Published on *The National Law Review* https://natlawreview.com

The Evolution of COVID-19 Related Cyber Threats

Article By:

Womble Bond Dickinson Communications, Technology and Media

On April 8th, the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) released a statement warning of cybercriminal and advanced persistent threat groups (APT) exploiting the COVID-19 pandemic. The statement provided that the surge in teleworking and virtual private networks use would amplify the existing cyber threat to individuals and organizations. At that point, the DHS, CISA, and NCIS had already identified some APT groups and cybercriminals as targeting individuals and entities of various sizes in COVID-19-related scams and phishing emails.

Five days later, the New York State Department of Financial Services (DFS) provided guidance to regulated entities regarding cybersecurity awareness during the COVID-19 pandemic. DFS also identified several areas of heightened cybersecurity risk as a result of this crisis, including remote working, phishing and fraud, and third party risk. The DFS recommended using more secure connections for employees using remote access such as utilizing multi-factor authentication and secure VPN connections that will encrypt all data in transit. DFS further advised regulated entities ensure that devices that are repurposed be properly secured and that BYOD policies account for mass remote working and mitigate security risks involved with it.

As of early as March 20h, the FBI had already reported a significant increase in online fraud and phishing attempts related to COVID-19. They specifically cited to the use of fake emails pretending to be from the Centers for Disease Control and Prevention, asking for charitable contributions. A greater threat has since emerged. On April 14, the New York Times reported that scientists have been "creating a global collaboration unlike any in history. Never before, researchers say, have so many experts in so many countries focused simultaneously on a single topic and with such urgency." But as this united front on combating COVID-19 appears in the scientific community, there is COVID-19 related acts of war taking place.

On May 13th, the FBI and CISA issued an announcement that there was a cyber threat directly facing COVID-19-related research. The FBI is currently conducting an investigation into the targeting and compromise of U.S. organizations conducting COVID-19-related research by cyber actors and non-traditional collectors linked to the People's Republic of China (PRC). These malicious actors are attempting obtain "intellectual property and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research." The statement warns that these cyber attacks may jeopardize the delivery of secure, effective, and efficient treatment options.

The announcement also provided some advice to entities involved in COVID-19 related research, including making the assumption that media attention surrounding this work may lead to defending more attacks. The cyber threats related to COVID-19 have changed and expanded since March and April. Malicious actors remain, looking to take advantage of system vulnerabilities among the populous who are working under different security environments than prior to the pandemic. But now the very people and entities that are leading the charge towards finding a vaccine and/or therapeutic that may resolve this crisis are the very ones being targeted by cyber actors and non-traditional collectors linked to an adversary, the PRC.

National Law Review, Volume X, Number 135