



| Brief |

iSoon Data Breach and China's Geopolitical Strategy

B-2024-02-28a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Geopolitical, Cyber

February 28, 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 06:00 AM (EST) on February 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | iSoon Data Breach and China's Geopolitical Strategy

› Key Findings

- The iSoon breach provides meaningful evidence that the Chinese Communist Party (CCP) leverages the Chinese private sector to achieve its geopolitical goals and illustrates the role the CCP has on priority-setting in the Chinese technology sector.
- The breach shows that contractors are used to target China's adversaries with cyberattacks designed to exfiltrate data in line with CCP's geopolitical priorities, which is then sold to Chinese state bodies.
- There is evidence from the breach to suggest China has deployed this strategy against targets with which it has geopolitical disputes. While the targeting of entities in these locations may be in line with CCP geopolitical aims, it is unknown if these efforts are at the direction of the CCP.

Analyst Commentary

While foreign intelligence services have repeatedly warned that China utilizes the private sector, the iSoon breach provides meaningful information on the inner workings of how third-party hacking services are leveraged by the Chinese Communist Party (CCP). The

iSoon data disclosures also underscore the role the CCP has in directing private cyber threat actors and the Chinese technology industry in general.

For decades, the CCP has played a key role in setting priorities across private sector industries—including employing private firms to conduct hacking and cyber espionage on behalf of the state.¹ However, under President Xi Jinping (who came to power in 2010), state intervention in the private sector has increased, particularly in the technology sector.

- Since 2020, the technology sector has been subjected to a harsh crackdown, which has decimated the value of Chinese private tech companies no longer seen as independent bodies but rather as entities closely aligned with the CCP.²

Across sectors, private firms are constrained by Xi's unique definition of national security and required to operate in line with China's geopolitical aims.

- Even before the data breach, iSoon advertised its close relationship with the Chinese government, listing the Ministry of Public Service and other Chinese government agencies as clients on its website.
- The company also mentions implementing the spirit of President Xi Jinping's instructions on developing cybersecurity education and expertise on its website.³
- The type of wording used on the iSoon website is similar to the messages being relayed by official Chinese government outlets, which, under Xi, are required to push a uniform view of national security.⁴
- Implemented in 2014, Xi's vision of national security is all-encompassing and applies across industries. It includes a broad obligation for ministries and the private sector to educate the public on what constitutes national security in China.

¹ [hXXps://yris.yira\[.\]org/essays/1447](https://yris.yira[.]org/essays/1447)

²

[hXXps://www.scmp\[.\]com/tech/big-tech/article/3227753/timeline-chinas-32-month-big-tech-crackdown-killed-w](https://www.scmp[.]com/tech/big-tech/article/3227753/timeline-chinas-32-month-big-tech-crackdown-killed-worlds-largest-ipo-and-wiped-out-trillions-value)
[orlds-largest-ipo-and-wiped-out-trillions-value](https://www.scmp[.]com/tech/big-tech/article/3227753/timeline-chinas-32-month-big-tech-crackdown-killed-worlds-largest-ipo-and-wiped-out-trillions-value)

³

[hXXps://www.rfi\[.\]fr/en/international-news/20240222-massive-leak-shows-chinese-firm-hacked-foreign-govts-act](https://www.rfi[.]fr/en/international-news/20240222-massive-leak-shows-chinese-firm-hacked-foreign-govts-activists-analysts-1)
[ivists-analysts-1](https://www.rfi[.]fr/en/international-news/20240222-massive-leak-shows-chinese-firm-hacked-foreign-govts-activists-analysts-1)

⁴ [hXXps://www.12371\[.\]cn/special/xxzd/hxnr/aqg/](https://www.12371[.]cn/special/xxzd/hxnr/aqg/)

Targeted Entities

The entities targeted by iSoon closely mirror the CCP's geopolitical priorities, indicating that for-hire hacker groups may be liaising with the CCP to provide valuable information on China's adversaries. Internal data seen in the breach demonstrates that the hackers accessed foreign networks and attempted to sell the data to the CCP; the CCP then purchased any data it determined would be useful.

- The breach shows that China is relying, at least partially, on third-party services to conduct offensive cyber operations.

In one instance, data stolen from the Vietnamese economic ministry was being advertised for USD 55,000.⁵

- China's interest in targeting Vietnam's economic ministry is likely linked to Vietnam's closer economic ties with the United States since the pandemic. The United States has been urging companies with operations in China to move them away from China to U.S.-allied nations in a trade move called friendshoring.⁶
- Vietnam is a leading friendshoring destination because it has similar manufacturing expertise to China, large deposits of rare-earth minerals, and even lower wages.

A number of nations that China has territorial disputes with were also listed in the breach. In early February 2024, ZeroFox warned that Chinese threat actors were likely targeting government agencies in nations that contest Chinese claims to the East China and South China Seas.

- Due to China's encroachment, these nations have forged closer security and economic ties with the United States and have created an unbroken military alliance from Japan and South Korea all the way to Australia.
- This likely explains the repeated targeting of entities like the Malaysian Foreign Affairs and Defense Ministries and the Philippine Navy Service.⁷ The Philippines in particular has been especially confrontational with China since 2022, and ZeroFox

⁵ [hXXps://www.securityweek\[.\]com/an-online-dump-of-chinese-hacking-documents-offers-a-rare-window-into-pervasive-state-surveillance/](https://www.securityweek.com/an-online-dump-of-chinese-hacking-documents-offers-a-rare-window-into-pervasive-state-surveillance/)

⁶ [hXXps://www.aseanbriefing\[.\]com/news/exploring-friendshoring-shifting-operations-in-asia-and-china/](https://www.aseanbriefing.com/news/exploring-friendshoring-shifting-operations-in-asia-and-china/)

⁷ [hXXps://internet2-0\[.\]com/iSoon-victims/](https://internet2-0[.]com/iSoon-victims/)

国家/地区	目标类型	目标名称	域名	样本数据量	数据类型	样本日期	权限说明	原权限组	备注
中国	运营商	AMT通信公司		11GB	话单	2020.06 - 2021.09	权限情况不明	一組	样本数据为用户基本身份信息，主要字段：手机号、姓名
	运营商	CSL通信公司		82.3MB	用户表	2020.06 - 2021.11	权限情况不明	一組	主要字段：手机号、身份证号、社交安全号码、地址等
	政府	工业和信息化部	MI	5.49GB	PC文件	2021.04 - 2021.10	用户产生的机器都去了	一組	样本为多个内部办公的文件
二組									
缅甸	政府	政府邮箱/服务器	le-mofa.gov.mm	1.06GB	邮件	2021.05.26	权限不明	二組	
三組									
香港	教育	民主民生協進會	adulte.org	89.4MB	用户上传	2021.05	权限丢失	三組	主要字段：人员名字、地址、公司信息、身体情况等
香港	政府	高斋学生数据		430MB	邮件	2017 - 2020	权限丢失	三組	主要字段：用户的邮箱、地址、姓名、电话、网页等
中国	新闻	新闻	weilisa.gov.vn				权限：有hash	三組	
欧开									
阿富汗	运营商	roshan运营商		2TB	话单	2016 - 2018	权限丢失	欧开	样本主要字段：姓名、类型、付款信息、服务流程、国家代码、工作代码等
菲律宾	安海云	Bayan运营商数据		3.31GB	数据表		权限丢失	欧开	数据主要字段：姓名、地址、电话号的等
哈萨克斯坦	安海云	用户信息		14.9GB	数据表		权限丢失	欧开	数据主要字段：姓名、地址等
韩国	安海云	用户信息	id2000_99	10.24MB	数据表		权限丢失	欧开	数据主要字段：姓名、地址、电话号码、生日等信息
韩国	安海云	人口数据		14.7GB	数据表		权限丢失	欧开	数据主要字段：姓名、地址、电话号码等
韩国	运营商	LG U+运营商		3TB	话单	2019 - 2021	权限丢失	欧开	
缅甸	安海云	运营商数据		4.05GB	数据表		权限丢失	欧开	数据主要字段：电话号码等
台湾	安海云	人口数据		17GB	数据表		权限丢失	欧开	数据主要字段：姓名、邮编、地址、电话号等等
台湾	运营商	VMO通信公司		2.23GB	用户上传		权限丢失	欧开	主要字段：手机号、ID、电话号码、地址以及邮编等
台湾	政府	道路信息数据		459GB	建模数据	2021	权限情况不明	欧开	样本包含台湾各市的三维建模模型数据，以及台湾108、全台国道3d和数据库数据，台湾各城市建筑3d模型
土耳其	安海云	人口数据		13.4GB	数据表		权限丢失	欧开	数据主要字段：姓名、ID、地址、生日等信息
香港	安海云	手机号		9.23MB	数据表	2009 - 2016	权限丢失	欧开	数据主要字段：姓名、社交安全号码、手机号等等
香港	运营商	PCW运营商数据		245MB	用户上传	2015 - 2016	权限情况不明	欧开	主要字段：手机号、姓名、地址、号码、用户上传的SHA和所属服务等等
香港	运营商	和记电讯		5.54GB	用户上传	2021.05	权限情况不明	欧开	主要字段：手机号、姓名、地址、号码所属服务等
香港	运营商	香港数据		11.1MB	数据表		权限丢失	欧开	主要字段：用户的邮箱、地址、姓名、电话、网页等
印度	安海云	人口数据		3.19GB	数据表		权限丢失	欧开	数据主要字段：姓名、地址、电话号码等
越南	安海云	运营商数据		38.9MB	数据表		权限丢失	欧开	数据主要字段：地址、邮编、密码、身份证号、姓名等
泰国	运营商	tot运营商	tot.co.th				权限归属不明		在部分用户电脑
中国	宗教	智慧课程	www.basmayra.com				权限归属不明		网站后台权限，可查看用户数据

https://github.com/mttaggart/I-S00N/blob/main/0/01cdc26f-e773-4ad7-8808-d04abf16aae7_2_0.png

- The iSoon breach reveals that data from 2020 was stolen from the Indian Home Affairs, Foreign Affairs, and Defense departments in 2021 and advertised for sale.⁹ During this period, India and China were engaged in a year-long border standoff that saw dozens of Indian officers killed and thousands of troops stationed along the shared border of Galwan, India.¹⁰
- The border issue has not been resolved and impacts several smaller nations that share boundaries with both countries—including Nepal, whose presidential palace, Foreign Affairs and Defense departments, and an important telecom outlet were all targeted.¹¹ China has been battling for influence in Nepal (which has historically been closer to India)in recent years, and threat actors have likely

¹¹ [hXXps://internet2-0\[.\]com/iSoon-victims/](https://internet2-0[.]com/iSoon-victims/)

sought useful information that could be used to undermine India's relationship with Nepal and increase Chinese influence.

In some instances, contractors carried out surveillance abroad that Chinese police routinely carry out at home.

- Leaked data shows iSoon would surveil foreign social media outlets for anti-government sentiment and instead push pro-CCP messaging. Chinese authorities already have the power to do this against domestic social media firms. Both domestic and foreign Chinese dissidents were heavily targeted, as the CCP views them as a threat to national security.
- The data breach revealed hacking of networks in Hong Kong and Taiwan, which China considers part of its territory. The leaks pertaining to Hong Kong higher education entities were particularly centered on the pro-democracy protests often organized on campus in 2019–2020.¹²

Entities linked with the Uyghur Muslim region of Xinjiang in Western China were also hacked. Hacks against Pakistani and Afghan government entities were tied to Uyghur groups, even though both nations maintain good relations with China.

- Uyghur militants are known to have ties to the Taliban and Al-Qaeda, and iSoon advertised its services as “anti-terror” support to assist the Xinjiang police in investigating potential Muslim extremists.¹³
- It is unclear why the CCP took up the anti-terror offer.
- The leaked data is around 1.43 GB stolen from Pakistan's anti-terrorism center in Punjab province between May 2021 and January 2022.¹⁴
- The documents also indicate that the Chinese government sanctioned spying on Pakistan's Ministry of Foreign Affairs and the Pakistan telecommunication company Zong.

¹²[hXXps://hongkongfp\[.\]com/2024/02/24/hackers-for-sale-what-we-know-about-chinas-massive-iSoon-cyber-leak/](https://hongkongfp.com/2024/02/24/hackers-for-sale-what-we-know-about-chinas-massive-iSoon-cyber-leak/)

¹³[hXXps://www.securityweek\[.\]com/an-online-dump-of-chinese-hacking-documents-offers-a-rare-window-into-pervasive-state-surveillance/](https://www.securityweek.com/an-online-dump-of-chinese-hacking-documents-offers-a-rare-window-into-pervasive-state-surveillance/)

¹⁴

[hXXps://www.indiatoday\[.\]in/india/story/chinese-hackers-target-government-home-ministry-air-india-reliance-isoon-leak-data-2505682-2024-02-22](https://www.indiatoday.in/india/story/chinese-hackers-target-government-home-ministry-air-india-reliance-isoon-leak-data-2505682-2024-02-22)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED 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.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER 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. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR 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%