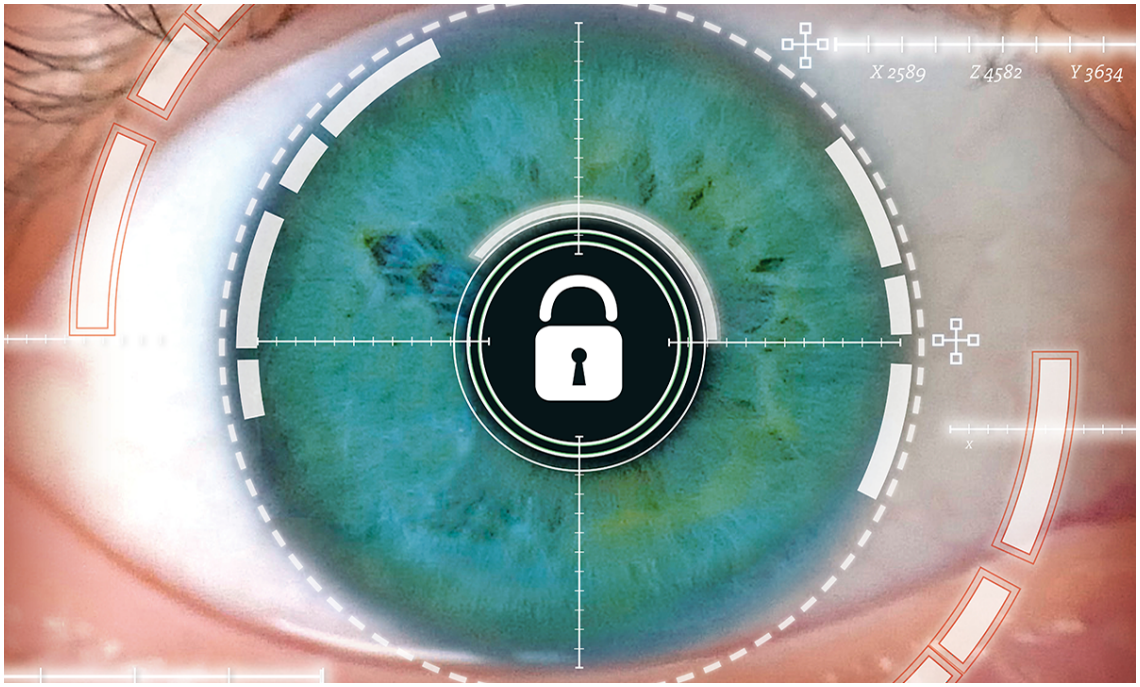
Ransomware 2.0 - The New Generation of Ransomware



By Rana McSpadden, FACMPE

On May 7, 2021, the U.S. felt firsthand the consequences of a ransomware attack when the Colonial Pipeline Company was hacked by the criminal cybergroup DarkSide. This hack disrupted a major infrastructure system and caused panic for many Americans. Even though Colonial Pipeline paid the $4.4 million ransom, the pipeline remained offline for several days as IT experts worked to clean and restore the network.

Prior to the Colonial Pipeline hack, third-party service provider MedNetwoRX (which services Aprima's electronic medical records system) reported a ransomware attack on April 22, 2021[i] that affected some clients for more than two weeks. These clients scrambled to implement emergency procedures so they could continue serving their patients. As a result of the attack, patient records and schedules were rendered inaccessible. Affected practices did not know who would be coming in that day and could not schedule new patients nor could they access patient contact information to reschedule non-emergency visits for a later date. Without access to records, patient care was put at

risk since providers could not access histories, allergy lists, or medication lists. The attack, likewise, disrupted cash flow as affected practices were unable to submit claims. To these practices, this attack was just as devastating as the Colonial Pipeline attack.

According to a recent report from Check Point, there has been a 57%[ii] increase in ransomware attacks since the beginning of 2021, with healthcare being the number one affected industry. On average, healthcare organizations see 109 attempted attacks each week. Of course, large corporations are not the only groups at risk for ransomware attacks. An estimated 43%[iii] of all cyberattacks target small businesses. This is generally because small businesses lack the funding for strong internal cybersecurity programs staffed with full-time cybersecurity professionals and layers of the latest security technology. However, the relatively smaller cybersecurity budget of private medical practices does not mean that smaller practices necessarily have to be at greater risk. The first step to a good cybersecurity program is to know your risks and educate staff. In Justin Joy's June 2020 article, he outlined how practices should leverage the HIPAA Security Rule to help defend against these threats.

Emerging Ransomware Trends

Original ransomware tactics were to deposit malicious software into systems, either through phishing email scams that infect files or by downloaded software which would encrypt (lock up) the victims' systems. Then attackers would demand payment to unlock the system. For many victims, it was easier to pay the ransom than try to restore their system, particularly if they did not have adequate backups in place. As groups began instituting better system backups from which they could restore their systems, this original tactic began losing effectiveness. To combat this, hackers began using double extortion tactics. They began exfiltrating data from their victims' computers prior to encrypting the systems. Demand notices began informing victims to either pay the ransom or their data would be released to the dark web. They would send the victims proof of the data they stole. As a result of this new tactic, hackers saw a 171%[iv] increase in ransom payments. To increase their profits even further, towards the end of 2020 and into 2021, hackers began implementing triple extortion tactics. With this, not only does the initial victim receive a demand for payment, but their patients and customers whose data was involved in the theft also receive demand emails. Finally, in recent months, if ransomware victims fail to pay the ransom, some hackers have started deploying Distributed Denial of Service (DDoS) attacks, as well as making threatening phone calls to victims to encourage payment. A DDoS attack is where hackers flood a victim's network with malicious traffic that keeps the victim's system from communicating or working as it should. It is unknown how widespread these emerging trends are, but it is always necessary to remain vigilant.

Responding to Ransomware

Prevention is always the best policy, but what if you are the victim of a ransomware attack? What should you do? **Do not pay the ransom**. Contact SVMIC so that we can activate your cyberliability policy and put you in touch with Tokio Marine (our third-party cyberliability insurer) to speak with their legal experts. Each attack is unique, and the

response will vary based on the situation. Once Tokio Marine is involved, they will walk you through next steps which may include reaching out to IT professionals to get you up and running while still preserving evidence. Of course, paying the ransom may be a last resort but should **ONLY** be done under the direction of the experts at Tokio Marine.

Finally, the determination of whether a HIPAA breach has occurred because of the ransomware attack requires a legal analysis, often made based on findings from a digital forensic investigation and other information specific to the incident. If the determination is made that a breach has occurred, assistance will also be provided with the breach notification process, including notification to various federal and state government bodies (if applicable).

If you have questions about cybersecurity or access to these resources, call us at 800-342-2239 or email ContactSVMIC@svmic.com.

If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

[i] https://www.healthcareitnews.com/news/reported-ransomware-attack-leads-weeks-aprima-ehr-outages

[ii] https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

[iii] https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=The%20Growing%20Threat%20Of%20Ransomware&text=Ransomware%20has

[iv] https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/
