Issued 12/14/18

30 Percent of Healthcare Databases are Exposed Online

It took them some 90 hours to try to gain access to 50 databases used by healthcare organizations and they found that 15 of them (i.e., 30 percent) easily discoverable and accessible to anyone who knows where to look and has a basic understanding of healthcare technology solutions. The researchers concentrated on several popular technologies used for handling medical records, including known and widely used commercial databases, legacy services still in use today, and new sites or protocols that try to mitigate some of the vulnerabilities of past methods. They perused technical documentation, employed Google and Shodan searches, subdomain enumeration, and relied on some educated guessing about the combination of sites, systems and data to discover exposed data. "Simply knowing where to look (like the IP address, name or protocol of the service used) was often enough to access the data," they shared. As researchers affiliated with the Institute for Critical Infrastructure Technology pointed out a while ago [link], the medical identity theft that occurs as a result of the compromise of EHRs from healthcare organizations can financially devastate victims and presents a critical risk to their physical health. "Due to the longevity of the [electronic health] record, adversaries may continue to exchange and exploit the compromised information for the rest of the victim's life. For some, such as children, this can drastically hinder their future financial stability and limit the potential lives that they could lead," they added. The going rate for one EHR on online black markets is currently estimated at $1, which is much lower than the price of a single credit card record. This is because it takes scammers more effort and time to successfully use the information in EHRs to "earn"

money (e.g., by extortion) or get additional and more useful information (e.g., via phishing).