Data Leak From A Chinese Cybersecurity Agency

Why In News

- Large amounts of data from a **Chinese cybersecurity company** have been leaked online, showing its contracts and communications with the Chinese government for **collecting important digital information** at home and abroad — including in countries such as India, Nigeria, Indonesia and the United Kingdom.

- **I-Soon, a Shanghai-based company** (also transliterated from the Mandarin as Auxun), is believed to be one of the many private contractors that help the Chinese state conduct its intelligence-gathering, hacking and other surveillance activities. **Last week, 190 megabytes of information** were posted on the software and code-sharing platform GitHub.

What's In The Leaked Data

- The data trove shared on **GitHub contains emails, images**, conversations and a trove of documents. According to a report in The Washington Post, they **"detail contracts to extract foreign data over eight years** and describe targets within at least 20 foreign governments and territories, including India, Hong Kong, Thailand, South Korea, the United Kingdom, Taiwan and Malaysia".

- These documents do not contain the actual information that was secured. But they have details about the **targets of the surveillance**, and the contracts that were awarded to I-Soon.
- "**One spreadsheet listed 80 overseas targets** that iSoon hackers appeared to have successfully breached," the report said.
- This included **"95.2 gigabytes of immigration data** from India and a 3 terabyte collection of call logs from South Korea's LG U Plus telecom provider". Also, "**459GB of road-mapping data from Taiwan**, the island of 23 million that China claims as its territory," was listed, according to The Post report.

- Within China, the targets seemed to include **"ethnicities and dissidents in parts** of China that have seen significant anti-government protests, such as Hong Kong or the **heavily Muslim region of Xinjiang in China's far west**", the Associated Press reported.

Indian Targets

- The **leaked data mentions Indian targets** like the Ministry of Finance, the Ministry of External Affairs, and the "Presidential Ministry of the Interior", which likely refers to the Ministry of Home Affairs.
- The **advanced persistent threat (APT) or hacker groups retrieved 5.49GB of data relating** to various offices of the **"Presidential Ministry of the Interior"** between May 2021 and October 2021, at the height of India-China border tensions.

- “In India, the main work targets are the ministry of foreign affairs, ministry of finance, and other relevant departments. We continue to track this area in depth and can tap its value in the long term,” reads the translated India section of what appears to be an internal report prepared by iSoon.
- **User data of state-run pension fund manager**, the Employees' Provident Fund Organisation (EPFO), state telecom operator Bharat Sanchar Nigam Limited (BSNL), and private healthcare chain Apollo Hospitals were also allegedly breached. **Air India’s stolen data pertains** to details of daily check-in by passengers.

- **The list of targets ranged from then President Ram Nath Kovind** and Prime Minister Narendra Modi to Congress leader Sonia Gandhi and their families; then Chief Ministers Ashok Gehlot, Amarinder Singh, and Uddhav Thackeray; Cabinet Ministers Rajnath Singh, Nirmala Sitharaman, Smriti Irani, and Piyush Goyal; the late Chief of Defence Staff Bipin Rawat and at least 15 former Chiefs of the Army, Navy, and Air Force; then Chief Justice of India Sharad A Bobde; and top industrialists Ratan Tata and Gautam Adani.

- **About 95GB of India's immigration details** from 2020, described as "entry and exit points data", were also referred to in the leaked documents. Notably, 2020 saw an escalation in India-China relations following the Galwan Valley clash.
- "India has always been a huge focus of the Chinese APT side of things. The stolen data naturally includes quite a few organisations from India, including **Apollo Hospital, people coming in and out of the country in 2020,** the Prime Minister's Office, and population records," Taiwanese researcher Azaka, who first highlighted the GitHub leak.

- **John Hultquist, the chief analyst at Google Cloud-owned Mandiant Intelligence**, was quoted by the Washington Post saying the online dump was "authentic data of a contractor supporting global and domestic cyber espionage operations out of China". "We rarely get such unfettered access to the inner workings of any intelligence operation," he said.

Other Targets

- Apart from India, Beijing also allegedly targeted its **"all-weather friend" Pakistan.** Other apparent targets include Nepal, Myanmar, Mongolia, Malaysia, Afghanistan, France, Thailand, Kazakhstan, Turkiye, Cambodia, and the Philippines, among others.

- As per the leaked dataset, as much as 1.43GB of postal service data from the **"Anti-Terrorism Centre" in Pakistan's Punjab province** was obtained by the Chinese hacker group between May 2021 and January 2022. The documents also indicate that the Chinese government sanctioned snooping on Pakistan's Ministry of Foreign Affairs and telecommunication company Zong.

- Huge amounts of data were also allegedly **stolen from Nepal Telecom, Mongolia's Parliament and police departments**, a French university, and Kazakhstan's pension managing authority. The hackers also allegedly accessed the official systems of the Tibetan government-in-exile and its domain, Tibet.
- **For years, hacking groups linked to China's Communist Party,** like Mustang Panda or APT41, have been running malicious campaigns, targeting organisations and countries including the US to gather intelligence. The US recently launched an operation to fight a pervasive Chinese hacking operation that compromised thousands of internet-connected devices.
- **This isn't the first time China has been** in the spotlight for cyber attacks in India. In 2022, China-linked hackers reportedly targeted seven Indian power hubs. Threat actors attempted to get into India's power infrastructure in 2021 as well.