Report: Chinese hackers targeted Southeast Asian nations

December 8 2021, by David Rising

Morning traffic moves in front of the main building of the Malaysia Prime Minister's office is seen in Putrajaya, Malaysia, Wednesday, Dec. 8, 2021. Chinese hackers, likely state-sponsored, have been broadly targeting government and private-sector organizations across Southeast Asia, including Malaysia, according to a report released Wednesday by a U.S.-based private cybersecurity company. Credit: AP Photo/Vincent Thian

Chinese hackers, likely state-sponsored, have been broadly targeting government and private-sector organizations across Southeast Asia, including those closely involved with Beijing on infrastructure development projects, according to a report released Wednesday by a U.S.-based private cybersecurity company.

Specific targets included the Thai prime minister's office and the Thai army, the Indonesian and Philippine navies, Vietnam's national assembly and the central office of its Communist Party, and Malaysia's Ministry of Defense, according to the Insikt Group, the threat research division of Massachusetts-based Recorded Future.

Insikt said it determined that the high-profile military and government organizations in Southeast Asia had been compromised over the last nine months by hackers using custom malware families such as FunnyDream and Chinoxy. Those custom tools are not publicly available and are used by multiple groups believed to be Chinese state-sponsored, the group said.

The targeting also aligns with the political and economic goals of the Chinese government, bolstering the suspicion it is state-sponsored, Insikt said.

"We believe this activity is highly likely to be a state actor as the observed long term targeted intrusions into high value government and political targets is consistent with cyberespionage activity, coupled with identified technical links to known Chinese state-sponsored activity," the company told The Associated Press.

Security guards stand outside the Department of Foreign Affairs in Manila, Philippines on Friday, Jan. 29, 2021. State-sponsored Chinese hackers have been broadly targeting government and private sector organizations across Southeast Asia, including the Philippines Department of Foreign Affairs and the Armed Forces, according to a report released Wednesday by a U.S.-based private cybersecurity company. Credit: AP Photo/Aaron Favila, File

China's Foreign Ministry did not immediately respond to a request for comment on the allegations.

In the past, Chinese authorities have consistently denied any form of state-sponsored hacking, instead saying China itself is a major target of cyberattacks.

Of the cyber intrusions it tracked, Insikt Group said Malaysia, Indonesia and Vietnam were the top three targeted countries. Also targeted were Myanmar, the Philippines, Laos, Thailand, Singapore and Cambodia.

All countries were notified in October of the findings, though it is thought that at least some of the activity is ongoing, the company said.

"Throughout 2021, Insikt Group tracked a persistent cyber espionage campaign targeting the prime minister's offices, military entities, and government departments of rival South China Sea claimants Vietnam, Malaysia, and the Philippines," the company said. "Additional victims during the same period include organizations in Indonesia and Thailand."

The Coordinating Ministry for Maritime and Investment Affairs building is seen in Jakarta, Indonesia, Wednesday, Dec. 8, 2021. State-sponsored Chinese

hackers have been broadly targeting government and private sector organizations across Southeast Asia, including Indonesia's Coordinating Ministry for Maritime and Investment Affairs and the Ministry of Foreign Affairs, according to a report released Wednesday by a U.S.-based private cybersecurity company. Credit: AP Photo/Achmad Ibrahim

Much of that campaign was attributed to a group being tracked under the temporary identifier of Threat Activity Group 16, or TAG-16, Insikt Group said.

"We also identified evidence suggesting that TAG-16 shares custom capabilities with the (China's) People's Liberation Army-linked activity group RedFoxtrot," the group said.

Overall, Insikt Group said it had identified more than 400 unique servers in Southeast Asia communicating with malware, but it was not clear what information had been compromised.

"Many of the identified incidents spanned several months, so it is highly likely that the respective threat actors maintained long-term access to the victim networks and were able to obtain victim data over this time period in support of intelligence gathering efforts," Insikt told AP. "At this time, we do not have insight into the specific data obtained by the threat actors."

Some of the information on Indonesia was disclosed in a previous report from the Insikt Group in September, and Indonesian authorities said at he time they had found no evidence their computers had been compromised.

People ride a moped pass the National Assembly building in Hanoi, Vietnam on Wednesday, Dec. 8, 2021. State-sponsored Chinese hackers have been broadly targeting government and private sector organizations across Southeast Asia, including those closely involved with Beijing on infrastructure development projects, according to a report released Wednesday by a U.S.-based private cybersecurity company. Credit: AP Photo/Hau Dinh

Insikt Group said the earlier activity directed at Indonesia from malware servers operated by the "Mustang Panda" group gradually stopped in mid-August, following a second notification the company provided to the country's authorities.

Indonesian Ministry of Foreign Affairs spokesman Teuku Faizasyah said he did not have any information regarding Insikt Group's new findings

that the ministry had also been targeted.

Similarly, Thailand's army said it had no immediate information that its cybersecurity team had detected any intrusions into its servers.

Col. Ramon Zagala, spokesman for the Philippine armed forces, said the military had not yet seen Insikt's report but that "it takes all kinds of potential attacks seriously and has measures in place to protect our vital systems."

Insikt Group said it had also detected activity in Cambodia and Laos believed linked to Beijing's Belt and Road Initiative to build ports, railways and other facilities across Asia, Africa and the Pacific.

Soldiers check vehicles entering military headquarters Camp Aguinaldo in Manila, Philippines on Monday, March 22, 2021. State-sponsored Chinese hackers have been broadly targeting government and private sector organizations across Southeast Asia, including the Armed Forces of the Philippines and the Department of Foreign Affairs, according to a report released Wednesday by a U.S.-based private cybersecurity company. Credit: AP Photo/Aaron Favila, File

Poorer countries have welcomed the initiative, but some have complained they are left owing too much to Chinese banks.

Just last week, Laos inaugurated a $5.9 billion Chinese-built railway linking the country with southern China.

"Historically, many Chinese cyber espionage operations have heavily overlapped with projects and countries strategically important to the BRI," the Insikt Group noted, referring to the Belt and Road Initiative.

Cambodian government spokesman Phay Siphan said the country's own agencies had not detected any hacking of servers noted by Insikt Group.