United States Senate
WASHINGTON, DC 20510

April 20, 2020

The Honorable Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, D.C. 20528

General Paul M. Nakasone
Commander, U.S. Cyber Command
Fort George G. Meade, M.D. 20755

Dear Mr. Krebs and General Nakasone,

We write to raise our profound concerns that our country's healthcare, public health, and research sectors are facing an unprecedented and perilous campaign of sophisticated hacking operations from state and criminal actors amid the coronavirus pandemic. These hacking attempts pose an alarming risk of disrupting or undermining our public health response at this time of crisis. We write to urge the Cybersecurity and Infrastructure Security Agency (CISA), in coordination with United States Cyber Command, and its partners to issue guidance to the health care sector, convene stakeholders, provide technical resources, and take necessary measures to deter our adversaries in response to these threats.

In recent weeks, Russian, Chinese, Iranian, and North Korean hacking operations have targeted the health care sector and used the coronavirus as a lure in their campaigns. In March, the cyber security firm FireEye reported that a Chinese hacking group, APT41, carried out one of the broadest hacking campaigns from China in recent years, beginning at the onset of the pandemic.[1] According to researchers, APT41 is a sophisticated Chinese state sponsored group that specializes in espionage against healthcare, high-tech, and political interests.[2] This latest campaign sought to exploit several recent vulnerabilities in commonplace networking equipment, cloud software, and office IT management tools—the same systems that we are now more reliant on for telework and telehealth during this pandemic. Included in the new Chinese

[1] Glyer, Christopher, Dan Perez, Sarah Jones, and Steve Miller. "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits." FireEye, March 25, 2020. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html.s
[2] FireEye. "Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation." FireEye. https://content.fireeye.com/apt-41/rpt-apt41/.

espionage campaign are the healthcare and pharmaceutical nonprofits and companies bracing to respond to the coronavirus. APT41's campaign also appears to reflect a broader escalation from Chinese groups in recent weeks.[3]

China is not alone in exploiting the coronavirus pandemic against our interests. Russian, Iranian, and North Korean government hackers have reportedly targeted international health organizations and the public health institutions of U.S. allies.[4] Additionally, the State Department has identified disinformation operations from Russia, Iran, and China that sought to spread false information about coronavirus to undermine the nation's response to the pandemic.[5] Unless we take forceful action to deny our adversaries success and deter them from further exploiting this crisis, we will be inviting further aggression from them and others.

The cybersecurity threat to our stretched and stressed medical and public health systems should not be ignored. Prior to the pandemic, hospitals had already struggled to defend themselves against an onslaught of ransomware and data breaches. Our hospitals are dependent on electronic health records, email, and internal networks that often heavily rely on legacy equipment. Even a minor technical issue with the email services of the Department of Health and Human Services meaningfully frustrated efforts to coordinate the federal government's service.[6] Disinformation, disabled computers, and disrupted communications due to ransomware, denial of service attacks, and intrusions means critical lost time and diverted resources. During this moment of national crisis, the cybersecurity and digital resilience of our healthcare, public health, and research sectors are literally matters of life-or-death.

The Cybersecurity and Infrastructure Security Agency and Cyber Command are on the frontlines of our response to cybersecurity threats to our critical infrastructure. Hospitals, medical researchers, and other health institutions need the expertise and resources your agencies have developed defending against these same sophisticated threats. We urge you to take all necessary measures to protect these institutions during the coronavirus pandemic, including:

1.) Provide private and public cyber threat intelligence information, such as indicators of compromise (IOCs), on attacks against the healthcare, public health, and research sectors, including malware and ransomware.

2.) Coordinate with the Department of Health and Human Services, the Federal Trade Commission, and the Federal Bureau of Investigation on efforts to increase public awareness on cyberespionage, cybercrime, and disinformation targeting employees and

---

[3] Bing, Christopher. "U.S. Cybersecurity Experts See Recent Spike in Chinese Digital Espionage." Reuters. Thomson Reuters, March 25, 2020. https://www.reuters.com/article/us-usa-china-cyber-idUSKBN21C1T8.

[4] Cimpanu, Catalin. "State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect Their Targets." ZDNet. ZDNet, March 13, 2020. https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/. Satter, Raphael. "Exclusive: Elite Hackers Target WHO as Coronavirus Cyberattacks Spike." Reuters. Thomson Reuters, March 24, 2020. https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN.

[5] MacMillan, Arthur, Shaun Tandon. "Russia-Linked Disinformation Campaign Fueling Coronavirus Alarm, US Says." AFP, February 22, 2020. https://news.yahoo.com/russia-linked-disinformation-campaign-fueling-coronavirus-alarm-us-134401587.html.

[6] "Exclusive: Email Crash Impeded HHS Response to Coronavirus." POLITICO, March 10, 2020. https://www.politico.com/news/2020/03/10/email-crash-coronavirus-hhs-125302.

consumers, especially as increased telework poses new risks to companies.

3.) Provide threat assessments, resources, and additional guidance to the National Guard Bureau to ensure that personnel supporting state public health departments and other local emergency management agencies are prepared to defend critical infrastructure from cybersecurity breaches.

4.) Convene and consult partners in the healthcare, public health, and research sectors, including its government and private healthcare councils, on what resources and information are needed to reinforce efforts to defend healthcare IT systems, such as vulnerability detection tools and threat hunting.

5.) Consider issuing public statements regarding hacking operations and disinformation related to the coronavirus for public awareness and to put adversaries on notice, similar to the joint statement on election inference issued on March 2nd.

6.) Evaluate further necessary action to defend forward in order to detect and deter attempts to intrude, exploit, and interfere with the healthcare, public health, and research sectors.

We stand ready to work with you to provide any further resources necessary in this effort. Thank you for your attention to this urgent matter.

Sincerely,

/s/ Richard Blumenthal

RICHARD BLUMENTHAL
United States Senate

/s/ Tom Cotton

Tom Cotton
United States Senate

/s/ Mark R. Warner

MARK R. WARNER
United States Senate

/s/ David A. Perdue

David A. Perdue
United States Senate

/s/ Edward J. Markey

EDWARD J. MARKEY
United States Senate