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

# Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up

Article By:

Megan Hardiman

Doron S. Goldstein

Jeremy Merkel

The health care industry has long been a primary target of malicious cybercriminals, but since the emergence of COVID-19, organizations on the front lines of fighting the pandemic have experienced a rise in cybersecurity incidents and attacks. Between February and June of 2020, HIPAA-covered entities reported 192 large scale data breaches to the US Department of Health and Human Services, Office of Civil Rights (OCR) – more than twice as many as were reported during the same period in 2019.[1]

While the types of cyber threats health care organizations have encountered during the COVID-19 pandemic are not wholly original, factors including the rapid shift to remote work, the expansion of telehealth and the strain on resources experienced by many organizations, have combined to create new security vulnerabilities and challenges. For example, in recent months, some health care organizations may have temporarily relaxed firewall rules to facilitate additional work-from-home capabilities, short-circuited vendor diligence or contracting protocols in order to rapidly deploy or expand telehealth capabilities, or quickly erected temporary medical facilities in parking lots and convention halls that lacked traditional security infrastructure. While governmental authorities have (temporarily) waived various regulatory standards and eased enforcement for certain privacy, security and breach notification requirements during the public health emergency, malicious cyber actors cannot be expected to show similar restraint.

## The Evolving COVID-19 Cyber Threat Landscape

While the types of cyber threats health care organizations have encountered during the COVID-19 pandemic are largely similar to the pre-COVID landscape, cyber threat actors are exploiting pandemic-related fear and uncertainty, as well as new vulnerabilities created by the shift to virtual environments. The FBI's Internet Crime Complaint Center (IC3) reported that it had received 1,200 complaints related to coronavirus cyber threats through March, which far surpasses the number of complaints it received for all types of internet fraud in 2019.[2] Authorities have warned that cyber actors are targeting health care bodies, pharmaceutical companies, academia, medical research

organizations, and local governments, as well as others involved in the national pandemic response. In addition to seeking to steal information for commercial gain, hackers may attempt to steal valuable information related to the pandemic response strategy, such as sensitive COVID19-related research or intelligence on national and international healthcare policy.

The sophisticated threat actors that are exploiting the COVID-19 crisis have a global reach. In March, Canada's Centre for Cybersecurity warned of malicious hackers targeting their health care sector to gain unauthorized access to intellectual property and research and development related to COVID-19. Simultaneously, the Czech Republic faced a series of cybersecurity incidents, including an attack against one of its largest COVID-19 testing facilities, which caused it to terminate operations and relocate patients to other hospitals. The danger to public health and safety resulting from such malicious activity prompted the U.S. Department of State to condemn this cyber warfare in a call for global action.[3]

Below are a few examples of cyber threats in the era of COVID-19, as well as some practical steps organizations can take to manage cyber risk in today's increasingly virtual environment.

### *Ransomware Threats Targeting Health Care Organizations*

In the early stages of the pandemic, hacking groups pledged to spare hospitals and health care organizations from cyberattacks. These "assurances" were short-lived. In March, hackers deployed the ransomware variant known as *Maze* to attack a U.K.-based laboratory that was testing COVID vaccines. *Maze* has the ability to exfiltrate files on a system, and pressures the victim to pay a ransom by threatening to publish the data on the dark web. Fortunately, the facility was able to restore their systems, but that didn't stop the hackers from pressuring them to pay the ransom by publishing thousands of patient records containing medical questionnaires and copies of passports on the Internet (reportedly, the facility never paid).[4] In June, the University of California San Francisco reported that it paid a $1.14 million ransom after malware encrypted certain servers within its school of medicine.[5]

In response to the continued threat of ransomware attacks targeting the health care sector, Microsoft's Threat Protection Intelligence Team warned hospitals that their network devices and VPNs were specific targets as organization transitioned to a remote workforce.[6] The warning was consistent with a joint alert issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI on May 22, in which the agencies reported that unpatched VPNs topped the list of vulnerabilities being routinely exploited by sophisticated foreign cyber actors in 2020.[7] The *REvil* (a.k.a. *Sodinokibi*) variant is one of the ransomware campaigns that actively exploits these vulnerabilities to penetrate an organization's infrastructure. Following a successful exploitation, the hackers can steal credentials, elevate privileges and move laterally across compromised networks, installing ransomware or other malware payloads. In contrast to auto-spreading ransomware, like *WannaCry* or *NotPeya*, in which hackers employ credential theft and lateral movement methods traditionally associated with nation-state actors, *Maze* and *REvil* are human-operated ransomware campaigns, which incorporate social engineering tactics that exploit users' fears and need for information. This is why the hackers behind these types of ransomware target organizations that are most vulnerable to disruption, like those that have not had the time or resources to assess security hygiene, install the latest patches, update firewalls, or check the privilege levels of users and endpoints. In the age of COVID-19, health care organizations may be particularly vulnerable.

### *COVID-Related Phishing Attacks and Voicemail Phishing*

Bad actors carrying out email phishing attacks have exploited fears about the coronavirus and relied on impersonation tactics, like spoofing communications from governmental agencies like the Center for Disease Control or World Health Organization to induce users to enter credentials or click links that install malware and put sensitive and confidential information at risk. According to Bitdefender, hospitals and clinics, pharmaceutical institutions, and distributors of medical equipment are the most frequent targets of phishing email campaigns, with messages about COVID treatments and therapies, or personal protective equipment (PPE) that is in low supply.[8] In fact, American, Canadian and British organizations that are rushing to develop a coronavirus vaccine have been targeted by Russian cyber criminals aimed at stealing research and medical supply chain data in order to win the race for a vaccine. According to the National Security Agency, the hackers responsible for this espionage are known as APT29 and Cozy Bear, which are the same groups associated with hacking the Democratic National Committee's servers during the 2016 election.[9]

Another phishing method is voicemail phishing. Some health care organization are using legacy phone systems known as Private Branch Exchange (PBX) to automate calls and record voicemail messages that are sent to users' inboxes so employees don't miss important messages while working remotely.[10] The scheme involves the attackers spoofing messages from the PBX system and informing an employee that they have a new voicemail message. To hear the message, the user is directed to a website that spoofs PBX integrations with the aim of stealing credentials. The hackers rely on the fact that users have the same access credentials across multiple platforms, which may contain personal or proprietary information.

***Password Spraying (and Credential Stuffing) Directed at Health Care Organizations***

Password spraying is a type of brute-force attack in which hackers try to obtain the passwords of multiple accounts at once by feeding many usernames or email addresses into a program that attempts to match those accounts with commonly used passwords. A joint advisory issued by CISA and the UK's National Cyber Security Centre (NCSC) warned of this threat being directed at health care and medical organizations, and advised users to change any passwords that could be reasonably guessed to one created with three random words.[11?]

Similarly, credential stuffing involves the automated injection of usernames and password combinations that have previously been compromised, usually in an older data breach, to gain access to user accounts. In April, over 500,000 Zoom account credentials that were gathered through credential stuffing were sold on dark web for less than a penny, and in some cases, were given away for free.[12] The consequences of this have been seen through the rise of "Zoom-bombing" and other malicious activity involving video-teleconferencing platforms.[13] To reduce the risk of these types of attacks, organizations are strongly encouraged to implement multi-factor authentication and require that employees change their passwords frequently

## Tips for Better Cyber Health

- **Update your security risk analysis and risk management plans.** Ensure your security risk analysis is updated for technology and operational changes made in response to the pandemic and implement any corresponding risk treatment plans to reduce the likelihood of being impacted by a cybersecurity incident, such as a ransomware attack. In particular, be sure to identify potential risks and vulnerabilities related to expanded remote work, deployment of new telehealth capabilities and technologies and development of additional testing and treatment locations.

- **Confirm full compliance of telehealth operations.** Providers that rolled out telehealth services in a manner that may not have fully complied with HIPAA standards in reliance on OCR's Notice of Enforcement Discretion and/or other temporary waivers of privacy/security requirements should ensure that they have, at a minimum, implemented all recommendations set forth in the Notice (for example, enabling all available encryption and privacy settings, providing notification to patients that of potential privacy risks, entering into appropriate business associate agreement with the technology vendor).[14] In accordance with the US Department of Health and Human Services' guidelines of voluntary cybersecurity practices for health care organizations, providers should also identify any HIPAA and other privacy and security law gaps, and develop a plan to remediate any vulnerabilities as soon as possible.[15]

- **Review privacy and security policies and procedures.** Review, and if necessary expand, your privacy and security policies and procedures to be sure they adequately address current operations, particularly in regards to remote work, telehealth and any other new or expanded operations. More information from Katten on best practices for remote work is available here.

- **Update training to reflect the current environment.** To ensure personnel are aware of their privacy and security obligations in the COVID era, train regularly on your policies and post the policies on the organization's intranet and/or circulate them to personnel via email. Training should be practical and reflect today's virtual environment – from using secure collaboration tools, to identifying COVID phishing emails and scams, to securely disposing of paper when working from home.

---

[1] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.* U.S. Department of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 29, 2020).

[2] *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments.* Federal Bureau of Investigation, https://www.ic3.gov/media/2020/200401.aspx (April 1, 2020).

[3] *The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector.* US Department of State, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attackagainst-the-czech-republics-healthcare-sector/ (April 17, 2020).

[4] *COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online. Forbes,* https://www.forbes.com/ sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-postedonline/#78b40ab218e5 (March 23, 2020).

[5] *Update of IT Security Incident at UCSF.* https://www.ucsf.edu/news/2020/06/417911/update-it-securityincident-ucsf (June 26, 2020).

[6] *Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do.* https://www.microsoft.com/ security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-whatto-do/ (April 1, 2020).

[7] *Top 10 Routinely Exploited Vulnerabilities.* US Department of Homeland Security, https://www.us-cert.gov/ncas/alerts/aa20-133a (May 12, 2020).

[8]*5 Times More Coronavirus-themed Malware Reports during March.* Bitdefender, https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themedmalware-reports-during-march/ (March 20, 2020).

[9] R*ussia Is Trying to Steal Virus Vaccine Data, Western Nations Say. New York Times,* https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html?searchResultPosition=5 (July 16, 2020).

[10]*Voicemail Phishing Scam Identified Targeting Remote Healthcare Workers. HIPAA Journal,* https://www.hipaajournal.com/voicemail-phishing-scam-identifiedtargeting-remote-healthcare-workers/ (June 8, 2020).

[11]*APT Groups Target Healthcare and Essential Services.* US Department of Homeland Security, https://www.us-cert.gov/ncas/alerts/AA20126A (May 5, 2020).

[12] *Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords.* Forbes, https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-getsstuffed-heres-how-hackers-got-hold-of-500000-passwords/#4768c0cb5cdc (April 28, 2020).

[13]*FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing.* Federal Bureau of Investigation, https://us-cert.cisa.gov/ncas/currentactivity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom (April 2, 2020).

[14]*Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency.* US Department of Health and Human Services, Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notificationenforcement-discretion-telehealth/index.html (March 30, 2020).

[15]*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.* US Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response, https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf (last visited July 14, 2020).



National Law Review, Volume X, Number 217