Capstones

Craig Newmark Graduate School of Journalism

Fall 12-16-2019

Ransomware is Quietly Devastating American Healthcare Facilities

Benjamin Powers
Craig Newmark Graduate School of Journalism

Ransomware is Quietly Devastating American Healthcare Facilities

The patient didn't attract any attention initially. They were just one more cog moving through the system that was the massive hospital complex on your average day. That was, until they were shown to a room, and left alone. At that point, they removed a flash drive from their pocket and tried to insert it into a computer — with the goal of accessing the hospitals systems.

This is according to the Chief Information Security Officer at a major Northwest university hospital system, who asked for anonymity due to the sensitive nature of such attacks.

The imposter patient was attempting to install malware on the hospitals system, potentially with devastating effects. And although security was alerted to their presence, the imposter was able to sneak out, and was not caught.

This happens more often than you might think. In fact, it also happens with people impersonating residents.

“Every July we have brand new physicians as residents coming in, and even though we have pictures of everybody, it's easy to slip in,” says the officer.

And the impact of such malware isn't benign, it can have acute consequences — consequences that are being felt across the United States.

Ransomware attacks, in which malware denies the victim (such as a hospital) access to a computer system or data until a ransom is paid, have exponentially increased across the U.S. in the last few years, according to recent reports. They've resulted in ambulances having to be diverted over a hundred miles to get care for the patients they carry, chief medical officers being unable to administer important medications because they're locked out of patient medical records, and even some smaller medical practices having to shut down entirely after their patient records were deleted for refusing to pay the ransom, according to experts.

In conversations with more than a dozen experts, hospital representatives, government authorities and others, they contend the pace of ransomware attacks on US healthcare facilities such as hospitals is only set to increase. The costs of dealing with such attacks, the life-threatening impacts it can have on patients, and the technical expertise of repelling them are a never-ending game of cat and mouse, in which security practitioners and IT officers are perpetually trying to defend against new threats. Whether they'll succeed is still an open question.

“They're using the social part of humans,” says Cris Ewell, Chief Information Security Officer at the University of Washington Medical System. “And knowing how busy people it’s easy to entice them to click on something to gain information.”

The rise of ransomware

Ransomware attacks can occur through a number of means, and be carried by a number of actors. One of the highest profile attacks involving ransomware is one that some people may have heard of — WannaCry.

In May of 2017, the attack, which exploited a Windows operating system vulnerability, rapidly spread to hundreds of thousands of computers in over 130 countries in mere hours. It temporarily crippled Britain's National Health Service (NHS), affecting more than a third of NHS facilities, resulting in nearly 7,000 appointments being canceled as a direct result of the attack, including medical operations, according to a subsequent report by Britain’s National Audit Office (NAO). It also found that 19,000 additional appointments were affected. These cases included 139 people who potentially had cancer and had urgent appointments canceled, according to the report. Other patients needing urgent care were diverted to facilities that were not affected. It didn’t just affect the NHS though. It affected systems across the world, including those in the US, such as the University of Washington hospital system.

“It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice. There are more sophisticated cyber threats out there than WannaCry so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks,” said Amyas Morse, head of the National Audit Office at the time.

The updates to fix the Windows vulnerability had been released two months before the WannaCry attack.

WannaCry is generally seen as the largest ransomware attack in history. But two years later, in 2019, there are still computers that are sometimes infected with the program, according to TechCrunch, a technology publication. Using Shodan, a search engine that identifies unsecure databases and devices, TechCrunch found nearly a million endpoint devices were still vulnerable to WannaCry, with the majority of those in the US.

That’s a problem because ransomware attacks aren’t slowing down.

“With the combination of nefarious hackers and nation states as well as targeted individuals, institutions, and infrastructures, this thing becomes much more problematic,” says Matt Rahman, the COO of IOActive, a cybersecurity firm with offices across the world. “The tools and techniques that's being used today by these other people today are very sophisticated. Right now we're in an arms race.”

Research from the American Medical Association found that AMA 83% of physicians work somewhere that has experienced a cyberattack. A report from McAfee, a cybersecurity company that develops countermeasures for such attacks, saw a "resurgence of ransomware along with changes in campaign execution and code" in the first quarter of 2019. Ransomware incidents were up 118 percent across all sectors, and up 18 percent in the healthcare sector, third most among the industries McAfee looked at. In early October, the FBI released an alert warning against increased ransomware attacks on healthcare facilities, among other industries.

The alert notes at since 2018 "the incidence of broad, indiscriminate ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly."

The human cost of ransomware

Far from a removed computer program that sits benignly on a computer and merely means that it needs to be replaced, ransomware has a tangible effect on the people in the systems it targets. In the last few months, at least two smaller doctors offices, neither of which responded to interview requests, have had to shut down entirely after declining to pay ransoms to decrypt their data, including billing and patient records. In Alabama, a ransomware attack against three hospitals run by DCH Health Systems resulted in ambulances en route to those hospitals having to alter their course and head to different facilities. DCH Health Systems did not respond to multiple interview requests. Even as recently as late November, an IT provider of data storage and security called Virtual Care Provider Inc. (VCPI) was the victim of a ransomware attack, in which the hackers demanded $14 million to restore the seized data. The cost is high, but also the fact that VCPI services the data of more than 100 nursing homes here in the US, meaning that these facilities lack access to patient and billing records for acutely vulnerable patients.

Karen Christienson, the owner of VCPI, told Krebs On Security, a cybersecurity publication, that the ongoing attack was "preventing these care centers from accessing crucial patient medical records" and that she worried "this incident could soon lead not only to the closure of her business, but also to the untimely demise of some patients."

And these are just some of the variety of ways that ransomware attacks can result in patient harm.

John Riggi, the Senior Advisor for Cybersecurity and Risk at the American Hospital Association, and who previously spent 30 years at the FBI, was unable to speak to specific instances of cyber attacks on specific hospitals, like almost every hospital representative and expert I spoke to, but said he meets with top level executives at hospitals on the issue, and they've shared a variety of experiences with him.

"You have the ambulance diversions, canceled surgeries, and an inability to assess appropriate medication and prescribe medication," says Riggi. "So think about it, you have an incapacitated patient that is delivered to the emergency room, if the ambulance can make it there,and then they're not quite sure how to treat them because of allergies or even the history of the patient. So that comes down to care."

Riggi stresses that when he talks to hospital executives, he emphasizes cyber risk is, first and foremost, a risk to care delivery and patient safety.

These attacks are, by and large, usually one-offs and uncoordinated, according to Parham Eftekhari, the co-founder of the Institute for Critical Infrastructure Technology, a nonpartisan think tank that provides objective advisory to the House and Senate, federal agencies and critical infrastructure stakeholders.

He echoes many of the situations that Riggi shares when it comes to the challenges hospitals and healthcare facilities are currently facing when it comes to ransomware attacks. But it could get worse.

"Imagine the scenario if it was an actual coordinated campaign to really cause massive chaos and panic in a community," says Eftekhari. "What if there were numerous ransomware attacks in a rural area where there's only three hospitals within a hundred mile radius. What if you have ransomware launched against all of those? What are you going to do? Where are you going to go? These are the types of things that I think are very frightening and actually plausible scenarios."

Numerous experts, security practitioners, and hospitals declined to go into detail about the attacks they've dealt with, or the harm that's resulted from them. While there are patient privacy regulations regarding individual patient data, the lack of willingness to discuss specifics of these cases creates a barrier to the public understanding the urgency of ransomware, both when it comes to healthcare facilities but also in their own lives.

Hospitals may often be reluctant to identify specific instances where patient harm has occurred because of regulation and liability concerns, says Riggi. He says the industry has to move beyond that and recognize that a hospital that's a victim of a cyber attack is a victim of crime should be treated as such.Pushing the issue of ransomware and healthcare to the forefront of a public debate on it highlights what it is — a public health issue.

"The message I'm sending back to my former colleagues in government is that ransomware has crossed the line from an economic crime to a direct threat to public health and safety" says Riggi.

But that doesn't help increase the public's understanding of this right now.

Human error is the wild card

The obvious question then is, how are hospitals combating these ever evolving threats, or are they even doing so?

But that doesn’t get at some of the ways that hospital security is directly tied up in the people that work there. Numerous experts described natural human error as one of the biggest vulnerabilities when it came to preventing ransomware from getting into systems.

Take, for example, the instance of Campbell County Health (CCH), which was hit with a ransomware attack in September of 2019. The attack forced them to cancel numerous appointments and therapies, transfer patients to facilities in places as far flung as South Dakota and Colorado, and encrypted everything from email to prescription records, according to the Wall Street Journal.

CCH declined an interview to discuss the ransomware attack, but in the email doing so, the signature from the hospital representative included a couple of sentences in large, red, comic sans lettering:

“**This Email originated from outside of the CCH organization. Use caution when opening attachments or clicking links. Never share your CCH password, CCH will never ask for your password.** “

What they’re alluding to here, are phishing attacks, in which people are sent emails from someone else requesting they click on a link, or download a document, are fairly common. In fact, you’ve probably seen a number of them in your spam filter on your own email account.

A stressed and tired campaign operative might unknowingly click on a phishing link because, first, they’re tired and stressed, but also because of the sheer number of emails people receive and the ways it connects in many instances to a person’s job. It’s not a stretch at all to imagine a similar situation in which a medical practitioner or hospital employee who is overworked accidentally downloads something, or clicks on a phishing link. And that’s all it takes — one click.

So to say the least, protecting against the multitude of forms and sheer volume of cyberattacks can be tricky at best.

It may not be a question of it, but when

While there are a number of systems, firewalls, security patches, and expertise that can be brought to bear on systems preventatively, bad actors are constantly forming work arounds for the existing methods of protection.

These sorts of things remain challenges for healthcare facilities, according to Donna Dodson, the Chief Cybersecurity Advisor for the National Institute of Standards and Technology (NIST) Information Technology Laboratory and Director of the National Cybersecurity Center of Excellence. The NIST is heavily involved in providing IT oversight and support for the federal government.

But there is a greater awareness about these issues.

“There's a recognition today that we didn't have 10 years ago where people outside of the IT shop are understanding their reliance on technology and thinking about it” says Dodson.

The NIST Cybersecurity framework gives people and companies a way to think across the board about resiliency, and about things like ransomware, including what security controls they should have in place and what sort of plan can get you there. But the NIST Special Publication 1800-11, entitled “Data Integrity, Recovering from Ransomware and Other Destructive Events” looks at ransomware specifically, and offers advice and best practices about how to recover from an attack.

Even something as simple as implementing multi-factor authentication, so that clicking on a phishing link doesn’t immediately give up your single password to a number of systems can make a big difference according to Dodson.

But preventative systems can’t do everything.

Mark Dill, who served for 15 years as the Director of Security for the Cleveland Clinic, and now works in security consulting, says that even if hospitals are investing in security programs, they have to also invest in people.

“You can have all the preventive tools you want, but, you know, the talent levels that are out there internationally can get past some of those things,” says Dill.

And when it comes to recruiting the talent to counter these sorts of attacks, there is only so much top level talent, and it’s hard for hospitals to compete with the likes of places such as Google or Apple.

“Some of these campaigns can be ultra sophisticated. Even if you're talking about a talented IT team, they’re sometimes going against a nation state, or somebody's going to try multiple times throughout a campaign to achieve their objective,” says Dill. “And it is a challenge. It is a chess game that’s subject to talents and the processes and maturity that an organization has.”

Even with this awareness implementation is a tricky process. Unlike standard businesses, which might have reliable operating hours, hospitals are a 24/7 operation that involve complicated process and equipment that can mean the difference between life and death. You can't exactly shut down a hospital for regularly scheduled maintenance. A hospital can't deploy a software security patch on a critical medical device such as a ventilator, drug infusion pump, or an imaging device, without testing it to make sure it doesn't cause a malfunction in the machine which could result in patient harm.

And this isn't even taking into account the Internet of Things, or internet connected devices, which now extend to medical devices as integral as pacemakers.

But is the upfront inconvenience worse than the potential harm on the backend? Outside of patient harm, John Riggs of the AHA estimates that revamping an IT system after a ransomware attack costs hospitals $10 million on average. Additionally, after a full IT overhaul, recent research has shown in a limited capacity that as doctors and nurses familiarize themselves with new systems it slows down their work, and can lead to a slight increase in patient harm. The research, which was published in September of 2019, found that death rates among heart attack patients increased in the aftermath of a data breach for months and even years.

At the end of the day, it's unlikely that ransomware attacks are going to decrease. They may well just become a fact of life moving forward for healthcare facilities, a shadowy program always lurking just outside of a network, poking and prodding, waiting for someone to make a mistake. And it really comes down to money.

"There's money to be made here," says Rahman of IOActive. " If you look at it for whatever industry ransomware gets into, people are paying for this and there's a return on investment on it. That's going to continue.

So looking forward to the next ten, twenty years, it may not be a question of if. It may just be a question of when.