

Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: US Not-for-Profit Hospital Cyberattacks Could Signal Greater Risk

Fitch Ratings-New York/Austin/Chicago-03 February 2023: Recent coordinated cyberattacks on US not-for-profit (NFP) hospitals and health systems' websites are unlikely to drive any downgrades, but the attacks highlight the growing risks and capabilities of threat actors who could cause greater harm through more malicious attacks that affect healthcare delivery, Fitch Ratings says.

The websites of a number of US hospitals were taken down in a single coordinated distributed denial of service (DDoS) attack, which sent a flood of traffic to overload a server or website, slowing or shutting them down, potentially for days. This seems to be the most widespread and coordinated attack against the sector to date, with roughly 20 hospitals reporting and some affected hospitals and systems likely not publicly disclosing an attack. Some affected entities have been able to quickly restore their websites, and it currently appears that no personal healthcare information or data was compromised in these attacks.

Given what we know at this point, the DDoS attacks are not expected to have any material financial or operational effect on targeted hospitals due to their brief and relatively superficial impact. However, deployment of a more sophisticated cyber weapon that compromises service and affects a hospital's financial profile could negatively affect ratings. Critically, the disruption highlights the risks to the sector of a similarly scaled, but more severe, attack that could have dire effects on health and safety.

KillNet, the hacking group that has claimed responsibility for the attacks, has previously targeted healthcare organizations, according to recent release from Health and Human Services' Health Sector Cybersecurity Coordination Center that indicates that follow-on ransomware attacks are likely. Healthcare and public health is one of the sectors that the Cybersecurity and Infrastructure Security Agency (CISA) has identified as a critical infrastructure sector, which is the focus of federal security policy. KillNet has also taken credit for similar attacks on other entities outside of the US.

Contacts:

Omid Rahmani
Associate Director, US Public Finance
+1 512 215 3734
Fitch Ratings, Inc.
2600 Via Fortuna
Austin, TX 78746

Gregory Dziubinski
Associate Director, US Public Finance
+1 312 606 2347

Kevin Holloran
Senior Director, US Public Finance

+1 512 813 5700

Sarah Repucci
Senior Director, Fitch Wire
Credit Policy - Research
+1 212 908 0726

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email:
sandro.scenga@thefitchgroup.com

Copyright © 2024 Bond Case Briefs | bondcasebriefs.com