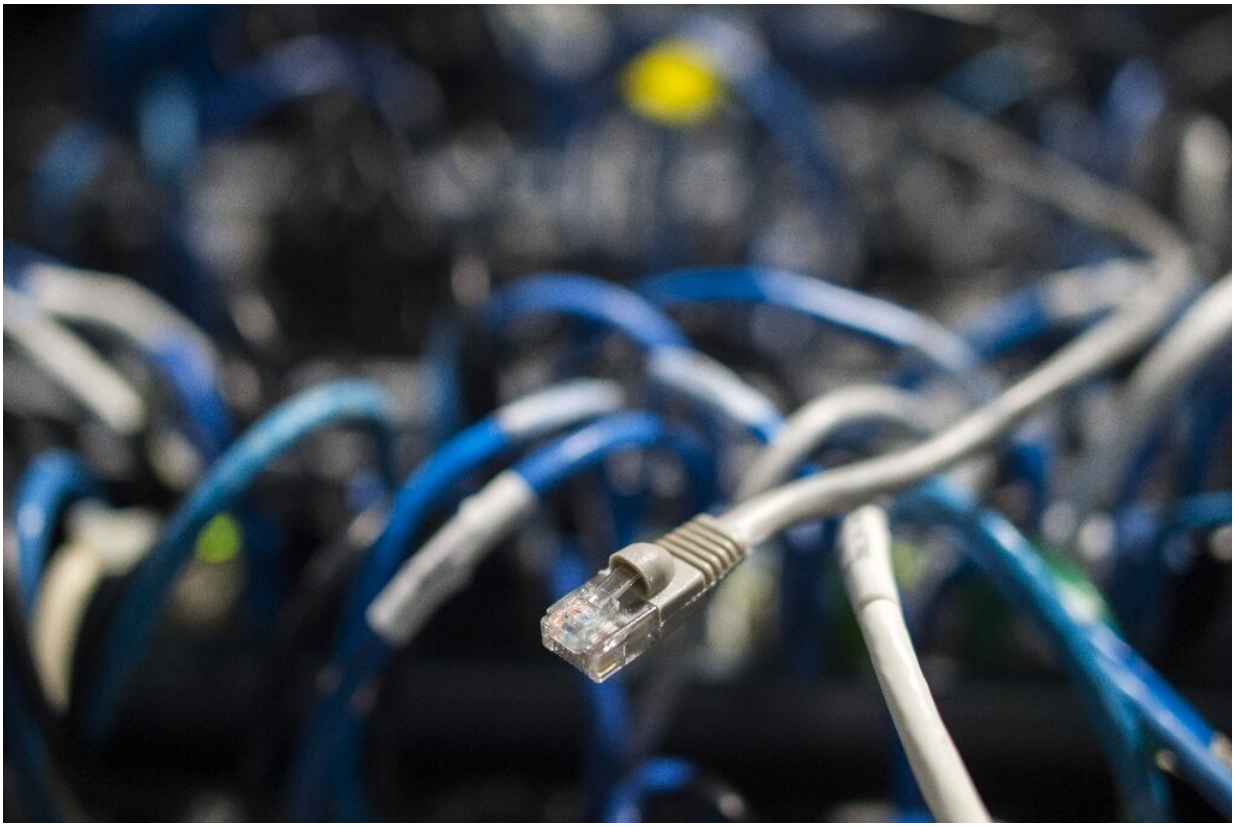
US, Britain warn that hackers increasingly use coronavirus bait

April 8 2020



US and British cybersecurity agencies say foreign government hacking operations are making use of the coronavirus pandemic to step up hacking efforts

US and British cybersecurity agencies warned Wednesday that foreign

government-backed hacking groups are using coronavirus themes to ply their way into computers and networks.

The groups are sending phishing emails and setting up websites with COVID-19 virus subjects, aiming to lure users to click on links that will expose their computers to penetration or introduce malware.

Some use email and SMS subject lines like "2020 Coronavirus updates" or "Coronavirus outbreak in your city(Emergency)", while others might offer an attached file with purported updates on national policies to deal with the pandemic, said an alert jointly issued by the US Cybersecurity and Infrastructure Agency and Britain's national Cyber Security Center.

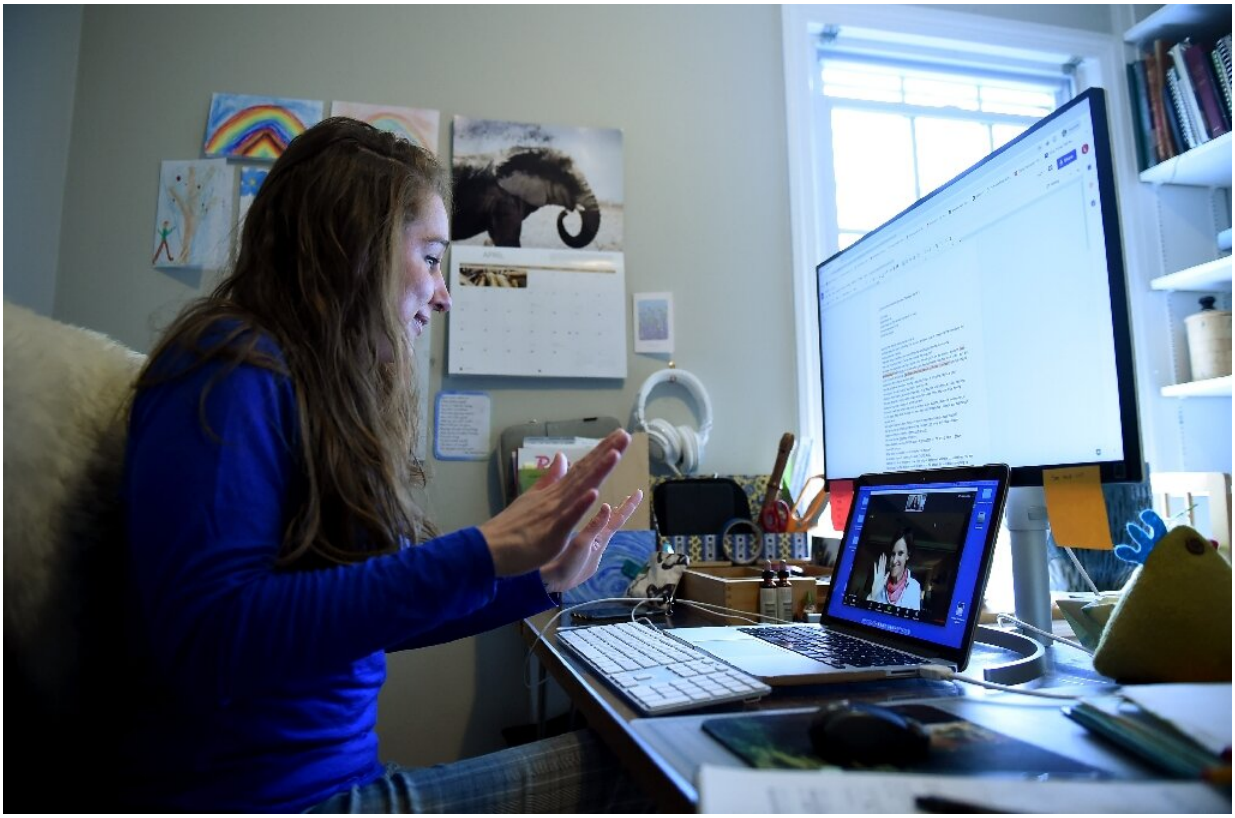
"APT groups are using the COVID-19 pandemic as part of their cyber operations, they said, referring to the "Advanced Persistent Threat" designation that Western intelligence agencies use for hacking operations tied to governments in Russia, China, North Korea and Iran.

"These cyber threat actors will often masquerade as trusted entities.... Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations."

In addition, the two cybersecurity agencies said, "cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware."

They released 2,500 web addresses tied to the scams, warning that the situation is "fast-moving" so that the list is not exhaustive.

They gave examples of an SMS sent to phones in announcing coronavirus payments to residents, and saying to click on a link that is then used to harvest personal and banking information.



The surge in teleworking in the COVID-19 pandemic has created more opportunities for foreign government-backed and criminal hacking operations to penetrate computer networks, according to the US and British cybersecurity agencies

A number of phishing emails in multiple languages pretend to come from the World Health Organization.

One sent to Italians purports to be from a senior WHO doctor and has an attached document detailing "precautions necessary to fight infection."

The attachment introduces a batch file onto the computer which opens the way for a bot to permeate the user's computer system.

One fake website pretends to be an official British government page for applying for COVID-19 relief to steal personal and financial account data.

In addition, the two cybersecurity groups said, hackers are trying to take advantage of the kinds of networking services millions of people are using to work from home.

They warn of the popular use of VPN tools that appear to offer security but in fact are commonly exploited by hackers, including products from Citrix, Pulse Secure, Fortinet and Palo Alto.

And the hackers have targeted conferencing apps like those of Zoom and Microsoft Teams, they noted.

"Malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software," they said.