It's not just Scripps. Ransomware has become rampant in health care during pandemic

May 10 2021, by Paul Sisson

Credit: CC0 Public Domain

On a local level, the ransomware attack that engulfed Scripps Health this past week, paralyzing digital resources from hospitals to outpatient

clinics, was isolated. Other health care systems in the region have been unaffected and able to assist diverted patients with serious and immediate needs including heart attacks and strokes.

But, look around and it is obvious that Scripps is not alone.

A recent report from software firm VMWare Carbon Black estimates that its health care customers experienced a 9,851% increase in hacking attempts in 2020 compared to the previous year. And activity intensified with the COVID-19 pandemic, attempts spiking 87% from September to October.

Beau Woods, a senior adviser for the federal government's Cybersecurity and Infrastructure Security Agency, confirmed that attacks like the one still unfolding at Scripps simply metastasized in the past year.

"Ransomware is increasing in sophistication, it's increasing in prevalence," Woods said. "The purveyors of ransomware are generally reinvesting the fees that they collect from the entities they extort to acquire more capabilities.

"They're getting better, they're getting more frequent, particularly during the pandemic where we've opened up more connectivity to allow more remote work."

Scripps' current predicament, which, according to several sources was unable to offer radiation treatments to its cancer patients until the proper equipment was finally able to be returned to service on Friday, follows an even more widespread attack late last year.

On Sept. 27, what is believed to be the biggest ransomware attack in health care, hit Universal Health Services Inc., a 400-hospital nationwide health care system with facilities in California, including Temecula

Valley Hospital and Inland Valley Medical Center in Wildomar.

It took three weeks for all UHS facilities to return to full operation, and the publicly traded company lists $67 million in negative financial impact from the attack in its fourth-quarter earnings report though it has not said whether or not it paid the ransom that hackers demanded.

That impact included diversion of ambulances to other hospitals when electronic medical records were locked down and inaccessible.

Ransomware—malicious software that, once having gained access to a digital network can encrypt information and threaten deletion or worse if cash is not paid—is increasingly targeted at the health care industry, concludes a recent analysis from IBM's Security X-Force consultancy.

Big Blue's write up, which is based on its own consulting work with affected companies, found that 28% of attacks on health care in 2020 were ransomware, making the industry the seventh most attacked, up from tenth place in 2019.

And the attacks are getting nastier.

As noted in a report from the Office of Information Security at the U.S. Health and Human Services, "double extortion" ransomware attacks exploded in 2020. While there was just one ransomware platform offering this dismal two-for-one in 2019, others quickly copied the approach. Now 18 different types of ransomware are double extortion.

The ominous term refers to an attempt to make it more difficult for hacked companies to refuse to pay ransoms and simply restore their systems from backups made before ransomware took hold.

Hacker gangs usually operating from overseas locations have countered

by downloading sensitive data from the networks they penetrate before making ransom demands.

Now, those demands include double threats to pay up or risk losing encrypted data and also pay up or risk private information from one's customers being leaked on websites that they operate.

One such double-extortion ransomware type called Ryuk was widely reported to have been the culprit in the UHS attack, though the company has never formally disclosed the digital pathogen involved.

It remains unclear exactly which type of ransomware is involved at Scripps.

The region's second-largest health care system, with four hospital campuses and a vast network of clinics, outpatient surgical centers and other assets, said on Thursday that "malware" was detected on its systems. An internal memo obtained by the Union-Tribune Sunday clearly implicated ransomware but did not list the type. On Tuesday, the California Department of Public Health confirmed in an email that ransomware is involved.

It is clear, though, that the attack has hit Scripps very, very hard at a moment when the nation's health care workers were just starting to recover from a year fighting the COVID-19 pandemic.

The attack caused a widespread ambulance diversion from all Scripps hospitals, taking them out of the emergency medical response system when a boat capsized off Point Loma Sunday. Survivors were sent to eight different hospitals throughout the region, but not to Scripps Memorial Hospital La Jolla, the closest trauma center, because its systems were down.

As computers remained offline through the week, the diversion softened, said Dr. Eric McDonald, recently appointed to serve as the county's chief medical officer in the absence of Dr. Nick Yphantides who was put on administrative leave early this year for still-unexplained reasons.

While not operating at usual efficiency levels, McDonald said that Scripps hospitals have been able to continue serving patients, receiving some ambulance traffic when required. The cruelty of these kinds of attacks, he added, falls on those who deserve it least.

"This is another significant stress on what has been a long-standing level of stress on our entire hospital system," McDonald said. "You really have to give kudos and support to the doctors and nurses and many other kinds of workers who are continuing to deliver care while this is going on."

Patients have generally said that they have found Scripps workers competent and cordial over the past week, though some are starting to experience significant frustration with the situation, especially around the lack of communication regarding previously-scheduled appointments.

Kyle Long, a local resident and Scripps patient, said he had a bone marrow biopsy scheduled for Monday delayed with only last-minute communications from Scripps.

"As far as I am concerned, Scripps receives an F for how they handled this breach," Long said in an email.

Scripps has provided little detail into exactly which of its systems, beyond its electronic medical record, have been taken down by the attack. And it has not said whether some amount of its sensitive patient

records were siphoned out of its systems and into cyber terrorist servers under threat of disclosure or sale to the highest bidder.

That uncertainty left many Scripps customers demanding answers on the company's Facebook page. Many wondered whether they should freeze their credit reports and hire reputation-protection services to protect themselves if information does leak out.

Dr. Christian Dameff, an emergency medicine specialist and cybersecurity researcher at UC San Diego Health, said last week that, though he is not familiar with the details of what exactly went down at Scripps, protecting oneself in those ways generally make sense even if an attack is not already underway.

He said that, in general, it is difficult for companies to immediately know whether and how much of their private information has left the building. It's not like there is some sort of electronic dashboard able to show what has gone where. Locked down systems are not easy to analyze, and outside experts generally must be brought in to conduct forensic examinations of impacted systems in order to determine just how deep the damage goes.

"I'm sure that work is ongoing at Scripps, but it's complicated, tedious work that requires very specialized expertise to figure out exactly what they took and when they took it, and then to give recommendations as to what patients should do moving forward," Dameff said.

Many, though, are surely wondering how this could have happened to an organization with a multibillion-dollar budget, one named one of the "most wired" organizations in American health care as recently as 2019.

The IBM X-Force report indicates that recent attacks, whether they deliver ransomware or facilitate record theft, have been exploiting a flaw

in the software than runs servers made by Citrix Systems Inc. The company boasts that 100% of the nation's 10 largest health care organizations use its technology, especially to host electronic medical records systems such as the Epic software employed by Scripps and many others across the region.

In 2019, the company issued a security bulletin on a vulnerability in one of its products called an application delivery controller which it formerly called NetScaler. There is a case study posted on Citrix's website that specifically says the product was employed at Scripps.

Citrix provides instructions on how to fix the vulnerability, but it seems clear that many organizations aren't getting that critical maintenance work done before hackers uses it to gain access. IBM's X-Force report estimates that 8% of all incidents that its X-Force team handled last year had to do with the Citrix vulnerability.

Is this how hackers found their way onto the Scripps network? The company isn't saying.

"Because this is an ongoing investigation, we are limited in what we can say. We will share more information as we are able," said Scripps spokesman Keith Darce in an email Friday.

But scanning for and exploiting equipment vulnerabilities is only one way among many that hackers gain the access they need to unleash digital destruction.

Duping employees who already have access is among the most common methods. A process called phishing is often employed to get employees to share logins and passwords on dummy websites that look just like those run by their companies or to open email attachments said to be from trusted sources that turn out to be malicious programs. Once inside

a company's digital defenses, it's easier for software to reach out to remote servers and download a more-damaging payload.

Sure, Dameff said, there are plenty of very good ways to make phishing attacks less likely to succeed. Two-factor authentication, a process that requires employees to verify their logins not just with passwords but also with a program that runs on their smartphones, can help a lot. But two factor can be cumbersome in situations where life and death is literally on the line day in and day out. Nobody wants to create a situation where a nurse responding to a dying patient can't access critical information in the electronic health record because they forgot their smartphone.

"Multi-factor authentication, password managers and good password practices like choosing complex passwords, email attachment scanning, endpoint security, I'm sure that they had all of that," Dameff said. "It just takes one person in the enterprise clicking a link to have something like this happen, regardless of all the great security controls you put in place."