The Mystery of China's Sudden Warnings About US Hackers

The Chinese government recently began saber-rattling about American cyberespionage. The catch? It's all old news.

Matt Burgess May 26, 2022 7:00 AM

Photograph: ANTHONY WALLACE/Getty Images

For the best part of a decade, US officials and cybersecurity companies have been naming and shaming hackers they believe work for the Chinese government. These hackers have stolen terabytes of data from pharmaceutical companies to video game firms, compromised servers, stripped security protections, and highjacked hacking tools, according to security experts. And as China's alleged hacking has grown in aggression, individual Chinese hackers face indictments. However, things may be changing.

Since the start of 2022, there has been a marked uptick in China's Foreign Ministry and the country's cybersecurity firms calling out alleged US cyberespionage. Until now, these allegations have been a rarity. But the disclosures come with a catch: They appear to rely on years-old technical details, which are already publicly known and don't contain fresh information. The move may be a strategic change for China as the nation tussles to cement its position as a tech superpower.

"These are useful materials for China's tit-for-tat propaganda campaigns when they faced US accusation and indictment of China's cyberespionage

activities," says Che Chang, a cyber threat analyst at Taiwan-based cybersecurity firm TeamT5.

China's accusations, which were noted by security journalist Catalin Cimpanu, all follow a very similar pattern. On February 23, Chinese security company Pangu Lab published allegations that the US National Security Agency's elite Equation Group hackers used a backdoor, dubbed Bvp47, to monitor 45 countries. The *Global Times*, a tabloid newspaper that's part of China's state-controlled media, ran an exclusive report on the research. Weeks later, on March 14, the newspaper had a second exclusive story about another NSA tool, NOPEN, based on details from China's National Computer Virus Emergency Response Center. A week later, Chinese cybersecurity firm Qihoo 360 alleged that US hackers had been attacking Chinese companies and organizations. And on April 19, the Global Times reported on further National Computer Virus Emergency Response Center findings around HIVE, malware developed by the CIA.

The reports are accompanied with a flurry of statements—often in response to questions from the media—by China's Foreign Ministry spokespeople. "China is gravely concerned over the irresponsible malicious cyber activities of the US government," Foreign Ministry spokesperson Wang Wenbin said in April after one of the announcements. "We urge the US side to explain itself and immediately stop such malicious activities." Over the first nine days of May, Foreign Ministry spokespeople commented on US cyber activities at least three times. "One cannot whitewash himself by smearing others," Zhao Lijian said in one instance.

While cyber activity undertaken by state actors is often wrapped in highly classified files, many hacking tools developed by the US are no longer a secret. In 2017, WikiLeaks published 9,000 documents in the Vault7 leaks, which detailed many of the CIA's tools. A year earlier, the mysterious Shadow

Brokers hacking group stole data from one of the NSA's elite hacking teams and slowly dripped the data to the world. The Shadow Brokers leaks included dozens of exploits and new zero-days—including the Eternal Blue hacking tool, which has since been used repeatedly in some of the largest cyberattacks. Many of the details in the Shadow Brokers leaks match up with details about NSA which were disclosed by Edward Snowden in 2013. (An NSA spokesperson said it has "no comment" for this story; the agency routinely does not comment on its activity.)

Ben Read, director of cyberespionage analysis at US cybersecurity firm Mandiant, says China's state media push of alleged US hacking seems to be consistent, but it mostly contains older information. "Everything that I've seen they've written about, they tie back to the US through either the Snowden leaks or Shadow Brokers," Read says.

Pangu Lab's February report on Bvp47—the only publication on its website—says it initially discovered the details in 2013 but pieced them together after the Shadow Brokers leaks in 2017. "The report was based on a decade-old malware, and the decryption key is the same" as in WikiLeaks, Che says. The details of HIVE and NOPEN have also been available for years. Neither Pangu Labs or Qihoo 360, which has been on the US government sanctions list since 2020, responded to requests for comment on their research or methodology. Although a Pangu spokesperson previously said it recently published the old details, and it had taken a long time to analyze the data.

Megha Pardhi, a China researcher at Takshashila Institution, an Indian think tank, says the publications and follow-up comments from officials can serve multiple purposes. Internally, China can use it for propaganda and to send a message to the US that it has the capability to attribute cyber activity. But beyond this, there is a warning to other countries, Pardhi says. "The message is that even though you're allied with the United States, they're still

gonna come after you."

"We oppose and crack down in accordance with law all forms of cyberespionage and attacks," Liu Pengyu, a spokesperson for the Chinese Embassy in the US, says in a statement. Liu did not respond directly to questions around the apparent uptick in finger-pointing at the US this year, the evidence that was being used to do so, or why this may be happening years after details originally emerged. China is widely considered to be one of the most sophisticated and active state cyber actors—involved in spying, hacking for espionage, and gathering data. Western officials consider the country to be the biggest cyber threat, ahead of Russia, Iran, and North Korea.

"Recently, there have been many reports of US carrying cyber theft and attacks on China and the whole world," Liu says in a statement that reflects comments made by China's Foreign Ministry spokespeople this year. "The US should reflect on itself and join others to jointly safeguard peace and security in cyberspace with a responsible attitude."

Many of the disclosures in 2022—there are only a handful of previous Chinese accusations against the US—stem from private cybersecurity companies. This is similar to how Western cybersecurity companies report their findings; they are not always incorporated into government talking points, however, and state-backed media is all but nonexistent.

The potential shift in tactics could play into wider policies around technology use and development. In recent years, China's policies have focused on positioning itself as a dominant force in technology standards in everything from 5G to quantum computers. A raft of new cybersecurity and privacy laws have detailed how companies should handle data and protect national information—including the potential for hoarding previously unknown

vulnerabilities.

"One explanation is, possibly, that we are engaged in a kind of ideological—or if you want to put it more prosaically, a marketing—battle with China," says Suzanne Spaulding, a senior adviser at the Center for Strategic and International Studies and previously a senior cybersecurity official in the Obama administration. The US-China relationship has been fraught in recent years, with tensions rising over national security issues including concerns of telecom giant Huawei. "China is offering, around the world, a competing model to Western-style democracy," Spaulding says, noting that China may be responding to Western countries coming together on multiple issues since Russia invaded Ukraine.

In July 2021, China's Ministry of Industry and Information Technology published plans to boost the private security industry by 2023. Companies based in China should spend more on their defenses against cyberattacks, the government department said at the time. It also said the whole cybersecurity industry within China should look to grow in size in the coming years, as well as bolster the development of network monitoring systems and threat detection techniques. "What we've started to see over the last couple of years, increasingly, is that companies in China are building their own capabilities," says Adam Meyers, vice president of intelligence at US cybersecurity firm CrowdStrike. "There's been a few that have waded into the threat intelligence space."

But publicizing details of the long-known incidents still raises plenty of questions. Mandiant's Read says he wonders exactly how many cyberespionage cases Chinese companies and authorities are finding. The answer would provide significant clues about their true capabilities. Read says: "Is this 50 percent of what they're finding? Is this 1 percent of what they're finding? Is this 90 percent of what they're finding?"

The move appears to be strategic, says TeamT5's Che. "Considering the close relationship between China's cybersecurity firms and the Chinese government, our team surmises that these reports could be a part of China's strategic distraction when they are accused of massive surveillance systems and espionage operations."