Lessons from the iSOON Leaks

BushidoToken ⁝⁝ 2/23/2024

Introduction

- A Chinese Ministry of Public Security (MPS) contractor called iSOON (also known as Anxun Information) that specializes in network penetration research and related services has had its data leaked to GitHub.
- Preliminary findings from less than one week since the leak revealed that it contains unprecedented insights into how the Chinese MPS operates by using Chinese commercial surveillance vendors and what their technical capabilities are.
- The Chinese MPS is China’s internal security service that primarily focuses on internal and border security, counter-terrorism, surveillance. The MPS is comparable to the Russian FSB, the US DHS or the UK’s MI5.
- The most interesting findings have come from iSOON’s product whitepapers and confidential slide deck presentations given to their MPS clients.

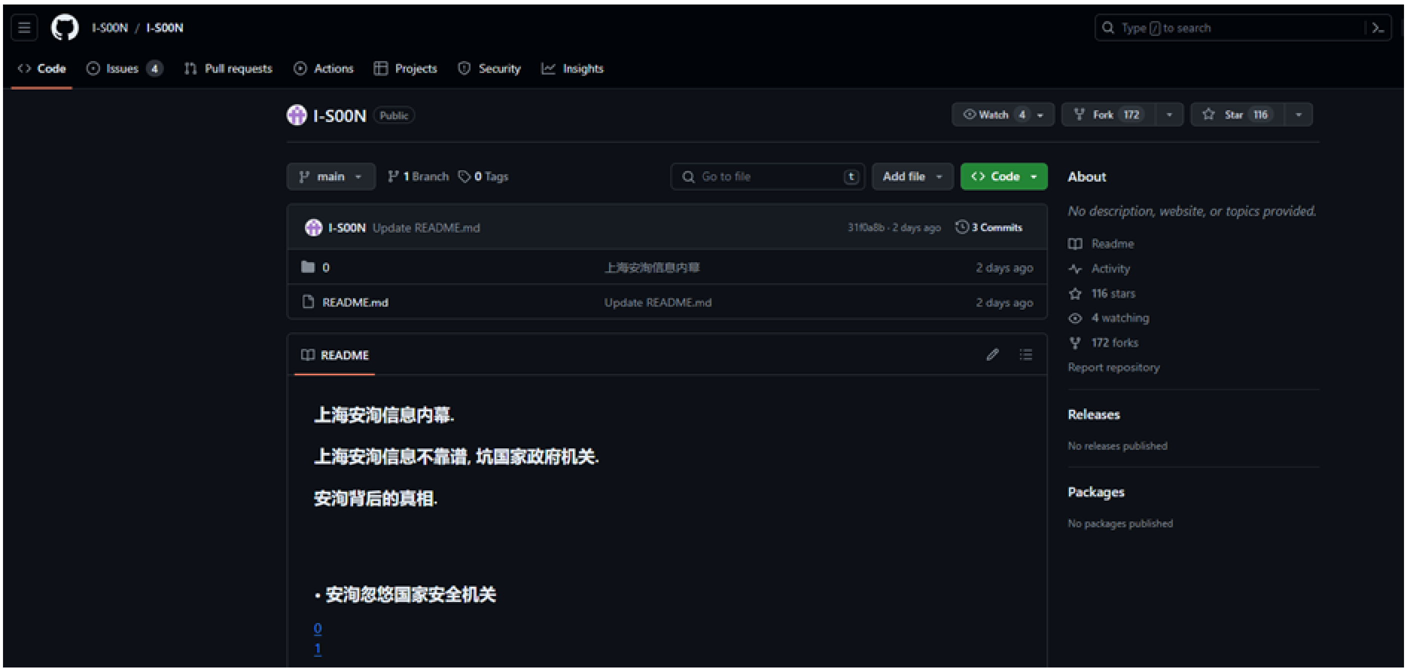
About the iSOON Leak

The iSOON leak has revolutionized the open source intelligence (OSINT) community's general understanding of the Chinese MPS' cyber operations. Its significance is comparable to the NTC Vulkan leak that impacted the Russian military intelligence (GRU) and Russian federal security service (FSB) as well as the Snowden Leak or the Shadow Brokers Leak, both of which impacted the US National Security Agency (NSA).

The leak is around 170MB and contains images of documents in Mandarin. They were machine translated to English for this blog. Therefore, not all of the facts will be available for a some time as the community digs in and there may be some misunderstandings in this blog due to not being a Chinese-speaking analyst myself.

The company, iSOON has had a long development history. Established in 2010, iSOON has been involved in various activities related to "network penetration research" and "overseas special case network work" and has conducted national training programs on network security. They have received commendations from CCP ministerial and central leaders for their contributions. In 2019, iSOON was selected as one of the first units installed by the Cyber Security Bureau of the MPS.

On 16 February 2024, a GitHub repository ("github[.]com/I-S00N/I-S00N") containing the data dumped from iSOON was uploaded to the site by an unknown source:



No description, website, or topics provided.

I-S00N Update README.md 31f0a8b · 2 days ago 3 Commits

0	上海安洵信息内幕	2 days ago
README.md	Update README.md	2 days ago

上海安洵信息内幕.

上海安洵信息不靠谱, 坑国家政府机关.

安洵背后的真相.

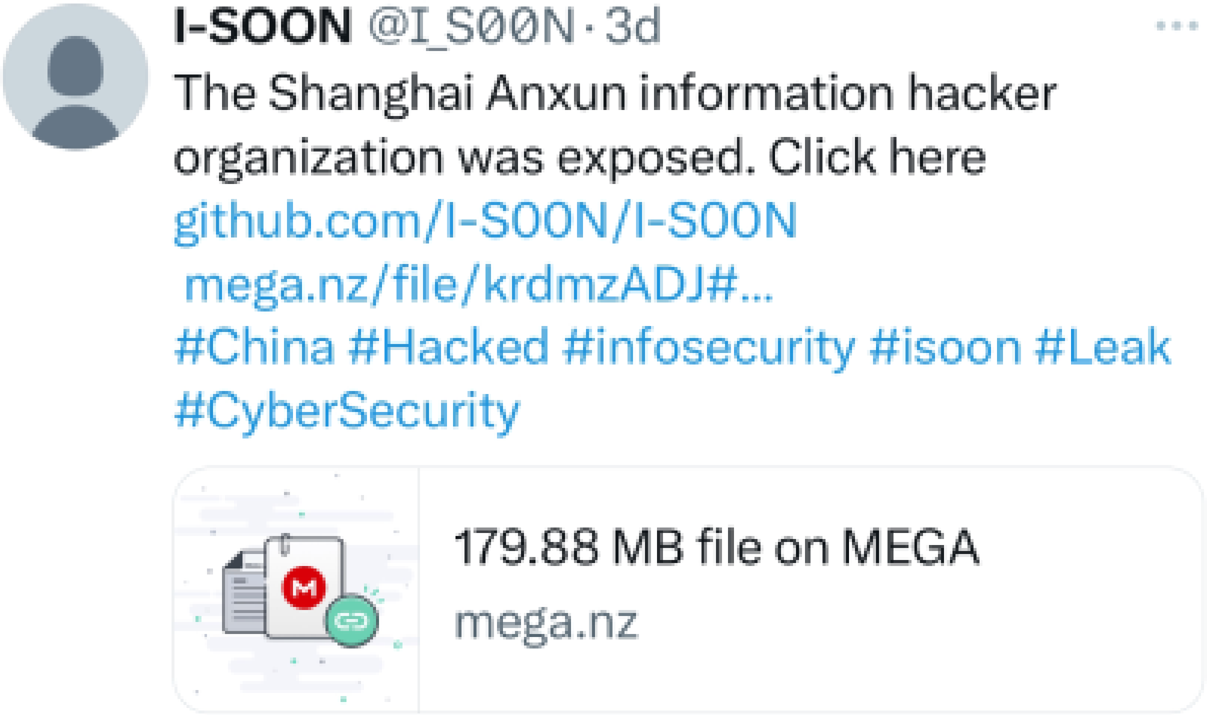
- 安洵忽悠国家安全机关

0
1

No releases published

No packages published

And also on Twitter:



I-SOON @I_S00N · 3d

The Shanghai Anxun information hacker organization was exposed. Click here github.com/I-SOON/I-SOON mega.nz/file/krdmzADJ#... #China #Hacked #infosecurity #isoon #Leak #CyberSecurity

179.88 MB file on MEGA
mega.nz

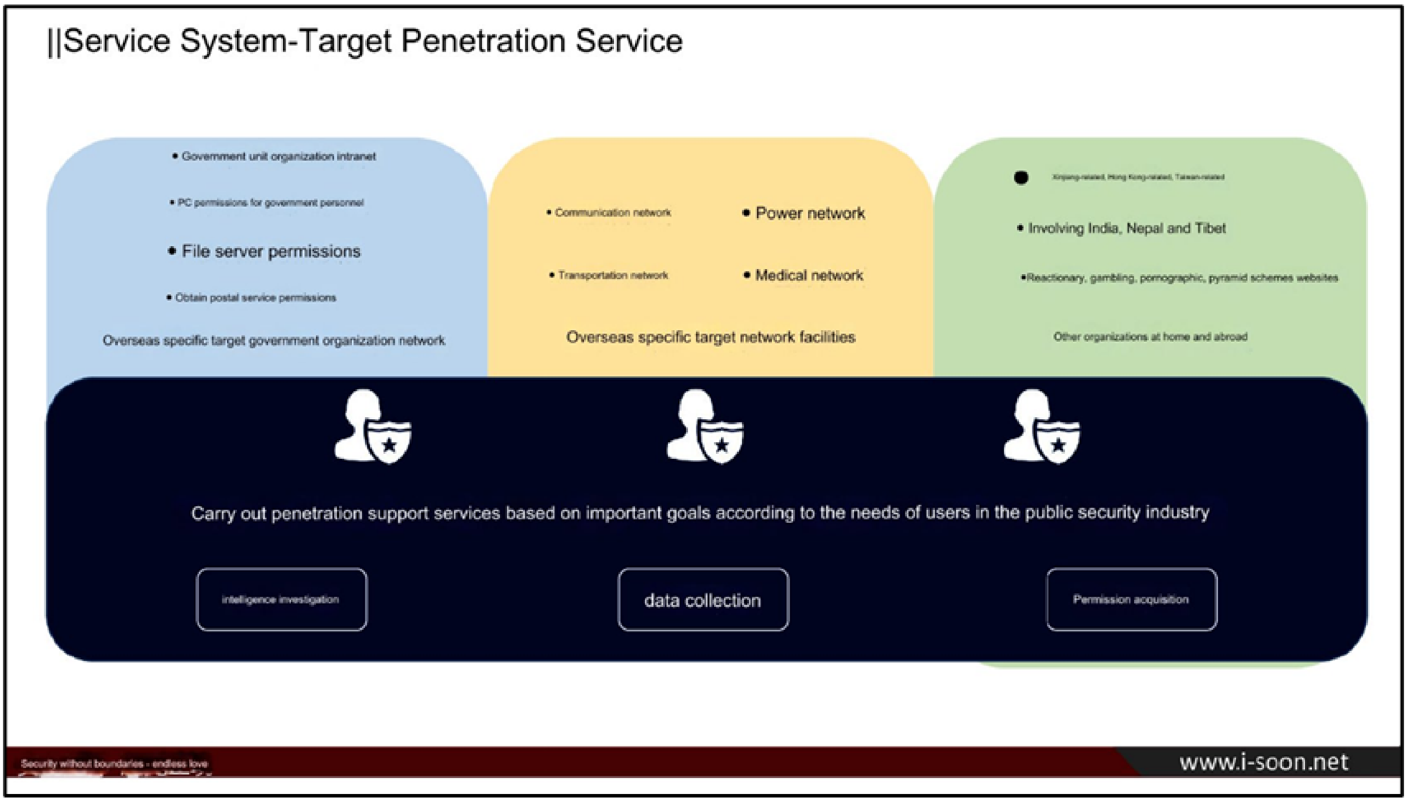
iSOON's Services

According to an iSOON presentation in the leak, the structure of firm includes three penetration teams, one security research team, and one basic support team, comprising a total of around 70 people.

Their primary targets are countries and regions such as Central Asia, Southeast Asia, Hong Kong, Macao, and Taiwan. iSOON offers services such as "APT Service System," "Target Penetration Services," and "Battle Support Services" to their MPS clients.

They have also reportedly targeted various regions in China, including Xinjiang and Tibet, which includes dissidents, illegal gambling rings, illegal pornography rings, as well as illegal pyramid schemes (which all come under MPS jurisdiction).

Notably, iSOON featured in a slide deck their attacks on the Indian and Nepalese governments, targeting government departments such as the Ministry of Foreign Affairs, Defense, Home Affairs, Finance, and the Nepalese Presidential Palace.



||Service System-Target Penetration Service

- Government unit organization intranet
- PC permissions for government personnel
- File server permissions
- Obtain postal service permissions

Overseas specific target government organization network

- Communication network
- Power network
- Transportation network
- Medical network

Overseas specific target network facilities

- Xinjiang-related, Hong Kong-related, Taiwan-related
- Involving India, Nepal and Tibet
- Reactionary, gambling, pornographic, pyramid schemes websites

Other organizations at home and abroad

Carry out penetration support services based on important goals according to the needs of users in the public security industry

intelligence investigation
data collection
Permission acquisition
Security without boundaries - endless love
www.i-soon.net

iSOON's Victims

Fellow security researcher @azakasekai_ also was first to find that the leak contains conversations and spreadsheets about iSOON's victims, including how many terabytes of data has been exfiltrated from certain government entities, telecommunications firms, medical organizations, and academic sectors of countries such as: Pakistan, Kazakhstan, Kyrgyzstan, Malaysia, Mongolia, Nepal, Turkey, India, Egypt, France, Cambodia, Rwanda, Nigeria, Hong Kong, Indonesia, Vietnam, Myanmar, Philippines, and Afghanistan.

Examples of some of the victim organizations include:

- Ministry of Foreign Affairs, Myanmar
- National Taiwan University Hospital
- Tamkang University, Taiwan
- National Intelligence Agency, Thailand
- Ministry of Foreign Affairs, Thailand
- Ministry of Health, Rwanda
- Apollo Hospital, India
- Punjab Anti-Terrorism Center, Pakistan
- Beeline Communications, Kazakhstan
- Tele2 Communications, Kazakhstan
- Skytel Communications, Mongolia
- Ministry of Public Security, Mongolia
- Nepal Telecom
- Chinese University of Hong Kong
- Hong Kong Shue Yan University

- Tung Wah College, Hong Kong
- Paris Institute of Political Studies, France

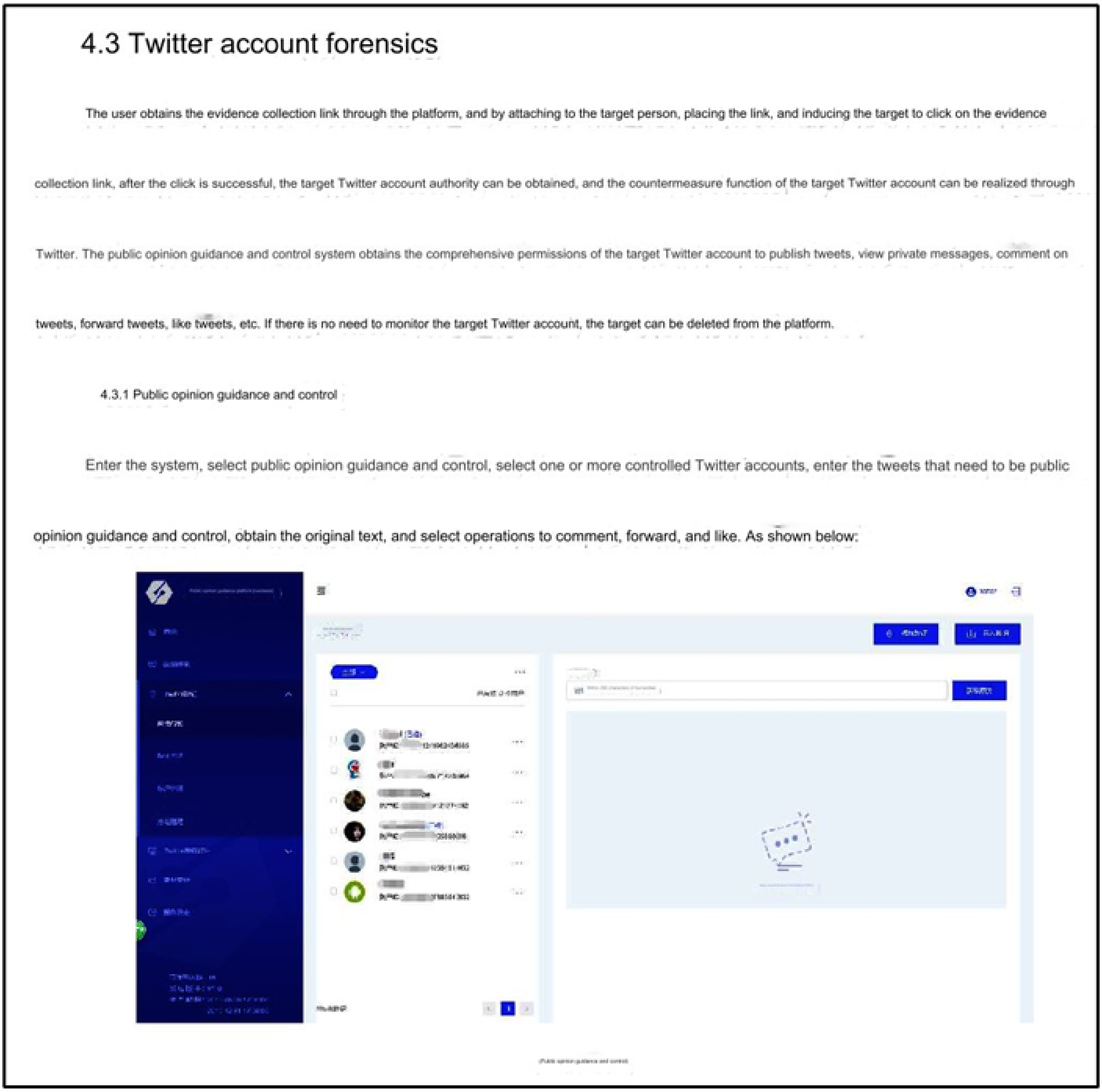
Fellow security researcher @haxrob also noticed that some of the leaked files in the GitHub repository also contain call detail records (CDR) and location based services (LBS) related systems stolen from telecommunications entities. This highlights that the iSOON operators compromised telecommunications entities with the aim to obtain subscriber metadata to support intelligence collection objectives, in support of Chinese MPS requirements. With persistent access to LBS records it would be possible for iSOON and MPS operators to perform real time lookups of a subscriber's location, quite possibly to a very high degree of accuracy.

iSOON's Products

A range of products and tools are offered by iSOON. This includes a "Twitter Public Opinion Guidance and Control System," for monitoring dissidents; custom remote access software for Windows, Linux, macOS, iOS, and Android; custom hardware for "WiFi Proximity Attack Systems," disguised as Xiaomi battery packs; an "Email Analysis Intelligence Decision-Making Platform," an "Individual Tool Box," consisting of various hacking tools; a "Microsoft Email Encryption" platform, for email exfiltration and analysis; and an "Automated Penetration Testing Platform," that combines various public hacking tools into a Software-as-a-Service (SaaS) platform.

Twitter Public Opinion Guidance and Control System

The Twitter Tool whitepaper in the leak was used by iSOON to sell its commercial surveillance platform to the Chinese MPS for monitoring dissents. Notably, the iSOON developers also claimed to have a 1-click exploit to bypass Twitter two-factor authentication (2FA) security controls to gain control over the target’s account. This exploit was to be distributed via Twitter direct messages (DMs) in the form of URLs, which iSOON called forensic links. These forensic links can gain access to the accounts but also gather IP addresses, IP locations, device type, and browser version.



4.3 Twitter account forensics

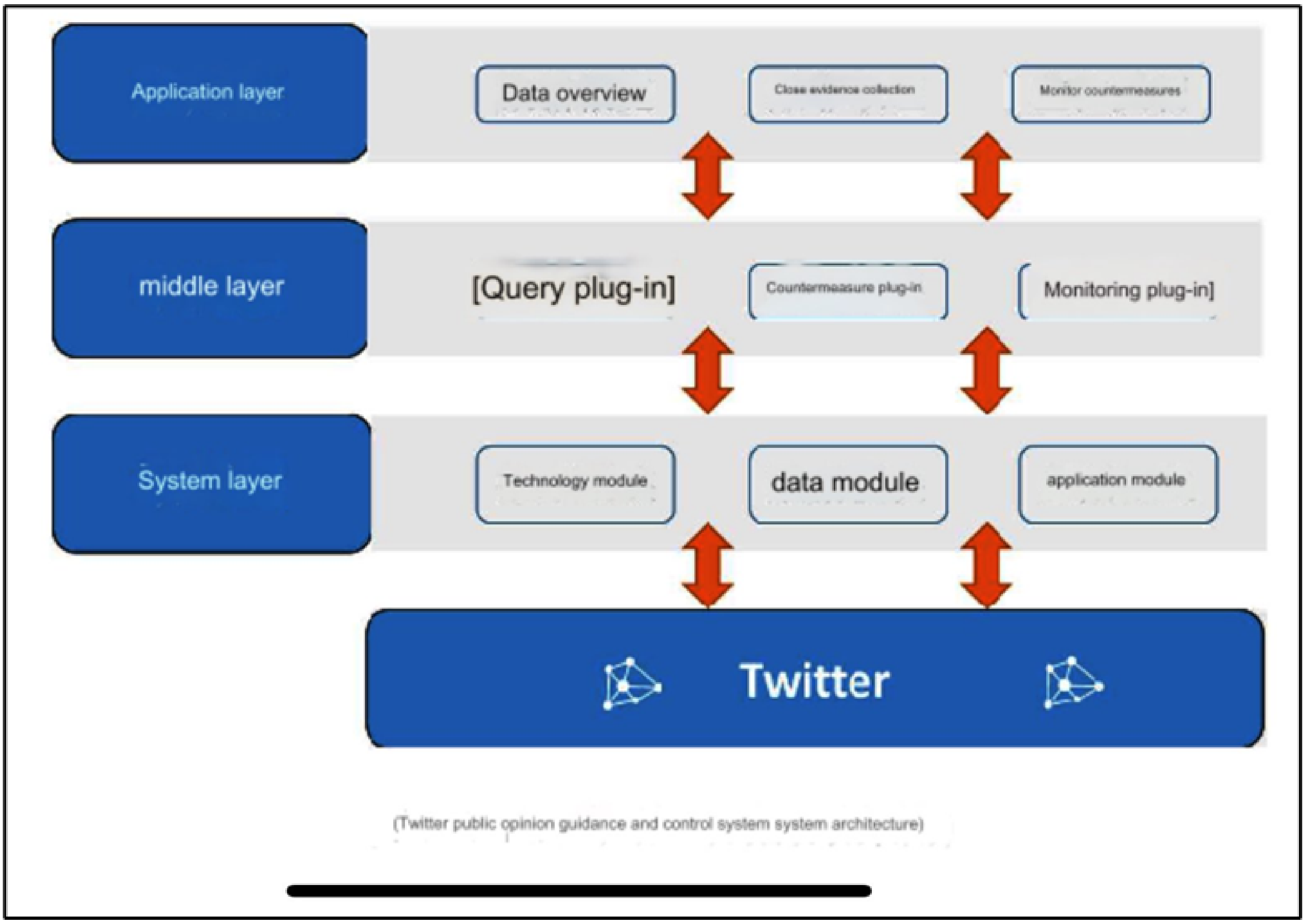
The user obtains the evidence collection link through the platform, and by attaching to the target person, placing the link, and inducing the target to click on the evidence collection link, after the click is successful, the target Twitter account authority can be obtained, and the countermeasure function of the target Twitter account can be realized through Twitter. The public opinion guidance and control system obtains the comprehensive permissions of the target Twitter account to publish tweets, view private messages, comment on tweets, forward tweets, like tweets, etc. If there is no need to monitor the target Twitter account, the target can be deleted from the platform.

4.3.1 Public opinion guidance and control

Enter the system, select public opinion guidance and control, select one or more controlled Twitter accounts, enter the tweets that need to be public opinion guidance and control, obtain the original text, and select operations to comment, forward, and like. As shown below:

(Public opinion guidance and control)

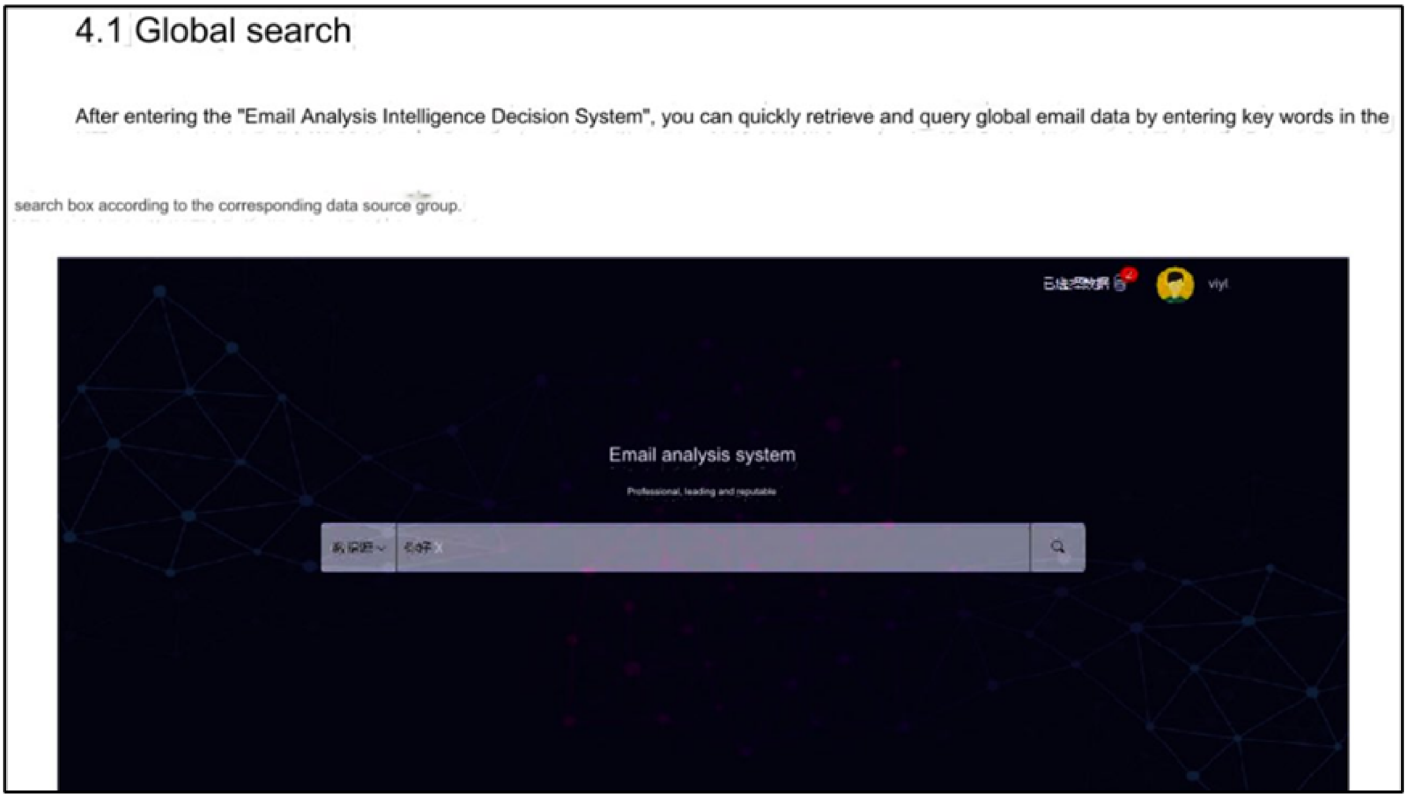
The Twitter Tool whitepaper also showed in detail how the Chinese intelligence services access Western social media services and bypassing the Great Firewall of China. The platform enabled the Chinese MPS to view tweets and Twitter account profiles of target dissidents. The Chinese MPS operators using the iSOON platform could obtain "evidence" using the collection system in the platform, which involves indexing content from Twitter users criticizing the Chinese government.



(Twitter public opinion guidance and control system system architecture)

Email Analysis Intelligence Decision-Making Platform

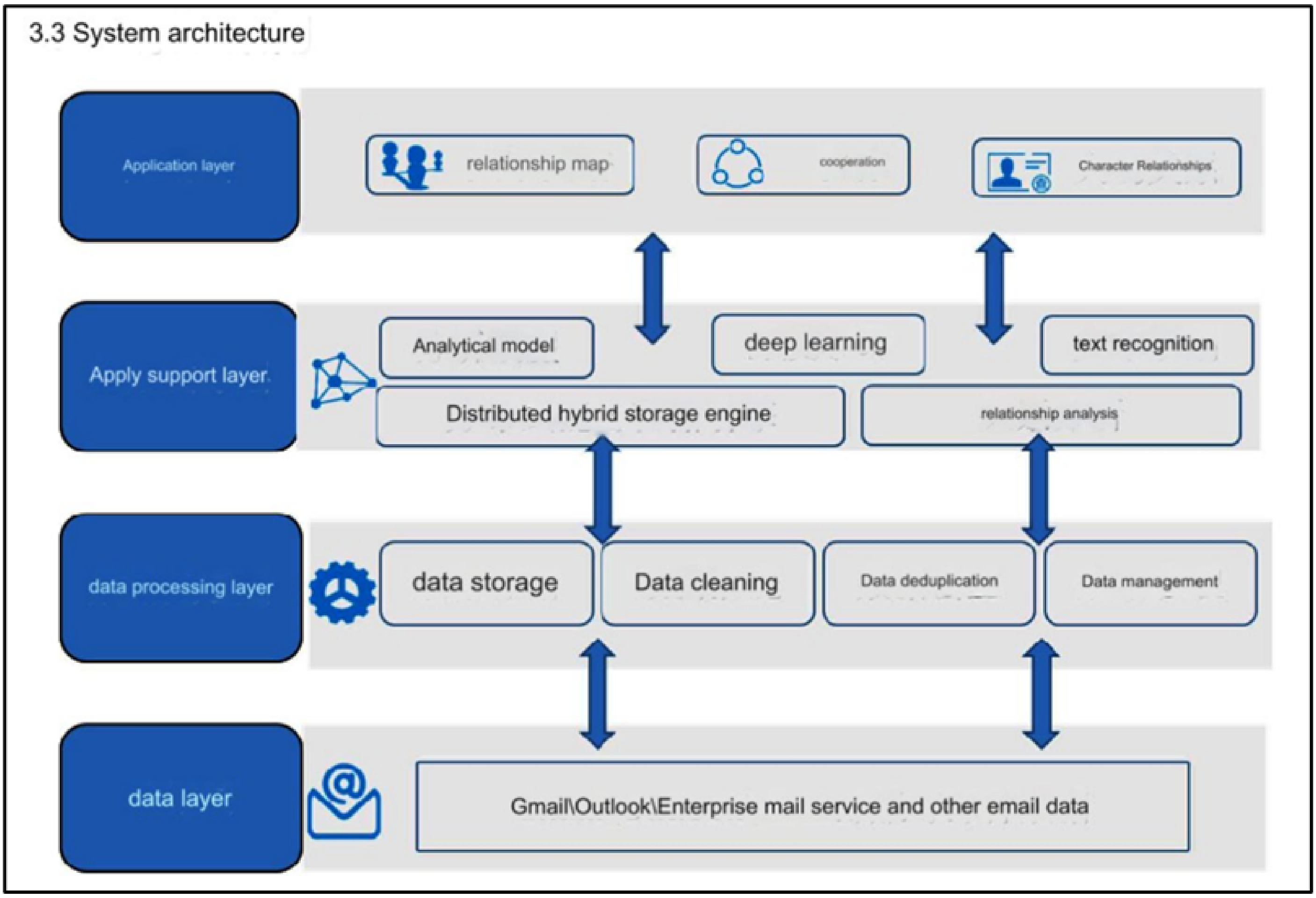
The Email Analysis Intelligence Platform developed by iSOON was sold to the Chinese MPS to support intelligence production from massive amounts of stolen emails. The platform was designed for mass email data analysis that enabled them to mine mailboxes and conversations for personal information, as well as IP addresses from email headers and extract details from email attachments. It boasted that it can handle terabytes of email data and index it for performing keyword searches and performs automatic email translation from any language.



4.1 Global search

After entering the "Email Analysis Intelligence Decision System", you can quickly retrieve and query global email data by entering key words in the search box according to the corresponding data source group.

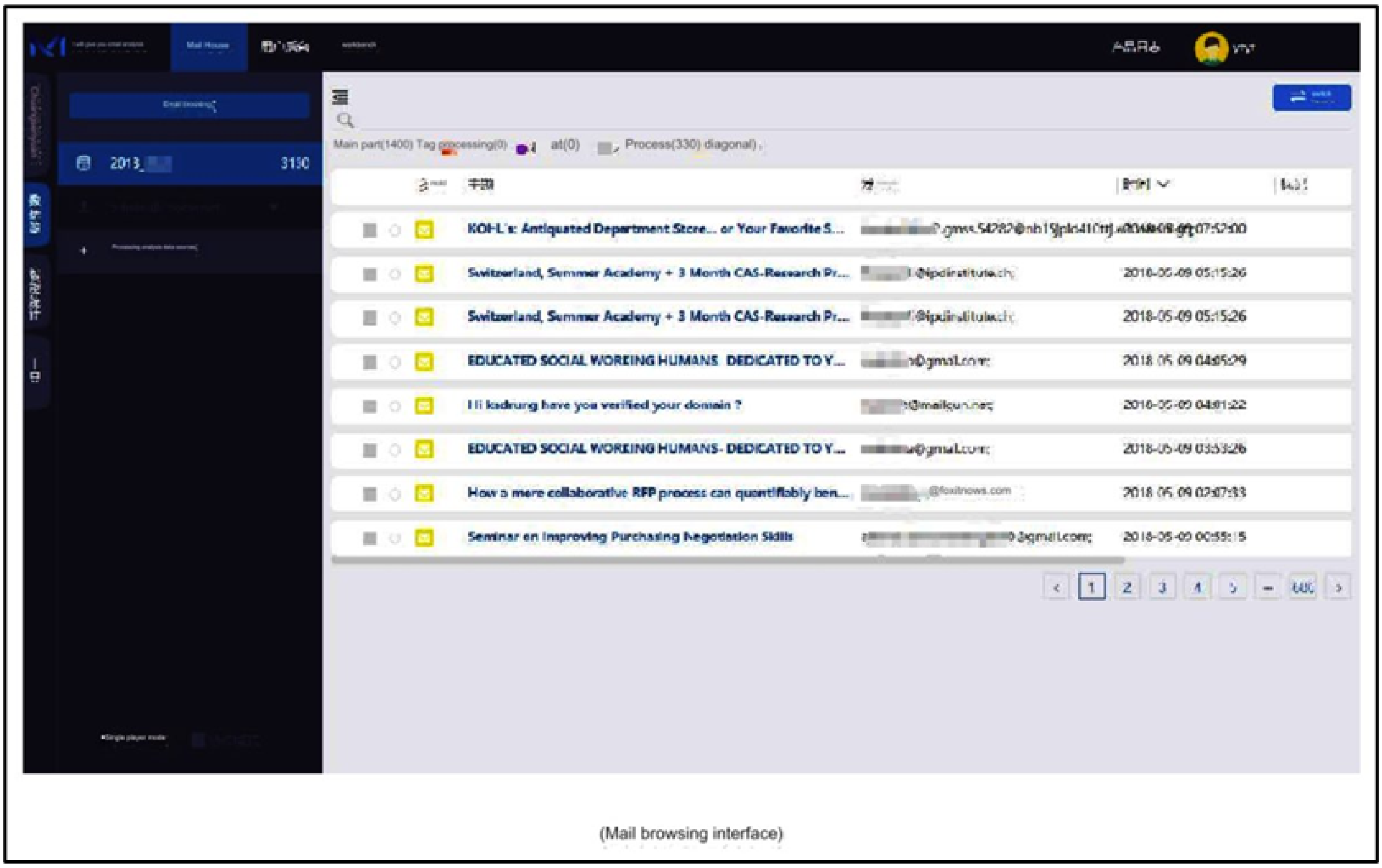
The Email Tool whitepaper included the architecture of the system that enables mass email data analysis using machine learning (ML) algorithms, optical character recognition (OCR), and other methodologies.



3.3 System architecture

One of the notable screenshots from the Email Tool whitepaper showed that the platform can also enable

MPS operators to recreate their target's inbox and read through their stolen emails



Main part(1400) Tag processing(0) at(0) Process(330) diagonal)

KOHL's: Antiquated Department Store... or Your Favorite S...	[redacted]?.gmss.54282@nb19plo410tj	2018-05-09 07:52:00
Switzerland, Summer Academy + 3 Month CAS-Research Pr...	[redacted]@ipdinstitute.ch;	2018-05-09 05:15:26
Switzerland, Summer Academy + 3 Month CAS-Research Pr...	[redacted]@ipdinstitute.ch;	2018-05-09 05:15:26
EDUCATED SOCIAL WORKING HUMANS DEDICATED TO Y...	[redacted]@gmail.com;	2018-05-09 04:45:29
Hi kadrung have you verified your domain ?	[redacted]@mailgun.net;	2018-05-09 04:01:22
EDUCATED SOCIAL WORKING HUMANS- DEDICATED TO Y...	[redacted]@gmail.com;	2018-05-09 03:53:26
How a more collaborative RFP process can quantifiably ben...	[redacted]@foxitnews.com	2018-05-09 02:07:33
Seminar on Improving Purchasing Negotiation Skills	[redacted]@gmail.com;	2018-05-09 00:55:15

< 1 2 3 4 5 … 600 >

(Mail browsing interface)

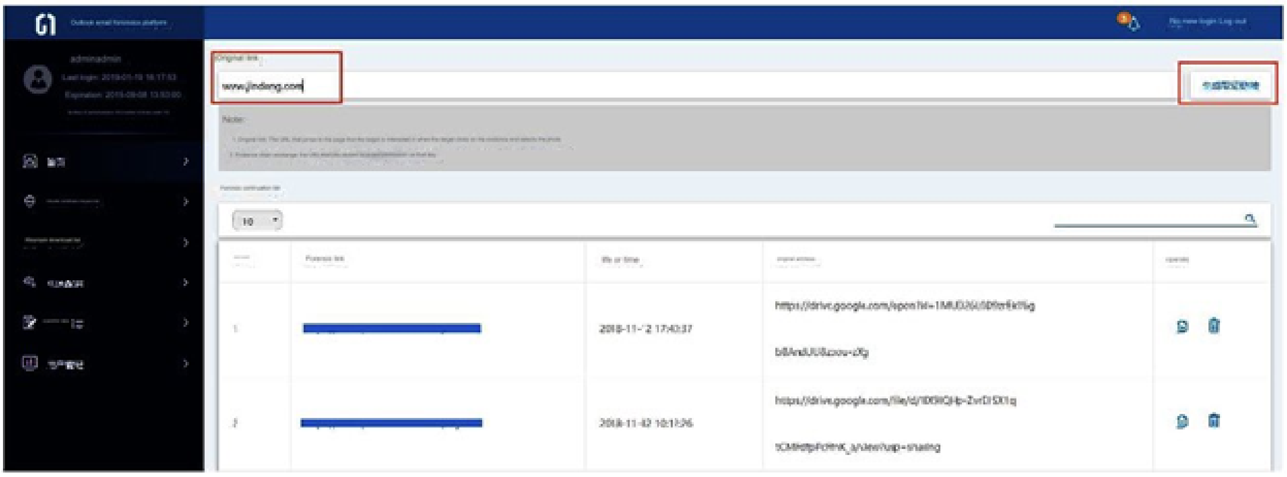
Automated Penetration Testing Platform

Another platform developed by iSOON for the Chinese MPS is used for offensive cyber operations against a range of targets, like those mentions in the iSOON services section above. The automated penetration testing platform is made of various modules built using custom and publicly available tools. It offers capabilities for all sorts of offensive techniques (shown below), such as running phishing campaigns, application exploitation, cross-platform payload generation, and RATs, which includes legitimate remote monitoring and management (RMM) tools.

4 product features

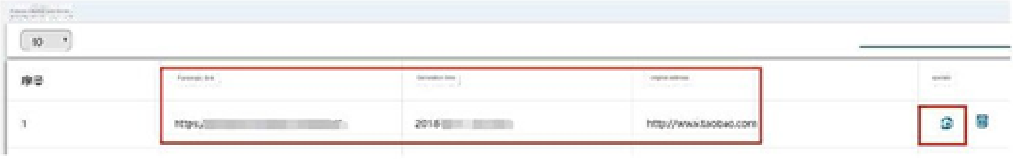
4.1 Generate phishing links

Go to the homepage, enter the original address in the original link box (the original link is the URL that jumps to the page that the forensic target is interested in after clicking on the forensic link), and click "Generate forensic link", as shown in the figure below:



[illegible]	Forensic link	[illegible]	Original address	operate
1	[redacted]	2018-11-`2 17:40:37	https://drive.google.com/open?id=1MUDJ6USDfzrFkf%g b8AndUU&zoou-zKg	
2	[redacted]	2018-11-42 10:17:36	https://drive.google.com/file/d/1D6IIQHp-ZvrDSX1q tCMHdfpFcHhK_s/view?usp=sharing	

After generation, you will see the generated forensic-link in the latest forensic link list (the URL that the user deceives the target to click to obtain its permissions). Click the copy button in the operation to copy the forensic link, as shown in the figure below:



序号	Forensic link	Generation time	Original address	operate
1	https://[redacted]	2018[redacted]	http://www.taobao.com	

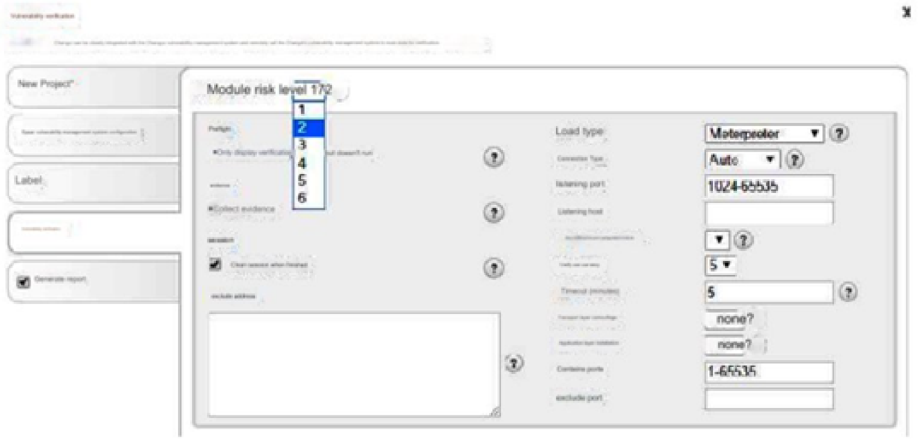
When the original link of the generated forensic link is the same in the forensic link list, the platform will prompt that the generation failed. In this case, you need to use other original links or delete the generated forensic link, as shown in the following figure:

attack. At the same time, the platform supports the import of scanning results and vulnerability verification from a variety of third-party security scanning tools, automatically identifying and importing reports.

In the system, choose to conduct penetration verification on the imported host and corresponding vulnerabilities. After confirming that the vulnerabilities are real, you can attack. Support includes: Green Alliance Extreme

Light, Venus Sky Mirror, AppScan, NeXpose, Acunetix, Core Impact, Nessus, NetSparker,

Nmap et al. As shown below:



New Project*

Label

☑ Generate report

Module risk level 1?2

*Only display verification ... doesn't run

*Collect evidence

☑ Clean session when finished

exclude address

Load type: Meterpreter ▼

Connection Type: Auto ▼

listening port: 1024-65535

Listening host:

▼

5 ▼

Timeout (minutes): 5

none?

none?

Contains ports: 1-65535

exclude port:

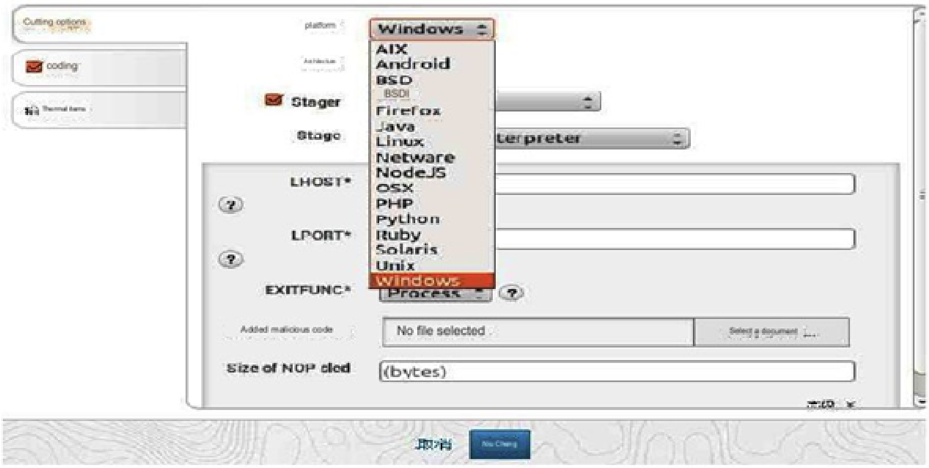
(Exploit interface)

4.8 Load Generator

Classic payload: The platform supports generating a variety of attack payloads for penetration testing. The generated payload supports various operating systems and commonly used web server-side languages, including: Linux, Unix, AIX, BSD, R, Windows, OSX, Netware, iOS, Android, Firefox, Java, Python, Ruby, NodeJS, etc.

Dynamic payload: The system supports the generation of a variety of dynamically encoded attack payloads targeting the Windows platform to evade detection by anti-virus software.

Measurement.



platform: Windows

Stager

Stage: ...terpreter

LHOST*

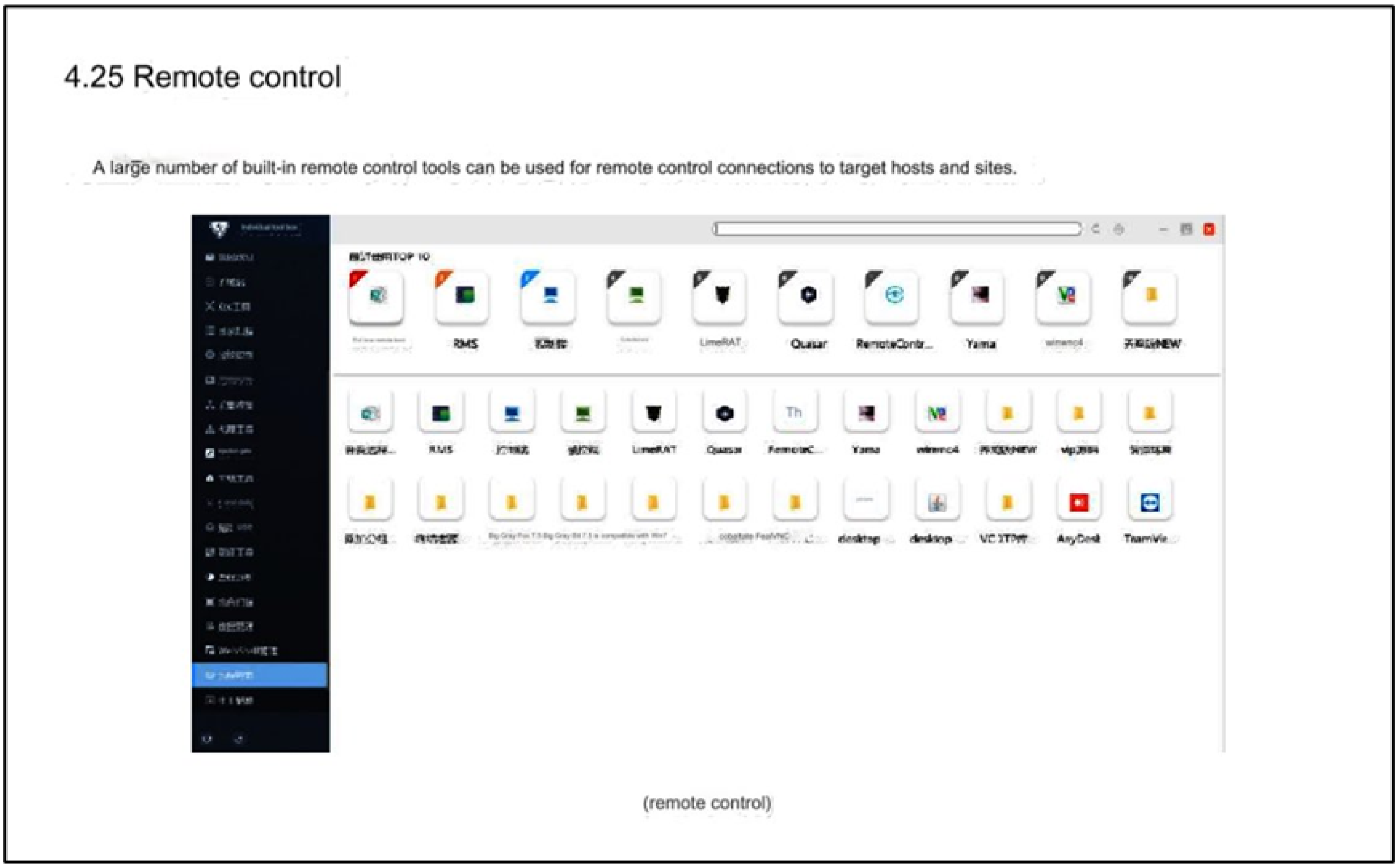
LPORT*

EXITFUNC*: Process

Added malicious code: No file selected

Size of NOP sled: (bytes)

(Load generation)



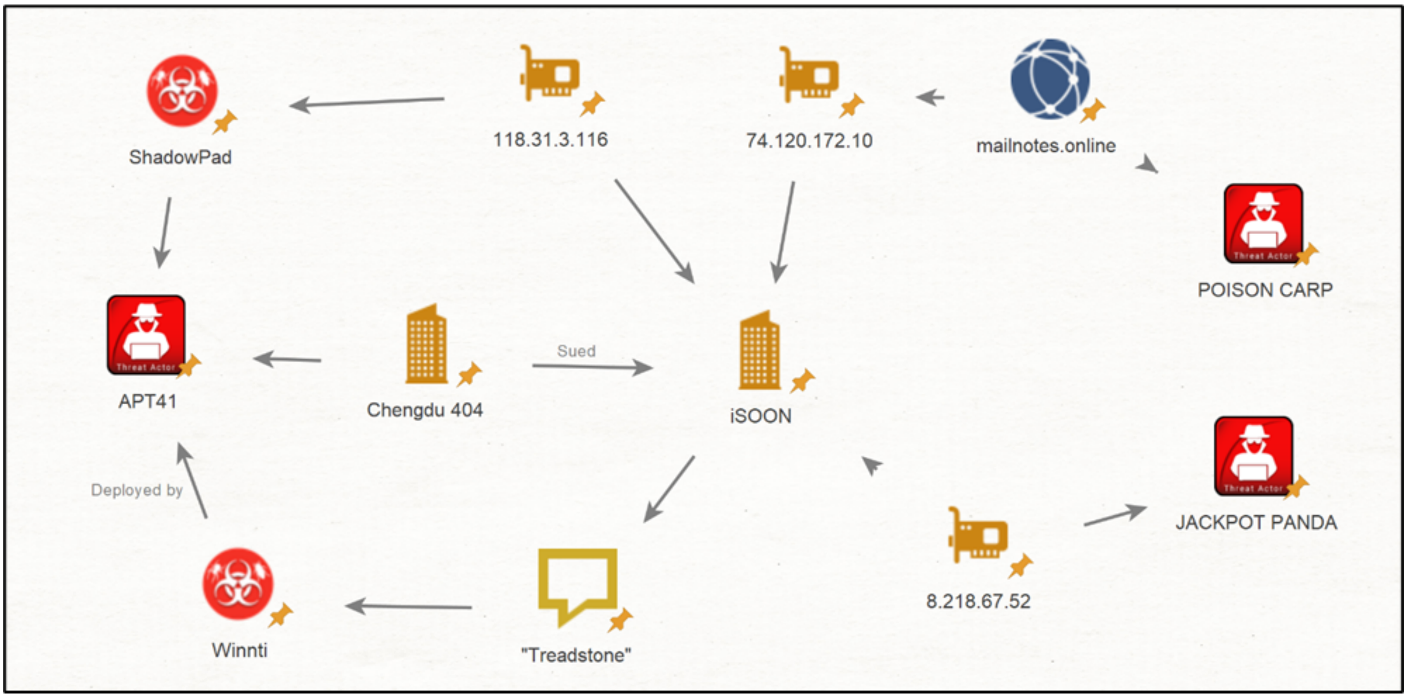
4.25 Remote control

A large number of built-in remote control tools can be used for remote control connections to target hosts and sites.

(remote control)

iSOON Overlaps

Several overlaps and connections associated with iSOON and known threat groups have already been discovered. The company already had a few ties to known Chinese advanced persistence threat (APT) groups such as Chengdu 404 (linked to APT41). Additional ties were uncovered through pivoting on indicators of compromise (IOCs) present in the leak, which adds further legitimacy to the validity of the leak.



The connection to threat group called POISON CARP was via an IP address (74.120.172[.]10) that appeared in the iSOON data leak that hosted a phishing site (mailnotes[.]online). The phishing site was observed as one of the IOCs in CitizenLab's “Tibetan Groups Targeted with 1-Click Mobile Exploits” report, which is in-line with the Chinese MPS’ operations supported by iSOON.

The connection identified between iSOON and another Chinese commercial spying firm called Chengdu 404 was identified in Chinese court documents after the sanctioned firm Chengdu 404 sued iSOON over an intellectual property dispute.

The connection between iSOON and an APT group CrowdStrike track as JACKPOT PANDA was identified through another IP address (8.218.67[.]52) that appeared in the data leak. This IP address was referenced in Trend Micro's report “Probing Weaponized Chat Applications Abused in Supply-Chain Attacks” which appeared to be focused on targeting the online gambling industry, something iSOON also referenced as a target sector in their services slide deck.

Further pivots on some of the IP addresses spotted in the screenshots of the custom Windows malware in the iSOON product whitepapers as well as an overlapping reference to “TreadStone” in US Justice Department’s indictment of APT41 and Chengdu404. This revealed ties to the infamous ShadowPad and Winnti malware families. These custom Windows malware families have been tied to numerous Chinese cyber-espionage campaigns and used by multiple Chinese APT groups.

Using ACH to judge who was responsible for the iSOON leak

Note: *This section of the blog is aimed towards my readers who are CTI professionals as well as those interested in the process of making intelligence assessments. Feel free to skip this part.*

The answer, at the time of writing, is... we simply don't know. However, this is a good opportunity to perform what we call in the intelligence biz Analysis of Competing Hypothesis (ACH) to mitigate our unconscious biases when making an assessment. ACH was developed by Richards Heuer a CIA veteran analyst, who wrote the Psychology of Intelligence Analysis. It can help make judgments that entail a high risk of error in reasoning (in my case, I have only a few years experience investigating Chinese APT groups). The goal of ACH is to help an analyst overcome/minimize, some of my cognitive limitations to provide prescient intelligence analysis.

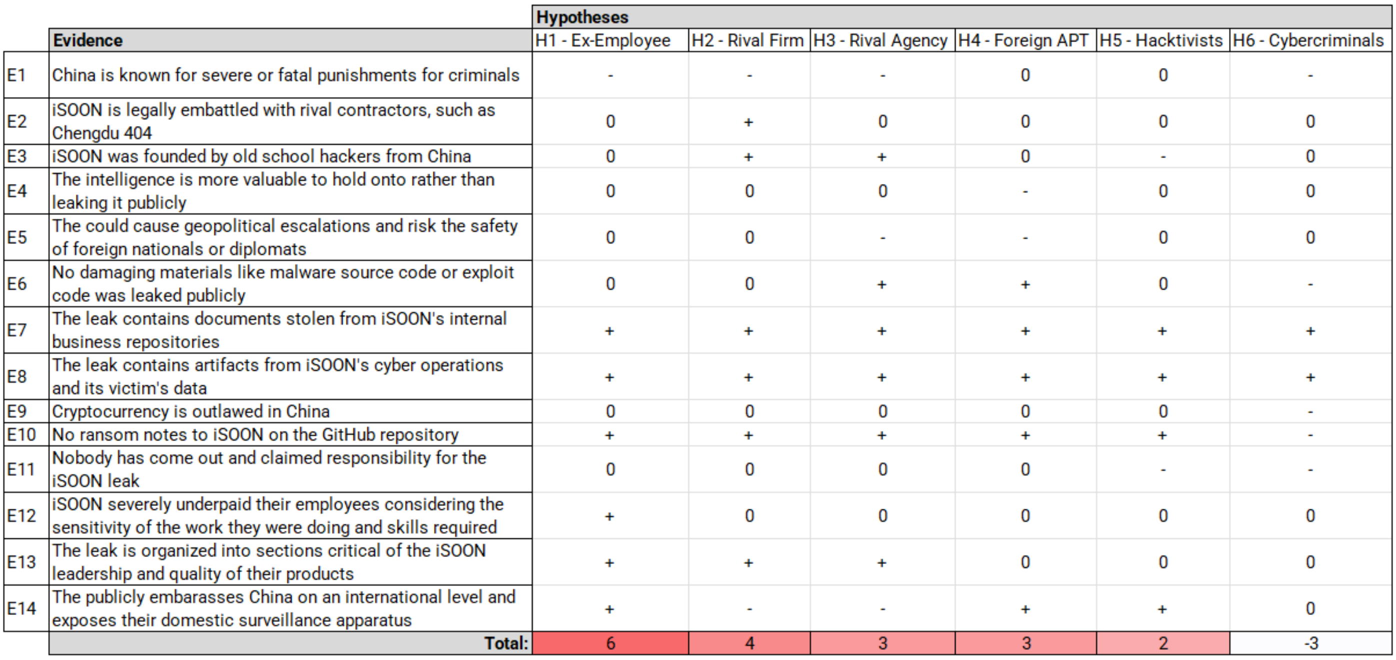
The three main steps to ACH is Hypothesis Generation (identify all possible explanations), Evidence Collection (list arguments for and against), and Diagnostics (test the arguments against each hypothesis). ACH encourages an analyst to consider one piece of evidence at a time, and examine it against all possible hypotheses. We then refine and prioritise our hypotheses before making a final conclusion. To perform an ACH, a Matrix is needed with evidence on the horizontal and our hypotheses on the vertical. This ACH Matrix will be used to determine which data points are the most helpful in assessing the likelihood of the presented hypothesis.

The first step involves developing our hypotheses based on the currently available intelligence. Generating as many hypothesis as necessary is best practice to ensure the inclusion of all available evidence. Ideally, when new evidence becomes available, all of our hypotheses should be evaluated again.

List of hypotheses of potential candidates for the iSOON leak:

1. An iSOON Revengeful Ex-Employee
2. A rival Chinese Contractor
3. A rival Chinese Agency to the MPS
4. A Foreign Intelligence Agency
5. An Anti-CCP Hacktivists
6. Chinese Cybercriminals

In an ACH Matrix, a "+" sign means the evidence may support the hypothesis and a "-" sign indicates it may not. A "0" sign means it neither supports nor disproves the hypothesis. We then use the ACH Matrix to prioritise the hypothesis with the most supporting evidence



		Hypotheses					
	Evidence	H1 - Ex-Employee	H2 - Rival Firm	H3 - Rival Agency	H4 - Foreign APT	H5 - Hacktivists	H6 - Cybercriminals
E1	China is known for severe or fatal punishments for criminals	-	-	-	0	0	-
E2	iSOON is legally embattled with rival contractors, such as Chengdu 404	0	+	0	0	0	0
E3	iSOON was founded by old school hackers from China	0	+	+	0	-	0
E4	The intelligence is more valuable to hold onto rather than leaking it publicly	0	0	0	-	0	0
E5	The could cause geopolitical escalations and risk the safety of foreign nationals or diplomats	0	0	-	-	0	0
E6	No damaging materials like malware source code or exploit code was leaked publicly	0	0	+	+	0	-
E7	The leak contains documents stolen from iSOON's internal business repositories	+	+	+	+	+	+
E8	The leak contains artifacts from iSOON's cyber operations and its victim's data	+	+	+	+	+	+
E9	Cryptocurrency is outlawed in China	0	0	0	0	0	-
E10	No ransom notes to iSOON on the GitHub repository	+	+	+	+	+	-
E11	Nobody has come out and claimed responsibility for the iSOON leak	0	0	0	0	-	-
E12	iSOON severely underpaid their employees considering the sensitivity of the work they were doing and skills required	+	0	0	0	0	0
E13	The leak is organized into sections critical of the iSOON leadership and quality of their products	+	+	+	0	0	0
E14	The publicly embarasses China on an international level and exposes their domestic surveillance apparatus	+	-	-	+	+	0
	Total:	6	4	3	3	2	-3

We then need to determine evidentiary dependence. This involves checking if our leading hypothesis has been prioritized based on critical evidence that, if deemed inauthentic and dismissed later on, would cause us to reconsider our entire assessment.

In the iSOON leak case, one of the most telling pieces of evidence that it came from a revengeful ex-employee was the headings of the files in the GitHub repo display a common sentiment that iSOON was a bad company to work for. The other key pieces of evidence that support it was a revengeful ex-employee include that they had the permissions and access to the resources and showed that their employees were working in less than ideal conditions, which involve difficult-to-perform tasks, such as domestic surveillance that supports arrests and ethnic cleansing of their fellow citizens.

Another valid hypothesis worth considering were whether a foreign intelligence agency was involved in the leak. However, key evidence that goes against this hypothesis is that the intelligence revealed in this leak would be much more valuable for a foreign agency to exploit rather than leak to the world and other intelligence agencies, who are undoubtedly studying this leak as well (and potentially this blog too! Hi guys 👋). The other arguments against the idea that a foreign agency was responsible is the potential danger it could cause, such as putting foreign nationals in China in physical danger or create escalations with China who would likely retaliate with a targeted hack-and-leak operation of their own. There is ultimately little benefit for a foreign agency to leak this information if they had managed to steal it themselves from iSOON's network.

The final hypothesis that seasoned analysts would be interested in discussing is whether an anti-CCP hacktivist group like IntrusionTruth was involved in this leak. However, in a very un-hacktivist fashion, nobody has publicly claimed responsibility for this leak, as a victory. Hacktivism is often described as a cyber-enabled influence operation and by leaking it anonymously, it goes against this common behavioural trait of theirs.

Conclusion

The iSOON leak is one of the most significant cyber threat updates related to China in recent years. The tools offered by iSOON and campaigns run by their operators highlight how both the Chinese MPS and Chinese Ministry of State Security (MSS) outsource their intelligence gathering to commercial surveillance vendors.

The links already uncovered between multiple long-running APT campaign and iSOON as a single entity has essentially taken a hammer and smashed the notion of neatly defined “threat groups” conducting campaigns in a siloed manner. The leak reinforces the idea that APT groups in China are connected to each other in many ways like the cybercrime underground or even the Western cyber defense industry in many ways than we admit.

Overall, I anticipate a lot more interesting findings and analysis to arise from the iSOON leak. I recommend all CTI teams to keep an eye out for mentions of iSOON as more revelations are bound to appear.

Further Reading:

- The original thread by Azaka: https://twitter.com/AzakaSekai_/status/1759326049262019025
- Machine Translation of the leak by my colleague DE7AULTsec: https://x.com/de7aultsec/status/1759394807091245286
- The Associated Press' investigation: https://apnews.com/article/china-cybersecurity-leak-document-dump-spying-aac38c75f268b72910a94881ccbb77cb
- The AP journalist's thread: https://twitter.com/dakekang/status/1760497207013241189
- MemeticWarfare Summary: https://memeticwarfareweekly.substack.com/p/memetic-warfare-weekly-my-data-leaks
- Kris McConkey's Thread on Red Scylla: https://twitter.com/smoothimpact/status/1760636928716689784
- Mark Kelly's Thread on Red Hotel: https://twitter.com/markkelly0x/status/1760408290255663170
- Dakota Cary's analysis: https://twitter.com/DakotaInDC/status/1760347298494599197