Chinese hackers reportedly target India's power grid

April 7 2022, by David Rising

In an image taken from video, Chinese Foreign Ministry spokesperson Zhao Lijian speaks during a media briefing Thursday, March 10, 2022, in Beijing. India's power sector has been targeted by hackers in a long-term operation thought to have been carried out by a state-sponsored Chinese group, a U.S.-based private cybersecurity company detailed in a new report. China's Foreign Ministry spokesman Zhao said Thursday, April 7, the report had been "noted" by Beijing, but that China "firmly opposes and combats any form of cyber attacks, and will not encourage, support or condone any cyber attacks."

Credit: AP Photo, File

India's power sector has been targeted by hackers in a long-term operation thought to have been carried out by a state-sponsored Chinese group, a U.S.-based private cybersecurity company detailed in a new report.

Over the last several months, the Insikt Group, the threat research division of Massachusetts-based Recorded Future, said it has collected evidence that hackers targeted seven Indian state centers responsible for carrying out electrical dispatch and grid control near a border area disputed by the two nuclear neighbors.

The group primarily used the trojan ShadowPad, which is believed to have been developed by contractors for China's Ministry of State Security, leading to the conclusion that this was a state-sponsored hacking effort, the group reported.

"ShadowPad continues to be employed by an ever–increasing number of People's Liberation Army and Ministry of State Security-linked groups, with its origins linked to known MSS contractors first using the tool in their own operations and later likely acting as a digital quartermaster," Recorded Future said in the report late Wednesday.

China's Foreign Ministry spokesman Zhao Lijian said Thursday the report had been "noted" by Beijing, but that China "firmly opposes and combats any form of cyberattacks, and will not encourage, support or condone any cyberattacks."

"I would like to advise the company concerned that if they really care about global cybersecurity, they should pay more attention to the

cyberattacks by the U.S. government hackers on China and other countries, and do more to help promote dialogue and cooperation among countries, instead of using the cyberattack issue to stir up trouble and throw mud at China," he told reporters.

Indian External Affairs Ministry spokesperson Arindam Bagchi said India hasn't discussed the issue with China.

"We have seen reports. There is a mechanism to safeguard our critical infrastructure to keep it resilient. We haven't raised this issue with China," he said.

Indian Minister of Power R.K. Singh said the report was not a cause for concern.

"We are always prepared," he said. "We have a very robust security system. We are always alert."

Insikt Group already detected and reported a suspected Chinese-sponsored hack of 10 Indian power sector organizations in February 2021 by a group known as RedEcho. The more recent hack "displays targeting and capability consistencies" with RedEcho, but there are also "notable distinctions" between the two so the group has been given the working name of Threat Activity Group 38, or TAG-38, as more information is gathered.

Following a short lull after its first report, Recorded Future said the Insikt Group again started tracking hacking attempts on India's power grid organizations. Over the last several months, through late March, it identified likely network intrusions targeting at least seven of India's so-called "State Load Dispatch Centers"—all in proximity to the disputed border in Ladakh, where Chinese and Indian troops clashed in June 2020, leaving 20 Indian soldiers and four Chinese dead.

"Recorded Future continues to track Chinese state-sponsored activity groups targeting a wide variety of sectors globally—a large majority of this conforms to longstanding cyber espionage efforts, such as targeting of foreign governments, surveillance of dissident and minority groups, and economic espionage," the report said.

"However, the coordinated effort to target Indian power grid assets in recent years is notably distinct from our perspective and, given the continued heightened tension and border disputes between the two countries, we believe is a cause for concern," it added.

Hackers are thought to have gained access through third-party devices connected to the internet, like IP cameras, which had been compromised, the company said.

Investigators have not yet determined how they had been compromised, but Recorded Future suggested they may have originally been installed using default credentials, leaving them vulnerable.

Because the prolonged targeting of India's power grid "offers limited economic espionage or traditional intelligence-gathering opportunities," Recorded Future said it seems more likely the goal is to enable information gathering around surrounding critical infrastructure systems, or to be pre-positioned for future activity.

"The objective for intrusions may include gaining an increased understanding into these complex systems in order to facilitate capability development for future use or gaining sufficient access across the system in preparation for future contingency operations," Recorded Future said.