NATIONAL SECURITY

China backed off from hacking U.S. companies. Now it is at it again.

BY TIM JOHNSON
tjohnson@mcclatchydc.com

June 07, 2018 05:00 AM
Updated June 07, 2018 05:00 AM

WASHINGTON — After a hiatus of several years, Chinese state hackers are once again penetrating networks at a range of U.S. corporations in a campaign to steal secrets and leapfrog ahead in a race for global technology supremacy, cyber researchers say.

Companies in fields such as biomedicine, robotics, cloud computing and artificial intelligence have all been hit by cyber intrusions originating in China, the researchers say.

“It’s definitely accelerating. The trend is up,” said Dmitri Alperovitch, cofounder and chief technology officer at CrowdStrike, a threat intelligence firm based in Sunnyvale, Calif.,

Chinese state hacking teams linked to the People's Liberation Army and the Ministry of State Security are becoming visible on U.S. networks again, although they are using new methods to remain undetected, researchers said.

"In the last few months, we've definitely seen ... a reemergence of groups that had appeared to have gone dormant for a while," said Cristiana Brafman Kittner, principal analyst at FireEye, a cybersecurity firm that has tracked China hacking extensively.

The activity comes after a sharp drop in Chinese hacking that began in September 2015, when former President Barack Obama and Chinese leader Xi Jinping reached an agreement to end the hacking theft of commercial secrets. The agreement quelled U.S. anger over its charge that China is the "world's most active and persistent perpetrator of economic espionage."

U.S. prosecutors in 2014 indicted five PLA officers for economic espionage for hacking into firms like Westinghouse, U.S. Steel and Alcoa. The 56-page indictment said the five men worked for Unit 61398 of the PLA's Third Department in Shanghai. The highly detailed complaint entered into details that U.S. officials later said were meant to "name and shame" China for commercial hacking.

Why China's hackers may be getting back into the game is not readily clear. Renewed trade tensions may be a reason. President Donald Trump has threatened to impose $50 billion of tariffs on China-made products to cut the U.S. trade deficit of $375 billion with China.

Another factor may be the conclusion of a massive reorganization of China's military, which began in late 2015 and under which various signals intelligence and cyber hacking units "were dissolved and absorbed into this one mega organization, called the Strategic Support Force," said Priscilla

Moriuchi, an expert on East Asia at Recorded Future, a cyber-threat intelligence firm based in Somerville, Mass.

China's Xi has laid out ambitious goal of catching up with the United States and Europe in 10 key sectors, including aerospace, semiconductors and robotics, under its "Made in China 2025" program.

Moriuchi, who spent 12 years in the U.S. intelligence community, eventually leading the National Security Agency's East Asia and Pacific cyber threats office, said China's hackers are broadening tactics, burrowing into telecommunications networks even as they steal secrets to help party leaders achieve "Made in China 2025" goals.

"The sectors that they are going after are things like cloud computing, (Internet of Things), artificial intelligence, biomedicines, civilian space, alternative energy, robotics, rail, agricultural machinery, high-end medical devices," Moriuchi said.

"There are companies in all of these sectors that have experienced intrusions over the past year from actors who are believed to be China state-sponsored," she said.

Since early in the past decade, U.S. officials have alleged that Chinese state hackers were tasked with obtaining commercial secrets from Western corporations to help Chinese firms, many of them state-owned, overtake competitors to the global forefront in technology.

In a renewed warning alert for China, a March 22 report from the Office of the U.S. Trade Representative on China's trade actions said, "Beijing's cyber espionage against U.S. companies persists and continues to evolve.

RELATED STORIES FROM MCCLATCHY DC

U.S. charges 3 Chinese with hacking but stops short of blaming Beijing directly

U.S. 'incredibly lucky' to have avoided cyber calamity this long

US losing dominance in cyber war

“The U.S. Intelligence Community judges that Chinese state-sponsored cyber operators continue to support Beijing’s strategic development goals, including its (science & technology) advancement, military modernization, and economic development,” it added.

The report said one of three state-owned oil companies, China National Offshore Oil Corp., “submitted formal requests to Chinese intelligence services seeking intelligence information on several U.S. oil and gas companies and U.S. shale gas technology.”

For his part, Alperovitch said CrowdStrike has seen Chinese efforts to breach medical research facilities, law firms, and manufacturing facilities.

When Chinese state hacking was at a peak in 2013, FireEye said it identified 72 concurrent hacking attempts, a number that fell to "fewer than 30" in the months leading up to the 2015 Obama-Xi agreement, and then to as low as six.

FireEye's Mandiant division said in an April 4 report that it had recently seen "a surge in cyber espionage campaigns targeting business-to-business services such as cloud providers, telecommunications companies and law firms." It said China may select those kinds of businesses "to collect intelligence on a broad group of targets in (a) manner than is less likely to be detected."

Cybersecurity experts say they have blocked some Chinese intrusions.

“In some cases, you’re able to detect the intrusion and remediate it before anything is stolen, so you don’t actually know what they are going after,” Moriuchi said. “In other cases, it’s not possible to see what was exfiltrated or stolen. Attackers have been and continue, some of them, to be quite good at covering their tracks.”

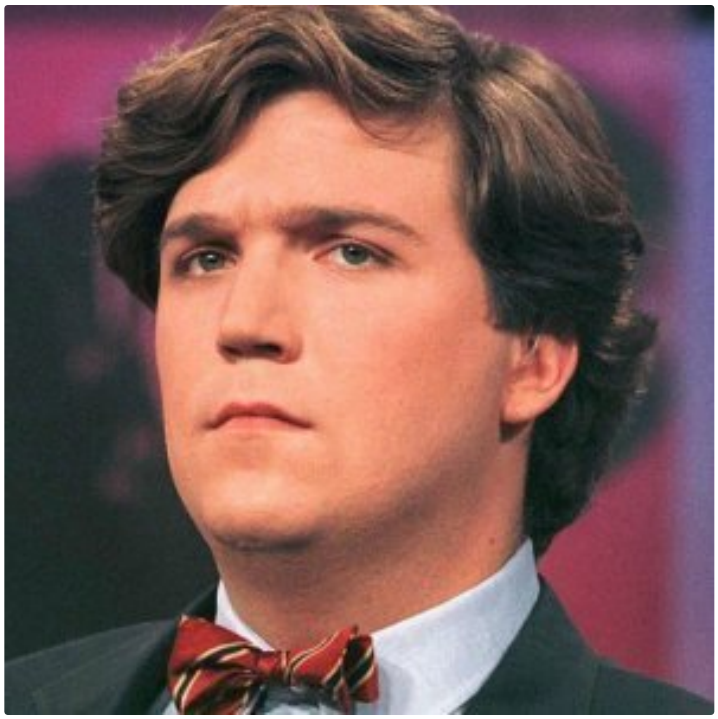
While concerned about the increased pace of Chinese hacking, Moriuchi said she's more concerned about new tactics of using off-the-shelf cyber tools to penetrate U.S. firms. Unlike tailored software, these off-the-shelf tools leave less of a signature of the group responsible, making it harder to assign blame.

“There’s greater emphasis to not get caught, to be less sloppy,” she said of Chinese hackers. “And they are taking all these actions that will make it much more difficult to defend and track their activities in the future.”

Tim Johnson, 202-383-6028, @timjohnson4

Did you get a notice that says your personal information was exposed in a data breach? Visit IdentityTheft.gov/databreach to learn what you can do to protect your identity. **Federal Trade Commission** — lena Blietz

Here's Who Jackie Kennedy Thought Had Her Husband Killed



Shady Things Everyone Ignores About Tucker Carlson

Fired 'Tonight Show' Staffers File Lawsuit

This May Be the Real Reason Hope Hicks Left Her White House Job

COMMENTS

SUBSCRIPTIONS

Newsletters

SITE INFORMATION

Customer Service

Securely Share News Tips

Contact Us

SOCIAL, MOBILE & MORE

Text News Alerts

Mobile & Apps

Beyond The Bubble Podcast

The ACC Now Podcast

ADVERTISING

Advertise With Us

MORE

Copyright

Privacy Policy

Terms of Service