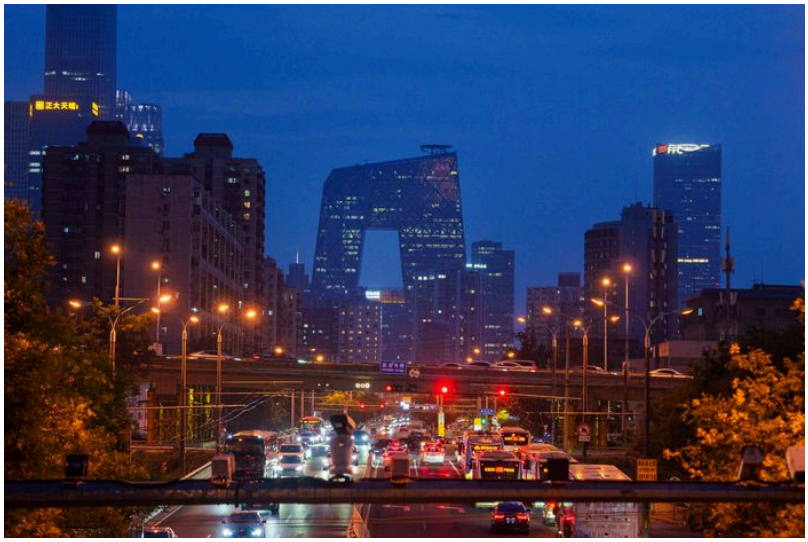
POLITICS | NATIONAL SECURITY

U.S., Allies Issue Rare Warning on Chinese Hacking Group

An advisory by Australia, along with the U.S. and six other countries, details a group known as APT40

By Mike Cherney Follow

July 9, 2024 7:38 am ET



Beijing accused the U.S. and its allies of hyping China's cyber activities. PHOTO: VINCENT THIAN/ASSOCIATED PRESS

SYDNEY—Australia, the U.S. and six other allies warned that a Chinese state-sponsored hacking group poses a threat to their networks, in an unusual coordinated move by Western governments to call out a global hacking operation they say is directed by Beijing's intelligence services.

Tuesday's advisory was a rare instance of Washington's major allies in the Pacific and elsewhere joining to sound the alarm on China's cyber activity. Australia led and published the advisory. It was joined by the U.S., U.K., Canada and New Zealand, which along with Australia are part of an intelligence-sharing

group of countries known as the Five Eyes. Germany, Japan and South Korea also signed on.

The warning marked the first time South Korea and Japan joined with Australia in attributing malicious cyber activity to China. It was also the first time that Australia—which has been reluctant to point the finger at China, its largest trading partner—led such an effort, according to a person familiar with the matter.

"In our current strategic circumstances, these attributions are increasingly important tools in deterring malicious cyber activity," said Richard Marles, Australia's deputy prime minister and defense minister.

On Tuesday, China accused the U.S. and its allies of hyping China's cyber activities to smear Beijing and distract from Washington's efforts to engage in surveillance and espionage worldwide. "Who is the biggest threat to global cybersecurity? I believe the international community sees this clearly," said Foreign Ministry spokesman Lin Jian.

Australian Deputy Prime Minister and Defense Minister Richard Marles. PHOTO: VINCENT THIAN/ASSOCIATED PRESS

The technical advisory detailed a group known in cybersecurity circles as Advanced Persistent Threat 40, or APT40, which conducts cybersecurity operations for China's Ministry of State Security and has been based in the southern island province of Hainan. The advisory detailed how the group targeted two networks in 2022—though it didn't identify the organizations—and said the threat is continuing.

"Having all eight nations collectively call this out is significant," said Rachael Falk, chief executive of the Cyber Security Cooperative Research Centre in Australia. "You don't see collective attribution from so many agencies about one malicious cyber threat actor very often."

Falk said APT40 carefully carries out reconnaissance, can look like a legitimate user and is very effective at stealing valuable data. She said APT40 rapidly exploits new, and sometimes old, public vulnerabilities in widely used software and uses compromised small home office devices. That enables the group to launch attacks and blend in with traffic.

"They are highly skilled at hiding within the network," she said, noting the group's tradecraft continues to evolve. "They look like legitimate traffic or normal users and strike with precision when the time is right, stealing valuable data."

In one of the incidents, the hackers accessed large amounts of sensitive data and got privileged authentication credentials that enabled the group to log in, the advisory said. In the other incident, the group got several hundred unique username and password pairs, as well as multifactor authentication codes and technical artifacts related to remote access sessions.

Officials didn't publicly say why the advisory was released now, though cybersecurity experts said it takes time to determine who is responsible for an attack.

The advisory suggests the group is still active despite previous efforts to disrupt it. In 2021, U.S. prosecutors charged four Chinese nationals tied to APT40 with a campaign to hack into the computer systems of dozens of companies, universities and government entities as part of an effort to steal information that would benefit Chinese companies, the Justice Department said at the time.

Three of the defendants in that case were officers in the Hainan State Security Department, a provincial arm of the Ministry of State Security, who coordinated computer hackers at front companies for the ministry. The stolen information included technologies for submersibles and autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, and proprietary genetic

sequencing technology, the Justice Department said. Infectious-disease research was also targeted.

Concerns about China's hacking campaign have grown since the 2021 case. U.S. officials are now worried that China's aims involve not just stealing sensitive data and weapons information, but also targeting infrastructure that underpins civilian life. U.S. officials have said that China is seeking to "preposition" in critical infrastructure networks for future attacks, unleashing chaos when the time is right.

Microsoft revealed last year that the state-sponsored Chinese campaign went after a range of networks on Guam and elsewhere in the U.S., including communication, transportation, maritime and other sectors. The company said the hackers were likely developing capabilities that could disrupt critical communications infrastructure between the U.S. and Asia during future crises.

The U.S. and its allies have stepped up their public criticism of Beijing in recent months. In March, the U.S. hit more alleged Chinese hackers with sanctions and criminal charges, and the U.K. government accused Beijing of hacking into its electoral register to steal personal details of voters. In New Zealand, officials also said in March that APT40 was behind an August 2021 cyberattack on networks in the nation's parliament.

Grace Zhu in Beijing contributed to this article.

Write to Mike Cherney at mike.cherney@wsj.com

Appeared in the July 10, 2024, print edition as 'U.S., Allies Issue Rare Warning on China Hacking Group'.

Videos