June 5, 2018

Hacking Healthcare

TLP White

We have a lot in store for you this week, folks. We start with a request from the American Hospital Association that the FDA create a single repository for medical device manufacturers to report cyber vulnerabilities and then we'll discuss the FBI's claims about going-dark and end-to-end encryption. We also address the Trump Administration's recent botnet and distributed threats report and then shed some light on a new device that would allow Autonomous Vehicles to monitor a passenger's health and alert local healthcare officials of a medical emergency. We conclude with a discussion about a new Maryland law that incentivizes companies to invest in cybersecurity controls. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Single Repository for Reporting Vulnerabilities.*** The American Hospital Association ("AHA"), a national organization that represents and serves hospitals and healthcare networks,[1] requested that the US Food and Drug Administration ("FDA") create a single repository for medical device manufacturers to report cyber vulnerabilities.[2] The request came as a response to the FDA's recent *Medical Device Safety Action Plan* ("Action Plan")[3] for improving device safety, which includes cybersecurity guidance and was covered in our April 24th edition of *Hacking Healthcare.*

   Overall, the AHA appreciates and supports the FDA's plan but suggests that the FDA "consider creating a single repository of information for disclosures so that end-users can easily access it during times of crisis." The AHA also asks that the FDA quickly adopt its Action Plan, set timely disclosure and patch requirements, and partner with healthcare providers in creating and deploying the Action Plan's CyberMed Safety (Expert) Analysis Board. The AHA acknowledges that nothing can "completely eliminate cybersecurity risks from healthcare" but states that "swift action by the FDA to improve the security of medical devices will address a significant source of vulnerability."

[1] https://www.aha.org/about

[2] https://www.aha.org/system/files/2018-05/180524-CL-fda-device-safety-plan.pdf

[3] https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf

A single, centralized repository for reporting cybersecurity vulnerabilities, as AHA suggests, would allow members of the healthcare industry to coordinate with one another in disclosing, mitigating, and even avoiding cybersecurity vulnerabilities found in medical devices. In fact, such repositories are relatively common. For example, NIST's National Vulnerability Database, which includes a "Common Vulnerabilities and Exposures" feature,[4] [5] is highly regarded as a legitimate resource for disclosing and mitigating known security vulnerabilities. Indeed, the AHA's recommendation aligns well with the Action Plan's consideration to "require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified"[6] so the FDA may be open to the AHA's recommendation.

2. ***Shining a Light on Going Dark.*** When it comes to encryption, tech companies have taken the position that it is an important part of economic and national security. The Federal Bureau of Investigation ("FBI"), on the other hand, has often asserted that end-to-end encryption allows criminals to "go dark," enabling them to operate beyond the reach of law enforcement. The FBI's credibility on the topic of encryption has recently been called into question and has brought to light that law enforcement manipulated efforts and exaggerated statistics to advance its position in the encryption debate.

   A recent report[7] by the Department of Justice's Inspector General suggests that some FBI staff purposely slowed efforts to unlock San Bernardino shooter Syed Rizwan Farook's iPhone to amplify pressure on Apple to build a backdoor. The report also suggests that senior investigators did not pursue all available avenues for unlocking the device because they wanted to use legal action against Apple to set new precedent in the encryption space.[8]

   Beyond the San Bernardino case, the FBI distributed erroneous figures regarding the total number of devices that the FBI was allegedly unable to access. In late 2017, FBI Director Christopher Wray stated that in the 2017 budget year the FBI "was unable to access the content of approximately 7,800 mobile devices using appropriate and available technical tools, even though there was legal authority to do so" and that "as horrifying as 7,800 in one year sounds, it's going to be a lot worse in just a couple of years if we don't find a responsible solution."[9] In early May, Attorney General Jeff Sessions reiterated the same statistic in remarks delivered to the Association of State

[4] https://nvd.nist.gov
[5] https://nvd.nist.gov/general/faq#eeabbb01-eb9f-488d-ac31-40a8b92c1473
[6] https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf
[7] https://oig.justice.gov/reports/2018/o1803.pdf
[8] https://www.cyberscoop.com/fbi-going-dark-encryption-ari-schwartz-op-ed/
[9] https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.18c545af79b2

Criminal Investigative Agencies, and stated that each of those devises "was tied to a threat to the American people."[10]

As it turns out, the total number was much smaller, likely in the 1,000-2,000 range.[11] This number is much closer to the total for 2016 which the FBI claimed was around 880, and much more in line with what privacy and security advocates would have expected.

The FBI's manipulation of the San Bernardino investigation and dissemination of inaccurate figures with respect to the number of devices that they claimed it could not open is more than just a blow to the agency's credibility. It is an important reminder that lawmakers must take care to scrutinize the claims made by law enforcement when it comes to encryption just as they have done for claims made by the tech industry. Legislators wishing to take action in areas with such significant security ramifications must do so on the basis of complete and accurate information.

3. ***The Administration's Botnet and Distributed Threats Report.*** The Trump Administration recently released a joint report conducted by the US departments of Homeland Security and Commerce titled, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* ("Report").[12] For context, botnets are networks of connected devices infected with malware or are otherwise remotely controlled by third-parties for nefarious purposes.[13] In fact, botnets are used for many such purposes, including to facilitate assaults like Distributed Denial of Service ("DDoS") attacks. DDoS attacks come in a variety of forms but the end goal of these attacks are the same: to overwhelm a network and its resources so that the network fails to work properly. This in turn leads to a service or information being unavailable to those who are authorized to access it, leading to loss of revenue, reputation or worse. The Report is a follow up to a previous draft released earlier this year and provides a guide to reduce the threats associated with botnets and similar cyber threats like DDoS attacks.[14]

Overall, the Report states that automated, distributed attacks like botnets are a global problem and cannot be addressed by one single stakeholder and further emphasizes that effective tools currently exist but are not used as commonly as they could be. The Report also states that products should be secured throughout their entire lifecycle and that market incentives should be created in order to align more with the goal of reducing attacks. In addition to these themes, the Report lists out specific goals,

[10] https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-association-state-criminal-investigative

[11] https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.18c545af79b2

[12] https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

[13] https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf

[14] https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets

including, among other things: (1) identifying a clear pathway toward adapting, sustaining, and securing the technological marketplace; (2) establishing a more resilient and collaborative ecosystem as well as standards and best practices that deter, prevent, and/or mitigate automated attacks like botnets and DDoS attacks; (3) promoting and supporting coalitions between the security, infrastructure, and operational technology industries in the US and throughout the world; and (4) increasing awareness and education about cybersecurity and associated threats.

4. ***Autonomous Vehicles and Healthcare.*** Sony, in a recent patent application, offers a device that would monitor an Autonomous Vehicle ("AVs") passenger's health and alert local health officials of medical emergencies.[15] As background, there are 5 levels of vehicle automation. A level 1 vehicle is controlled by the driver but includes driver assistance technology while a level 5 vehicle is capable of performing all driving tasks under all conditions (a level 5 vehicle does not yet exist).[16]

   Specifically, Sony's device would receive health data from a passenger's sensing device – e.g., smart phone, smartwatch, fitness tracker, etc. – and compare the data to the passenger's normal health parameters, as determined by the passenger's sensing device. If Sony's device discovers an abnormality equivalent to a medical emergency, the vehicle would alert local doctors and hospitals, provide the passenger's estimated time of arrival, coordinate treatment, and subsequently drive the passenger to the nearest healthcare facility. Currently, no such device exists for AVs.

5. ***Maryland Small Businesses Get Big Credit.*** Despite the importance of cybersecurity for entities large and small, the resources needed to establish adequate security safeguards can be prohibitive for small businesses. New legislation in Maryland uses a tax credit to help small businesses better protect themselves against cyber-attacks. Under the new law, Maryland small businesses that purchase cybersecurity products or services from eligible Maryland cybersecurity providers will be able to claim a state income tax credit equal to 50% of the purchase price up to $50,000.[17] The statute provides that entities that have fewer than 50 full-time employees in Maryland and are required to file an income tax return in the state may be considered a "qualified buyer" and thus eligible for the credit.

   Investors in cybersecurity startups also benefit from the new legislation. The bill includes tax credits to individuals or entities that invest at least $25,000 in a Maryland-based company that is primarily dedicated to the development of innovative and proprietary cybersecurity technology. Under this program, investors may be eligible for

[15] http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180132081%22.PGNR.&OS=DN/20180132081&RS=DN/20180132081

[16] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[17] http://mgaleg.maryland.gov/2018RS/Chapters_noln/CH_578_sb0228e.pdf

a refundable tax credit for 33% of the investment in a qualified company, not to exceed $250,000.

Maryland is leading the way for using tax credits to incentivize better cybersecurity practices and investment in cybersecurity startups. Maryland has a reputation for having a high-tech base, ranking fifth for concentration of tech industry employment in the total workforce in 2017.[18] Maryland will be an interesting case study to demonstrate whether the total number of cyber incidents in Maryland decreases as a result of the credit. Hopefully, if successful, we will see other states advance similar legislation.

Congress –

Tuesday, June 5:
--No relevant hearings

Wednesday, June 6:
--Hearing to examine the policies and priorities of the U.S. Department of Health and Human Services (House Committee on Education and the Workforce)[19]
--Hearing to examine lowering costs and expanding access to health care through consume-directed health plans (House Subcommittee on Health)[20]

Thursday, June 7:
--Hearing to examine the electric grid of the future (House Subcommittee on Energy)[21]

Conferences and Webinars –

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>

[18] https://msa.maryland.gov/msa/mdmanual/01glance/economy/html/economy.html
[19] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108384
[20] https://waysandmeans.house.gov/event/hearing-on-lowering-costs-and-expanding-access-to-health-care-through-consumer-directed-health-plans/
[21] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108392

--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Glasnost for US Intelligence: Will Transparency Lead to Increased Public Trust?**
<https://www.lawfareblog.com/glasnost-us-intelligence-will-transparency-lead-increased-public-trust>
-- **Pentagon Will Expand AI Project Prompting Protests at Google**
<https://www.wired.com/story/googles-contentious-pentagon-project-is-likely-to-expand>
-- **Will the Real Joker's Stash Come Forward?**
<https://krebsonsecurity.com/2018/05/will-the-real-jokers-stash-come-forward/>
-- **Canadian Banks Hacked**
<https://www.darkreading.com/attacks-breaches/canadian-banks-hacked/d/d-id/1331914>
-- **How to Empower Today's 'cISOs'**
<https://www.darkreading.com/threat-intelligence/how-to-empower-todays-cisos/a/d-id/1331865>
-- **NPM Fails Worldwide With "ERR! 418 I'm a Teapot" Error**
<https://www.bleepingcomputer.com/news/technology/npm-fails-worldwide-with-err-418-im-a-teapot-error/>
-- **Python May Let Security Tools See What Operations the Runtime Is Performing**
<https://www.bleepingcomputer.com/news/security/python-may-let-security-tools-see-what-operations-the-runtime-is-performing/>
-- **Oracle Plans to Drop Java Serialization Support, the Source of Most Security Bugs**
<https://www.bleepingcomputer.com/news/security/oracle-plans-to-drop-java-serialization-support-the-source-of-most-security-bugs/>
-- **Hacker Steals $1.35 Million From Cryptocurrency Trading App Taylor**
<https://www.bleepingcomputer.com/news/security/hacker-steals-135-million-from-cryptocurrency-trading-app-taylor/>
-- **New Threats, Old Threats: Everywhere a Threat**
<https://www.darkreading.com/attacks-breaches/new-threats-old-threats-everywhere-a-threat/a/d-id/1331879>

June 5, 2018

Contact us: follow @NHISAC and email at contact@nhisac.org