Coronavirus scientists are big targets for foreign cyber-espionage, FBI says

Shannon Vavra

Written by
Apr 16, 2020 | CYBERSCOOP

Nation-state hackers have been running cyber-espionage operations against medical research organizations in the U.S. that are studying the novel coronavirus, according to the FBI.

"We have certainly seen reconnaissance activity and some intrusions into some of those institutions, especially those that have publicly identified themselves as working on COVID-19 related research," the deputy assistant director of the FBI's cyber division, Tonya Ugoretz, said Thursday while speaking on a virtual panel hosted by the Aspen Institute.

Ugoretz did not specify the nature of the intrusions, the timing of the targeting and intrusions, or which entities had been targeted.

Ugoretz noted that some of the research labs or hospitals that had been the focus of the foreign intelligence operations in recent weeks include those that have publicly shared that they are working on research related to the coronavirus, such as those entities working on developing vaccines against the virus.

Several U.S. drug making titans and startups alike have begun efforts to develop treatments or vaccines for the COVID-19 illness, including Gilead Sciences Inc. and Johnson & Johnson, according to MarketWatch. The National Institute of Allergy and Infectious Diseases, a branch of the

National Institutes of Health, and the Biomedical Advanced Research and Development Authority, a division of the Department of Health and Human Services (HHS) have been supporting COVID-19 vaccine research as well.

The HHS itself has seen an increase in network scanning since it has been working to manage the pandemic in the U.S., although it was unclear if the origins of this targeting were linked to a foreign government, as CyberScoop reported.

"Countries have a very high desire for information … about how other countries are responding — about things like research on vaccines, what's happening in the U.S. healthcare sector in our research institutes," Ugoretz said Thursday. "There's certainly good reasons for those [targeted] institutions to tout the work that they're doing and educate the public. The sad flip side is that it kind of makes them a mark."

Not new for the sector

Biomedical and health-care-related research has long been a target of nation-state espionage efforts. For years, Chinese hackers have been conducting cyber-espionage campaigns against cancer-related research entities, organizations with medical intellectual property, and medical device manufacturers, according to FireEye. Suspected Chinese hackers are also believed to have targeted the German drug company Bayer in 2018 with Winnti malware. Last year a Chinese hacker was indicted for hacking health insurer Anthem in 2015.

Ugoretz' disclosure Thursday adds to the growing body of evidence that state-backed hackers are taking advantage of the fears surrounding the pandemic to advance intelligence collection. Some nation-states, such as Syria, are reported to have tried distributing illegitimate coronavirus-related

applications to citizens that are actually aimed at running surveillance, not preventing the spread of the pandemic. Other state-linked hackers have been seen targeting individuals and enterprises with coronavirus-themed spearphishing emails that seek to steal credentials or infect victim machines with malware.

The Department of Justice writ large has made it a priority in the last several months to track down scammers seeking to exploit the pandemic, and a flurry of information security experts have banded together to help the health care sector better defend against nation-states and cybercriminals alike during the global health crisis.

Overall, the number of internet crimes being reported to the FBI are currently skyrocketing, Ugoretz said. Typically, the IC3 receives 1,000 complaints a day submitted through its online portal, a number that has jumped to 3,000 to 4,000 reported online crimes per day, Ugoretz said.

"For cybercriminals there was this brief shining moment when we hoped that gosh cybercriminals are human beings too, and maybe they would think that targeting or taking advantage of this pandemic for personal profit, that might be beyond the pale. Sadly that has not been the case," Ugoretz said.