April 28th, 2020

TLP White

In this edition of Hacking Healthcare, we begin with a discussion of the H-ISAC's media kit on medical device security and coordinated vulnerability disclosure and how it will help educate media partners and the general public on those critical issues. Next, we briefly explore the potential security and privacy concerns related to Facebook's pop-up COVID-19 surveys. Finally, we try and decipher the puzzling and threatening press release that the U.S. State Department issued to an unspecified cyber actor earlier this month.

Welcome back to *Hacking Healthcare*.

1. **H-ISAC Releases Medical Device Security Media Kit.** Last week, the H-ISAC's Medical Device Security Information Sharing Council (MDSISC) released educational materials designed to better inform the media and general public about medical device security and medical device coordinated vulnerability disclosure.[1] These documents will serve as a much-needed resource to help ensure that those reporting on medical device issues are better prepared to understand the general processes and unique challenges posed by operating in the highly regulated healthcare environment.

   In total, the materials are made up of three approachable, high-level documents:

   - General Education[2]
   - Abbreviated General Education[3]
   - Coordinated Vulnerability Disclosure[4]

   The MDSISC, which designed the materials, is currently made up of 331 volunteers from 49 medical device manufacturers who worked in close partnership with 64 health delivery organizations to ensure comprehensive guidance from a range of perspectives.

   While there have been significant improvements in the ways that medical device and cybersecurity issues are presented in the media, expertise is still generally limited to a handful of industry focused publications. In this context, the development of accessible healthcare-specific guidance on these issues is very welcome. It is the H-ISAC's hope that this content will help raise the standard of reporting when it comes to medical device and vulnerability disclosure issues.

The need for improved and accurate reporting surrounding security issues is critical when it comes to the healthcare sector, as misunderstandings and unintended distortions can cause unnecessary panic and confusion, particularly during times of crisis. At a time when the public's trust in the safety and integrity of the healthcare sector is of paramount importance, accurately representing how medical devices are secured, and how vulnerabilities are handled, is essential. The H-ISAC encourages everyone to review and make use of these new documents, which can be found on the H-ISAC's website and in the links cited below.

2. **Facebook and CMU: COVID-19 Surveys** For better or worse, social media companies have been and will continue to be prominent actors during the COVID-19 pandemic. While much of the negative focus remains on the use of social media as a platform for (mis)information and its role and responsibilities as a gatekeeper and curator, Facebook has garnered positive attention for attempting to directly participate in mitigating the pandemic.

   At the beginning of April, reports began to surface that Facebook, in conjunction with Carnegie Mellon University (CMU), would begin to roll out pop-up opt-in surveys to some Facebook users about COVID-19.[5] The effort is self-described as a way to map and forecast the spread of COVID-19 using the unique resources that Facebook has to offer—namely, the ability to potentially reach 2 billion individuals.[6, 7] By targeting the largest possible audience, researchers at CMU hoped to receive millions of responses per week to gather comprehensive data on where COVID-19 is spreading and what hospitals might expect a surge in patients.[8] The goal in amassing this data would be to help inform COVID-19 response efforts.

   Naturally, any project involving sensitive personal information is bound to bring security and privacy concerns and questions. Questions such as, where is the survey data being stored? Who has access to it? Is this HIPAA compliant? Are all obvious ones to ask. As are security related questions around the possibility of fake surveys leading to malicious activity.

   Facebook is keen to tell the public that they "designed this effort with privacy in mind from the start," and according to Ryan Tibshirani, co-leader of CMU's research group, "Facebook is providing us with users, but they are not involved in conducting the survey."[9, 10] CMU explains the process as follows:

   > "Facebook will share a random ID number with CMU for each participant. Once that participant completes the survey, CMU will send the ID number back to Facebook — but none of the replies. Facebook will then provide a statistic known as a weight value that will help CMU correct for any sample bias."[11]

A Wired report further elaborates that the project was reviewed by CMU's Institutional Review Board to ensure strict policies around data-sharing, and that "survey responses aren't linked to a person's Facebook account."[12] Mark Zuckerberg has also corroborated that Facebook does not have access to the survey responses.[13]

3. **Forceful State Department Press Release Provides More Questions Than Answers.** On April 17th, Michael Pompeo, Secretary of State, released a press statement regarding cyber-attacks against the Czech Republic's healthcare sector.[14] The press release is notable for its mix of boilerplate U.S. policy language and terse warning that "anyone that engages in such an action should expect consequences."[15] The form, timing, context, and content of the release seem to raise more questions than answers.

   On its face, calling out malicious actors for attacking the healthcare organizations of a U.S. ally during a global pandemic appears unremarkable. However, it is in fact somewhat odd for a number of reasons.

   First, there is the context and timing. The healthcare sector in the U.S. has been hit numerous times by ransomware and other malicious cyber activity over the past year. Many if not most of these attacks are likely to have originated in other countries, and they have the same potential to negatively impact patient outcomes as the recent incident in the Czech Republic. Furthermore, there has been a noted increase in attacks against the healthcare sector globally since the advent of COVID-19. However, these events did not elicit the kind of forceful warning on display here. Even a State Department advisory on North Korean cyber threats issued only 2 days prior to the agency's April 17th response lacked the cutting tone and anything resembling a veiled threat.[16]

   Second, there is the lack of outright attribution. The press release calls upon the unspecified actor to cease its activities and twice warns states that harboring such actors could result in them being held accountable. However, no group, individual, or state is named or even suggested as the culprit for this attack. The U.S. has increasingly made the naming and shaming of state-linked malicious cyber actors a fairly routine exercise. For example, the US has been willing to call out China, Russia, Iran, and North Korea directly in the past. Rarely has it ever made such a specific pointed remark while remaining vague as to its intended target. That said, such tactics are not unheard of. International politics can be complex and there are situations where naming and shaming specifically may not be advisable if it would negatively impact other political or economic efforts with the nation in question. Striking a balance is something every administration must do carefully.

Congress –

<u>Tuesday, April 28th</u>:
- No relevant hearings

April 28th, 2020

Wednesday, April 29th:
- No relevant hearings

Thursday, April 30th:
- No relevant hearings

International Hearings/Meetings –

EU – No relevant hearings/meetings

Conferences, Webinars, and Summits –

--Leverage SecurityScorecard's Self-Monitoring and Vendor Risk Management Solution for H-ISAC Members (TLP GREEN) – Webinar (4/30/2020)
https://h-isac.org/hisacevents/leverage-securityscorecards-self-monitoring-and-vendor-risk-management-solution-for-h-isac-members-tlp-green/
--H-ISAC Monthly Member Threat Briefing – Webinar (5/26/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-8/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020) (POSTPONED)
https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/
--H-ISAC Security Workshop - Buffalo, NY (6/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/
H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (7/17/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Forchheim, Germany
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)

https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

Sundries –

--Unproven Coronavirus Therapy Proves Cash Cow for Shadow Pharmacies
https://krebsonsecurity.com/2020/04/unproven-coronavirus-therapy-proves-cash-cow-for-shadow-pharmacies/
--As contact tracing gains attention, a researcher pokes a hole in Bluetooth technology
https://www.cyberscoop.com/bluetooth-exploit-jan-ruge-contact-tracing/
--Cerner, AWS partner to make COVID-19 data available to researchers
https://www.healthcareitnews.com/news/cerner-aws-partner-make-covid-19-data-available-researchers
-- FBI enlists internet domain registries in fight against coronavirus scams
https://www.cyberscoop.com/fbi-coronavirus-scams-internet-domains/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://h-isac.org/cvd-media-kit/
[2] https://h-isac.org/wp-content/uploads/2020/04/HISAC-media-backgrounder_FINAL_CLEAN_full-version-1.pdf
[3] https://h-isac.org/wp-content/uploads/2020/04/HISAC-media-backgrounder_FINAL_abbreviated-version_CLEAN.pdf
[4] https://h-isac.org/wp-content/uploads/2020/04/HISAC-CVD-process_FINAL_CLEAN.pdf
[5] https://techcrunch.com/2020/04/06/facebook-covid-19-survey-cmu/
[6] https://www.cmu.edu/news/stories/archives/2020/april/facebook-survey-covid.html
[7] https://covid-survey.dataforgood.fb.com/
[8] https://www.cmu.edu/news/stories/archives/2020/april/facebook-survey-covid.html
[9] https://www.cmu.edu/news/stories/archives/2020/april/facebook-survey-covid.html
[10] https://covid-survey.dataforgood.fb.com/
[11] https://www.cmu.edu/news/stories/archives/2020/april/facebook-survey-covid.html
[12] https://www.wired.com/story/survey-data-facebook-google-map-covid-19-carnegie-mellon/
[13] https://about.fb.com/news/2020/04/symptom-surveys/

[14] https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/
[15] https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/
[16] https://www.state.gov/the-united-states-issues-an-advisory-on-north-korean-cyber-threats/