US Accuses Chinese Hackers in Targeting of COVID-19 Research

Hackers working with the Chinese government targeted firms developing vaccines for the coronavirus and stole hundreds of millions of dollars worth of intellectual property and trade secrets from companies across the world, the Justice Department said Tuesday as it announced criminal charges.

The indictment does not accuse the two defendants of actually obtaining the coronavirus research, but it does underscore the extent to which scientific innovation has been a top target for foreign governments and criminal hackers looking to know what American companies are developing during the pandemic. In this case, the hackers researched vulnerabilities in the computer networks of biotech firms and diagnostic companies from Maryland to California that were developing vaccines, testing kits and antiviral drugs.

The charges are the latest in a series of aggressive Trump administration actions targeting China. It comes as President Donald Trump, his re-election prospects damaged by the coronavirus outbreak, has blamed China for the pandemic.

The indictment includes charges of trade secret theft and wire fraud conspiracy against the hackers, former classmates at an electrical engineering college who prosecutors say had worked together for more than a decade. The hackers, identified as Li Xiayou and Dong Jiazhi, stole information not only for their personal profit but also that they knew would be of interest and value to the Chinese government, federal prosecutors say.

In some instances, according to the indictment, they provided an officer for a Chinese intelligence service with whom they worked, email accounts and passwords belonging to clergymen,

dissidents and pro-democracy activists who could then be targeted. The officer, in turn, provided the hackers with malicious software for use in compromising victim computers.

The two defendants are not in custody, and federal officials conceded Tuesday that they were not likely to step foot in an American courtroom. But the indictment carries important symbolic and deterrence value for the Justice Department, which decided that publicly calling out the behavior was more worthwhile than waiting for the unlikely scenario in which the defendants would travel to the U.S. and risk arrest.

The hacking began more than 10 years ago, with targets including pharmaceutical, solar and medical device companies but also political dissidents, activists and clergy in the United States, China and Hong Kong, federal authorities said.

The charges were brought as Trump administration officials, including national security adviser Robert O'Brien and Attorney General William Barr, have delivered public warnings about what they say are Chinese government efforts to use hacking and other tools to steal trade secrets for Beijing's financial benefit.

The charges are believed to be the first accusing foreign hackers of targeting scientific innovation related to the coronavirus, though U.S. and Western intelligence agencies have warned for months about those efforts. Last week, for instance, authorities in the U.S., Canada and the United Kingdom accused a hacking group with links to Russian intelligence of trying to target research on the disease, which has killed more than 140,000 people in the United States and more than 600,000 worldwide, according to figures compiled by Johns Hopkins University.

"China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals

being ‘on call’ to work for the benefit of the state, here to feed the Chinese Communist party’s insatiable hunger for American and other non-Chinese companies’ hard-earned intellectual property, including COVID-19 research,” said Assistant Attorney John Demers, the Justice Department’s top national security official.

There was no immediate indication from the indictment that the hackers had successfully obtained any COVID-19 research, despite efforts to snoop on the companies.

But prosecutors say the defendants in January conducted reconnaissance on the computer network of a Massachusetts biotech firm known to be researching a potential vaccine and searched for vulnerabilities on the network of a Maryland firm less than a week after it said it was conducting similar scientific work.

“There are literally hundreds of millions of dollars worth of trade secrets, intellectual property and other valuable information that has been stolen,” said William Hyslop, the U.S. attorney for the Eastern District of Washington state.

The case was filed earlier this month in federal court in Washington state and was unsealed on Tuesday.

An email sent by The Associated Press to the Chinese Embassy in Washington, D.C., seeking comment on the hacking charges got no immediately response. {eoa}