Hackers Target Healthcare Industry During COVID–19 Pandemic

Amidst the pandemic overwhelming the capacity of many hospital systems, hackers have been quick to target healthcare providers and medical agencies. These cyber-attacks have hit both the United States and Europe in recent days, serving as a reminder for organizations to closely review their information security posture during these times of uncertainty.

Despite certain hacker groups stating their intent to refrain from targeting healthcare organizations for the duration of the COVID-19 crisis, publicly reported cyber-attacks in March 2020 included a ransomware attack on the **Champaign-Urbana Public Health District** in the United States, and the downing of critical systems at **Brno University Hospital** in the Czech Republic. In addition, attacks against the **World Health Organization** have more than doubled while the **U.S. Department of Health and Human Services** was purportedly hit by an attempted DDoS attack.

While some activity can be attributed to cybercriminals motivated by profit who seek to exploit organizations with a weak security infrastructure, the targeting of healthcare agencies is also being carried out by Advanced Persistent Threat groups involved in cyber espionage. Media reporting indicates that proprietary information related to tests or vaccines would be considered highly valuable intellectual property to governments and businesses competing to find a cure.

The COVID-19 crisis will continue to test the resiliency of the global healthcare industry. Although no organization can remain invincible from a cyber-attack, there are numerous steps that can be taken to reduce the odds of becoming the next victim of a breach.

We suggest that healthcare providers take the following actions in response to this alert:

1. **Be prepared with a clear incident response plan:** is the organization prepared for a ransomware attack or other form of breach? Does the organization have relationships with incident response and digital forensics providers? When was the last time a test of current plans and processes was performed?
2. **Perform deep and dark web searches to avoid strategic surprise:** does your healthcare organization know what hacker groups are discussing about you online? How many of your employees' login and password credentials have been compromised in third party breaches that could be used to penetrate your network? Searches performed by Aon in March 2020 revealed over 5,000 compromised credentials associated with one of the most prestigious medical research centers and hospital systems in the United States.
3. **Redouble efforts for vulnerability management on critical technologies and platforms:** now is a good time to perform scanning, analysis and testing for vulnerabilities in the environment. Does the organization have a holistic approach to identifying, analyzing, remediating and tracking weaknesses across the environment?

Continued >

4. **Ensure that restricted access controls and mechanisms are optimized:** has the organization sufficiently restricted access to systems, networks, applications and data? Have multifactor authentication, privileged access management (PAM), and other critical identity and access management (IAM) controls been reviewed and validated recently?

5. **Test patient-specific aspects of business continuity plans**: although many organizations have already activated components of their business continuity plans due to the national emergency, hospitals may wish to consider testing scenarios in which critical systems related to patients become unavailable for multiple days.ut Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Empower Results®