www.washingtonpost.com /world/2024/02/21/china-hacking-leak-documents-isoon/

Leaked files from Chinese firm show vast international hacking effort

Christian Shepherd, Cate Cadell, Ellen Nakashima, Joseph Menn, Aaron Schaffer ⋮ 13-16 minutes ⋮ 2/21/2024

---

correction

A previous version of this article incorrectly asserted that, in leaked documents, the Chinese hacking group iSoon claimed to be able to exploit vulnerabilities in U.S. companies, including Microsoft, Apple and Google. In fact, the hackers claimed that they were able to target users of these platforms to install malicious software and extract data. The article has been corrected.

A trove of leaked documents from a Chinese state-linked hacking group shows that Beijing's intelligence and military groups are attempting large-scale, systematic cyber intrusions against foreign governments, companies and infrastructure — with hackers of one company claiming to be able to target users of Microsoft, Apple and Google.

The cache — containing more than 570 files, images and chat logs — offers an unprecedented look inside the operations of one of the firms that Chinese government agencies hire for on-demand, mass data-collecting operations.

The files — posted to GitHub last week and deemed credible by cybersecurity experts, although the source remains unknown — 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. Indian publication BNN earlier reported on the documents.

"We rarely get such unfettered access to the inner workings of any intelligence operation," said John Hultquist, chief analyst of Mandiant Intelligence, a cybersecurity firm owned by Google Cloud. "We have every reason to believe this is the authentic data of a contractor supporting global and domestic cyberespionage operations out of China," he said.

U.S. intelligence officials see China as the greatest long-term threat to American security and have raised alarm about its targeted hacking campaigns.

(Video: Illustration by Emma Kumer/The Washington Post; I-S00N/GitHub)

Experts are poring over the documents, which offer an unusual glimpse inside the intense competition of China's national security data-gathering industry — where rival outfits jockey for lucrative government contracts by pledging evermore devastating and comprehensive access to sensitive information deemed useful by Chinese police, military and intelligence agencies.

The documents come from iSoon, also known as Auxun, a Chinese firm headquartered in Shanghai that sells third-party hacking and data-gathering services to Chinese government

bureaus, security groups and state-owned enterprises.

The trove does not include data extracted from Chinese hacking operations but lists targets and — in many cases — summaries of sample data amounts extracted and details on whether the hackers obtained full or partial control of foreign systems.

One spreadsheet listed 80 overseas targets that iSoon hackers appeared to have successfully breached. The haul 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. The group also targeted other telecommunications firms in Hong Kong, Kazakhstan, Malaysia, Mongolia, Nepal and Taiwan. The Indian Embassy in Washington did not respond to a request for comment on the documents.

ISoon clients also requested or obtained infrastructure data, according to the leaked documents. The spreadsheet showed that the firm had a sample of 459GB of road-mapping data from Taiwan, the island of 23 million that China claims as its territory.

Road data could prove useful to the Chinese military in the event of an invasion of Taiwan, analysts said. "Understanding the highway terrain and location of bridges and tunnels is essential so you can move armored forces and infantry around the island in an effort to occupy Taiwan," said Dmitri Alperovitch, a national security expert and chairman of Silverado Policy Accelerator, a think tank.

Among other targets were 10 Thai government agencies, including the country's Foreign Ministry, intelligence agency and Senate. The spreadsheet notes that iSoon holds sample data extracted from those agencies from between 2020 and 2022. The Thai Embassy in Washington did not respond to a request for comment.

Most of the targets were in Asia, though iSoon received requests for hacks further afield. Chat logs included in the leak describe selling unspecified data related to NATO in 2022. It's not clear whether the data was collected from publicly available sources or extracted in a hack.

"The Alliance faces persistent cyber threats and has prepared for this by investing in extensive cyber defences. NATO reviews every claim of cyber threats," a NATO official said.

Another file shows employees discussing a list of targets in Britain, including its Home and Foreign offices as well as its Treasury. Also on the list were British think tanks Chatham House and the International Institute for Strategic Studies.

"In the current climate, we, along with many other organizations, are the target of regular attempted attacks from both state and non-state actors," said a Chatham House spokesperson. The group is "naturally concerned" about the leaks but has protection measures in place, the spokesperson said.

Asked about the leaked documents, the U.K. Foreign Office declined to comment.

The hackers also facilitated attempts to extract information from close diplomatic partners including Pakistan and Cambodia.

China encourages hacking rivalry

ISoon is part of an ecosystem of contractors that emerged out of a “patriotic” hacking scene established over two decades ago. It now works for a range of powerful government entities including the Ministry of Public Security, the Ministry of State Security and the Chinese military.

According to U.S. officials, hackers with the People’s Liberation Army have breached computer systems in about two dozen key American infrastructure entities over the past year in an attempt to establish a foothold and be able to disrupt power and water utilities as well as communications and transportation systems.

China’s model of mixing state support with a profit incentive has created a large network of actors competing to exploit vulnerabilities and grow their businesses. The scale and persistence of their attacks are headaches for American technology giants like X, Microsoft and Apple, which are now locked in a constant race to outsmart the hackers.

All software products have vulnerabilities, and a robust global marketplace rewards those who find security weaknesses or develop tools known as exploits to take advantage of them. Many software vendors offer bounties to reward researchers who report security flaws, but government contractors in the United States and elsewhere often claim these exploits — paying more for the right to use them in espionage or offensive activity.

U.S. defense and intelligence contractors also develop tools for breaking into software, which are then used by federal officials in surveillance and espionage operations, or in offensive cyberweapons.

Chinese security researchers at private companies have demonstrably improved in recent years, winning a greater number of international hacking competitions as well as collecting more bounties from tech companies.

But the iSoon files contain complaints from disgruntled employees over poor pay and workload. Many hackers work for less than $1,000 a month, surprisingly low pay even in China, said Adam Kozy, a former FBI analyst who is writing a book on Chinese hacking.

The leaks hint at infighting and dissatisfaction in the network of patriotic Chinese hackers, despite the long-standing collaboration between groups.

Although it’s unclear who released the documents and why, cybersecurity experts said it may be an unhappy former employee or even a hack from a rival outfit.

The leaker presented themselves on GitHub as a whistleblower exposing malpractice, poor work conditions and “low quality” products that iSoon is using to “dupe” its government clients. In chats marked as featuring worker complaints, employees grumbled about sexism, long hours and weak sales.

Hackers for hire

Within China, these groups present themselves as essential to the Communist Party’s extensive campaign to eliminate threats to its rule from cyberspace.

China in recent years has escalated its efforts to trawl international public social media and trace targets abroad, though the crossover between public mass-monitoring and private

hacking is often unclear.

ISoon has signed hundreds of deals with Chinese police that range from small jobs priced at $1,400 to multiyear contracts costing as much as $800,000, one spreadsheet showed.

The company's leaked product manuals describe the services they offer and their prices, and boast about being able to steal data without detection. The product descriptions, targeted at state security clientele, at times use wartime language to describe a data-extraction mission underpinned by extreme threats to China's national security.

(Video: Illustration by Emma Kumer/The Washington Post; I-S00N/GitHub)

"Information has increasingly become the lifeblood of a country and one of the resources that countries are scrambling to seize. In information warfare, stealing enemy information and destroying enemy information systems have become the key to defeating the enemy," reads one document describing an iSoon package for sale that, it claims, would allow clients to access and covertly control Microsoft Outlook and Hotmail accounts by bypassing authentication protocols.

ISoon's product manuals also advertise a $25,000 service for a "remote access" control system to obtain Apple iOS smartphone data from a target, including "basic mobile phone information, GPS positioning, mobile phone contacts" and "environment recording."

One pitch advertised a service in which iSoon could efficiently conduct phishing campaigns against individuals or groups of Twitter users. Another outlined services that would allow the firm to remotely control targeted Windows and Mac operating systems.

Apple, Microsoft and X, formerly Twitter, did not respond to requests for comment.

Google said that the documents did not list specific vulnerabilities in its software. A spokesperson said the hackers were probably trying to get targets to install malicious software, which then persisted undetected.

In addition to striking long-term agreements, iSoon regularly worked on demand in response to requests from police in smaller Chinese cities and with private companies, according to pages of chat logs between the company's top executives.

Sometimes the clients knew exactly what they wanted — for example, to find the identity of a specific Twitter user — but they also often made open-ended requests. In one exchange, employees discussed a request from a state security bureau in southern China asking if iSoon had much to offer on nearby Hong Kong. An iSoon employee suggested emails from Malaysia instead.

The scattershot approach appeared motivated in part by pressure from clients to deliver more and higher quality information. But despite the company boasting of cutting-edge capabilities, chats show that clients were regularly unimpressed with the hacked information.

ISoon repeatedly failed to extract data from government agencies, internal discussions showed, with some local authorities complaining about subpar intelligence.

(Video: Illustration by Emma Kumer/The Washington Post; I-S00N/GitHub)

Although some of iSoon's services focused on domestic threats, the company often highlighted its ability to hack overseas targets in the region — including government departments in India and Nepal, as well as in overseas Tibetan organizations — to attract clients. In December 2021, the group claimed that it had gained access to the intranet of the Tibetan government in exile, setting off a frantic search for a buyer. Some 37 minutes later, the company had found an interested client.

Another product — priced at $55,600 per package — is meant to allow control and management of discussion on Twitter, including using phishing links to access and take over targeted accounts. ISoon claims the system then allows clients to find and respond to "illegal" and "reactionary sentiments" using accounts that are centrally controlled by the client to "manipulate discussion."

The documents show that iSoon met and worked with members of APT41, a Chinese hacking group that was charged by the U.S. Justice Department in 2020 for targeting more than 100 video game firms, universities and other victims worldwide.

Afterward, iSoon's founder and CEO, Wu Haibo, who goes by the alias "shutdown," joked with another executive about going for "41" drinks with Chengdu 404 — the organization that APT41 is a part of — to celebrate them now being "verified by the Federal Bureau of Investigation."

But chat messages between executives from 2022 suggest that relations between the groups had soured because iSoon was late in paying Chengdu 404 more than 1 million yuan ($140,000). Chengdu 404 later sued iSoon in a dispute over a software development contract.

Wu and his team appeared blasé about the idea that they would one day be charged by U.S. authorities like APT41. In July 2022, an executive asked Wu whether the company was being closely watched by the United States. "Not bothered," Wu replied. "It was a matter of sooner or later anyway."

Neither iSoon nor Wu responded to emailed requests for comment.

Pei-Lin Wu and Vic Chiang in Taipei and Lyric Li in Seoul contributed to this report.