August 7, 2018

TLP White

We start with a DNC announcement regarding the use of Chinese telecom companies Huawei and ZTE and then dive into recently released guidance on healthcare mobile device security. We conclude with an FBI PSA regarding IoT security and how to protect and defend against attacks. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***No Way Huawei.*** The Democratic National Committee ("DNC") Chief Security Officer Bob Lord warned state parties and the DNC's sister committees to steer clear of devices made by Chinese telecom companies Huawei and ZTE.[1] In his email, Lord cautioned that devices made by these companies pose a security risk, and advised against using them even if the devices are provided for a low price or even free. Lord's sentiments are in line with those expressed by U.S. intelligence officials earlier this year. During a February congressional hearing, U.S. intelligence officials recommended that Americans do not purchase Huawei or ZTE devices because they pose a security risk. In his email to DNC candidates, Lord emphasized that the intelligence community does not make statements like this lightly, and asked candidates not to use the devices anywhere within their staff, neither for personal nor work-related use.

   The DNC's decision to ask candidates not to use a particular technology is emblematic of some interesting shifts in the private sector and related policy choices. These types of decisions have the potential to have a broad impact on the Internet of Things ("IoT") and technology supply-chain moving forward.

2. ***NIST and NCCoE Publish Mobile Device Security Guide.*** The National Institute of Standards and Technology ("NIST") in conjunction with the National Cybersecurity Center of Excellence ("NCCoE") released a guide[2] titled, "Securing Electronic Health Records on Mobile Devices" in an effort to help healthcare providers improve healthcare mobile device security and ultimately protect personal health information

[1] https://www.cyberscoop.com/zte-huawei-dnc-warning-bob-lord/
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

("PHI") from unauthorized access and disclosure.[3] The guide includes a modular, standards-based reference design which is intended to be used in whole or in part by IT professionals and security engineers.

As it is, the healthcare sector is already dealing with particularly high cybersecurity incident rates. Adding mobile to the equation only complicates the matter by significantly increasing the attack surface. As a result, healthcare providers have expressed that mobile device security is a top concern with respect to mobile programs.[4] Notwithstanding these concerns, a recent survey of healthcare IT professionals noted that 90% of respondents indicated that their institution either currently or has future plans to implement a mobile initiative, and roughly half of respondents indicated that within the next two years their organization planned to increase mobile device usage.

The guide acknowledges the trend towards increased use of mobile devices by healthcare providers and the increased risks that accompany the misuse, theft, modification, or unauthorized disclosure of health information, including penalties, loss of consumer trust, and patient care and safety. In response to this reality, the guide demonstrates how health care providers can share patient information with caregivers who are using mobile devices in a way that is more secure while relying on open-source and commercially available tools and technologies.

3. ***FBI PSA: Your IoT is a Target.*** On August 2, the Federal Bureau of Investigation ("FBI") issued a public service announcement ("PSA") warning healthcare organizations that IoT devices are increasingly targeted by cybercriminals.[5] As we have discussed in previous newsletters, healthcare organizations are increasingly using IoT, but these capabilities are often accompanied by increased risks. The FBI's PSA notes that cyber actors actively search for and compromise vulnerable IoT devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and compute network exploitation.[6]

   The PSA explains that "IoT proxy servers are attractive to malicious cyber actors because they provide a layer of anonymity by transmitting all Internet requests through the victim device's IP address. Devices in developed nations are particularly attractive targets because they allow access to many business websites that block traffic from suspicious or foreign IP addresses. Cyber actors use the compromised device's IP address to engage in intrusion activities, making it difficult to filter regular traffic from malicious traffic."[7]

---

[3] https://healthitsecurity.com/news/nist-nccoe-publish-guide-on-healthcare-mobile-device-security
[4] https://healthitsecurity.com/news/mobile-device-security-worries-plague-healthcare-providers
[5] https://www.ic3.gov/media/2018/180802.aspx
[6] https://www.ic3.gov/media/2018/180802.aspx
[7] https://www.ic3.gov/media/2018/180802.aspx

> The FBI has seen compromised IoT devices used as proxies to engage in a variety of nefarious activities, from sending spam e-mails and obfuscating network traffic to buying, selling, and trading illegal images and goods and selling or leasing IoT botnets to other cyber actors for financial gain. The FBI notes that cyber actors tend to compromise devices with weak authentication, unpatched firmware or other software vulnerabilities, or by using brute force attacks on devices with default usernames and passwords.

Congress –

Tuesday, August 7:
--No relevant hearings

Wednesday, August 8:
--No relevant hearings

Thursday, August 9:
--No relevant hearings

Conferences, Webinars, and Summits –

--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA– Washington, DC (8/9) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--NH-ISAC Blended Threats Exercise Series – CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--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/>
--Biotech/Pharma Security Workshop at Amgen – Tokyo, Japan (8/29) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-at-amgen-tokyo/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--NH-ISAC & Cleveland Clinic Medical Device Security Workshop – Breachwood, OH (10/17-18) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-cleveland-clinic-beachwood-oh/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**Democratic candidates told not to use ZTE, Huawei devices: source** <https://www.reuters.com/article/us-usa-china-democrats/democratic-candidates-told-not-to-use-zte-huawei-devices-source-idUSKBN1KP02F>
--**Tech Support Scams Using Call Optimization Services to Insert Phone Numbers** <https://www.bleepingcomputer.com/news/security/tech-support-scams-using-call-optimization-services-to-insert-phone-numbers/>
--**How FBI's global reach took down a cybercrime unicorn** <https://www.cyberscoop.com/fin7-carbanak-fbi-arrests-fedir-hladyr/>
--**FBI struggles to retain top cyber talent** <https://www.politico.com/story/2018/08/03/fbi-cyber-security-talent-drain-hacking-threat-russia-elections-760740>
--**Google Faces Hurdles in China Beyond Censorship** <https://www.wired.com/story/google-faces-hurdles-in-china-beyond-censorship>

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