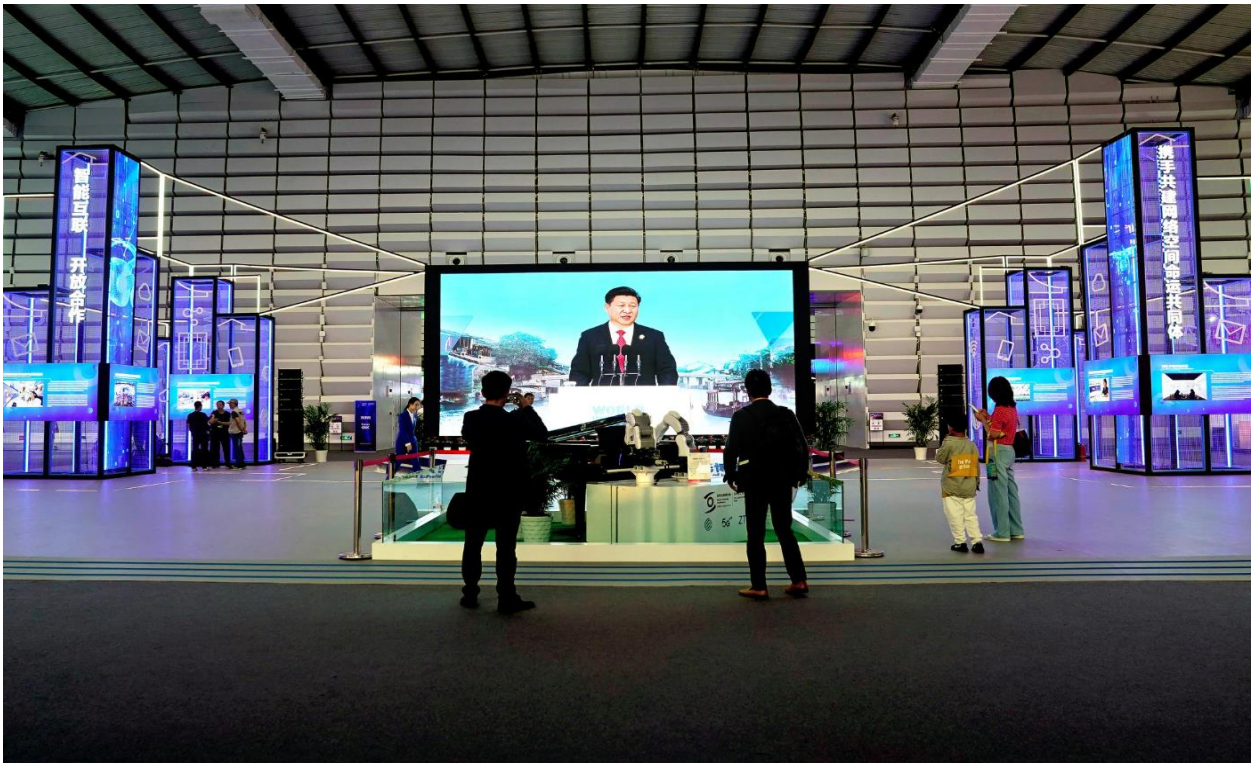
China's Military Is Tied to Debilitating New Cyberattack Tool

An Israeli security company said the hacking software, called Aria-body, had been deployed against governments and state-owned companies in Australia and Southeast Asia.



On the morning of Jan. 3, an email was sent from the Indonesian Embassy in Australia to a member of the premier of Western Australia's staff who worked on health and ecological issues. Attached was a Word document that aroused no immediate suspicions, since the intended recipient knew the supposed sender.

The attachment contained an invisible cyberattack tool called Aria-body, which had never been detected before and had alarming new capabilities. Hackers who used it to remotely take over a computer could copy, delete or create files and carry out extensive searches of the device's data, and the tool had new ways of covering its tracks to avoid detection.

Now a cybersecurity company in Israel has identified Aria-body as a weapon wielded by a group of hackers, called Naikon, that has previously been traced to the Chinese military. And it was used against far more targets than the office of Mark McGowan, the premier of Western Australia, according to the company, Check Point Software Technologies, which released a report on Thursday about the tool.

"The Naikon group has been running a longstanding operation, during which it has updated its new cyberweapon time and time again, built an extensive offensive infrastructure and

worked to penetrate many governments across Asia and the Pacific," said Lotem Finkelstein, head of the cyberthreat intelligence group at Check Point.

What made these attacks so alarming, according to Check Point and other experts on Chinese cyberespionage, was the intrusive capabilities of Aria-body, the group's new tool.

Gil Shwed, founder of Check Point Software Technologies. The company says a Chinese hacking group has targeted the governments of Australia and a number of Southeast Asian countries.Credit...Baz Ratner/Reuters

Aria-body could penetrate any computer used to open the file in which it was embedded and quickly make the computer obey the hackers' instructions. That could include setting up a secret, hard-to-detect line of communication by which data on the targeted computer would flow to servers used by the attackers.

It could also replicate typing being done by the target user, meaning that had the Australia attack not been detected, the tool would have allowed whoever controlled it to see what a staff member was writing in the premier's office, in real time.

The Australian Department of Foreign Affairs and Trade did not immediately respond to questions about the report.

"We know that China is probably the single biggest source of cyberespionage coming into Australia by a very long way," said Peter Jennings, a former Australian defense official who is the executive director of the Australian Strategic Policy Institute.

China's cyberespionage efforts have shown no sign of relenting globally and may be intensifying as tensions with Australia, the United States and other countries have risen over trade, technology and, more recently, disputes over the coronavirus pandemic. Experts say its aim is to steal vast amounts of data from foreign governments and companies.

"This may be different in design, but these attacks all have the same purpose," said Matthew Brazil, an American former diplomat and author of a new book on Chinese espionage, referring to Aria-body.

According to Check Point, the hacker using Aria-body was able to take over the computer used by an Indonesian diplomat at the embassy in Canberra, the Australian capital. The hacker found a document that the diplomat was working on, completed it and then sent it to the staff member in the Western Australian premier's office, armed with the Aria-body tool.

It was discovered only because of a simple human error.

The hacker sending the email dispatched it to the wrong address. When the server in the premier's office returned it with a note saying the email address had not been found, the transmission aroused suspicion that something in the original message was fishy, the authors of Check Point's report wrote. That prompted the investigation that revealed the attempted attack — and its novel weapon.

Naikon was previously investigated by an American cybersecurity company, ThreatConnect, which in 2015 published a wide-ranging report on the group's connection to the People's Liberation Army.

The hacking group appeared to operate as part of the military's Second Technical Reconnaissance Bureau, Unit 78020, based mainly in the southern city of Kunming, according to ThreatConnect. It is said to be responsible for China's cyberoperations and technological espionage in Southeast Asia and the South China Sea, where Beijing is embroiled in territorial disputes with its neighbors.

Check Point's report suggests that Naikon may have remained active, though it is not clear whether it has shifted out of the military chain of command.

Since early 2019, according to the Check Point report, the group has accelerated efforts to expand its online infrastructure. The hacking group has purchased server space from Alibaba, the Chinese technology company, and registered domain names on GoDaddy, an American web-hosting firm.

"Throughout our research we found that the group adjusted its signature weapon to search for specific files by names within the compromised ministries," said Mr. Finkelstein, the Check Point expert. "This fact alone strengthens the understanding that there was a significant, well-thought infrastructure and pre-operation intelligence collection."

An earlier version of this article, using information from Check Point Software Technologies, the cybersecurity company that produced the report on a new computer hacking tool, misidentified the Australian target of the Jan. 3 attack. It was the office of Mark McGowan, the premier of Western Australia, not the office of Scott Morrison, the prime minister of Australia. The error was repeated in a picture caption.

https://www.nytimes.com/2020/05/07/world/asiaa/china-hacking-military-aria.html