Could Russian hackers cripple US health care systems?

March 11 2022

Sick people seeking lifesaving care in the United States could fall victim

to a hidden part of Russia's war on Ukraine—vicious cyberattacks aimed at sowing disruption, confusion and chaos as ground forces advance.

Cybersecurity experts warn that attacks launched against Ukrainian institutions have the potential to spill over into America's health care systems, potentially endangering patients' lives.

The cybersecurity program at the U.S. Department of Health and Human Services last week issued an analysis warning health care IT officials about two pieces of Russian malware that could wipe out hospital data vital to patient care.

And since early December, the American Hospital Association has been warning about increased risk related to Russian cyberattacks, said John Riggi, the association's national adviser for cybersecurity and risk.

"We were issuing advisories to the nation's hospitals and health system, saying the geopolitical tensions would certainly increase the risk of cyberattacks which would impact potentially U.S. health care," Riggi said.

Such attacks have the potential to cost lives, by cutting doctors and nurses off from needed patient data and causing hospitals under attack to delay scheduled procedures and divert critically ill people to other facilities, Riggi explained.

Nearly a quarter of health care organizations hit by a ransomware attack during the past two years said the attack resulted in increased patient death rates, according to a September 2021 report sponsored by the cybersecurity company Censinet.

Further, about two in five (37%) said such attacks caused an increase in complications from medical procedures, while more than two-thirds

(69%) said delays in procedures and tests have led to poor patient outcomes, the report says.

"That is not a financial crime," Riggi said. "It is a threat-to-life crime, and the government needs to respond to such, including offensive operations against these foreign-based bad guys."

Not if but when

Even before Russia launched its attack on Ukraine, cyberattacks had been considered the top technological threat facing U.S. health care.

The nonprofit health care think tank ECRI recently listed cybersecurity attacks as the top health technology hazard for 2022.

"All health care organizations are subject to cybersecurity incidents," the ECRI wrote. "The question is not whether a given facility will be attacked, but when."

Health care systems face a constant barrage of phishing attacks, in which rigged e-mails are used to gain access to their computer networks, as well as internet-based onslaughts against IT security, said Lee Kim, a senior principal of cybersecurity and privacy for the Healthcare Information and Management Systems Society (HIMSS).

"The reality of cybersecurity today is that cyberattacks are really rampant, even in times where there isn't any kind of geopolitical conflict," Kim said. "They happen by the hundreds, if not thousands, every day."

La Monte Yarborough, chief information security officer for the U.S. Department of Health and Human Services, agreed.

"While events such as those occurring in Eastern Europe right now can indicate a heightened threat environment and the need for greater vigilance, bad actors will frequently leverage any event to launch cyberattacks," Yarborough said. "Bad actors capitalize on many types of events such as holidays, elections and geopolitical conflict."

Delays in emergency care

Ransomware attacks—in which computer data is seized until a ransom is paid—is "the most prevalent cybersecurity risk we've seen," Yarborough said, adding that such an attack "absolutely poses potential health risks to patients."

In one of the worst ransomware incidents, about one-third of England's National Health Service trusts lost access to patient records and other important electronic systems in May 2017 after their computers became infected by WannaCry, as part of a global attack.

And the University of Vermont Health Network lost access to electronic health records for nearly a month in October 2020 following a massive ransomware attack that forced doctors to, among other measures, reschedule chemotherapy sessions for cancer patients.

Hospitals under these sort of attacks have to divert ambulances to other facilities, delaying critical care for stroke patients and heart attack victims. "It's intuitive that it certainly increases the risk of a negative outcome whenever there's a delay in urgent care," Riggi said.

Hospital systems also are targeted by cybercriminals who want to steal data for financial gain, Riggi added.

"Cybercriminals realized they could monetize health care records. They were very valuable, to be sold on the dark web," Riggi said.

"We're the only sector that aggregates not only protected health information, but we have a vast quantity of personally identifiable information on patients—date of birth, address, Social Security numbers," Riggi said. "We also have a vast aggregation of financial data, payment data, bank account numbers, credit card numbers. And then of course we do have vast quantities of medical research and innovation.

"All of those data sets are uniquely valuable to cybercriminals," he continued. "Any one of those data sets could be individually targeted. But when you combine all of them together in one location, they become exponentially valuable."

New malware threats

The Russian attack on Ukraine presents an even deeper threat to the U.S. health care system, experts said.

Shortly before the launch of the Russian invasion, malware that can completely wipe out a computer's data began popping up in Ukraine, according to the HHS cybersecurity report.

The malware, HermeticWiper and WhisperGate, were only two out of a number of cyberattacks targeting Ukrainian institutions that occurred in January and February, the report said. Ukraine responded by creating its own crowdsourced "IT Army" to target Russian infrastructure.

The problem is that once malicious programs are released into the wild, there's no telling where they will end up, Riggi said.

In June 2017, Russian military intelligence attacked Ukraine with the NotPetya virus, which resembled a ransomware attack but was actually a program that completely wiped out data rather than locking it down.

The attack spread beyond Ukraine and caused massive disruption to governments and businesses around the world, including U.S. health care.

"What happened is we had major U.S. firms that had third- and fourth-party relationships in the Ukraine," Riggi said. "NotPetya, this digital virus, spread like a biological virus that then impacted a major U.S. pharmaceutical company." The virus also infected a popular medical transcription firm.

NotPetya then spread from those companies to hospitals and health care systems, disrupting patient care across the United States, Riggi said.

"We're concerned that a scenario like that could happen again," Riggi said. "We are also concerned that a mission-critical third part provider, which we rely upon for services to deliver care and operations, might be struck unintentionally and become collateral damage by a Russian cyberattack, which then disrupts patient care."

Shoring up defenses

Such an attack robs doctors of access to patients' electronic health records, but also could spill over into the computer systems that manage pathology labs, imaging systems, drug dispensing cabinets, drug infusion pumps and other important technology, Riggi said.

There's also the chance that the battery of economic sanctions that have been unleashed on Russia could prompt a direct computer-based counterattack against the United States, given that the Kremlin has accused the U.S. of mounting an "economic war" on Moscow.

Attacks might also come from countries allied with Russia, such as Belarus or China.

"We shouldn't just simply be on the lookout for cyberattacks from Country X," Kim said. "If they've had a defense pact historically with other countries, you need to be on alert in terms of cyberattacks from allied countries as well."

"It's worth noting that cybersecurity attacks on other sectors may impact health care," Yarborough added. "An attack on energy or transportation sectors, for example, could have a negative impact on the ability of health care organizations to provide care or transport individuals to health care facilities."

In the face of this threat, security experts have been warning U.S. health care systems that they need to be on high alert.

"Now is not the time to simply rely on faith that we'll be OK," Kim said. "Now is the time for health care organizations and all other stakeholders within the U.S. to ramp up their defenses and ensure that the foundation is strong against any kind of actor, whether it's nation-state, cybercriminal, [or] amateur script kiddies. I really do think it's time for us to raise our defense levels."

"A strong, risk-based cybersecurity posture must assume that IT systems are always under threat of a cybersecurity attack," Yarborough said. "At HHS, we work internally to ensure that our systems and networks are protected from such attacks while working across the health care and public health sector to ensure everyone in the sector is aware of emerging threats."

Malicious links

Experts urge that health care systems inventory their data and routinely back it up, in the event of a successful attack.

"Look at the critical assets within your organizations and the patients that you serve, and from that you can create a cyber-defense plan to protect what's most critical," Kim said.

Security experts also urge that all health care employees be trained to see themselves as part of the cybersecurity team, so they might be more aware of phishing e-mails and other attempts to break into their institution's systems.

"Phishing is indeed more often than not the way attackers are getting into our systems," Kim said.

An HIMSS report noted that 45% of significant security incidents in 2021 were the result of a phishing attack, and that the initial point of compromise for their most significant security incident was phishing 71% of the time.

"Basically, any end user could bring the organization to its knees by clicking on a malicious link in a phishing e-mail," Riggi said.

Electronic health records and internet-connected medical devices have helped vastly improve patient care, Kim and Riggi said. Now health officials need to cement those gains by protecting vital computer systems against attack.

"Even pre-pandemic, there has been a push to rely on the expanded use of medical technology in health care to improve patient outcomes and the efficient delivery of patient care," Riggi said. "Patient outcomes have been significantly improved, so all that is absolutely necessary.

"However, it has created additional risk, for as we roll out network-connected and internet-connected devices and technologies and increase our reliance on cloud providers, that expands what we call the 'attack

surface,'" Riggi added. "Basically more opportunities for the bad guys or foreign-based cyberhackers to penetrate our networks."

More information: The Healthcare Information and Management Systems Society (HIMSS) has more about cybersecurity in health care.