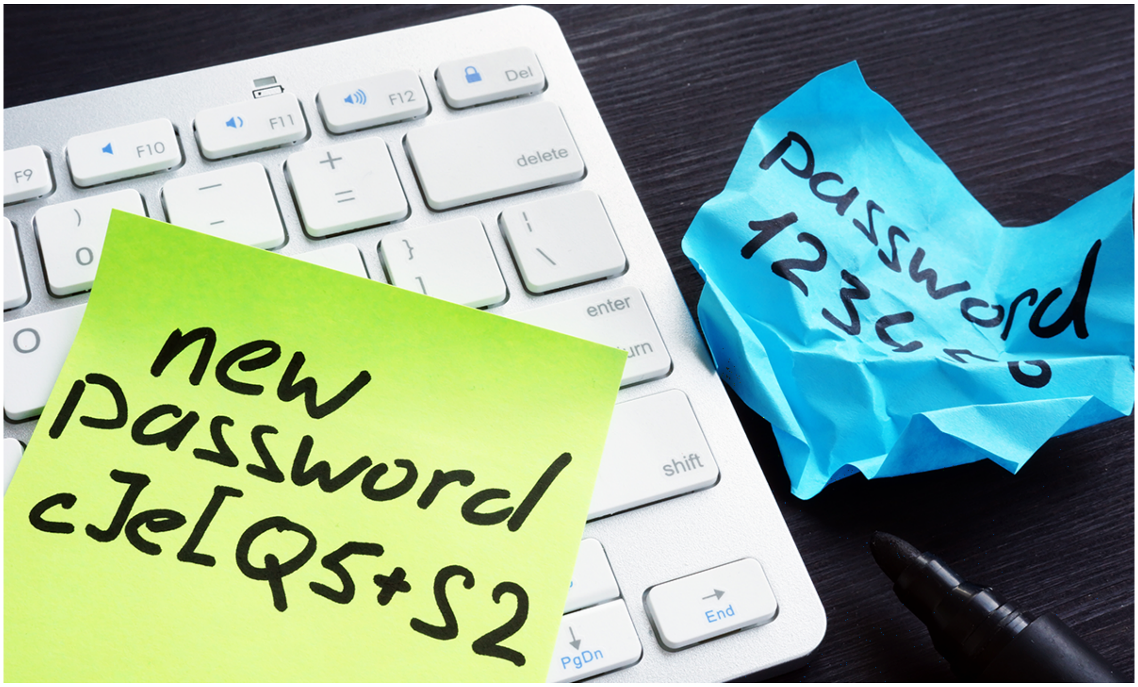
Weak Password Allows Major Cyber Extortion



By Justin Joy, JD, CIPP

After arriving at the office on a Tuesday morning following a holiday weekend, a medical assistant at an ophthalmology practice* logged into her workstation to pull up the clinic schedule for the day. For an unknown reason, the assistant received an error message on her computer screen when she attempted to access the schedule. Around the same time, a physician was attempting to pull up a diagnostic test stored on the practice's picture archiving and communication system (PACS) server. Similar to the problem experienced by the medical assistant, the physician was also unable to access the imaging of her patient performed the Friday before the holiday weekend. Both the medical assistant and the physician contacted the practice's administrator about the unexplained problems they were experiencing with the group's system. The practice administrator then placed a call to the help desk at the group's third-party IT vendor about the two problems.

Upon receiving the report of the two problems, a technician employed by the vendor, a local IT managed service provider (MSP) firm, promptly accessed the practice's computer system using a remote access tool. The technician attempted to access the server hosting the practice's data to troubleshoot the problem.   In viewing the files contained on the server, the tech immediately noticed that all of the files had time stamps indicating that they had been changed within the past 72 hours and the filenames had been appended with text that did not appear to be correlated to the data. Upon further investigation, the MSP tech discovered a text file containing a note demanding a ransom payment be made in cryptocurrency of 5 bitcoin (which, at the time of the attack, was the equivalent of over $50,000) in order to regain access to the data. The note indicated the group had less than 36 hours remaining to pay the ransom or else the ransom would double. The note also indicated that if the ransom was not subsequently paid in 72 hours, the data would become permanently inaccessible.

The technician, along with the owner of the MSP firm, contacted the practice administrator to report the findings. The MSP owner stated to the practice administrator that the group appeared to have been hit with a ransomware attack, and all the practice's data stored on the impacted servers had been encrypted and rendered inaccessible.   The practice administrator immediately contacted SVMIC thereafter to provide notice of the incident. The SVMIC claims attorney taking the call then contacted SVMIC's third-party cyberliability insurer, Tokio Marine,[1] about the incident.

Tokio Marine promptly contacted a law firm to request that they advise the insured medical practice. Following a couple of initial telephone calls with the practice administrator, the retained law firm contacted a digital forensic investigation firm which focused on responding to data security incidents and requested that they assist in the incident response. Specifically, the digital forensic investigation firm was requested to immediately confirm that the medical practice's system was not subject to ongoing or persistent compromise. Once there was some assurance that the attacker had been fully eradicated from the system, the digital forensic investigation firm began an investigation to determine the initial point of entry the adversary exploited to attack the network and took steps to determine whether any protected health information (PHI) had been accessed or stolen ("exfiltrated") by the attacker. Additionally, the investigation/cyber incident response firm was requested to contact the adversary to begin ransom demand negotiations in the event it was necessary to pay the ransom in order to attempt to restore the practice's data.

In the meantime, while the practice administrator, the group's retained legal counsel, and the investigation firm were looking into the matter, the practice's waiting room continued to fill up for the day. Many patients were turned away, as no records could be accessed. For patients with more acute conditions who needed to be seen that day, they were examined, with the findings recorded on paper and stored in a secure file drawer. One patient presented who needed a medication refill urgently. A nurse had to spend an hour looking for the key to the drawer where one physician's paper prescription pad was stored because the practice's electronic prescribing system was not functional due to the ransomware attack. No billing for any of the services provided that day could be entered into the system, as the practice's financial management system was also inaccessible.

While the group's MSP firm was very cooperative in the efforts, by the end of the day on Tuesday, it was unclear whether the medical practice had a full and viable backup of its data. As a result, the investigation firm proceeded to engage in negotiations with the adversary in the event that the ransom payment was necessary in order to attempt to recover the data. The MSP had required all user passwords to be reset shortly after the ransomware attack was discovered. The investigation firm was able to provide some preliminary assurance that it appeared the immediate threat had been eradicated from the group's system. However, as the cyber incident response firm made clear from the outset, a payment of any amount of ransom was no guarantee that any of the data would be retrievable.

On Wednesday morning, following some negotiation with the adversary by the incident response firm, the ransom demand had been reduced slightly, to 3.5 bitcoin, or around $35,000. Fortunately, the MSP was able to confirm that a backup of the practice's data had completed at approximately 2:00 AM on the preceding Saturday morning, just about three hours before the attacker began encrypting the practice's data. It was also with relief that the MSP confirmed that the malicious software had not encrypted the data on the backup system. New hard drives were inserted into the workstations and servers that had been identified as impacted, and the MSP began restoring the practice's data from the backup. The old hard drives were preserved for evidence. The MSP provided an estimated recovery time of all systems no earlier than mid-day on Friday.

For the remainder of the week, as the practice's systems were restored piece by piece, patient care capacity was significantly reduced, with many patients continuing to be turned away. It was not until after noon on Friday that the practice had regained full access to all its data from the rebuilt systems and recovered data. It took the practice another full week to input the medical record information that was recorded on paper while the systems were down, and it was another two weeks until all the billing information had been brought up to date.

Within about a week and a half after the attack, the forensic investigation firm had completed its initial investigation. It determined that the adversary had accessed the practice's network by way of its Windows Remote Desktop Protocol. The user account, which had administrator-level privileges, and which was compromised to access the system remotely, had a weak password that had not been changed in at least two years. Additionally, multi-factor authentication was not enabled for the user account. Fortunately, however, there was sufficient evidence from the investigation indicating that the attacker was only in the system long enough, about 30 minutes, to install and launch the malicious software that encrypted the practice's data over the long holiday weekend. Based on the evidence examined, there was no indication that the adversary viewed, accessed or exfiltrated any of the practice's PHI as a result of the incident.

Lessons Learned

While estimates vary considerably, by any annual measure—whether it is dozens or hundreds of attacks—ransomware is an undeniable threat to healthcare entities, as covered in a recent SVMIC newsletter article. Under the framework of the ransomware guidance from the U.S. Department of Health and Human Services (HHS) addressing ransomware in the context of HIPAA, it is generally believed that many, if not most, ransomware attacks do not result in reportable HIPAA breaches. As a result, the actual number of attacks against healthcare entities is unknown.

Taking proper preventative steps is the most effective means of avoiding ransomware attacks in the first place. In this claim scenario, the practice suffered a ransomware attack due to a weak remote access account password, which was likely acquired from a darkweb site or easily guessed. The extended period of time since the password was last changed (if ever) makes a weak password even more vulnerable. Additionally, the practice had not implemented multifactor authentication (MFA) to the Internet-facing account. MFA is not readily and conveniently available for all systems, but it is something that should be explored for an additional layer of protection. Finally, while not a specific issue in the investigation, it was not clear whether the practice had evaluated if every user needed to have administrator-level privileges. Limiting levels of access can, in some cases, help prevent the installation of malicious software.

One positive takeaway from this claim is that the practice had a viable and fresh backup. When a practice is hit by a ransomware attack, there are usually two options: #1, recover your data from a backup; or #2, pay the ransom and cross your fingers that you get a valid decryption utility from the hacker. Unfortunately, in many instances, a viable recent backup is not available, eliminating the preferable option. There are a number of reasons why a viable backup may not be available, not the least of which is that the backup system is not segregated from the network and the backup data is also encrypted by the same malicious software impacting the other data. It is important that groups work with their IT staff or their outside MSP vendor to configure their backup systems to be resilient against ransomware while also reliably and frequently backing up the practice’s critical data. Backup system resiliency and comprehensiveness should be periodically evaluated.

Another positive outcome from this otherwise unfortunate claim is that the digital forensic examination was able to determine with a reasonable degree of certainty that there was not any improper access or exfiltration of PHI or other sensitive data. For a variety of reasons, there are some instances where such a reassuring finding cannot be made. In those cases, where either there is an indication that data has likely or actually been accessed or acquired, or there is insufficient evidence to reach a point where a determination can be reasonably made that such access or acquisition was unlikely, notification to patients, HHS, and in some instances, the media, may be necessary. Additionally, it is becoming increasingly common that ransomware actors are extorting victims twice: first by demanding a ransom to be paid, purportedly in exchange for a decryption utility; and then, even in cases where a good backup is available, demanding a ransom be paid or else the adversary will disclose sensitive data that it claims to have stolen from the practice’s system.

Healthcare entities of all sizes are prime targets for ransomware attacks. The threat has increased in recent years and shows no signs of abating. As this claim scenario demonstrates, even with a relatively good outcome—where no ransom had to be paid, and no notification was required—ransomware attacks are extremely challenging, disruptive, and costly to healthcare groups. Preventative measures are the best first step to take to avoid ransomware attacks. Groups should also be ready to quickly respond in the event they become a victim.

* Several facts about this claim have been changed to anonymize the individuals and entities involved, but the consequences of ransomware attacks, as presented here, are real.

[1]. For more information about resources available from Tokio Marine HCC and its role in cyber liability claims, see these articles from May 2021 and June 2021.

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.