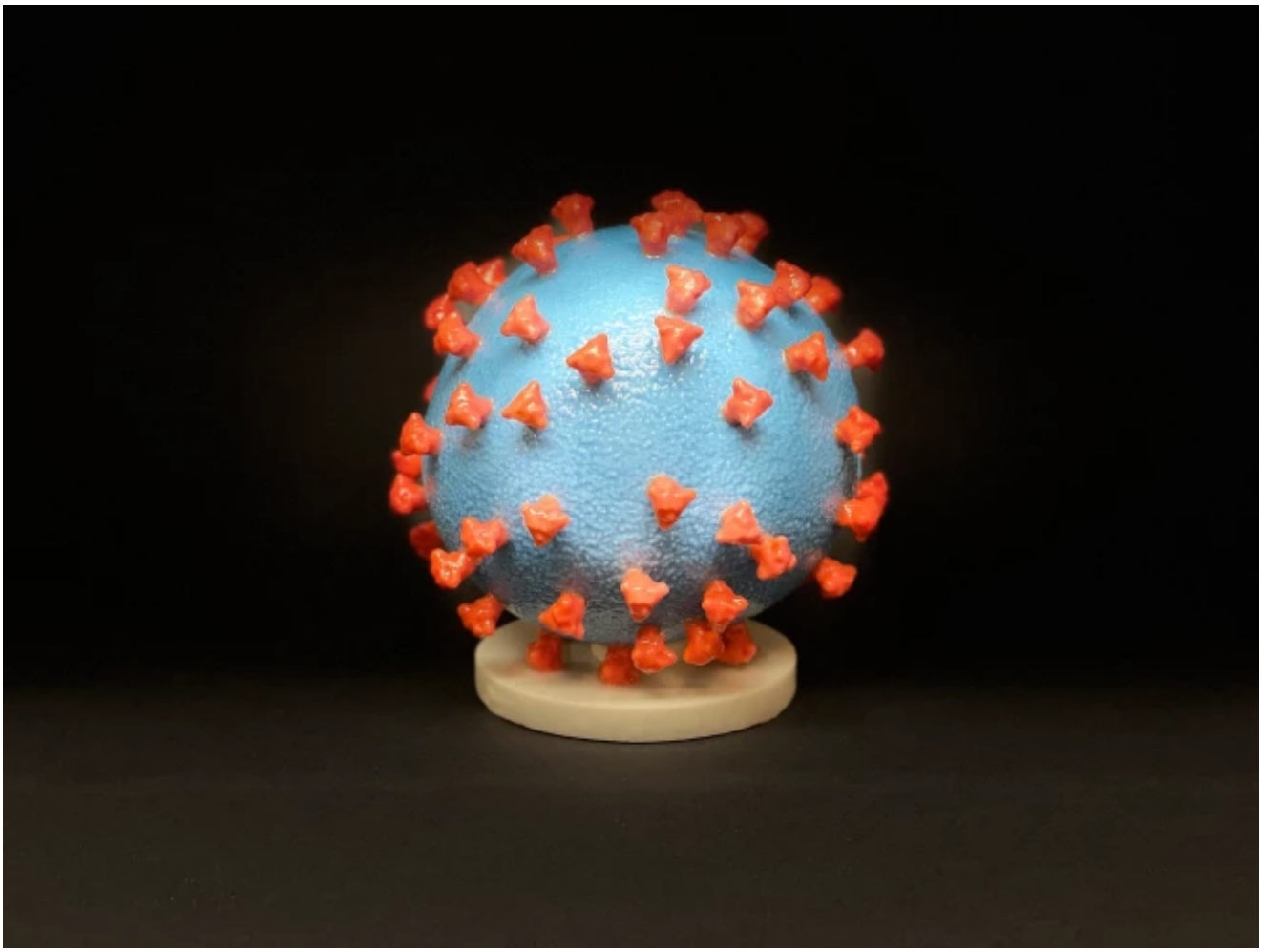
# Related news

cyberscoop.com/coronavirus-hacking-disinformation-ransomware-spearphishing/

June 24, 2020



technology

## Hackers are still running coronavirus-related campaigns, CrowdStrike warns

A three-dimensional print of a SARS-CoV-2, the virus that causes COVID-19, or coronavirus. (NIH)
Written by Shannon Vavra
Jun 24, 2020 | CYBERSCOOP
Although many municipalities around the world have begun to ease up on stay-at-home orders, hackers are still running spearphishing and disinformation campaigns taking advantage of the pandemic.

Adam Meyers, CrowdStrike's Vice President of Intelligence, says nation-state and criminal spearphishing campaigns that leverage COVID-19 themed lures are still on the rise.

"We've been seeing an increase of … behavior of social engineering where they're impersonating things like the WHO, CDC, HHS, hospitals, healthcare [entities], and even insurance companies to entice people to click links or to click on on phishing [and] open files," Meyers said Wednesday while speaking at the virtual CrowdStrike's Fal.Con for Public Sector Conference, produced by FedScoop and CyberScoop. "This is an increasing problem and it demonstrates that the threat actors have found an unprecedented level of awareness around COVID-19…and they're taking advantage of that and they're capitalizing on it."

Hackers working for China, Russia, Iran, North Korea, Pakistan, and India, as well as hacktivists and criminals, have each been using COVID-19 themed lures to either seek out information on coronavirus vaccines or collect information on how to respond to the pandemic, says Meyers.

The FBI and Department of Homeland Security have alleged that Chinese government hackers in particular have been targeting medical research entities focused on finding vaccines or treatments for COVID-19.

And as the pandemic continues to roil economies around the world, hackers are also continuing to spoof government relief packages in their spearphishing efforts, Meyers said.

"We've seen them spoofing things like the U.S. Small Business Administration, the IRS, Her Majesty's Revenue and Customs, the government of Canada, the government of France, and again sending a link or attachment, saying, 'Hey, we have a package for you … sign this digitally and we'll send you the money right away,'" Meyers said.

Ransomware actors have also been running pandemic-related hacking campaigns, Meyers said, including Traveling Spider, which has been impersonating healthcare organizations, and Circus Spider, the actors behind NetWalker ransomware, which generally targets hospitals in the U.S. and Spain.

Just in the last several days, hackers behind NetWalker said they had attacked a Philadelphia-area health system.

One active ransomware actor, which CrowdStrike refers to as Graceful Spider, is known to engage in leaking stolen victim data in order to force payment, an increasingly popular tactic among ransomware campaigns, Meyers said.

Efforts to run information operations about the pandemic that paint China in a positive light are ongoing, Meyers added. Some "manufactured videos" depicting Italians singing "thank you, China" from their balconies have circulated online, for example. Chinese efforts to

spread disinformation about the pandemic have also included campaigns questioning the origin of the coronavirus, which is believed to have originated in China, and cracking down on dissent online, according to CrowdStrike.

Social media bots, which have alphanumeric handles and were dormant for long periods before spreading pro-China messages, have recently amplified official Chinese posts, such as those from Chinese embassies, Meyers added.

“That’s pretty much a red flag in terms of influence operations on [platforms] like Twitter,” Meyers said.