Spies for Hire: China’s New Breed of Hackers Blends Espionage and Entrepreneurship

nytimes.com/2021/08/26/technology/china-hackers.html

Paul Mozur, Chris Buckley

August 26, 2021

Continue reading the main story

China’s buzzy high-tech companies don’t usually recruit Cambodian speakers, so the job ads for three well-paid positions with those language skills stood out. The ad, seeking writers of research reports, was placed by an internet security start-up in China’s tropical island-province of Hainan.

That start-up was more than it seemed, according to American law enforcement. Hainan Xiandun Technology was part of a web of front companies controlled by China’s secretive state security ministry, according to a federal indictment from May. They hacked computers from the United States to Cambodia to Saudi Arabia, seeking sensitive government data as well as less-obvious spy stuff, like details of a New Jersey company’s fire-suppression system, according to prosecutors.

The accusations appear to reflect an increasingly aggressive campaign by Chinese government hackers and a pronounced shift in their tactics: China’s premier spy agency is increasingly reaching beyond its own ranks to recruit from a vast pool of private-sector talent.

This new group of hackers has made China’s state cyberspying machine stronger, more sophisticated and — for its growing array of government and private-sector targets — more dangerously unpredictable. Sponsored but not necessarily micromanaged by Beijing, this new breed of hacker attacks government targets and private companies alike, mixing traditional espionage with outright fraud and other crimes for profit.

China's new approach borrows from the tactics of Russia and Iran, which have tormented public and commercial targets for years. Chinese hackers with links to state security demanded ransom in return for not releasing a company's computer source code, according to an indictment released by the U.S. Department of Justice last year. Another group of hackers in southwest China mixed cyber raids on Hong Kong democracy activists with fraud on gaming websites, another indictment asserted. One member of the group boasted about having official protection, provided that they avoid targets in China.

"The upside is they can cover more targets, spur competition. The downside is the level of control," said Robert Potter, the head of Internet 2.0, an Australian cybersecurity firm. "I've seen them do some really boneheaded things, like try and steal $70,000 during an espionage op."

Investigators believe these groups have been responsible for some big recent data breaches, including hacks targeting the personal details of 500 million guests at the Marriott hotel chain, information on roughly 20 million U.S. government employees and, this year, a Microsoft email system used by many of the world's largest companies and governments.

The Microsoft breach was unlike China's previously disciplined strategy, said Dmitri Alperovitch, the chairman of Silverado Policy Accelerator, a nonprofit geopolitical think tank.

"They went after organizations they had zero interest in and exploited those organizations with ransomware and other attacks," Mr. Alperovitch said.

China's tactics changed after Xi Jinping, the country's top leader, transferred more cyberhacking responsibility to the Ministry of State Security from the People's Liberation Army following a slew of sloppy attacks and a reorganization of the military. The ministry, a mix of spy agency and Communist Party inquisitor, has used more sophisticated hacking tools, like security flaws known as zero days, to target companies, activists and governments.

Image
President Xi Jinping was embarrassed by revelations of the People's Liberation Army's hacking activities and gave more responsibility to the Ministry of State Security.Credit...Ng Han Guan/Associated Press
While the ministry projects an image of remorseless loyalty to the Communist Party in Beijing, its hacking operations can act like local franchises. Groups often act on their own agendas, sometimes including sidelines in commercial cybercrime, experts said.

The message: "We're paying you to do work from 9 to 5 for the national security of China," Mr. Alperovitch said. "What you do with the rest of your time, and with the tools and access you have, is really your business."

A grand jury indictment released last year charged that two former classmates from an electrical engineering college in Chengdu, in southwest China, marauded through foreign computer servers and stole information from dissidents and engineering diagrams from an Australian defense contractor. On the side, the indictment said, the two tried extortion: demanding payment in return for not revealing an unidentified company's source code on the internet.

Under this system, Chinese hackers have become increasingly aggressive. The rate of global attacks linked to the Chinese government has nearly tripled since last year compared with the four previous years, according to Recorded Future, a Somerville, Mass., company that studies the use of internet by state-linked actors. That number now averages more than 1,000 per three-month period, it said.

"Considering the volume that's going on, how many times has the F.B.I. gotten them? Precious few," said Nicholas Eftimiades, a retired senior American intelligence officer who writes about China's espionage operations. "There's no way you can staff up to be able to contend with this type of onslaught."

Though their numbers make them hard to stop, the hackers don't always try hard to cover their tracks. They sometimes leave clues strewn online, including wedding photos of agents in state security uniforms, telltale job ads and boasts of their feats.

Hainan Xiandun was set up to recruit young talent and create a veneer of deniability, prosecutors said. It posted job ads on the message boards of Chinese universities and sponsored a cybersecurity competition.

The operations from Hainan — an island jutting into the South China Sea — sometimes reflected local priorities, like stealing marine research from a university in California and hacking governments in nearby Southeast Asian countries, according to the May indictment. Its job ad for Cambodian speakers was placed three months before Cambodian elections.

While some targets had clear espionage goals, others appeared less focused. The hackers tried to steal Ebola vaccine data from one institution, prosecutors said, and secrets about self-driving cars from another.

Image
The Department of Justice unsealed an indictment in July detailing the exploits of a Chinese hacking group.Credit...Stefani Reynolds for The New York Times
In January 2020, a mysterious blog with a track record of exposing Chinese state security hackers picked up the scent. The blog, "Intrusion Truth," was already known in Washington cybersecurity circles for naming Chinese intelligence officers well before they appeared in U.S. indictments.

The operators of “Intrusion Truth” scoured job boards for Hainan companies advertising for “penetration testing engineers,” who secure networks by exploring how they could be hacked.

One posting from Hainan Xiandun stood out. The ad, on a Sichuan University computer science hiring board from 2018, boasted that Xiandun had “received a considerable number of government-secret-related business.”

The company, based in Hainan’s capital, Haikou, paid monthly salaries of $1,200 to $3,000 — solid middle-class wages for Chinese tech workers fresh out of college — with bonuses as high as $15,000. Xiandun’s ads listed an email address used by other firms looking for cybersecurity experts and linguists, suggesting they were part of a network.

Chinese hacking groups are increasingly “sharing malware, exploits and coordinating their efforts,” the operators of “Intrusion Truth” wrote in an email. The operators have not disclosed their identities, citing the sensitivity of their work.

Xiandun’s registered address was the library of Hainan University. Its phone number matched that of a computer science professor and People’s Liberation Army veteran who ran a website offering payments for students with novel ideas about cracking passwords. The professor has not been charged.

Other records and phone numbers led the blog authors to an email address and a frequent-flier account owned by Ding Xiaoyang, one of the managers of the company.

The indictment asserted that Mr. Ding was a state security officer who ran the hackers working at Hainan Xiandun. It included details the blog did not find, like an award Mr. Ding received from the Ministry of State Security for young leaders in the organization.

Mr. Ding and others named in the indictment couldn’t be reached.

Though trackable for now, China’s state security apparatus may be learning how to better hide its footprints, said Matthew Brazil, a former China specialist for the Department of Commerce’s Office of Export Enforcement who has co-written a study of Chinese espionage.

“The abilities of the Chinese services are uneven,” he said. “Their game is getting better, and in five or 10 years it’s going to be a different story.”

Nicole Perlroth contributed reporting.