WSJ PRO

https://www.wsj.com/articles/human-rights-groups-ask-police-to-hunt-hackers-attacking-hospitals-11591003801

Human-Rights Groups Ask Police to Hunt Hackers Attacking Hospitals

As the coronavirus pandemic wears on, cyberattackers continue to strike

United Nations High Representative for Disarmament Affairs Izumi Nakamitsu addresses the U.N. Security Council in February.

PHOTO: BEBETO MATTHEWS/ASSOCIATED PRESS

By Catherine Stupp and David Uberti

June 1, 2020 5:30 am ET | WSJ PRO

The International Committee of the Red Cross and other human-rights groups are urging law enforcement to move against hackers targeting hospitals during the coronavirus pandemic.

A surge in cyberattacks targeting health-care facilities caring for Covid-19 patients and researchers working on treatments for the illness has made cybersecurity a top priority for increasingly digitized health systems.

Hospitals rapidly deployed digitized medical devices to manage the influx of Covid-19 patients, ramping up tools like virtual private networks to accommodate remote work and telemedicine for nonvirus care. The technological shifts, coupled with the chaos of responding to the crisis, have translated into more opportunities for phishing emails, ransomware and other attacks.

“Health care is susceptible at the moment because of the amount of pressure being put on health-care systems throughout the world,” said Craig Jones, director of cybercrime at Interpol. The law enforcement organization warned in April of an uptick in such attacks and is working with cybersecurity firms to identify threats and alert potential victims.

At an informal meeting of the United Nations Security Council in May, U.N. disarmament chief Izumi Nakamitsu highlighted “worrying reports of attacks against healthcare organizations and medical research facilities worldwide.”

The World Health Organization reported a 500% increase in cyberattacks on its systems during the spread of the coronavirus pandemic through April compared with the same period last year. Attackers also have created fake Gmail accounts to masquerade as the WHO to send malicious emails to executives at health-care groups and other companies, Google’s cyber threat analysis group said last week.

The WHO said in April that hackers stole and published around 450 employees’ email passwords. The organization said it has started using a more secure method to protect accounts. A spokesperson didn’t respond to a request for more information.

The International Committee of the Red Cross in a letter last week signed by international political and business leaders called for governments to take “immediate and decisive action” to punish cyberattackers.

“There are more and more cyberattacks…on the healthcare sector and unless there are really strong measures taken, they will continue,” said Cordula Droege, chief legal officer at the ICRC. “What we’re seeing at the moment are still indications of how devastating it could be.”

Investigating cyber threats can be challenging for law enforcement, in part because it is difficult to attribute attacks to a specific individual. If a suspect resides in a different country, negotiating extradition can take months or years. Some countries, such as Russia, don’t have extradition agreements with the U.S.

“We need to increase the effectiveness of cyber crime enforcement globally by making sure we’ve got meaningful laws addressing cybersecurity issues,” said Errol Weiss, chief security officer at the Healthcare Information Sharing and Analysis Center, a nonprofit that shares data about cyber threats to member companies.

Such alarm bells may ring particularly loud for health-care professionals who continue to battle the coronavirus outbreak and are bracing for a potential second wave.

In the U.S., the American Hospital Association has begun sharing more information with the Federal Bureau of Investigation, the Department of Homeland Security and the Department of

Health and Human Services in response to the crisis, said John Riggi, the trade group's senior adviser for cybersecurity and risk.

The association sends a daily newsletter to nearly 5,000 member hospitals that includes information about potential threats, such as cybercriminals trying to make a buck off of ransomware.

"We're also concerned now that we have these very sophisticated actors—nation states, particularly China and Russia— targeting Covid-19 research, treatment protocols and vaccine development," Mr. Riggi said.

Officials at the Johns Hopkins Bloomberg School of Public Health, a leading research institution, last week told faculty and staff to watch for intellectual property theft, according to an email viewed by The Wall Street Journal. The message relayed law enforcement warnings about Chinese hackers and urged employees to patch computer systems, avoid shady links and change passwords. Hackers in March mimicked Johns Hopkins's Covid-19 site, which tracks the spread of the virus, to lure visitors toward malware.

The situation shines a light on the growing cybersecurity divide among health-care institutions, said Aviel Rubin, a computer science professor at Johns Hopkins University and technical director of its Information Security Institute.

"The smaller, less well-to-do [organizations] have kind of been left behind to some degree because they don't have the budget," Mr. Rubin said.

Despite promises by some hackers to refrain from hitting hospitals, some have been targeted. The Brno University Hospital in the Czech Republic suffered a ransomware attack in March that forced staff to record coronavirus test results using pen and paper. The same month, hackers swarmed two websites belonging to Paris's hospital authority, known as AP-HP, in an attack thwarted by the organization's internet service provider, a spokesman for the authority said.

It appears that no cyberattacks on health-care facilities have led to deaths or other disastrous consequences, said Ms. Droege of the ICRC. But she hopes the scope and volume of threats highlight how cyberattacks on medical facilities could potentially be as destructive as physical attacks.

There have been at least 208 physical attacks on health-care infrastructure world-wide reported during the coronavirus pandemic, Ms. Droege said. That includes militants storming a hospital in Kabul in May. If hackers managed to shut down a hospital's computer networks, the impact might be even more devastating, she added.

"That could potentially be a quite toxic and dangerous combination," Ms. Droege said.

Write to Catherine Stupp at Catherine.Stupp@wsj.com and David Uberti at David.Uberti@wsj.com