Hacker 2017 Targets

Hospitals are the "bull's-eye" for hackers this year, with Bitcoin making it easier for criminals to pursue ransomware attacks.

The convergence of vulnerable legacy hardware and software systems and the emergence of connected health, Internet of Things devices that are not always built with security in mind, and the super-identity criminals can steal, all make healthcare more attractive to hackers than any other sector, according to Matt Anthony, vice president of incident response at the Herjavec Group.

Also, Bitcoin provides added motivation for cybercriminals to pursue their illegal activities.

"Bitcoin is the engine for cybercriminality, and as long as there is an anonymous way for criminals to get paid, it's not going to get better anytime soon," Anthony pointed out. "It's a winning combination for organised crime – not necessarily Italians in smart suits and fedoras, either. There are large organised communities in China and Russia."

Overall, ransomware damages are projected to reach $1 billion, according to new research from Cybersecurity Ventures. The report was sponsored by the Herjavec Group. Often hospitals don't hesitate to pony up after a ransomware attack as they really need the data cybercriminals just encrypted.

"Hospitals will pay, they'll pay fast and they'll pay what it takes to get data back," Anthony said. "We ask people not to pay but sometimes there's no alternative in healthcare."

The report also says global spending on cybersecurity in healthcare is set to surpass $65 billion by 2021. In fact, Anthony has observed that hospital IT departments are increasingly turning to cloud services for proactive monitoring, log aggregation and alerting. However, hospital IT teams need to get better at all of those more quickly than they currently are, Anthony said, noting that ransomware and other cybercriminal attacks are going to get a lot worse before they get any better.

Source: Healthcare IT News

Image credit: Pixabbay

Published on : Tue, 11 Apr 2017