Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 3bde1e76 | Apr 03, 2023, 08:43 AM

This week, *Hacking Healthcare* examines a politically motivated healthcare sector cyberattack to investigate both hacktivists and the potential necessity of healthcare entities to weigh high-profile patient data in their risk assessments. Next, we give you the heads-up on the Biden administration's attempts to ease the cybersecurity regulatory burden through harmonization.

Welcome back to *Hacking Healthcare*.

Hacking Healthcare – Hacktivism on the Rise

A recent breach of D.C. Health Link targeted prominent members of Congress and their families, exposing extremely sensitive identifying information and leaving all the victims of the attack vulnerable to identity theft. The attack raises questions around the impact of "patriotic hackers" and how organizations with high-profile patients may be at increased risk of attack.

The hacker who goes by "Denfur" engaged in a series of online conversations with CyberScoop over an encrypted messaging system. Denfur communicated that the breach "was an idea born out of Russian patriotism," that it purposely targeted "the DC area and services that people in Congress/Senate would use," and that it "was not an altogether complicated operation to execute."[1] On March 9, Denfur posted a sample of the stolen data containing over 200 entries to Breach Forums and commented that the "intended target WAS U.S. politicians and members of U.S. government…. Glory to Russia!"[2]

The breach included information such as names, email addresses, birthdates, Social Security numbers, and insurance policy information of at least 21 members of Congress, more than 1,800 people connected to Congress, hundreds of people linked to foreign embassies, and thousands of D.C. residents.[3]

A subsequent lawsuit has been filed, accusing the D.C. Health Benefit Exchange Authority, which administers D.C. Health Link, of negligence for maintaining data on systems vulnerable to attack. The connection of this breach to Russian patriotism is especially concerning, considering the hacker's blatant honesty about its targets.

Action & Analysis

Included with health-ISAC Membership

The Office of National Cyber Director Preparing for Regulatory Harmonization

The recently released U.S. National Cybersecurity Strategy has formally signaled the Biden administration's shift to embracing more cybersecurity regulation, especially for critical infrastructure sectors. An aspect of that issue that has concerned many is the proliferation of unaligned regulatory requirements, including cyber incident reporting. The time for critical infrastructure sector entities to have their voices heard on this issue may be near.

During a recent event hosted by the U.S. Chamber of Commerce, acting principal deputy national cyber Director Rob Knake is reported to have indicated that the Office of the National Cyber Director (ONCD) is working on a Request for Information (RFI) that will include asking industry for its thoughts on regulatory harmonization. Inside Cybersecurity reported that Knake hinted that the approach will include "understanding at a broad level where industry sees the issues of harmonization," and will look to "[come] up with processes by which regulators that are using the same rules are accepting reciprocity or some other mechanism."[10] Knake went on to suggest that the RFI is expected to be published within "the coming weeks."

Action & Analysis
Included with health-ISAC Membership

Congress
Tuesday, March 28th:
- No relevant hearings

Wednesday, March 29th:
- No relevant meetings

Thursday, March 30th:
- No relevant hearings

International Hearings/Meetings
- No relevant meetings
EU –

Conferences, Webinars, and Summits
https://h-isac.org/events/
Contact us: follow @HealthISAC and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who 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.

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

[1] https://cyberscoop.com/dc-health-link-breach-russia-hacker-congress/

[2] https://cyberscoop.com/dc-health-link-breach-russia-hacker-congress/

[3] https://cyberscoop.com/dc-health-link-breach-russia-hacker-congress/

[4] https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html

[5] https://www.zawya.com/en/press-release/research-and-studies/hacktivism-and-the-new-age-of-cyber-warfare-toepvb43

[6] https://economictimes.indiatimes.com/tech/technology/russian-hacktivist-group-phoenix-targets-indias-health-ministry-website-cloudsek/articleshow/98675059.cms

[7] https://www.csoonline.com/article/3691050/russian-hacktivist-group-targets-indias-health-ministry.html

[8] https://www.csoonline.com/article/3691050/russian-hacktivist-group-targets-indias-health-ministry.html

[9] https://blog.barracuda.com/2023/03/23/killnet-targeting-healthcare-sector--what-you-need-to-know/

[10] https://insidecybersecurity.com/daily-news/national-cyber-director-office-prepares-request-information-gather-input-regulatory

---

Reference | References

Zawya
Health-ISAC DDoS Whitepaper
New York Times
CSO Online
insidecybersecurity
Cyberscoop
barracuda
Times of India

Report Source(s)

Health-ISAC

Tags

Regulatory, Incident Reporting, Hacking Healthcare, hacktivism

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:

Written by John Banghart, who 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.

John can be reached at jbanghart@h-isac.org and jfbanghart@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.