PUBLICATION

# COVID-19 – Cybersecurity Risks for Health Care and Research Institutions are Heightened

**May 18, 2020**

**The health care industry and research organizations searching for vaccines and/or improved treatment protocols are on the front lines of the battle against COVID-19. There are obvious inherent risks to treating COVID-19 patients and performing research on infectious diseases, exposure to the virus chief among them. Another risk for COVID-19 health care providers and researchers that has been exacerbated by the COVID-19 crisis is the threat of cyber-attack.**

The United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) recently issued an alert warning that malicious cyber actors are targeting health care and other essential services related to COVID-19. According to the CISA and NCSC alert, health care providers, pharmaceutical companies, academia, medical research organizations and local governments face heightened risks. CISA and NCSC report observing advanced persistent threat (APT) actors scanning external websites and probing for vulnerabilities in unpatched software.

On May 13, 2020, the Federal Bureau of Investigation (FBI) and CISA issued a more specific warning to COVID-19-related research entities that malicious cyber actors associated with the People's Republic of China (PRC) have been observed targeting U.S. organizations conducting COVID-19-related research. The FBI and CISA announcement indicates that these "actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research."

The FBI announcement advises organizations engaged in COVID-19 research to "maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material." Implementing effective cybersecurity and insider threat policies and procedures was a necessity before the pandemic. It is even more critical now – particularly for those whose involvement in response and research related to the virus has been covered by the media. The time for heightened vigilance is now.

CISA and NCSC are actively investigating password spraying by APT actors against health care organizations. Password spraying involves the use of commonly used passwords until a single user's account is breached. Once a single compromise occurs, the malicious actors will obtain access to other systems where the same password is used. In addition, once in, the bad actors can attempt to move laterally through the system and attack additional users.

The recent CISA and NCSC guidance recommends several preventive measures to mitigate the likelihood of a password spraying attack:

- Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords.
- Review IT helpdesk password management related to initial passwords, password resets for user lockouts and shared accounts.
- Use additional assistance and tools to help detect and prevent password spray attacks.
- Require the use and protection of strong passwords.

- Use multi-factor authentication (MFA).
- Review MFA settings to ensure coverage over all active, internet facing protocols.
- Implement an effective password administration system.
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and configurations.
- Protect the management interfaces of your critical operational systems.
- Establish a security monitoring capability.
- Review and refresh your incident management processes.
- Use modern systems and software.
- Invest in preventing malware-based attacks.

Although not the focus of this alert, the May 13, 2020, FBI and CISA announcement stresses the importance of insider threat programs in protecting an organization's cyber systems. An insider threat program will make it more likely that users who have been exhibiting unusual behavior or activity will be identified and their access to cyber systems suspended. A discussion of CISA guidance regarding insider threat programs is available here. Establishing an insider threat program for a health care provider, university or other research institution engaged in COVID-19 response or research would have lasting effects – like protecting patients and intellectual property – after the threat of COVID-19 passes.

If you have questions, please contact your Baker Donelson attorney. Also, please visit our Coronavirus (COVID-19): What You Need to Know information page on our website.