# Huge cybersecurity leak lifts lid on world of China's hackers for hire

Publication Date: 2024-02-23

Author: Amy Hawkins

Section: Technology

Tags: Cybercrime, Hacking, China, Internet, Asia Pacific, news

Article URL: https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire


A big leak of data from a Chinese cybersecurity firm has revealed state security agents paying tens of thousands of pounds to harvest data on targets, including foreign governments, while hackers hoover up huge amounts of information on any person or institution who might be of interest to their prospective clients. The cache of more than 500 leaked files from the Chinese firm I-Soon was posted on the developer website Github and is thought by cybersecurity experts to be genuine. Some of the targets discussed include Nato and the UK Foreign Office. The leak provides an unprecedented insight into the world of China's hackers for hire, which the head of the UK's security services has called a "massive" challenge for the country. The files, which are a mixture of chat logs, company prospectuses and data samples, reveal the extent of China's intelligence gathering operations, while also highlighting the market pressures felt by the country's commercial hackers as they vie for business in a struggling economy. I-Soon appears to have worked with – and later been embroiled in a commercial dispute with – another Chinese hacking outfit, Chengdu 404, whose hackers have been indicted by the US Department of Justice for cyber-attacks on companies in the US as well as pro-democracy activists in Hong Kong, among other targets. Other targets discussed in the I-Soon leaks include the British thinktank Chatham House and the public health bureaux and foreign affairs ministries of Asean countries. Some of this data seems to have been gathered on spec, while in other cases there are specific contracts with a Chinese public security bureau to gather a certain type of data. A spokesperson for Chatham House said: "We are aware of this data coming to light and are naturally concerned. Chatham House takes data and information security extremely seriously. In the current climate, we, along with many other organisations, are the target of regular attempted attacks from both state and non-state actors. "We have protection measures in place including technology-based safeguards which are reviewed and upgraded on a regular basis." A Nato official said: "The alliance faces persistent cyber-threats and has prepared for this by investing in extensive cyber defences. Nato reviews every claim of cyber-threats." The UK Foreign Office declined to comment. The services offered by I-Soon are varied. In one example, the public security bureau of a city in Shandong paid nearly £44,000 to obtain access to the email inboxes of 10 targets for one year. The company claimed to be able to hack accounts on X, obtain personal information from Facebook, obtain data from internal databases and compromise various operating systems including Mac and Android. In one of the files there is a screenshot of a folder entitled "Notes from the secretariat of European Affairs of North Macedonia". Another screenshot shows files that appear to relate to the EU, including one entitled "Draft EU position with regard to COP 15 part 2". The file names reference an encryption system used by EU entities to secure official data. In some cases, is not clear what the purpose

of collecting the data was. “The Chinese state is basically hoovering up as much data as they can,” said Alan Woodward, a computer security expert at the University of Surrey. “They just want as much information as they can in case it proves useful.” Woodward noted that unlike Russian state-linked hackers who conduct ransomware attacks or other disruptive actions, Chinese attempts tended to focus on mass data harvesting. “Some of it could be interpreted as laying the groundwork for being disruptive at a later stage,” Woodward said. Last year, parliament’s intelligence and security committee report on China said: “China’s cyber expertise allows it to target a diverse range of organisations and datasets – and increasingly unusual ones.” Experts believe that the goal of data gathering may be to identify potential targets for human intelligence operations. I-Soon also targeted domestic victims. In an undated cooperation agreement with a local authority in Xinjiang, I-Soon stated that it could provide “anti-terrorism” support to the local police in monitoring Uyghurs. I-Soon said that it had more than a decade of experience in accessing “various server permissions and intranet permissions in multiple countries”. The company claimed to have obtained data from counter-terrorism authorities in Pakistan and Pakistan’s postal service. Pakistan’s embassy in London did not respond to a request for comment. Some of the promises to clients might have been sales bluster. In one discussion, an employee asked: “Are customers deceiving us, or are we deceiving customers?” The worker continues that deceiving customers about the company’s abilities is “normal, but it is not good for the company to deceive its employees”. Mei Danowski, a China cybersecurity expert and author of the Natto Thoughts newsletter, said: “We think about [Chinese hackers] as ‘Oh, the state gives them cash to do stuff.’ In reality, if these leaked documents are true, it’s not like that. They have to go and look for business. They have to build up a reputation.” Other chat logs were strikingly mundane. Employees discussed Covid-19 and the financial pressures at I-Soon. “Originally, everyone knew that the company was having a hard time, and they all understood. After all, the epidemic is so severe,” wrote one worker in March 2021. But, they complained, I-Soon “didn’t say they wouldn’t pay us wages”. By the following year, the pressures at the company seemed to have intensified. The chief executive, Wu Haibo, who uses the pseudonym Shutd0wn, said that the loss of core staff had dented customers’ confidence, leading to a loss of business. Wu did not respond to a request for comment. “The boss is really anxious,” wrote one employee in September 2022. “I don’t know if the company can survive until the end of the year.” In another chat log, workers spoke about the company’s poor sales and a souring mood in the office. One employee turned to a universal solace: “I’ll probably scream if I can’t have a drink.”