TechXplore

Health care bore brunt of cyberattacks in 2020, study says

February 23 2021, by Gopal Ratnam

Credit: Pixabay/CC0 Public Domain

The global health care and pharmaceutical industries bore the brunt of cyberattacks in 2020 as nation-state hackers and criminals targeted companies looking for information on COVID-19 as well as vaccine development, cybersecurity research firm CrowdStrike said in a report made public Monday.

As the COVID-19 pandemic continues to rage around the world with new variants appearing on multiple continents, forcing widespread closures despite the availability of vaccines, the health care industry is likely to remain in the crosshairs of hackers, the 2021 Global Threat Report from CrowdStrike said.

Compared with 2019, CrowdStrike's experts tracking cyberattacks across the globe saw a 214 percent increase in cyberattacks and attempts to break into computer networks during the past year, Adam Meyers, senior vice president of intelligence, said in an interview.

"That's pretty unprecedented," Meyers said. "I think one of the big drivers there was COVID."

Nation-state hackers focused on espionage while criminals looking to make money used the digital landscape created by the pandemic to "get into various organizations to conduct ransomware type attacks . . . so it was one of the dominant features of 2020."

Although criminals accounted for four out of five targeted intrusions uncovered by CrowdStrike, and deserve attention, "state-sponsored groups should not be neglected," the report said.

Hackers from Russia, China, North Korea, Iran and Vietnam were the major sources of attacks on the health care sector, CrowdStrike said.

Details about the hackers and their methods come from efforts by CrowdStrike to identify and stop attacks on its clients' networks, but it's hard to say which of the hackers' attempts were successful in stealing research or intellectual property, Meyers said. Online theft

In addition to theft of intellectual property, health care companies also face significant threats from criminals, CrowdStrike found.

The health care industry "faces a significant threat from criminal groups deploying ransomware, the consequences of which can include the disruption of critical care facilities," the report said. "Along with the possibility of significant disruption to critical functions, victims face a secondary threat from ransomware operations that exfiltrate data prior to the execution of the ransomware."

In addition to freezing a victim's computer network and demanding a ransom payment to unfreeze the network, criminals also steal the data and threaten to leak it in order to get around steps taken by companies to restore their computers from backups without paying ransoms, Meyers said.

The biggest incident involving a single nation-state and a target was the SolarWinds hack that was discovered in December by FireEye, another cybersecurity firm.

Russian intelligence services are said to have orchestrated the SolarWinds hack by penetrating the supply chain of software development and inserting malware into updates that were then downloaded by 18,000 clients of SolarWinds, including U.S. government agencies and Fortune 500 companies.

As details of the attack emerge, shedding light on the scope and scale of the intrusion, it's likely to become a template for other sophisticated nation-state hackers, Meyers said.

"I think the big takeaway is you know this is something that's going to be perceived as very attractive by threat actors who are going to try to replicate it, because they understand the value of [the attacks] and understand what that capability brings," he said.

White House deputy national security adviser Anne Neuberger, who's spearheading the Biden administration's efforts to investigate the SolarWinds attack, said she expects more victims to be found as the probe unfolds. As of now nine U.S. federal government agencies and at least 100 companies have been affected by the attack.

"We believe we're in the beginning stages of understanding the scope and scale, and we may find additional compromises," she said at a White House news conference last Wednesday.

Files, emails and other material on the networks of companies and agencies that have been affected may themselves be compromised, and the investigation that's underway is aiming to find the true scope of the exposure, Neuberger said.

Citing the proliferation of cyber criminals around the world, CrowdStrike said it had devised an index to track and quantify the level of activity and the monetary gains being made by criminals.

The index is constructed by taking observed incidents like the "number of ransomware incidents that we've seen in a given week, the average cost or the average ransom amount that's being demanded," Meyers said.

Other elements that go into building the index include the cost of buying a stolen identity and fluctuations in global cryptocurrencies, which has become the ransom payment of choice for criminals, Meyers said.

"We've kind of weighted [these factors] based on our confidence in knowing how much coverage we have, or how accurate it might be and then we've amalgamated that into this index," he said, adding that it's an experimental idea that may encourage other cybersecurity researchers to collaborate and expand on it.

Distributed by Tribune Content Agency, LLC

Citation: Health care bore brunt of cyberattacks in 2020, study says (2021, February 23) retrieved 20 April 2024 from https://techxplore.com/news/2021-02-health-brunt-cyberattacks.html