Security firm says Chinese hackers intercepted text messages

October 31 2019, by Tami Abdollah

In this Nov. 7, 2012 photo, U.S. and Chinese national flags are hung outside a hotel during the U.S. Presidential election event, organized by the U.S. embassy in Beijing. Government-linked Chinese hackers have intercepted the text messages of thousands of foreigners by penetrating a telecommunications provider and planting eavesdropping software on its servers, the cybersecurity firm FireEye says. (AP Photo/Andy Wong, File)

Chinese hackers with a history of state-sponsored espionage have intercepted the text messages of thousands of foreigners in a targeted campaign that planted eavesdropping software on a telecommunications provider's servers, a cybersecurity firm said.

FireEye said in a report issued on Thursday that the hackers belong to the group designated Advanced Persistent Threat 41 , or APT41, which it says has been involved in spying and cybercrime for most of the past decade. It said some of the targets were "high-value" and all were chosen by their phone numbers and unique cellphone identifiers known as IMSI numbers.

The cybersecurity firm would not identify or otherwise characterize the victims or the impacted telecoms provider or give its location. It said only that the telecom is in a country that's typically a strategic competitor to China.

The spyware was programmed to capture messages containing references to political leaders, military and intelligence organizations and political movements at odds with the Chinese government, FireEye said.

FireEye's director of advanced practices, Steven Stone, said that none of the known targets was a U.S. government official.

The discovered malware, which FireEye dubbed MESSAGETAP, was able to collect data on its targets without their knowledge but could not read messages sent with end-to-end encrypted applications such as WhatsApp and iMessage.

"If you're one of these targets you have no idea your message traffic is being taken from your device because your device hasn't been infected,"

Stone said.

FireEye said the hackers also stole detailed calling records on specific individuals, obtaining the phone numbers they interacted with, call durations and times.

A government representative at China's embassy in Washington, D.C., did not immediately respond to an emailed request for comment.

FireEye did not identify the maker of the equipment that was hacked or specify how the hackers penetrated the telecom provider networks.

It said APT41 began using MESSAGETAP during the summer, which is around when pro-democracy protests began in Hong Kong. The firm said since its discovery, it has found "multiple" telecoms targeted by the malware.

FireEye said it has observed APT41 targeting four telecoms this year as well as major travel services and healthcare providers in countries it did not identify.

Details of the espionage operation come as the U.S. tries to persuade allied governments to shun Chinese telecom equipment providers led by Huawei as they build next-generation wireless networks known as 5G, claiming they represent a risk to national security.

The U.S. government already has banned government agencies and contractors from using equipment supplied by Huawei and ZTE, another Chinese company. It is now seeking to bar their use in telecom projects that receive federal funding.

Huawei vehemently denies that it has allowed China's communist rulers to use its equipment for espionage, and Washington has presented no

proof of such. U.S. officials say a 2017 Chinese law requires organizations and citizens to help the state collect intelligence.