COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 8. August 06, 2020 Hit with Ransomware? Here's What Your Organization Is Up Against

By Jane Anderson

Ransomware attacks are changing and becoming far more sophisticated, meaning hospitals and other health care entities need to step up their games to defend against these potentially crippling security events, the American Hospital Association (AHA) concluded.[1]

“The threat I worry most about is a ransomware attack on an overloaded hospital caring for COVID-19 patients that would interrupt patient care, or worse, shut down operations at the facility—thereby putting frail patient lives at risk,” wrote John Riggi, AHA senior advisor for cybersecurity and risk. Riggi pointed out that a ransomware attack in the Czech Republic resulted in that exact outcome, with Brno University Hospital forced to redirect patients to other hospitals.

Most cyberattacks on health care facilities are carried out by skilled, sophisticated criminal groups, Riggi said, and therefore, hospitals need to work with federal investigators and coordinate among themselves. “Leveraging the entire law enforcement, intelligence and military capabilities of the U.S. government is necessary to achieve swift and certain consequences against these attackers,” he added in the document authored for AHA members.

COVID-19 Spikes Ransomware Cases

Sanjay Deo, president and founder of 24By7Security Inc. in Coral Springs, Florida, noted in a recent webinar that the coronavirus pandemic has led to a noticeable uptick in ransomware incidents.

“In the current state of COVID-19, we are seeing a tremendous increase of ransomware attacks,” Deo said. The biggest reason, Deo noted, is that advances in “ransomware-as-a-service” have made the tools for hacking available to anyone who can navigate the dark web, with little or no technical expertise needed.

In fact, more than 4,000 ransomware attacks have occurred every day since 2016, a 300% increase since 2015, when there were just more than 1,000 attacks per day, Deo said. However, he added, another reason is that people are staying at home because of the COVID-19 pandemic: “The whole world is sitting at home. They are not going to work. They have nothing else to do. So guess what? They are all trying to hire hackers and trying to make some money.”

Over the past two years, 24By7Security, which specializes in HIPAA compliance, security risk assessment and incident response management, has handled around 20 ransomware cases, ranging from attacks involving a two-person pharmacy with one laptop up to a Fortune 500 company with 400 servers, Deo said. “Hackers are not discriminating. It doesn’t matter where you are. If they find a victim, they’re going for it. They are basically focused on that weakness you have, and they basically go and attack you.”

Phishing Most Prevalent

By far, the most prevalent type of ransomware used is phishing or spear-phishing emails, Deo said, which accounts for 67% of ransomware attacks in North America. A lack of cybersecurity training, weak passwords and access management, poor user practices, and gullibility also play significant roles, he said, while malicious websites and web advertising play minor roles.

CryptoLocker currently is the most common type of ransomware out there, while WannaCry, which was responsible for multiple high-profile attacks in 2017 and 2018, also is prevalent, Deo said. "[Hackers] are very well organized, to the point where they have a quasi help desk," Deo said. "What that means is, when you send them your ransom questions, they will immediately respond to you."

Understanding of Attack Timeline Is Crucial

Deciding whether or not to try to negotiate with hackers can be difficult, Deo said. In order to negotiate with hackers, health care entities first need to understand the timeline that leads to a ransomware message on their networks, Deo said.

"We have gotten calls at 10:00 at night and at 6:00 in the morning—all sorts of times—but that doesn't mean that's when it all started. That's when the actual execution happened. That's the time when the ransomware notice comes on your screen," he said. "So before that, the hacker has already come and done reconnaissance on your network, they have sent you phishing emails, the weaponized emails have been delivered and some person has clicked on it. And the moment you click on it, that's when the command and control starts."

Common ways for malware to be delivered via phishing are faux links to small bonuses, such as Starbucks gift cards, Deo said. "If you click that email and you click the link, nothing [visible] would happen. But a piece of malware has been embedded on your laptop, and that malware, depending on which family it is, will start to do its thing. Some of them actually propagate—they go from one laptop to another. The others actually embed themselves and then start capturing key logs."

The hackers can build a "dictionary" of users, user IDs and passwords, Deo said. They can identify administrators and determine when and how often the company backs up its data, he added. "They're very organized. They're very strategic. They know exactly what they're doing. And in some of the latest [attacks] we've handled in the last year, we have seen that the hackers have become very sophisticated, that once they get in, they know where the actual crown jewels are that they can encrypt. They also know where your backups are."

In fact, in one case, the user had created backups using Amazon's cloud servers, and the hackers deleted all the backups in the cloud, along with the local backup, Deo said. "They will understand what your behavior is, and then they will try to exploit that behavior."

Once the hackers are ready, with a full understanding of how the target organization functions and where its data resides, they make their move, he said. "They will bring you to a point where you're completely helpless, and that's when they will encrypt all of your servers and desktops and laptops. So you can't do anything."

Contact Deo at contact@24by7security.com.

[1] John Riggi, "Ransomware Attacks on Hospitals Have Changed," American Hospital Association Center for Health Innovation, last accessed August 4, 2020, https://bit.ly/2DfNtGr.