Exclusive-Suspected Chinese hackers stole camera footage from African Union - memo

reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idUSKBN28Q1DB

Raphael Satter

Cyber Risk
Updated

By Raphael Satter

5 Min Read

WASHINGTON (Reuters) - As diplomats gathered at the African Union's headquarters earlier this year to prepare for its annual leaders' summit, employees of the international organization made a disturbing discovery.

A signage at an entrance to the African Union (AU) Mission is pictured in Washington, D.C., U.S. December 15, 2020. Picture taken with a long exposure. REUTERS/Raphael Satter

Someone was stealing footage from their own security cameras.

Acting on a tip from Japanese cyber researchers, the African Union's (AU) technology staffers discovered that a group of suspected Chinese hackers had rigged a cluster of servers in the basement of an administrative annex to quietly siphon surveillance videos from across the AU's sprawling campus in Addis Ababa, Ethiopia's capital.

The security breach was carried out by a Chinese hacking group nicknamed "Bronze President," according to a five-page internal memo reviewed by Reuters. It said the affected cameras covered "AU offices, parking areas, corridors, and meeting rooms."

"We cannot estimate the quantity and value of the data which have been stolen," the memo continued, adding that while AU technicians had managed to interrupt the flow of data, the hackers could easily regain the upper hand.

"We are still weak to prevent another attack," the memo said.

The alert, drafted in late January and circulated to senior officials, provides a glimpse of how world powers are jockeying for influence and visibility at the continent's paramount pan-African organization. Some American and European officials have voiced concern as Beijing has stepped in to meet the AU's needs - part of an Africa-wide shift that has seen China become the continent's top creditor. Chinese workers built the AU's showpiece new conference center in 2012 and Chinese technicians still help maintain the organization's digital infrastructure.

The Chinese mission to the AU said in an email that "the AU side has not mentioned being hacked on any occasion" and that Africa and China are "good friends, partners and brothers."

"We never interfere in Africa's internal affairs and wouldn't do anything that harms the interests of the African side," the email said.

Slideshow (3 images)

Repeated messages sent to AU spokesperson Ebba Kalondo asking about the January breach were marked as "read" but went unanswered.

Longstanding doubts over Beijing's role at the AU spilled into the open in 2018, when French newspaper Le Monde reported here that AU employees had found that the servers at the new conference center were sending copies of their contents to Shanghai every night and that the building itself had been honeycombed with listening devices.

Both the AU and the Chinese government vehemently denied the report at the time, but a former AU official told Reuters the article in Le Monde was accurate and had put officials there on high alert over cyberespionage.

The former official said the latest breach was discovered following a tip from Japan's Computer Emergency Response Team (CERT), which in a Jan. 17 email alerted AU officials to unusual traffic between the international organization's network and a domain associated with Bronze President.

Koichiro Komiyama, who directs the global coordination division of Japan's CERT, confirmed to Reuters that he sent the warning after a fellow researcher discovered the malicious traffic while picking through the hacking group's old infrastructure.

The AU memo said that, within days of Komiyama's email, the AU's information technology team had traced the suspicious traffic to a set of servers in the basement of the organization's Building C - part of an older complex across the road from the new conference center.

The memo said the hackers were able to siphon off "a huge volume of traffic" from the servers by hiding it in the regular flow of data leaving the AU's network during business hours, even pausing their data theft during lunch.

Secureworks, an arm of Dell Technologies Inc which has been tracking Bronze President since 2018, confirmed that the malicious domain identified by Japan's CERT was linked to the hackers.

Secureworks researcher Mark Osborn said his company had seen strong evidence that Bronze President operated from China, adding that it had been detected in several espionage campaigns targeting China's neighbors, including Mongolia and India.

Any official protest over the spying is unlikely, according to the former AU official. He said China plays a critical role in keeping the organization running, including during an incident in June when part of the AU's network was knocked out by a power failure and Chinese technicians swiftly repaired the damage.

For that reason, the former official expects that the surveillance camera incident - like the listening devices reported in 2018 - would be swept under the rug.

"Attacking the Chinese, for us, it's a very bad idea," he said.

Reporting by Raphael Satter; editing by Jonathan Weber and Edward Tobin

Our Standards: The Thomson Reuters Trust Principles.