneficiary, but not through publicly available channels; the beneficiary must ensure the confidentiality of the communication when forwarding it.  The information may be further provided and disseminated without restriction. Any restrictions based on the intellectual property rights of the originator and/or recipient or third parties are not affected by this provision.

## EXPRESSION OF NÚKIB PROBABILITIES

Expression	Probability
<i>Almost sure</i>	<i>90-100 %</i>
<i>Very likely</i>	<i>75-85 %</i>
<i>Probable</i>	<i>55-70 %</i>
<i>Cannot be ruled out/Real possibility</i>	<i>20-50 %</i>
<i>Improbable</i>	<i>15-20 %</i>
<i>Very unlikely</i>	<i>0-10 %</i>