December 10th, 2019

TLP White

In this edition of Hacking Healthcare, we spotlight the Food and Drug Administration's request for nominations to their Medical Devices Advisory Committee. Next, we brief you on Sen. Booker and Sen. Wyden's mission to combat bias in healthcare algorithms. Additionally, we highlight a new indictment against Russian hackers and why it matters despite the unlikeliness of there ever being a trial. Finally, we give you the lowdown on an expected cloud security advisory from the National Security Agency's Cybersecurity Directorate.   Welcome back to *Hacking Healthcare*.

Author's Note: *It was great to meet many of you at the H-ISAC Fall Summit last week in occasionally sunny San Diego! We greatly appreciate the positive feedback we received on the value Hacking Healthcare provides to our readers. As always, we welcome thoughts and suggestions on how we can improve, and on topics that are of interest. See you again in the Spring!*

1. **FDA Request for Nominations for Advisory Committee**. From our "Just In Case You Weren't Aware" department, we note that the Food and Drug Administration within the U.S. Department of Health and Human Services is currently requesting nominations for panels on the Medical Devices Advisory Committee. The committee "reviews and evaluates data on the safety and effectiveness of marketed and investigational devices and makes recommendations for their regulation" and engages on several safety and security issues. The letters of interest and nomination materials are due by 1/6/2020 and further information can be found on the federal register (link).

2. **U.S. Senators Demand Answers on Biases in Healthcare Algorithms**. With all the promise that big data holds in relation to the healthcare sector, including goals of creating personalized treatment plans, issues of representation are often forgotten. Within the United States, there is growing concern that data sets and algorithms may not be adequately adjusted to compensate for biases. Chief among these concerns is that minorities that have been historically socioeconomically marginalized are significantly underrepresented not only within the data sets themselves, but also in the creation of the algorithms that drive modern healthcare solutions. Last week, two Democratic Senators reached out to federal agencies and major healthcare organizations to raise this issue.

Sens. Ron Wyden and Cory Booker sent letters last week asking for more detailed information on how the private sector is accounting for potential bias in healthcare algorithms that could lead to negative or suboptimal treatment for underrepresented patients. They cite in their letter that while the usage of such algorithms is often done in an attempt to remove the fallible human element from complex decisions, not accounting for the biases in the creation of the algorithms can end up perpetuating these biases under the guise of scientific impartiality.[1] The Senators also reached out to the U.S. Federal Trade Commission and the Centers for Medicare and Medicaid Services to understand how "well-equipped their current enforcement mechanisms were to handle algorithmic biases and the scope of the challenge."[2]

3. **U.S. Prosecutors Charge Two Russian Hackers**. Last week, the U.S. Department of Justice charged two Russian nationals for their involvement in a multi-year hacking and fraud campaign that ultimately cost U.S. organizations roughly $70 million.[3] The two individuals, Maksim Yakubets and Igor Turashev, are alleged to have contributed to the development and distribution of malware dubbed Bugat and its follow-on Dridex, as well as being members of the cyber-criminal group Evil Corp. The 10-count indictment unsealed on Thursday includes charges of conspiracy, computer hacking, wire fraud, and bank fraud.[4] The two are believed to be at large in Russia and their apprehension is extremely unlikely.

    The malware that these two individuals are alleged to have helped develop and distribute has been a scourge to banks and financial institutions for nearly a decade.[5] The Dridex malware in particular has been used to target nearly 300 organizations in over 40 countries according to the U.S. Treasury Department.[6, 7] Russia is unlikely to ever willingly extradite its own nationals to the United States to face trial, and with the indictment now public the two individuals are sure to be very careful in traveling anywhere that may be willing to work with the U.S. in apprehending them.

4. **The U.S. National Security Agency (NSA) to Update Cloud Security Guidance**. In the wake of a number of attacks on service providers over the past few months, the NSA looks poised to update their guidance on cloud security. Speaking at the Wall Street Journal Pro Cybersecurity Executive Forum last Tuesday, Anne Neuberger, the director of the NSA's Cybersecurity Directorate, revealed that they will be issuing "an unclassified advisory on the techniques used to compromise clouds and some mitigation advice."[8] The expectation is that the advisory will be out before the end of the year.[9]

    While acknowledging the benefits that adopting the cloud can bring to businesses, Ms. Neuberger cited how small businesses are vulnerable to attacks against their service provider.[10] It's been these attacks that appear to be the catalyst for this latest revamping of cloud security guidance. While the NSA has put out cloud security guidance in the past, the Directorate has indicated that this upcoming release would be

more "sophisticated," likely in response to the increased complexity of recent attacks and the overall growth in cloud maturity.[11]

As a refresher, The NSA's Cybersecurity Directorate was stood up earlier this year by General Nakasone, but it only recently became operational. The Directorate's self-stated description and mission is to unify the "NSA's foreign intelligence and cyber defense missions," while also charging it with "preventing and eradicating threats to National Security Systems and the Defense Industrial Base."[12] The issuance of advisories and general information sharing is one of their core contributions.

U.S. Congress –

Tuesday, December 10th:
- Senate Judiciary Committee- Hearings to examine encryption and lawful access, focusing on evaluating benefits and risks to public safety and privacy.

Wednesday, December 11th:
- Senate Foreign Relations Committee – Business meeting including S.482 which details combatting international cyber crime

Thursday, December 12th:
- No relevant hearings

International Hearings/Meetings –
EU –

Conferences, Webinars, and Summits –
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
--Global Cyber Security in Healthcare & Pharma Summit - London, UK (2/6/2020)
http://www.global-engage.com/event/cybsec-health-summit/
--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/summits/apac-summit-2020/
-- 2020 APAC Summit – Singapore (3/31/2020-4/2/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/14/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/

Sundries –
--Scammers dupe Chinese venture capitalists out of $1 million with the 'ultimate' BEC heist
https://www.cyberscoop.com/bec-venture-heist-check-point-technologies/
--Chinese residents worry about rise of facial recognition
https://www.bbc.com/news/technology-50674909

December 10th, 2019

--Huawei sues FCC for icing U.S. business, claiming a lack of evidence
https://www.cyberscoop.com/huawei-sues-fcc-block/
--IBM sounds alarm about more data-wiping malware from Iran
https://www.cyberscoop.com/iran-destructive-malware-ibm/

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

[1] https://www.wyden.senate.gov/news/press-releases/wyden-booker-demand-answers-on-biased-health-care-algorithms

[2] https://www.wyden.senate.gov/news/press-releases/wyden-booker-demand-answers-on-biased-health-care-algorithms

[3] https://arstechnica.com/information-technology/2019/12/members-of-evil-corp-the-cybercrime-group-that-lived-in-luxury-are-indicted/

[4] https://arstechnica.com/information-technology/2019/12/members-of-evil-corp-the-cybercrime-group-that-lived-in-luxury-are-indicted/

[5] https://www.cyberscoop.com/dridex-begat-doj-indictment-russians-arrested/

[6] https://arstechnica.com/information-technology/2019/12/members-of-evil-corp-the-cybercrime-group-that-lived-in-luxury-are-indicted/

[7] https://www.cyberscoop.com/dridex-begat-doj-indictment-russians-arrested/

[8] https://www.wsj.com/articles/nsa-to-issue-updated-cloud-security-guidance-11575409110

[9] https://www.wsj.com/articles/nsa-to-issue-updated-cloud-security-guidance-11575409110

[10] https://www.wsj.com/articles/nsa-to-issue-updated-cloud-security-guidance-11575409110

[11] https://www.wsj.com/articles/nsa-to-issue-updated-cloud-security-guidance-11575409110

[12] https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1912825/faq-nsacss-cybersecurity-directorate/