Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare ○ TLP:WHITE Alert ID : df674f79 Dec 08, 2023, 04:23 PM

This week, *Hacking Healthcare*™ explores a potentially novel event in the world of cybersecurity: ransomware group AlphV's breach of and subsequent SEC complaint against lending company MeridianLink. We examine the substance of the incident and discuss a few takeaways for Health-ISAC members to consider. Next, we provide a brief update on last week's topic of proposed hospital cybersecurity regulations in New York State.

Welcome back to *Hacking Healthcare*™.

AlphV Ransomware Group Reports Its Victim to SEC Regulators After Hack

On November 7, members of the ransomware crime syndicate AlphV breached the network of MeridianLink, a publicly traded digital lending company that provides solutions for banks, credit unions, and fintechs. In an a potentially unprecedented step, members of AlphV allegedly filed a "failure to report" claim with the U.S. Securities and Exchange Commission (SEC). Let's take a deeper look at what occurred and how it may impact healthcare sector entities.

<u>AlphV's Complaint and Stakeholder Reactions</u>

On November 15, AlphV posted screenshots of what appears to be a digital complaint form it filed with the SEC. In the form, AlphV claims that MeridianLink violated the SEC's new incident- reporting rules because it "failed to file the requisite disclosure under item 1.05 of form 8-K within the stipulated four business days" after the breach.[i]

In response, MeridianLink released a statement saying that “upon discovery [of the breach], we acted immediately to contain the threat and engaged a team of third-party experts to investigate the incident.”[ii] The statement continued, “[B]ased on our investigation to date, we have identified no evidence of unauthorized access to our production platforms, and the incident has caused minimal business interruption. If we determine that any consumer personal information was involved in this incident, we will provide notifications, as required by law.”[iii]

Despite AlphV’s statement, the new reporting requirements it referred to in its alleged complaint were not yet entered into force. Additionally, as these are new rules, it is unclear whether MeridianLink would have been obligated to report the alleged breach anyway.

So what does this mean for Health-ISAC members?

Action & Analysis

*****Available with Health-ISAC Membership*****

New York State Proposed Hospital Cybersecurity Regulations Hit Open Comment Period

In a brief follow-up to last week’s *Hacking Healthcare*TM topic of proposed hospital cybersecurity regulations for New York State, the full 32-page proposed regulation has been posted.[vi] The New York State Register for December 6th has announced that the proposed regulations are now in a 60-day open comment period ending in early February.

Action & Analysis

*****Available with Health-ISAC Membership*****

Congress

<u>Tuesday, December 5</u>

No relevant hearings

<u>Wednesday, December 6</u>

No relevant meetings

Thursday, December 7

No relevant meetings

[i] https://cdn.arstechnica.net/wp-content/uploads/2023/11/meridianlink-sec-complaint.png
[ii] https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/
[iii] https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/
[iv] https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/
[v] https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals
[vi] https://regs.health.ny.gov/sites/default/files/proposed-regulations/Hospital%20Cybersecurity%20Requirements.pdf

Report Source(s)

Health-ISAC

Reference | References

Ars Technica
Ars Technica
Coveware
Attorney General

Tags

Legislation, Regulatory, Hacking Healthcare, New York State, New York, cybersecurity

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:
Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:
https://h-isac.org/events/

Hacking Healthcare:
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council�s efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council�s Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC�s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC�s monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org