



**| Flash |**

# **iSoon Data Leak Provides a Glimpse of Chinese State Cyber Espionage Priorities, Tools, and Tradecraft**

**F-2024-02-21a**

**Classification: TLP:CLEAR**

**Criticality: Medium**

**Intelligence Requirements: Threat Groups, APT, Deep and Dark Web, Nation State**

**February 21, 2024**

**Scope Note:** ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on February 21, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **| Flash | iSoon Data Leak Provides a Glimpse of Chinese State Cyber Espionage Priorities, Tools, and Tradecraft**

## **> Key Findings**

- The iSoon data disclosures reveal the priorities, tools, and tradecraft of ongoing cyber espionage and influence operations being perpetrated by China nation-state actors, shedding light on the relationship between government contractors and the breadth of cyber tools at the Chinese government's disposal.
- Although the authenticity of the documents remains unverified, preliminary analysis suggests iSoon is a Chinese Ministry of Public Safety-affiliated organization that, as of 2022, was tasked with offensive red team operations and monitoring Twitter (now X) to “curb illegal opinions” and to use accounts for “public opinion guidance and control.”
- Not much is known about the GitHub account and the user “I-S00N” that posted the leaked information (behavior consistent with both whistleblowing and disinformation campaigns), making it difficult to ascertain the ultimate goal of these disclosures.

## **Details**

The iSoon data disclosures reveal the priorities, tools, and tradecraft of ongoing cyber espionage and influence operations being perpetrated by China nation-state actors, shedding light on the relationship between government contractors and the breadth of cyber tools at the Chinese government's disposal. On or about February 16, 2024, GitHub account "I-S00N" published what they claimed were files associated with China-based company iSoon (aka Anxun), an organization affiliated with China's Ministry of Public Safety (MPS). The alleged leaker organized the data into eight sections, with the information dating between 2018 and 2022 on wide-ranging tools and programs.

- The materials included technical details about some automated offensive tools, like an all-in-one penetration testing software program that enabled the automation of brute forcing, network attacks, directory scanning, data collection, et cetera.
- There were also automated social engineering kits that could be utilized in phishing campaigns and social media account takeovers.

Although the authenticity of the documents remain unverified, preliminary analysis suggests that, as of 2022, iSoon was tasked with monitoring Twitter (now X) to "curb illegal opinions" and to use accounts for "public opinion guidance and control," suggesting that the organization developed something akin to a Twitter-monitoring platform that could be used in influence operations. Some of these software features included obtaining the user's Twitter email and phone number, real-time monitoring, publishing tweets on the user's behalf, and even retrieving and reading direct messages (DMs); additionally, iSoon claimed the tool could process over 100 million tweets daily.

- The company's mandate to monitor social media content appeared to go beyond Twitter (now X) and included Chinese social media platforms such as Weibo and Badu, which would be consistent with the MPS' largely-domestic mandate to oversee law enforcement agencies and the political security of the Chinese Communist Party.
- This separate product stack was designed to monitor Chinese social media users, with capabilities to look up and search on username, email, phone, historic IP address lookup, and even a user detail lookup via an image upload function.

Not much is known about the GitHub account and the user “I-S00N” that posted the leaked information (behavior consistent with both whistleblowing and disinformation campaigns), making it difficult to ascertain the ultimate goal of these disclosures. However, the named countries implicated as victims and the lack of public fallout from these revelations suggest the disclosures are unlikely to cause any major disruption to ongoing Chinese cyber espionage operations.

## **Recommendations**

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of malware threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## **Appendix B: ZeroFox Intelligence Probability Scale**

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |