KAUFMAN | DOLOWICH

"Killnet Group Targets U.S. Hospitals with Cyberattacks", quote from Avery Dial, Esq., Health Care Risk Management, April 2023

A pro-Russia hacktivist group is targeting American hospitals with Distributed Denial of Service (DDoS) attacks. Hospitals should revie their cybersecurity defenses.

- ***The attacks use bots to overwhelm websites, networks, or systems.***
- ***A DDoS attack may be a distraction to allow a ransomware attack.***
- ***Other groups may be inspired to conduct their own attacks on hospitals.***

Hospitals and health systems should review their defenses against the cyber breach known as Distributed Denial of Service (DDoS) in response to threats from the pro-Russia hacktivist group known as Killnet. The criminal group recently called on its members to target specific healthcare providers in the United States. More than a dozen hospitals have been hit by Killnet attacks….

A DDoS attack uses bots to flood the targeted website, system, or network with thousands or hundreds of thousands of requests per second to overwhelm it, causing the system to crash and be unavailable for hours or days, explains Avery Dial, JD, partner with Kaufman Dolowich Voluck in Fort Lauderdale, FL. "It's really hard to prevent a DDoS attack because it takes advantage of natural inputs that you need for your business, something as simple as receiving email or someone typing a search query on your website or filling out some type of forms," Dial says. "These are these natural interactions that you need the public to have with your website. Hackers use a network of machines they've infected with malware to access those services so that instead of getting 100 emails over the course of a day, the business is getting 100,000 emails." ***(See Read More Link for full article)***