A comprehensive analysis of I-Soon's commercial offering

harfanglab.io/en/insidethelab/isoon-leak-analysis/

Key Findings

- I-Soon's commercial offering reveals that their main issue is processing collected data, not breaching their targets in the first place. Their products leverage deep learning to help them sort and classify stolen documents.
- The company appears to have trouble sourcing malware and relies on generally crude methods (i.e., phishing). Yet they breached countless strategic targets worldwide in the last 10 years.
- The leaks confirm analyst suspicions about the Chinese cybersecurity apparatus organization, particularly regarding vulnerability management and regional tasking spread across provinces.
- Intelligence contractors such as I-Soon benefit from a large degree of operational autonomy and may proactively breach victims in the hopes that their clients will be interested in the collected data.
- Contrary to initial reporting, I-Soon's social media influence capabilities appear to be overblown and likely couldn't noticeably impact the public debate.

Introduction

On February 16, 2024, an anonymous user posted a large number of internal documents pertaining to a Chinese cybersecurity company named I-Soon on GitHub (repository now taken down). It contains a variety of information, ranging from internal chat logs to technical documentation of tools or services provided by the company to its customers.

The leak is particularly noteworthy because, at will be made clear in this report, I-Soon (also known as Shanghai Anxun Information Technology Co., Ltd.) belongs to an ecosystem of private actors providing hacking-for-hire services (candidly advertised as "APT research") as well as intrusion technologies to their customers, who appear to be local government bodies. It shines a new light on the so-called "Chinese-speaking APT nexus", where clustering campaigns and actors has traditionally proven difficult.

In the past, such a corpus would have been very difficult to comb through due to the language barrier. Thanks to the progress of AI technologies (machine-translations quickly provided by the community, the use of public LLMs to transcribe, translate and summarize conversations and documents)[1], we were able to effectively analyze the leak. This establishes a new baseline for how damaging a foreign-language leak can be.

In this article, we dive into the contents of the documents, with a strong focus on the technical capabilities reported by I-Soon, through the operations they claim and products they advertise to their customers. We also go over links to existing APT activities which have been discovered based on the information in the documents.

What is I-Soon?

I-Soon was founded in Shanghai in 2010. Its CEO, Wu Haibo (吴海波), is a "*first-generation red hacker or Honker and early member of Green Army which was the very first Chinese hacktivist group founded in 1997*" according to a Natto Thoughts blog post on the company from October 2023, where its links to the APT41 network were studied. I-Soon has roughly 70 employees and three subsidiaries:

- One in Chengdu, created in 2015, where the R&D and penetration testing activities are located. Chengdu is a known cybersecurity hub for China;
- One in Yunnan, created in 2017, taking care of "regional market work". It appears to be mostly composed of sales and technical support staff;
- The last in Jiangsu, created in 2020, is similar to the Yunnan one.

The company's mission, quoted from its official website, is to "*become a solid national defense reserve force with a strong sense of political responsibility and a spirit of high responsibility to the Party and the People*". The company is a certified supplier for the Cyber Security and Defense Bureau of the Ministry of Public Safety (MPS) to "*provide technologies, tools or equipment*". It received a "Class II secrecy qualification" – the local equivalent of a

security clearance. Its website (archived page) lists many government customers, essentially public security bureaus and departments from various provinces and autonomous regions (complete list provided in Annex I). The company holds 59 patents, such as “an intelligent platform and its application in assisting criminal investigation”, “special investigative warfare platform”, etc.

According to Le Monde, a spokesperson for the Chinese government said that it had “no links” to the reported activities and that “*China opposes and prosecutes any and all forms of cyberattacks, in accordance to its laws*”. We will update this article, should local authorities opt to take legal action against I-Soon.

Nonetheless, internal chat logs reveal that public actors represent a significant part of the customer base, to the point of weighing on company morale:

2022-06-13 07:53:29	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	Global proxy
2022-06-13 07:53:40	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	This is what we need to teach them
2022-06-13 07:53:50	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Generally, we sell here and also teach
2022-06-13 07:53:55	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	[Face covering] I want it
2022-06-13 07:54:01	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	I'm really drunk [laughing through tears]
2022-06-13 07:54:08	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	The public security customers are so stupid
2022-06-13 07:54:17	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Calm down
2022-06-13 07:54:19	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Haha
2022-06-13 07:54:21	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	I want to do a business that does not involve police this year
2022-06-13 07:54:23	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	So tired
2022-06-13 07:54:35	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	No fucking money for football
2022-06-13 07:55:08	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Normal
2022-06-13 07:55:13	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	You must deal with after-sales service
2022-06-13 07:55:22	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	[Face covering]

Figure 1: An employee complains about their interactions with public customers and hopes to be tasked on non-police missions[2].

The leak

A legitimate question to consider before proceeding any further is whether the leak is legitimate. We can start by noting that I-Soon employees, when questioned by AP, did not question the authenticity of the files: “*I-Soon and Chinese police are investigating how the files were leaked*”. Since the release, the community has discovered several indicators in the documents which link activities mentioned by I-Soon to known APT campaigns and are consistent with the targeting reported by I-Soon in its own materials. At the time of this writing, the credibility of these documents is not debated in the field.

It is however worth asking the question of how reliable this data is. Considering the mystery surrounding the context of this leak, it remains possible that while authentic, the documents could have been subtly manipulated:

- Some key information could have been redacted from the leak;
- Targeted tampering and/or doctoring might have taken place on specific documents.

Such actions would typically be harder to detect and all we can say is that we didn't observe any evidence of it. One last point to consider is that a significant portion of the leak is composed of commercial documents which, by nature, may not be entirely truthful.

Next, the source of the documents needs to be addressed. The files were posted on a GitHub account associated to the email address `I-S00N@proton.me`, created on January 23, 2024, not long before the leak went up. Another email address, `isoon@proton.me` also exists, with an associated GPG key generated on September 25, 2023, five months ahead of the release of documents:

```
pub   ed25519 2023-09-25 [SC]
      421EA93EC291A950BD33ECD504AC29C49FAAC430
uid           isoon@proton.me <isoon@proton.me>
sub   cv25519 2023-09-25 [E]
```

We could not determine whether the second address is linked to the leak, or if its earlier creation is coincidental. If not, this could indicate a leak carefully planned ahead of time. The identity of the person (or persons) who published these documents has been the subject of intense speculation. Popular hypotheses are:

- Third-party intrusion: a rival company, foreign APT group or hacktivists who broke into I-Soon's network and orchestrated the leak to damage the company's (or China's) reputation;
- Internal leak: a disgruntled employee enacted revenge by disclosing the information they were privy to.

Other options were discussed (cybercriminals, etc.) but we do not believe them credible enough to warrant further discussion. Two key factors must be considered when assessing a voluntary data breach:

- Access: who had access to the documents in question?
- Motivation: what did the leaker stand to gain by crippling I-Soon's reputation?

The presence of chat logs and mobile phone screenshots in the documents indicates with a high degree of certainty that the leak comes from someone with either administrative access to the company's internal systems, or that some measure of hacking was involved to acquire them. Conversations between employees contained in the leak contain multiple evidence of discontent workers complaining about low-pay or poor working conditions (across all positions), which has sparked a lot of interest in the "internal leak" theory. On the other hand, it is hard to imagine that an employee would be able to extract all this information without accidentally revealing their identity based on what they had access to. If this theory is correct, we hypothesize that they still obtained the information by hacking their own corporate network (which isn't so hard to believe in a hacking-for-hire outfit) and that they left China before acting, as they knew their identity would be discovered soon thereafter.

This analyst's opinion, not grounded in a factual basis, is that a leak orchestrated by a foreign APT actor who infiltrated I-Soon is the most credible theory.

I-Soon's products and services

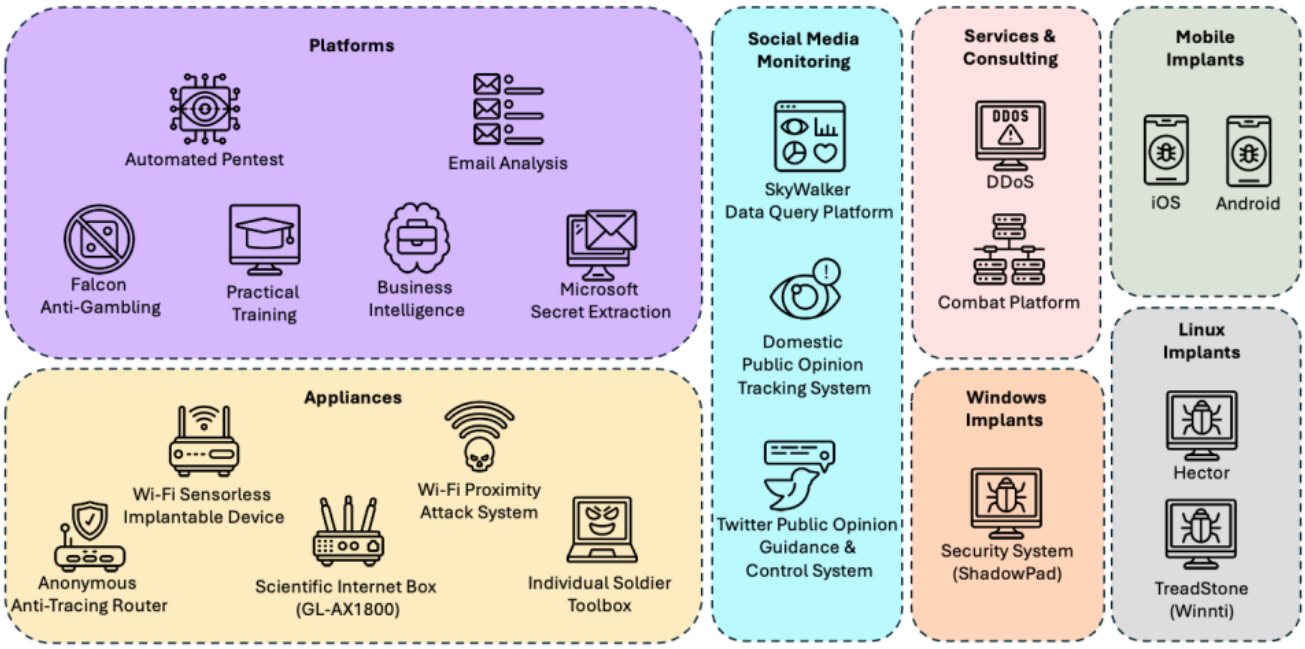

Figure 2: An overview of I-Soon's products and services

I-Soon's activities officially include penetration testing, the development of security solutions and trainings, and they developed partnerships with local universities to cultivate talent. In the leak, we discover that since 2013, they have established an "APT research" division (separated into 3 penetration teams and 1 security research team) tasked with completing "overseas APT projects". They offer various tiers of service:

- Access acquisition: providing an entry point into a designated victim's network;
- Data exfiltration: collecting data from a designated victim and providing it to the client;
- Intelligence production: analyzing the stolen data to produce briefing notes, reports, select documents of interest, etc.

One particularly interesting takeaway is that I-Soon isn't just a mercenary hacker operation: **it can act as a private intelligence service**. Beyond running cyber operations in-house, it can also send security experts to their customers' premises to take part in operations.

This is reflected in the products developed by the company, which present a surprising focus on "business intelligence" and data analysis – we understand that those products are both used internally to process the intel collected by I-Soon's operations, and offered to their customers who also run their own in parallel.

Offensive software

Windows

I-Soon's catalog contains CotS (commercial off-the-shelf) malware destined for their customers. Little technical information on their subject is provided in the customer documentation. All offer at least this basic set of features: interactive command execution capabilities and file management.

An unnamed RAT ("*Security System*" in the window names) offers more extensive capabilities: service management, screen capture, keylogging, monitoring of recent documents, etc. It connects to the C2 using either TCP or UDP and can pivot through other infected machines in the network to access the internet. It reportedly bypasses 95% of antivirus products on the market[3] thanks to "polymorphism" and may[4] be delivered with full source code and operator training. This latter malware is likely a ShadowPad variant (see discussion in the "Links to previously documented APT activities" section), and even possibly the origin of ShadowPad: this mode of distribution explains how so many variants of ShadowPad ended up being used by so many threat actors in the Chinese-speaking nexus.

The leak also contains specifications for a future backdoor (possibly to be developed by a technology partner). Points of interest include:

- The ability to choose the encryption algorithm between RC4, AES, RC2, GOST, IDEA, CAST (switchable during runtime);
- Automatic proxy traversal based on Windows and browser settings;
- Persistence method not monitored by the Sysinternals `autoruns.exe` utility.

Linux

A first Linux implant, *Hector*, has a dynamic plugin system and communicates with its C2 server using HTTP, HTTPS or websockets (see Figure 3).

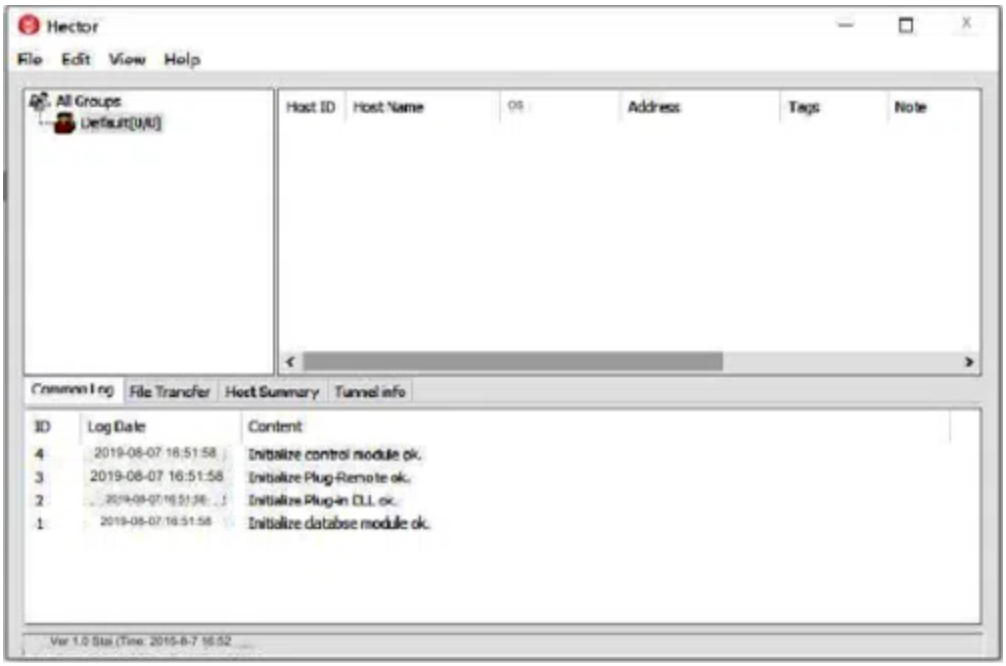

Figure 3: Screenshot of the client for the Hector malware

I-Soon offers a Linux implant featuring SOCKS5 proxying and TCP port reuse for communications. Security researcher @silascutler was the first to notice that the internal name of this tool (“TreadStone”, see Figure 4) was mentioned in the FBI indictment of Chengdu 404 (another cybersecurity company from the region) as the controller for Winnti.

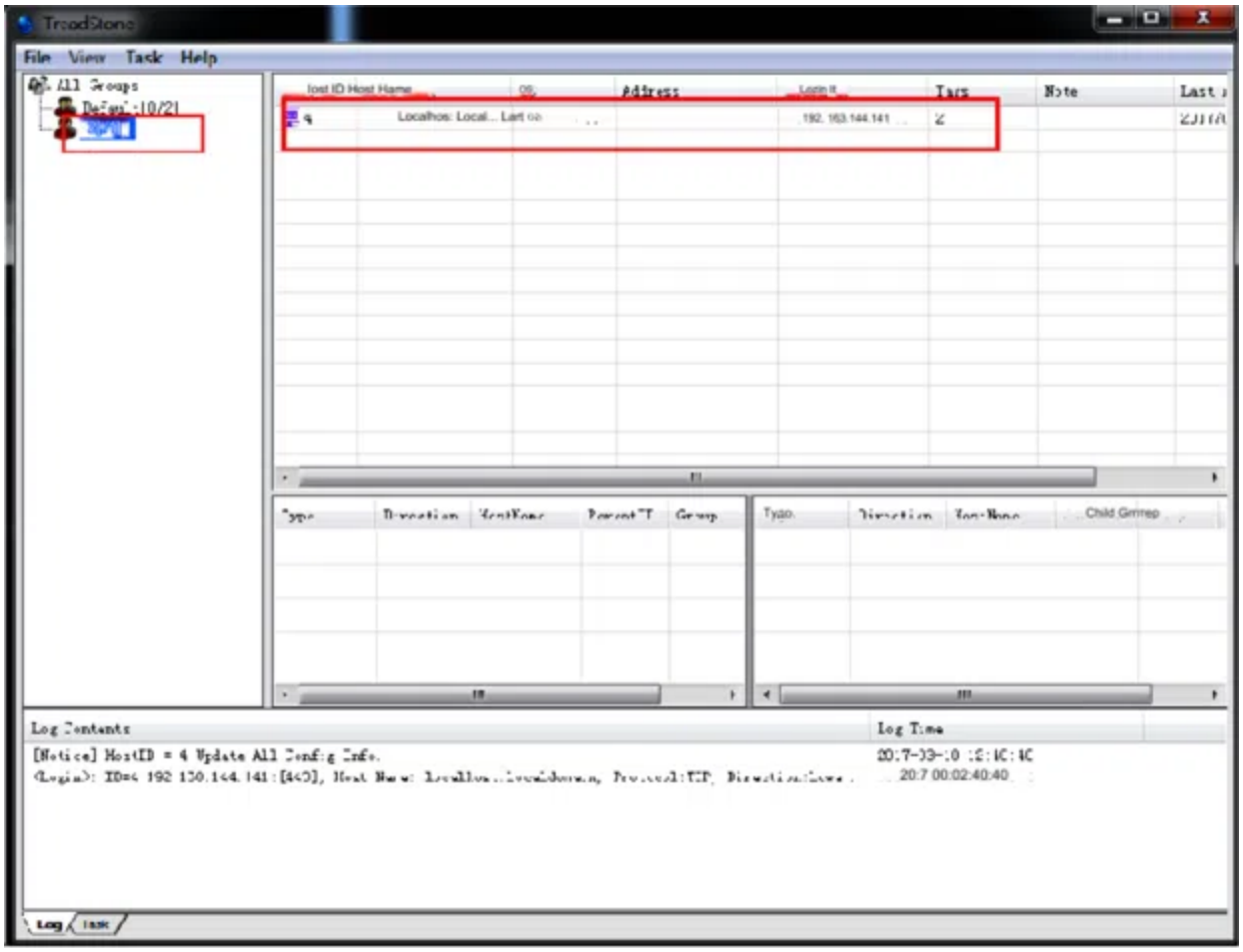

Figure 4: Client for the Linux implant, revealing the internal name “TreadStone”

Lending credence to this discovery, the following conversation between I-Soon’s CEO (“Shutd0wn”) and an unidentified high-ranking employee reads: “*One more thing, that project in Wuxi has a procurement of Linux 🐤**[5]**, but our company does not have one. The procurement was from Huaxin Network Security. Then I talked to Si Xu last time, and he and his friends also did it. Linux 🐤, because Windows 🐤 didn’t pay anyone last time, at the same price, can I use Si Xu’s one…*” This excerpt would indicate that I-Soon doesn’t actually own a bespoke Linux implant and sources it from partners (possibly Chengdu 404).

macOS

Commercial documents from I-Soon mention malware designed for macOS platforms, but details are scarce. It advertises the same features as the ShadowPad variant (screen capture, keylogging) but it is impossible to say whether they originate from the same codebase.

2021-11-23 08:27:17	lengmo	Shutd0wn	Jiangsu Provincial Department also wants to buy 3 this time, Windows, Linux and Android, any Android one will be fine. Depends on which house it is from.
2021-11-23 08:28:24	Shutd0wn	lengmo	We will definitely make a full version, supplemented by suppliers
2021-11-23 08:28:53	lengmo	Shutd0wn	Hmm... Then you need to organize a team to do it. It would be best if your own can meet the requirements. Gross profit is still higher.
2021-11-25 02:31:06	lengmo	Shutd0wn	The Wuxi project just won the bid for 7988000
2021-11-25 02:32:06	Shutd0wn	lengmo	niubility
2021-11-25 02:32:25	lengmo	Shutd0wn	Do you know what is the most important thing?
2021-11-25 02:32:26	Shutd0wn	lengmo	There was no mistake or cancellation of the mark. . . .
2021-11-25 02:32:37	lengmo	Shutd0wn	I won the bid at the direct closing price...no quotation was made
2021-11-25 02:32:38	Shutd0wn	lengmo	What?
2021-11-25 02:32:43	lengmo	Shutd0wn	Directly announce that we won the bid
2021-11-25 02:33:03	lengmo	Shutd0wn	After demolition and review, we were announced as the winner
2021-11-25 02:33:20	lengmo	Shutd0wn	It shows that network security is still very strong
2021-11-25 02:33:44	Shutd0wn	lengmo	Well, regional differences, Jiangsu Internet security should be generally strong

Figure 5: I-Soon's CEO ("Shutd0wn") and a high-ranking employee discuss the acquisition and sale of implants for the security bureau of the Jiangsu Provincial Department.

iOS

The trojan for iOS devices collects various information (IMSI, IMEI, IP and MAC addresses, OS version, etc.) and allows to track the location of the victim over time. The microphone can be activated at any time to record ambient conversations, and all files and contacts can be exfiltrated to the C2 server. Jailbreaking of the device not required.

Android

The Android implant offers the same features as the iOS one, with a few additions:

- Access to SMS and instant messenger data (root access required);
- Remote Wi-Fi and camera control;
- Network traffic capture;
- With root access, the malware can be installed as a system app, which allows it to survive factory resets.

Interestingly, I-Soon advertises a separate product named "Wi-Fi Sensorless Implantable Device", a rogue Wi-Fi access point which infects Android devices that connect to it. No information could be found regarding the infection method (baseband exploitation, traffic tampering, presentation with a fake installer, etc.).

0days and exploits

A glaring gap in I-Soon's catalog is the absence of software vulnerabilities. They are sometimes mentioned in the context of acquisition opportunities – rare occurrences overall[6]. Based on the documents we consulted, we assess that I-Soon doesn't possess an in-house exploit development capability and it doesn't appear that they make a business of reselling the vulnerabilities they acquire.

However, the following conversation excerpt caught our attention:

2021-10-26 01:53:17	Shutd0wn	lengmo	The 0DAY loopholes in the Tianfu Cup competition are said to have been given to the POC to the police. Can I get this?
2021-10-26 01:53: 49	lengmo	Shutd0wn	If not, I asked that day. The Ministry gave it to Jiangsu
2021-10-26 01:53:59	lengmo	Shutd0wn	Given every year
2021-10-26 01:54:17	lengmo	Shutd0wn	It is said that some loopholes are relatively useless
2021-10-26 01:54:37	lengmo	Shutd0wn	I can only see if there is any prefecture or city in the hall
2021-10-26 01:55:36	Shutd0wn	lengmo	It is said that the Ministry of Public Security obtained the POC, and it takes some effort to write it into EXP
2021-10-26 01:56:09	Shutd0wn	lengmo	For vulnerabilities like IOS, it is not easy to make EXP even if you know the POC
2021-10-26 01:56:13	lengmo	Shutd0wn	I talked about it during dinner that day
2021-10-26 01:56:18	lengmo	Shutd0wn	Let me ask
2021-10-26 01:56:54	lengmo	Shutd0wn	The provincial department seems to have given it to Wuxi
2021-10-26 01:57:07	lengmo	Shutd0wn	This was mentioned in our training that day
2021-10-26 01:57:24	Shutd0wn	lengmo	Well, please pay attention, we will ask for a copy when they spread.
2021-10-26 01:57:31	Shutd0wn	lengmo	It will be nothing if it spreads
2021-10-26 01:57:57	lengmo	Shutd0wn	Well, okay

Figure 6: I-Soon's CEO discusses sharing of 0days discovered in the Tianfu Cup

In it, participants discuss how they expect to receive proofs-of-concepts of vulnerabilities discovered in the context of the Tianfu Cup ("China's Pwn2Own"). The conversation reads: "*The Ministry will give it to Jiangsu every year, and it will not be given to all provinces. It is estimated that they are all given to strong provinces*": this indicates that a well-established institutional process exists so that vulnerabilities discovered during the event are collected by the Ministry of Public Safety, then dispatched to individual provinces for use in their own cyber operations, and finally trickle down to contractors who undertake some of these operations on behalf of the provinces. It is fair to assume that an identical process exists for any vulnerability reported to CNNVD (Chinese National Vulnerability Database).

Funnily though, in this conversation, the participants point out that only proof-of-concept vulnerabilities are shared in the context of the Tianfu Cup and that developing reliable exploits requires resources – implying that they do not possess them. They opt to wait until stable exploits "spread", supposedly in the local cybersecurity ecosystem.

Platforms

I-Soon's core service offering is the development of various platforms and support systems to help clients (and likely help themselves) deal with large quantities of stolen data, as well as organizing cyber operations and facilitating intrusion work.

Automated Penetration testing Platform

Possibly their flagship product, this modular ruby framework automates various steps of penetration testing engagements:

- Determining if the machine is up (via a ping);

- Scanning its ports (connect() scan, SYN scan, NULL scan, Idle scan…);
- Attempting exploitation.

The framework offers many interfaces (CLI, GUI, API, web interface, etc.) and integrates with standard industry tools (OpenVAS, Nessus, Acunetix, Burp Proxy, Core Impact, Nexpose…). It is capable of automatically crawling webpages to look for vulnerabilities from the OWASP top 10, has mobile penetration testing capabilities (no details provided) and integrated social-engineering modules (phishing generation, website cloning). Finally, it also contains password brute-forcing tools.

Our assessment, with medium-to-high confidence, is that this framework is built on top of existing open-source tools:

- Metasploit fits the description of a ruby framework with “modules” and “auxiliary modules”. We noticed references to meterpreter, as well as LHOST and LPORT parameters on a product screenshot. A line in the description alludes to the availability of all Metasploit Pro content;
- The port scanning feature supports the exact same scanning modes as nmap;
- The social-engineering features are reminiscent of SET (the Social-Engineer Toolkit);
- Protocols supported in the bruteforcing feature are almost identical to THC Hydra.

The main selling point of this solution appears to be its easy-to-use GUI, which would allow it to be marketed to organizations (i.e. military) tasked with conducting cyber-operations, but where the average employee wouldn’t be comfortable using Kali Linux.

Email analysis platform

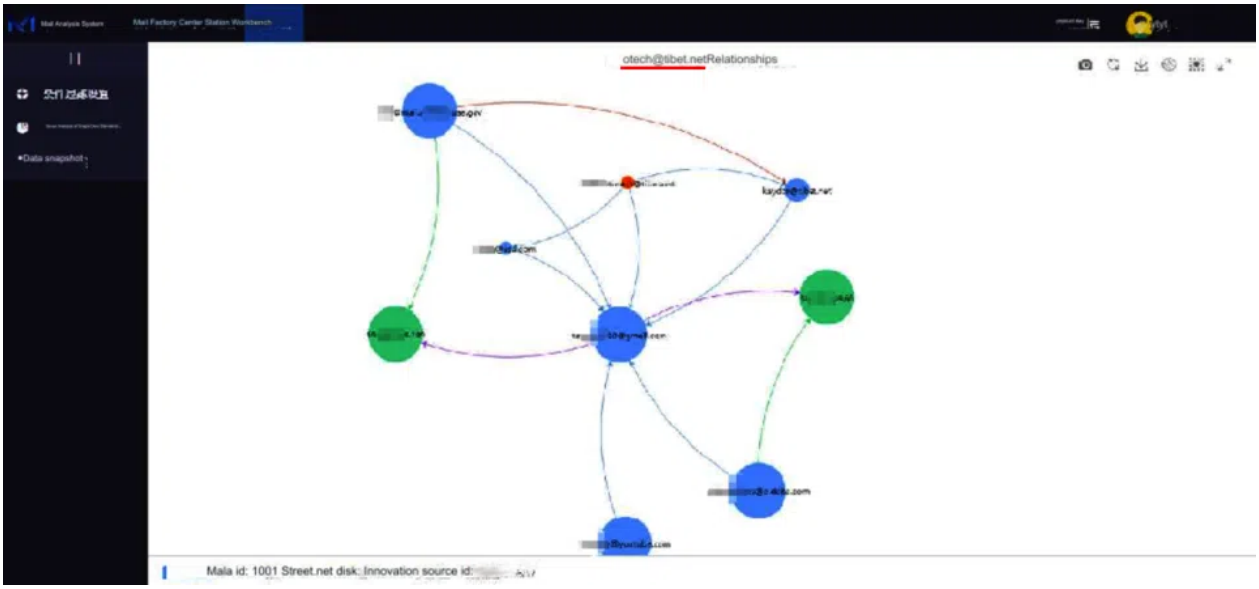

Figure 7: Screenshot from the email analysis platform

A more interesting product, in our opinion, is a platform which ingests emails (for instance, in .eml format) and helps analysts comb through the data. The platform allows users to perform full text searches on the corpus, builds a social graph based on the exchanges, looks for "sensitive words" such as "password", etc. The GUI reconstructs an inbox-like interface, so that analysts can browse the victim's email as if they were logged into the webmail.

The platform can continuously retrieve new emails from the victims if it is provided with the corresponding credentials and is sold both in SaaS and on-premises models.

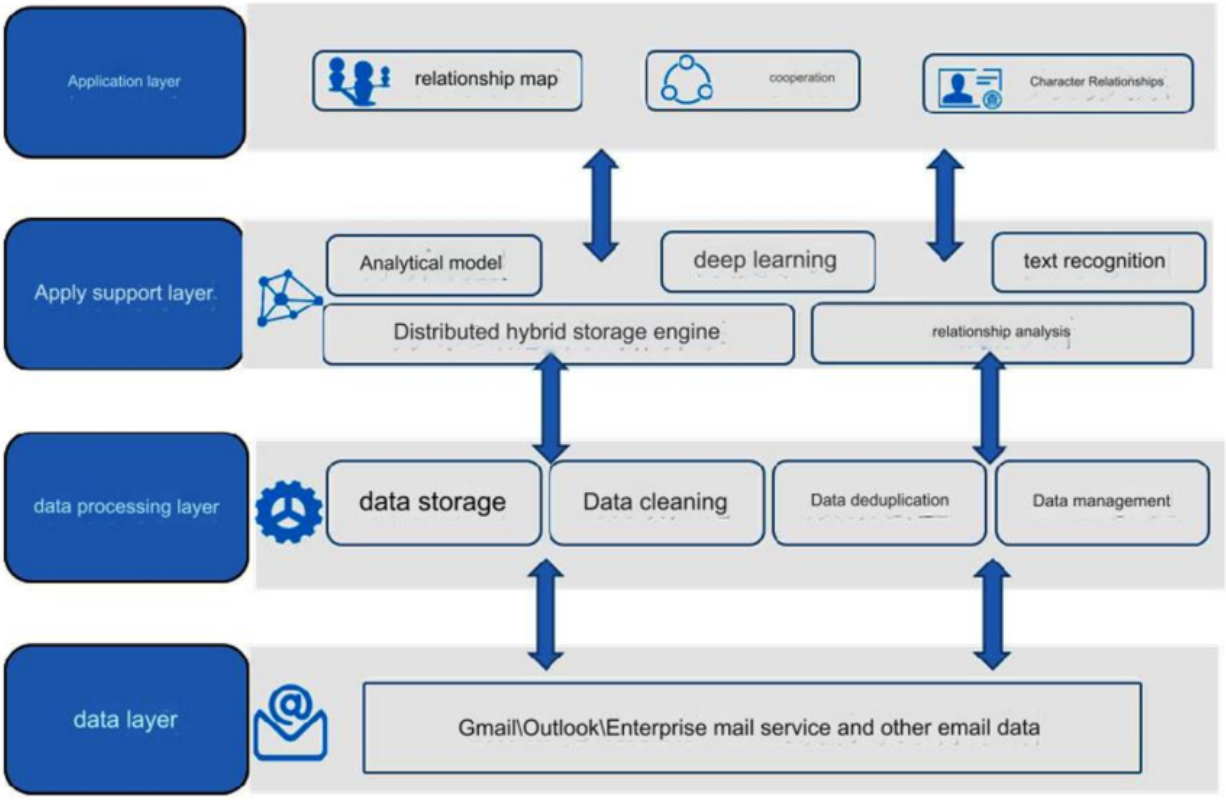

Figure 8: Architecture of the product, with the noteworthy mention of a "deep learning" brick.

The most interesting aspect of this platform is the advertised "deep learning" capabilities, thanks to which it can extract information and classify emails automatically (analysts can also manually tag emails or conversations). I-Soon does not provide a complete picture of the ends towards which deep learning is applied, but we made the following hypotheses based on the screenshots and documentation:

- "Relationship network mining" could mean that the social graph is automatically enriched with relationships ("Alice is the manager of Bob", etc.);
- Personally identifiable information (phone number, addresses, etc.) may be recognized and extracted automatically from email texts and signatures;
- The deep learning model possibly helps establishing correspondences between names and email addresses ("j.smith@victim.com is John Smith") and build a more reliable graph of who talks to/about whom.

At the end, the platform builds a full listing of all individuals discovered, with name, gender, age, nationality, etc.

An obvious comment here is that nobody builds such a platform unless they have more data than their analysts can reasonably work with. In various interviews about how AI would affect the cybersecurity field, we mentioned how we felt AI would prove crucial to help attackers process, classify and summarize the gigabytes of data they obtain. This leak shows that APTs came to the same conclusion since at least 2022.

Microsoft Secret Extraction Platform

But where do these stolen emails come from? Enter the Microsoft Secret Extraction Platform, a dashboard dedicated to breaching Outlook accounts. Schematics for a different[7] (but very similar product) reveal two possible infection paths, one where a malicious executable file is delivered, and another where a "forensics link" (phishing) is delivered to the victim – in both cases, it appears that the end-goal is to obtain the victim's Outlook credentials. An "access token" is obtained based on these credentials and is used to continuously siphon the user's inbox.

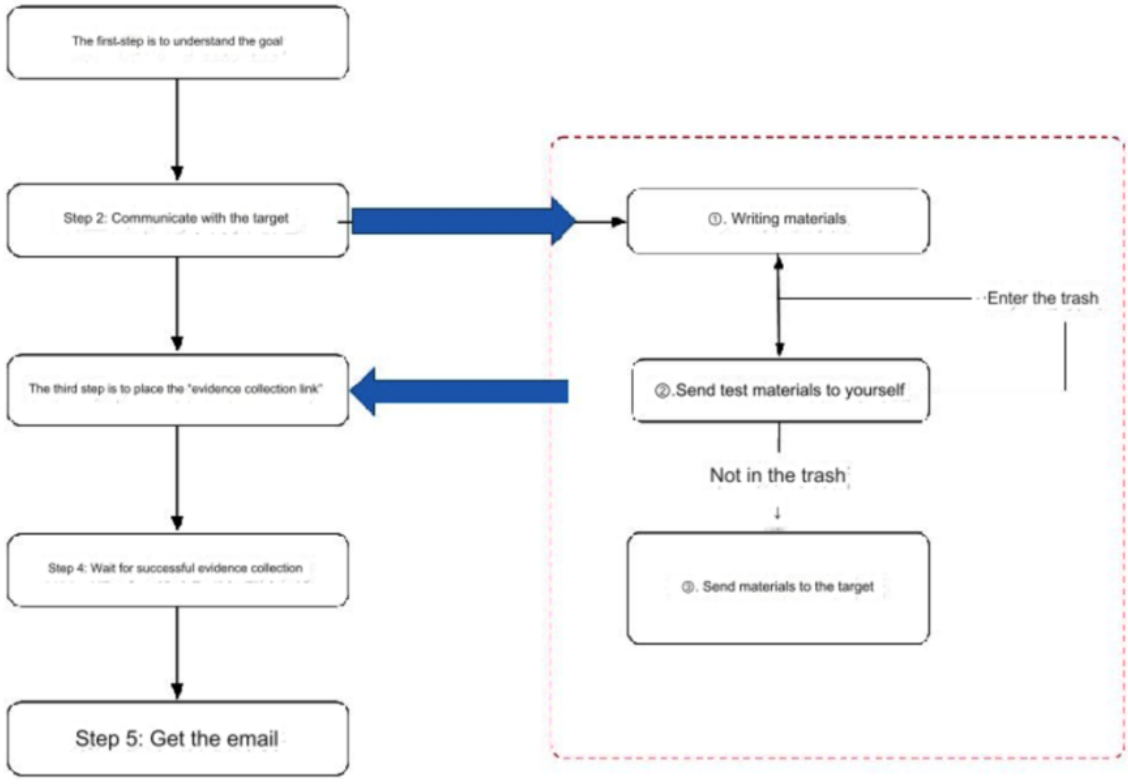

Figure 9: Phishing methodology suggested in the platform's documentation. Emphasis is placed on "building trust" first, implying that the actual payload is only sent after a lengthy conversation.

Another product from 2020 named "*Email Collection Platform*" appears to serve the exact same function, except that it also supports Gmail and POP3/IMAP. It supposedly bypasses two-factor authentication and checks on source IP addresses, but no additional details are provided. We speculate that direct connections through protocols such as POP3/IMAP are the means through which such protections were circumvented. This product is extremely similar to the *Microsoft Secret Extraction Platform*. It is possible that this one has been split into independent modules for business reasons (i.e., so it could be billed as 3 separate products). Yet another almost identical platform exists, "*Twitter Forensics Control Platform*": using the same workflow (phishing, then continuous siphoning of account data), it provides analysts not with emails but direct messages for given handles, their latest tweets, etc.

We suspect that all these platforms could themselves be submodules, or variants of the Email Analysis Platform described above, since it also reported the ability to keep obtaining data from the victims until the password is changed.

Anxun Integrated Data Platform / Anxun Cloud Intelligence Analysis & Decision-Making Platform / Xunzong Security Intelligence Platform

Similarly, we discovered a few additional "business intelligence" platforms which all appear to fill the same role: ingesting structured or unstructured specialized data, processing it and allowing non-technical analysts to easily browse through it, manually classify it, and create "cases" where they gather evidence. The last one ("security intelligence platform") is marketed as a knowledge and document management engine.

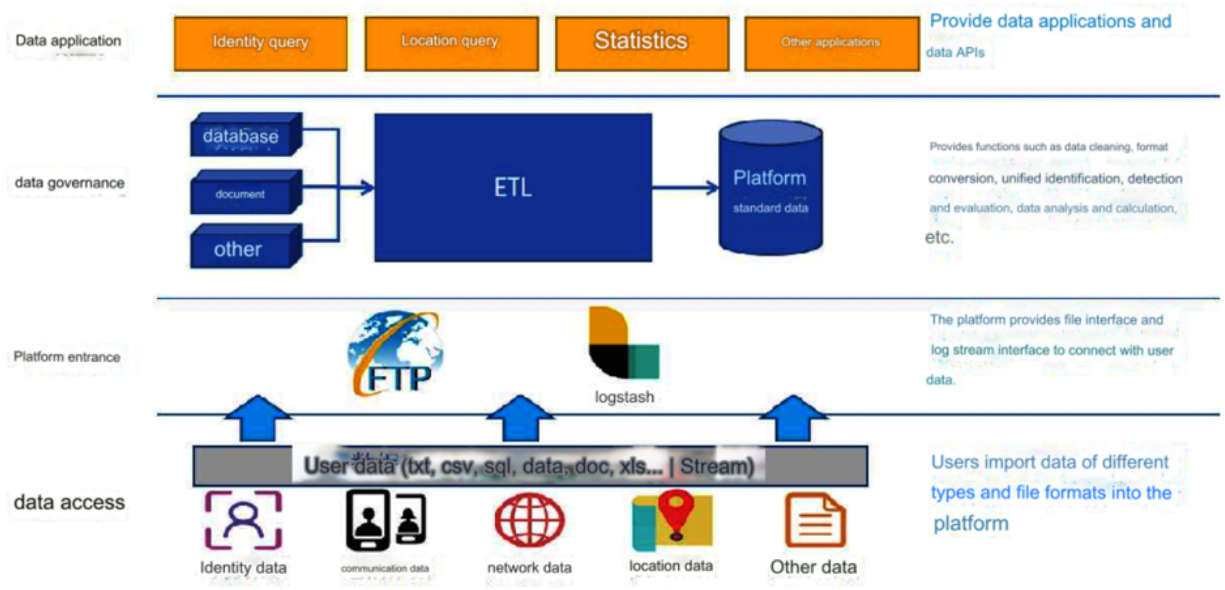

Figure 10: Architecture for one of these platforms. The presence of "communication" and "network" data hint at telco hacking.

These platforms also advertise "intelligent classification and extraction". This leads us to believe, with medium-to-high confidence, that they all share the same core engine and are variants of the Email Analysis Platform[8] repackaged to address different market verticals.

Falcon Anti-Gambling Platform

Another platform cast from the same mold, noteworthy only due to its focus on gambling activities. The presentation document reads: "*statistics show that 600 billions of yuan (77B€) flow overseas each year via gambling platforms*". To combat this outwards money flow, "*Falcon provides comprehensive gambling-related user data, provides law enforcement with a large amount of gambling-related PII [personally identifiable information] and regularly updates the platform to ensure the accuracy […] of the gambling data*"

The input for this platform is data taken from gambling websites (money transfers, account listings, etc.). The documentation only hints at the origin of this data, but chat logs between employees contain explicit references to hacking such websites. We deduce that in some cases (probably not limited to gambling), I-Soon not only provides the platform to its customers, but is also tasked with feeding it with information.

2022-05-11 05:02:10	wxid_7p054rmzkhqf21	gzp1991101	Yeah
2022-05-11 05:58:58	wxid_7p054rmzkhqf21	gzp1991101	Play mahjong
2022-05-11 05:59:24	gzp1991101	wxid_7p054rmzkhqf21	I just lost 1300 yesterday [angry]
2022-05-11 05:59:36	wxid_7p054rmzkhqf21	gzp1991101	Let's lose some more today
2022-05-11 05:59:47	wxid_7p054rmzkhqf21	gzp1991101	The leader will take care of you

Figure 11: I-Soon employees are not themselves fundamentally opposed to betting

Practical Training Platform

A final platform, distinct from the other ones, is a cyber range used for training exercises. It is based on "[the] company's years of experience in APT penetration attacks" and involves a dynamic environment to simulate "real combat". We couldn't find a lot of information about this product, except for feedback from the sales team that the lack of updates reflected poorly on the company.

Figure 12: Screenshot of I-Soon's cyber range

Appliances

I-Soon offers a limited number of hardware products, most of which aim at enabling anonymous or close-range cyber operations.

Individual Soldier Toolbox

The "toolbox" is a Windows notebook which contains a large collection of security testing tools, sorted in various categories and accessible via a graphical user interface. It essentially appears to be "bootleg Kali Windows", although we could not evaluate the quality and overall coverage of the bundled tools.

Wi-Fi Proximity Attack System

A small device disguised as a power outlet. In this attack scenario, the attacker would find a way to physically penetrate the target's premises and leave behind the fake power outlet somewhere. It automatically scans surrounding Wi-Fi networks and autonomously collects cryptographic material (WPA handshakes, etc.) that it sends to cloud cracking services using a 5G link. Once the device has obtained the Wi-Fi password, it deploys a SOCKS proxy so that the operators can tunnel into the victim's network, and starts sniffing the local network for cleartext credentials.

A creative feature is the automatic hacking of routers in the network – we guess it could be based on known default credentials based on the router's brand, or bruteforcing using common passwords. The power outlet can be wiped remotely.

In this case, I-Soon sells both the poison and the cure, as another product ("*WiFi Terminal Positioning Equipment*") can locate a WiFi device with a precision of 1 meter. It also appears to have deauthentication capabilities, or possibly jamming.

Anonymous Anti-Tracing Router

A 4-port, 100Mb router with an integrated 4G SIM card, used for "overseas operations". It routes the user's traffic through network nodes all around the world, which makes traffic impossible to trace.

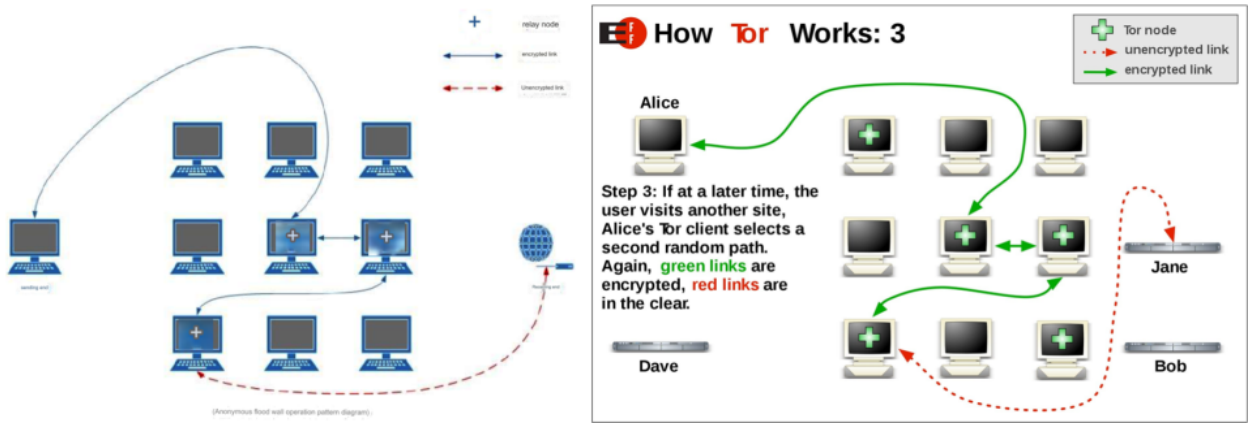

Figure 13: Product documentation, side-by-side with the official Tor project documentation.

We assess with medium-to-high confidence that any traffic going through the router is actually forwarded via the Tor network.

Scientific Internet Box

A similar product, which is used for "scientific" internet consultation (i.e., research on foreign and domestic opinions). Its sole purpose is to bypass the Great Firewall of China. Traffic is routed via nodes located "all around the world" (40 in Hong Kong, and 18 in Japan, Singapore and the USA). Our research indicates that this product is a GL-AX1800 router which tunnels traffic, one way or the other, through remote machines managed by I-Soon.

Services & consulting

Network Traffic Countermeasures System

Surprisingly, I-Soon offers a DDoS-as-a-Service. Thanks to "active scanning", it continuously gathers global traffic capabilities, which can then engage in SYN, TCP, UDP, ACK or GET flooding, and more. The documentation states that "kernel features are used to send UDP packets using asynchronous transmission", hinting that some of the code could be derived from projects such as Zmap or masscan. The information present in the description didn't allow us to provide an estimate of the bandwidth available with this product.

Integrated Combat Platform

Clients looking to develop their offensive capabilities can consult I-Soon on the creation of their attack infrastructure. The commercial documents insist on how all the network links need to be purchased anonymously, with untraceable/fake online personas. I-Soon suggests the following network design:

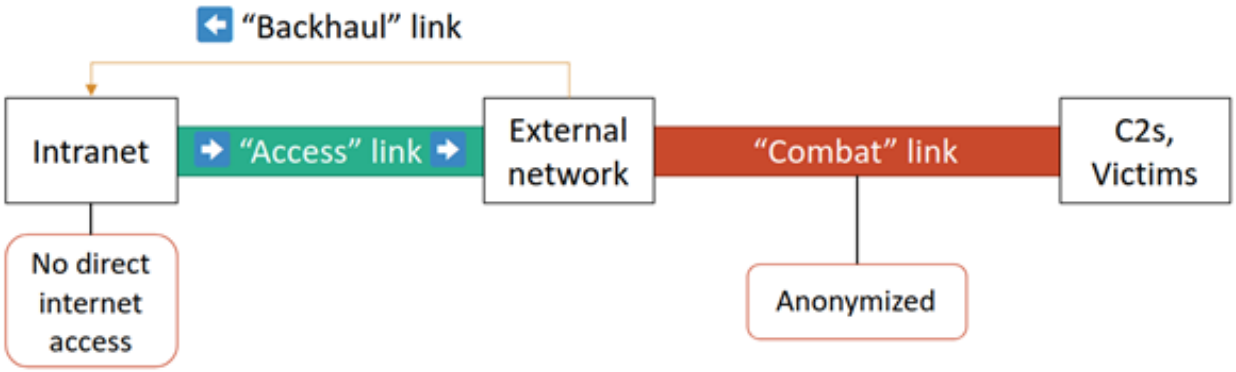

Figure 14: Suggested network architecture reconstructed from the I-Soon documents

The design includes the following network segments:

- "Scientific link" (not represented above), a separate network for general web searches;
- The intranet, where operator VMs are located;
- The extranet, a platform hosted on overseas VPS, protected by passwords, an innocuous interface and geofencing;

The "access" link is essentially one-way, although a distinct "backhaul" link allows operators to bring back stolen data into the intranet. The platform in the extranet is a management dashboard for pentesting teams, which offers user management (and scoring, based on completed tasks, for the purposes of manager evaluations!), a bulletin board to share TTPs, arsenal management where every tool downloaded must be authorized and logged, etc. The administrator can configure C2 templates to deploy on VPS servers. There is also a built-in malware sandbox, possibly used to detect malware in stolen data, test implants before sending them, or analyze enemy malware discovered during simultaneous infection cases.

The documentation offers OPSEC advice: "*the system language, time zone, font, system environment, input method, etc. used by the external platform must all be in non-Chinese language*".

Social Media

One of the aspects which caught the industry's attention when the leak was discovered was the presence of products supposedly aiming at conducting influence operations on social media. After a careful review of the corresponding documents, we assess that the threat was

overblown. The "*Twitter Public Opinion Guidance and Control System*" is much closer to the Outlook email extraction platform than it is to infamous troll farms. The product allows the monitoring of specific, predetermined Twitter accounts (as opposed to getting a stream of all of Twitter's content) – these accounts can be phished according to the same general workflow described in earlier sections. From there, "cases" can be created from collected content, etc.

It is possible to group the hijacked accounts and have them post similar content or interact with specific posts. However, there is no mention in the product of managing and creating fleets of fake accounts, and it seems that phishing individual (and likely high-value) accounts for astroturfing purposes is an inefficient approach at best. In all likelihood, the volume would be negligible and there is a significant risk that the victim would notice the unusual activity on their account. All in all, the "opinion guidance" aspect of this product doesn't appear very well thought out, and has all the hallmarks of a capability stapled onto a product after the fact to satisfy an important client's insistent request (or to match the specification for a public offering). It is unlikely it ever produced actionable results.

I-Soon however offers a similar platform focused on the local market, "*Domestic Public Opinion Tracking System*". It appears to be an OSINT (open-source intelligence) tool used to gather personal information on Chinese-speaking social media platforms (Baidu, Sina, Tianya, etc.). Use cases include finding a user's phone number or email address based on a handle, deanonymization of shared links, and so forth.

We also found references to a "*SkyWalker Data Query Platform*" – yet another platform – dedicated to storing and querying personal information. Users can input selectors such as a name, registration address, or ID card number, and the platform reconstructs the target's online presence. While the documentation doesn't specify which data sources are used, it is possible this system is a front-end for the *Domestic Public Opinion Tracking System*.

Victimology

The leak offers unprecedented insight into the activities of an APT actor, as it contains full listings of compromised targets and strategic discussions pertaining to their customers' interests.

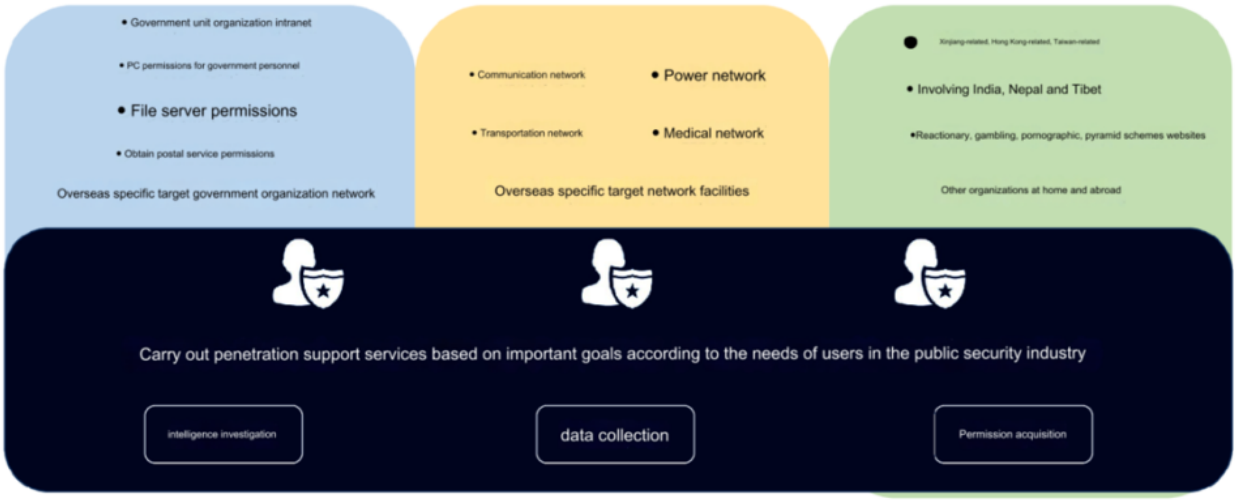

Figure 15: Targeted accesses and verticals advertised in I-Soon's documentation

While advertising its "APT research" capabilities to potential customers, I-Soon provides concrete examples of past victims and intrusions into specific organizations. A cooperation proposal with the Bazhou (Xinjiang) province security bureau reads: "*Based on our company's APT work for more than ten years, we have controlled various types of server permissions and intranet permissions in multiple countries.*"

At a high level, I-Soon doesn't appear to specialize in a specific type of intelligence collection: its activities range from domestic surveillance (information gathering on ethnic minorities such as the Uyghur, hacking of online gambling platforms or illicit drug marketplaces, etc.) to espionage (military intelligence, intrusion into telecommunication networks, universities, think tanks, etc.). Organization-wise, I-Soon benefits from a fair degree of operational autonomy: it may be given targets directly from customers, but in several cases, we noted that I-Soon had first obtained accesses or data it thought might be of interest to their customers and would then attempt to sell them. In such cases, they would extract a few documents to be pitched to clients as samples, in the hope to convince them the target was indeed relevant. Some conversations hint at the fact that I-Soon could maintain dormant infections in specific networks in the hopes of finding a customer in the future.

We compiled references to all I-Soon's targets in the leak to demonstrate the scope of their activities. It should be noted that:

- It is possible that I-Soon would have falsely claimed to have breached certain organizations in marketing documents;
- Conversely, it is almost certain that the view on I-Soon's targeting offered by this leak is only partial, and that many more victims, not mentioned in any documents, exist;
- For some cases, lacking contextual information, we could not determine if the mentioned organizations were breached, or only considered for intrusion. We opted to list them anyway as they still provide relevant information about I-Soon's interests.

South Asia and Central Asia	Pakistan	Punjab Anti-Terrorism Center
		Pakistani government postal service
		Punjab Police Postal Service
		Perouz Police Station Post Service
		Zong (mobile operator)
	Afghanistan	National Security Council intranet
		Postal service
		Southeast Asia Anti-Terrorism Center postal service
	Kyrgyzstan	Diplomatic Oil Service
		National Security Council Oil Service
		Megacom
	Kazakhstan	Kcell and Beeline (mobile operators)
		RDP access to “Defense Mail Service”
		Pension Fund
		Air Astana
	India	Ministries of Foreign & Home Affairs, Defense, Finance
		Indian Employees Provident Fund

		Apollo hospital chain
	Nepal	Presidential Palace
		National Defense
		Foreign Affairs
South-East Asia	Malaysia	Ministries of Foreign Affairs, Home Affairs and Works
		Military Network
	Thailand	Prime Minister’s Office
		National Intelligence Agency
		Ministries of Finance and Commerce, Interior, Digital Economy and Safety, Defense
		Armed Forces Preparatory School & Thai Army HQ, Communications
		Navy & Railway
		Thailand Royal Government Development Agency (“can be used to supply chain”)
		Geo-Informatics and Space Technology Development Agency
	Vietnam	Chiang Mai University
		Academy of Social Sciences
		Unspecified telecom operator
		Vietnam Airlines

	Myanmar	Myanmar Post and Telecommunications
	Cambodia	Ministry of Economy and Finance
	Indonesia	Ministry of Foreign Affairs
East Asia	Mongolia	Ministry of Foreign Affairs
		Police
		Mongolia Telecom & Skytel
	Taiwan	National Taxation Bureau of Taipei
		Ministry of Foreign Affairs
		National Taiwan University Hospital
		Tamkang University
		Institute of Applied Mechanics, National Taiwan University
	South Korea	Institute of Sejong Science and Culture Laboratory
	Philippines	Navy Postal Service
	China	Air Macau
	Tibet	Central Tibetan Administration
Europe	United Kingdom	Home office
		Ministry of Foreign Affairs (already taken by another contractor)

		Ministry of Justice
		British treasury
		Department for Business, Energy and Industrial Strategy
		Department for Environment, Food and Rural Affairs
		Department of Health and Social Care
		Department for Transport
		Department for Exiting the European Union
		National Crime Agency
		Center for Foreign Policy Studies
		Chatham House
	France	Sciences Po
	Romania	Ministry of Finances
	Macedonia	Secretariat of European Affairs
America	United States of America	Center for Foreign Policy Studies
	Peru	Armed Forces Joint Command
Middle East	Turkey	Scientific and Technological Research Council of Türkiye
	Palestine	Prime Minister’s Office

Oceania	Papua New Guinea	Department of the Prime Minister & National Executive Council
Africa	South Africa	South African Special Forces Brigade
	Ethiopia	National Bank of Ethiopia
	Egypt	Unspecified government targets

Needless to say, this is a very impressive list of victims (spanning all over the 5 continents), especially considering the size of I-Soon and its relatively unsophisticated intrusion methods. An internal document indicates that in 2022, the company planned on developing accesses in Afghanistan, Syria, Uzbekistan and Iran.

I-Soon's core focus appears to have been government and military organizations as well as education bodies located all around China, with the occasional targeting outside of this region as possible specific customer requests. In addition to those organizations, we noted from the leaked documents that I-Soon also went after the personal email or social media accounts of individuals. In one case, we could discover the identity of the target (based on their email address in a screenshot), who was a sales executive of an iron sheets manufacturing company in Bangladesh.

The leak contains a few references to NATO countries, but overall, they seemed to be of little interest to customers. This observation is consistent with the notion that targeting of various areas is roughly spread among the security bureaus of the country's many provinces. A notable exception is the massive targeting of UK organizations, for which we couldn't find a compelling explanation; maybe one of I-Soon's customers was heavily focused on the country. Finally, NGOs and think tanks such as Amnesty International, Human Rights Watch and RAND Institute Europe were also targeted.

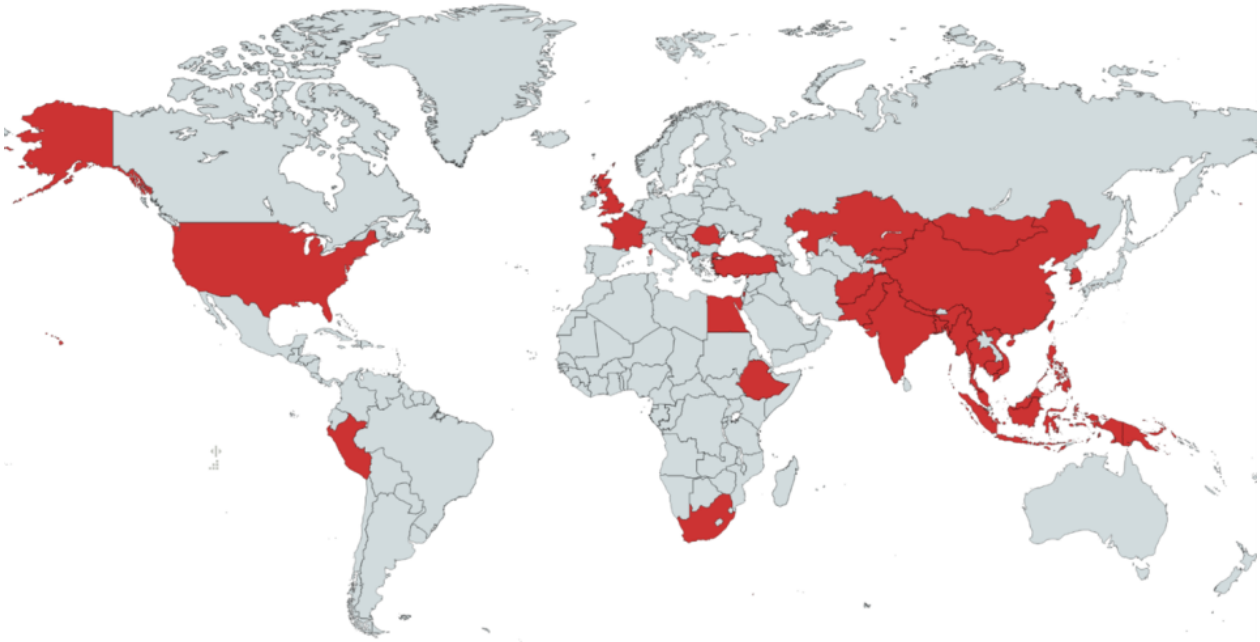

Figure 16: Countries targeted by I-Soon, as self-reported in the internal documents

Of note, I-Soon went after airline companies, likely to obtain Passenger Name Records (PNR), as well as telecommunication operators. Regarding the latter, the leak contains excerpts of Call Detail Records (CDR) and listings of Base Transciever Stations (BTS). This data allows the attackers to learn, for a specific subscriber (based on their phone number), who they called or called them, for how long, and where they were located when those calls took place. All this information is considered valuable intelligence material.

Links to previously documented APT activities

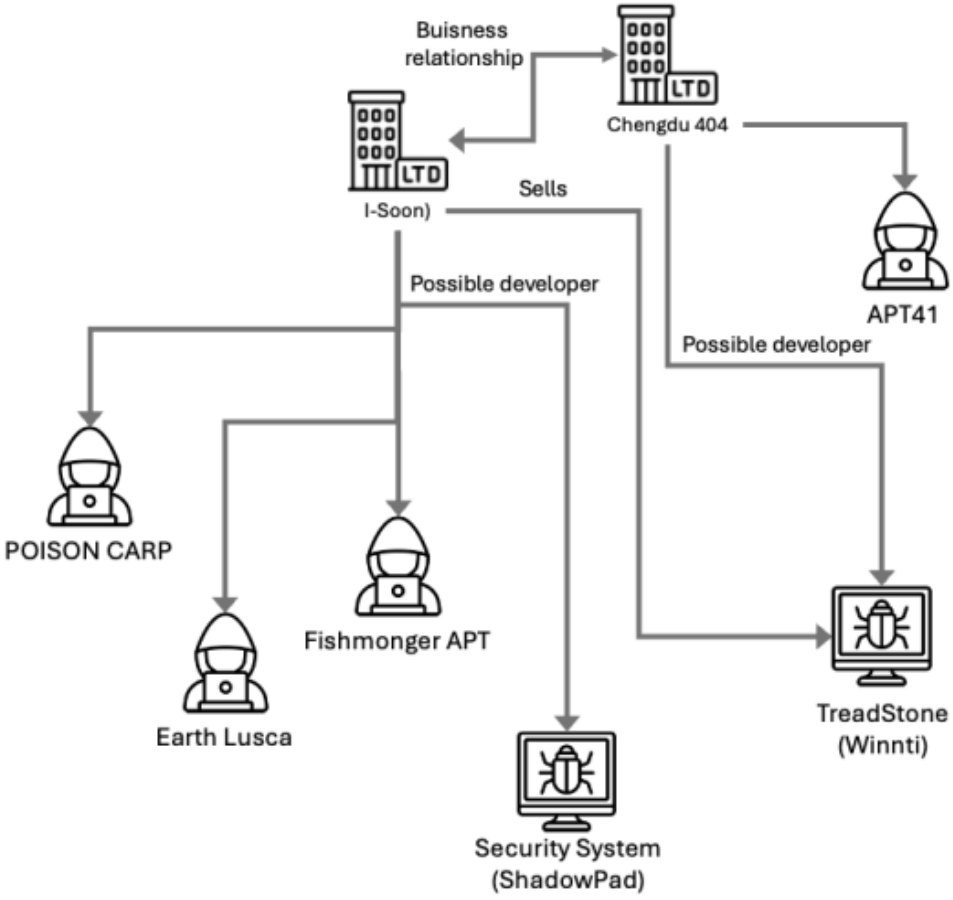

Figure 17: Links between I-Soon and known APT activities

Thanks to indicators contained in the leak (i.e., IP addresses or domains mentioned in chat logs or shown on product screenshots), researchers were able to tie the activities of I-Soon to known APT activities.

- ESET announced that campaigns they were tracking under the alias Fishmonger matched I-Soon's activities. Fishmonger was notably going after universities in Hong Kong in 2020 using the Winnti and ShadowPad malware.
- Trend Micro has attributed Earth Lusca's activities to I-Soon, citing similar targeting, the use of the Winnti and ShadowPad malware, and noted that "*Earth Lusca's source IP addresses are from Chengdu, Sichuan province, where the main office of I-Soon's penetration teams is also located.*" In the chat logs, an employee shares credentials to a machine whose IP address (8.218.67[.]52) was listed as a C2 in one of TrendMicro's reports on a supply-chain attack.
- Another IP address referred to in the chat logs as "the platform" (74.120.172[.]10) corresponded to mailnotes[.]online, listed in a Citizen Lab report on mobile attacks targeting the Tibetan community.
- An implant controller screenshot reveals the address 31.3[.]116, recorded by Sentinel One as a ShadowPad C2. They noted at the time that ShadowPad was used by APT41, Team Tonto, Fishmonger, and others.

- As mentioned previously, a screenshot for the Linux RAT carries the internal name “Treadstone”, a Winnti controller mentioned in FBI’s 2020 indictment of Chengdu 404.
- Security researchers working for other vendors confirmed to us that activities related to indicators contained in this leak matched campaigns that were not publicly discussed.

On that note, Chengdu 404 is another local company offering cybersecurity services and accused of being linked to APT41. I-Soon and Chengdu 404 had a business relationship, although they are currently undergoing litigation for unknown reasons. In an internal chat, I-Soon’s CEO confirms the FBI’s attribution:

2020-09-16 23:51:18	lengmo	Shutd0wn	FBI adds 5 Chinese APT41 hackers to its Cyber's Most Wanted List
2020-09-16 23:51:42	lengmo	Shutd0wn	Fuck
2020-09-16 23:51:44	lengmo	Shutd0wn	Fuck
2020-09-16 23:51:47	lengmo	Shutd0wn	Something happened
2020-09-16 23:51:53	lengmo	Shutd0wn	404 was exploded
2020-09-16 23:52:05	Shutd0wn	lengmo	Awesome
2020-09-16 23:52:26	lengmo	Shutd0wn	My day
2020-09-16 23:52:30	lengmo	Shutd0wn	All photos
2020-09-16 23:52:37	Shutd0wn	lengmo	Hahahahaha
2020-09-16 23:53:24	Shutd0wn	lengmo	No. 41
2020-09-16 23:53:38	Shutd0wn	lengmo	Tell them to drink 41 drinks next time

Figure 18: I-Soon’s CEO discusses Chengdu 404 being unmasked as APT41

Shortly thereafter, they go into damage control mode, double-checking that they don’t have any association with Chengdu 404. Another conversation reveals that the two companies had a non-poaching agreement.

Assessment

These leaks contain several takeaways, some less obvious than others. For starters, looking at the products offered by I-Soon, one cannot help but notice the major focus on data exploitation. While we would have expected mostly software vulnerabilities and malware, the company instead offers platforms whose role is to help analysts handle stolen data. This indicates to us that there is little market demand for bespoke offensive software (or that the demand is adequately fulfilled already). Local threat actors don’t appear to have any issues gathering intelligence; in fact, they’re so efficient at it that they cannot handle the volume. The use of AI technologies to support analysts is particularly noteworthy in this regard, and

there is little doubt that future versions will rely on LLMs. Products are primarily marketed towards public customers, as evidenced by the omnipresent legal vernacular: “cases”, “evidence collection”, “forensics”, etc.

On the tooling front, I-Soon’s catalog is rather underwhelming. The company doesn’t appear to produce innovations and is content with repackaging existing open-source technologies in homemade GUIs. I-Soon aims for ease-of-use, not sophistication. We assess with medium-to-high confidence that this position is dictated by the local market, where customers (police forces, military, etc.) are in the process of scaling up operations but face a skill gap during which tasks are conducted by workers of limited technical skills. Various chat logs from the leak allude to the challenges posed by talent acquisition for companies like I-Soon, and lowering the bar for entry is a sound strategy.

We would like to underline that contrary to initial reporting, the company’s social-media influence products were likely oversold to their customers. Specifically, their Twitter platform doesn’t appear to offer much more than monitoring and phishing of select accounts and is likely incapable of organizing a noticeable information warfare operation.

The common features observed in all tools we looked at also shed light on a very vertical work organization. Almost all platforms advertise extensive logging and auditing features. Employees receive tasks, their activities can be reviewed and scored. A paradox is that I-Soon, as a company, appears to benefit from enough autonomy that it can go after targets of its own choosing. Yet at the employee level, the tools they use seem to have been designed explicitly for micromanagement.

When it comes to I-Soon’s own APT operations, we would qualify them as “crude”. While public reporting shows they experimented with vectors such as supply-chain attacks, their main method of ingress appears to be phishing. Internal conversations make it clear that I-Soon lacks the ability to work on vulnerability research, and they appear to have trouble sourcing malware implants. OPSEC-wise, we cannot help but notice that I-Soon used the implants sold to their customers for their own operations, discussed (or approved) attacks on instant messaging platforms, explicitly mentioned victim names, etc. We would also like to remind that region specialists had been discussing I-Soon’s activities before the leak.

Despite all that, a sobering observation is that I-Soon was able to run massive and global hacking campaigns, affecting victims across many verticals during the past 10 years. Despite their low-sophistication methods, the “APT research team” met dazzling operation success and was able to extract intelligence from countless government bodies and telecommunication networks.

Conclusion

Harfang Lab's CTR team assesses that this leak is extremely damaging, in the sense that it:

- Exposes and allows correlation of past operations;
- Cripples I-Soon's reputation, especially with regards to its public customers;
- Embarrasses the Chinese government, which immediately distanced itself from the company.

The leaks betrayed low company morale overall and we expect that they will worsen the situation – especially after the publication of salary grids. On the other hand, to the best of our knowledge, Chengdu 404 is still operating years after the FBI's indictment… proof that local companies can survive being exposed.

On a grander scale, the leaks provide unique insight into how the public and private sector intertwine and complement each other in China when it comes to cybersecurity. It is highly likely that I-Soon is only an example of such partnerships: even if it were to fall, others would take its place.

We expect I-Soon's activities to continue in the future.

Indicators of Compromise

Note: the following indicators are outdated and presented for reference and historical value only. We strongly discourage using them to block network communications with security products.

```
101.219.17[.]111
118.31.3[.]116
1.192.194[.]162
171.88.142[.]148
171.88.143[.]37
171.88.143[.]72
221.13.74[.]218
66.98.127[.]105
66.98.127.105.16clouds[.]com
74.120.172[.]10
74.120.172.10.16clouds[.]com
8.218.67[.]52
mailnotes[.]online
```

Annex I – I-Soon government customers, as reported on their website

- 中华人民共和国公安部 – Ministry of Public Security of the People's Republic of China
- 北京市公安局 – Beijing Municipal Public Security Bureau
- 广东省公安厅 – Guangdong Provincial Public Security Department

- 江苏省公安厅 – Jiangsu Provincial Public Security Department
- 河南省公安厅 – Henan Provincial Public Security Department
- 重庆市公安局 – Chongqing Municipal Public Security Bureau
- 内蒙古自治区公安厅 – Public Security Department of Inner Mongolia Autonomous Region
- 宁夏回族自治区公安厅 – Public Security Department of Ningxia Hui Autonomous Region
- 广西壮族自治区公安厅 – Public Security Department of Guangxi Zhuang Autonomous Region
- 新疆维吾尔自治区公安厅 – Public Security Department of Xinjiang Uyghur Autonomous Region
- 西藏自治区公安厅 – Public Security Department of Tibet Autonomous Region
- 青海省公安厅 – Qinghai Provincial Public Security Department
- 甘肃省公安厅 – Gansu Provincial Public Security Department
- 陕西省公安厅 – Shaanxi Provincial Public Security Department
- 黑龙江省公安厅 – Heilongjiang Provincial Public Security Department
- 吉林省公安厅 – Jilin Provincial Public Security Department
- 辽宁省公安厅 – Liaoning Provincial Public Security Department
- 山东省公安厅 – Shandong Provincial Public Security Department
- 山西省公安厅 – Shanxi Provincial Public Security Department
- 河北省公安厅 – Hebei Provincial Public Security Department
- 天津市公安局 – Tianjin Municipal Public Security Bureau
- 上海市公安局 – Shanghai Municipal Public Security Bureau
- 浙江省公安厅 – Zhejiang Provincial Public Security Department
- 安徽省公安厅 – Anhui Provincial Public Security Department
- 福建省公安厅 – Fujian Provincial Public Security Department
- 江西省公安厅 – Jiangxi Provincial Public Security Department
- 湖南省公安厅 – Hunan Provincial Public Security Department
- 湖北省公安厅 – Hubei Provincial Public Security Department
- 四川省公安厅 – Sichuan Provincial Public Security Department
- 贵州省公安厅 – Guizhou Provincial Public Security Department
- 云南省公安厅 – Yunnan Provincial Public Security Department
- 海南省公安厅 – Hainan Provincial Public Security Department

Acknowledgements

The authors would like to thank the following researchers for their much appreciated comments on this report:

- Joan Calvet, for pointing out that the Hector malware had incorrectly been categorized as a Windows implant;
- Ian Roos, who provided us with the correct e-mail address corresponding to the GitHub account.

[1] Ironically, as will be shown below, I-Soon itself had invested a lot in such tools to analyze gathered intelligence.

[2] All text from the original leak is in Chinese language. English excerpts presented in this report come from machine translations.

[3] Commercial documents allude to a testing procedure on delivery day, to take place in the presence of members of I-Soon and the client. Statements on AV evasion are only valid for the day of the delivery and are supposedly demonstrated at that moment.

[4] Due to the scattered nature of the leak, we assume that the source-code delivery option applies to this implant with a high degree of certainty, but cannot say it categorically.

[5] We understand the horse emoji as a symbol for “trojan horse” in various discussions.

[6] One conversation mentions a Mikrotik 0day, and another one the Juniper SRX firewall series.

[7] The documentation specific to this platform only mentions phishing links.

[8] It is, however, unclear which of these platforms was released first.

Published on 1 March, 2024 Last update on 21 March, 2024