Protecting Hospitals During a Crisis

December 03, 2020

Hospital cybersecurity is not a foreign con

se of electronic health

According to the American Hospital Association (AHA), ransomware attacks on healthcare providers have increased in frequency, sophistication, and severity over the last few years. And phishing emails and other cyber attacks aimed at hospitals have only grown since the start of the COVID-19 pandemic.[1] So how can hospitals arm themselves against nefarious attacks? And what does the cybersecurity industry's response mean for the future of healthcare?

Hospitals and Cybersecurity In the Best of Times

Hospitals are common ransomware victims, mainly because scammers count on the urgent need to function to encourage administrators to just pay the ransom. Ransomware has traditionally been considered a white-collar crime in which the consequences are financially, but not physically, harmful. The AHA says that these attacks on hospitals cross the line from an economic crime to a threat to life crime

since these attacks nearly always pose a potential threat to patients' health and safety within the hospital.[1]

The first ransomware attack was in 1989 and involved a Trojan Horse virus sent to AIDS researchers.[1] Much has changed since then; there is more at stake as hackers target specific medical devices as well as networks, servers, PCs, databases and EHRs. In the spring of 2017, the world caught a glimpse of the havoc that attackers could wreak on the medical industry. A ransomware attack called WannaCry caused computer screens at National Health Services (NHS) hospitals to display pop-up messages demanding $300 in bitcoin to regain access to their files. But this attack went beyond the NHS hospitals in the UK. WannaCry hit 150 countries on the first day, infecting over 200,000 computers and 1,200 diagnostic devices worldwide. Email systems were down, doctors had no access to their patients' EHRs and blood test analysis devices and MRI machines were rendered useless. The NHS was forced to cancel 19,000 surgeries and appointments. The attack cost the NHS alone over $100 million.[2]

WannaCry should be viewed as a trend rather than an isolated incident. The FBI considers WannaCry to be the first ransomware attack that widely targets vulnerabilities found in medical devices. And while this ransomware is still active, there are patches and best practices to prevent it from infecting systems.[3] There are still active threat actors ready to strike in the best of times, and even more eager to act when fears and tensions are running high.

Hospitals and Cybersecurity In the Worst of Times (Or, How the Pandemic Has Increased Cyber Threats)

So if these are the types of attacks hospitals face under normal conditions, what are malicious actors doing when resources in the medical field are stretched to razor-thin margins?

If you keep tabs on cybersecurity news at all, you likely know that the pandemic has made everyone's data less secure. As we all shifted to work from home, the protections afforded to us by our companies' networks have gone and organizations are noticing attackers trying to exploit this weakness. The FBI's Cyber Division reported that the Internet Crime Complaint Center (IC3) receives between 3,000 and 4,000 cybersecurity complaints per day. Before the COVID-19 pandemic, that daily number was about 1,000.[4]

The rise in threats is particularly dire for hospitals since locking doctors out of patient records, and shutting down vital machines can have life-or-death consequences. And imagine if a hospital with an already tight budget has to spend money on a ransom. In that case, it may mean it doesn't have money to buy additional ventilators or personal protective equipment.

At the start of the pandemic, some known scammers and malware attackers promised to abstain from attacking healthcare organizations and hospitals. In an unsurprising turn of events, this truce was too good to be true. Within a few weeks of making that promise, they flooded the internet with phishing emails pretending to be healthcare organizations and attacked hospitals and critical health facilities. In April, Google was blocking 18 million COVID phishing and malware email deliveries daily.[5]

Currently, the dark web has seen a rise in real and fake hospital network administrator credentials for sale. Large quantities of stolen patient data, hydroxychloroquine pills and "Covid vaccines" are also up for grabs for those looking to buy.[2]

Hospital Cybersecurity During a Crisis

In response to this influx of malicious activity, a group of hackers and cybersecurity experts teamed up to form the COVID-19 Cyber Threat Intelligence League (CTI League). And if this sounds like the Avengers or Justice League for computers, then you're not far off.

Created in March of 2020, the CTI League is a self-described global volunteer cyberthreat community-CERT. They aspire "to protect the medical sector and the life-saving organizations (MS-LSO) worldwide from cyber-attacks, supplying reliable information, reducing the level of threat, supporting security departments and neutralizing cyber threats."[6] In its first month of existence, the invitation-only group garnered over 1,400 vetted members based in 76 countries and covering 22 time zones. These volunteers come from 45 different sectors ranging from cybersecurity and healthcare to computer emergency response teams (CERTs) and government.[7]

In the first month of operation, they found over 2,000 healthcare software vulnerabilities in 80 different countries. They identified almost 400 malicious files that standard antivirus software would be unlikely to stop and flagged around 3,000 domains for removal. They also helped to legally take down 2,833

cybercriminal assets on the web, including 17 that were designed to impersonate government organizations, the U.N. and the World Health Organization.[7]

The group uses Shodan, Greynoise, VirusTotal and Slack to perform their work. And while their initial intent was to protect hospitals, the League now has experts in everything from advanced persistent threats to dark web tracking. And more importantly, they have the sheer numbers to tackle the problems. They hunt for healthcare system vulnerabilities, track down malicious sites, analyze malware, sort through phishing scams and scour the dark web for compromised medical credentials and COVID-related scams. The deeper they dig, the more areas they find where they can help. And with members in nearly every time zone, that help is available around the clock in multiple languages.[2]

Escalating those threats proved to be a challenge at first. They had the information but couldn't get it to the authorities who could act on it. Now, the CTI League has medical contacts through the Health-ISAC (Information Sharing and Analysis Center), allowing them to quickly inform vulnerable parties about risks they may be unaware of. The League also includes law enforcement members across the globe, from the FBI and Interpol to local officers on remote islands. This is particularly helpful when the group finds malware or other attacks that appear to be produced by nation-states.[5]

What the Future Holds

As we cope with the reality of the pandemic, our mentalities have shifted from a two-week emergency response to a more sustained status quo. The question of what comes next looms large. Healthcare infrastructure will still need support from the cybersecurity community, and the CTI League and its volunteers look to be a permanent fixture. But events like the U.S. presidential election and eventually, the Olympics, will likely bring on a new wave of cyber threats. We will probably see attackers taking advantage of fear and misinformation, using rumors spread on the internet to get people to click on links that seem innocuous.

The best way to combat this is with facts and information, and to detect and remove the threats in all forms. The skills gap in the cybersecurity field needs to be filled by qualified individuals who are willing to help the most vulnerable. Now is the time to join their ranks by earning your MS in Cybersecurity online from the Katz School of Science and Health.

Sources

1. Retrieved on October 6, 2020, from aha.org/center/emerging-issues/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
2. Retrieved on October 6, 2020, from wired.com/story/cyber-avengers-protecting-hospitals-ransomware/
3. Retrieved on OCtober 6, 2020, from csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
4. Retrieved on October 6, 2020, from thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
5. Retrieved on October 6, 2020, from csoonline.com/article/3539319/legions-of-cybersecurity-volunteers-rally-to-protect-hospitals-during-covid-19-crisis.html
6. Retrieved on October 6, 2020, from cti-league.com/
7. Retrieved on October 6, 2020, from cti-league.com/wp-content/uploads/2020/04/CTI-League-Inaugural-Report-March-2020.pdf

Return to Blog

16 January 16, 2024

Spring 2024 Term

Stay Connected

Yeshiva University has engaged Everspring, a leading provider of education and technology services, to support select aspects of program delivery.

Questions? Let's Connect.

Schedule a Call

Apply Now

Request Info

onlinecyber@yu.edu
866-545-9506