Hackers for sale: what we've learned from China's enormous cyber leak

Publication Date: 2024-02-25

Author: Unknown

Section: Technology

Tags: Technology, Hacking, China, Cybercrime, features

Article URL: https://www.theguardian.com/technology/2024/feb/25/china-cyber-leak-hacking-program-security

A enormous data leak from a Chinese cybersecurity firm has offered a rare glimpse into the inner workings of Beijing-linked hackers. Analysts say the leak is a treasure trove of intel into the day-to-day operations of China's hacking programme, which the FBI says is the biggest of any country. The company, I-Soon, has yet to confirm the leak is genuine and has not responded to a request for comment. As of Friday, the leaked data was removed from the online software repository GitHub, where it had been posted. From staff complaints about pay and office gossip to claims of hacking foreign governments, here are some of the key insights from the leaks: Who got hacked? Every day, workers at I-Soon were targeting big fish. Government agencies of China's neighbours, including Kyrgyzstan, Thailand, Cambodia, Mongolia and Vietnam, had websites or email servers compromised, the leak revealed. There are long lists of targets, from British government departments to Thai ministries. I-Soon staff also boasted in leaked chats that they secured access to telecom service providers in Pakistan, Kazakhstan, Mongolia, Thailand and Malaysia, among others. They named the government of India – a geopolitical rival of Beijing's – as a key target for "infiltration". And they claimed to have secured back-end access to higher education institutions in Hong Kong and self-ruled Taiwan, which China claims as part of its territory. But they also admitted to having lost access to some of their data seized from government agencies in Myanmar and South Korea. Other targets are domestic, from China's north-western region of Xinjiang to Tibet and from illegal pornography to gambling rings. Who was paying I-Soon? Judging from the leaks, most of I-Soon's customers were provincial or local police departments – as well as province-level state security agencies responsible for protecting the Communist party from perceived threats to its rule. The firm also offered clients help protecting their devices from hacking and securing their communications – with many of their contracts listed as "non-secret". There were references to official corruption: in one chat, salesmen discussed selling the company's products to police – and planned to give kickbacks to those involved in the sale. There were also references to a client in Xinjiang, where Beijing is accused of grave human rights abuses. But workers complained about the challenges of doing business in the tense region. "Everyone thinks of Xinjiang like a nice big cake … but we have suffered too much there," one wrote. What hacking tools were for sale? In their chats, I-Soon staffers told colleagues their main focuses were making "Trojan horses" – malware disguised as legitimate software that allows hackers access to private data – and building databases of personal information. "At the moment, the trojan horses are mainly customised for Beijing's state security department," one said. It also laid out how the firm's hackers could access and take over a person's computer remotely, allowing them to execute commands and monitor what they type, known as key logging. Other services included ways to breach Apple's iPhone and other smartphone operating systems, as well as custom hardware – including a power bank

that can extract data from a device and send it to the hackers. In one screenshot of a conversation, someone describes a client request for exclusive access to the “foreign secretary’s office, foreign ministry’s ASEAN office, prime minister’s office, national intelligence agency” and other government departments of an unnamed country. One service offered is a tool that allows clients to break into accounts on social media platform X, formerly Twitter, claiming to be able to obtain the phone number of a user and break into their private messages. I-Soon also boasts of a technique to bypass two-step authentication – a common login technique that offers an extra level of security to the account. Who are the hackers? The leak also paints a less-than-flattering picture of the day-to-day goings-on at a mid-level Chinese cybersecurity firm. Employees’ chats are full of complaints about office politics, lack of basic tech expertise, poor pay and management, and the challenges the company faced in securing clients. One set of screenshots showed arguments between an employee and a supervisor over salaries. And in another leaked chat, a staffer complained to their colleague that their boss had recently bought a car worth over 1m yuan ($139,000) instead of giving their team a pay rise. “Does the boss dream about being an emperor?”