July 15th, 2020

TLP White

This week, Hacking Healthcare explores the full scope of China's intelligence gathering operations against healthcare entities in the United States and its allies in the wake of COVID-19 and outlines some practical and inexpensive ways to boost security. Next, we review how individual states are taking steps to permanently embrace telehealth changes and discuss what you can expect on telehealth from a federal standpoint. Finally, we briefly explain how a smartwatch and an accompanying healthcare related app demonstrate the security issues of not having comprehensive visibility into a product's underlying code. Welcome back to *Hacking Healthcare*.

1. **FBI: China's Intelligence Operations Lap the Field.** The threat from government sponsored Chinese Advanced Persistent Threats ("APTs"), patriotic hackers, and unaffiliated criminal organizations is well known in the West. However, last week, Federal Bureau of Investigation ("FBI") Director Christopher Wray helped to put the sheer scale of Chinese threat actors into focus when he stated that nearly half of the 5,000 active counterintelligence investigations that are open in the United States are related to China.[1] This translates into a new Chinese related matter being opened every 10 hours.[2]

   While not all of these Chinese intelligence activities contain malicious cyber components, many of the highest profile and most sensitive operations do. Director Wray acknowledged that Chinese related economic espionage cases, including those targeting research and conducting IP theft, had increased 1300% in the past decade.[3] He further outlined that Chinese threat actors use "a diverse range of sophisticated techniques" that include subtle cyber-intrusion as well as targeted attacks using social media to identify targets.[4]

   Wray specifically acknowledged the threat to healthcare, stating that the Chinese government is actively looking to compromise healthcare and pharmaceutical companies conducting COVID-19 research. The FBI has noted that American healthcare organizations making prominent announcements related to COVID-19 research often find themselves being targeted within 24 hours.[5] This echoes statements from close allies like Canada.

   While not specifically calling out China, Scott Jones, Head of the Canadian Centre for Cyber Security, noted numerous successful breaches against organizations conducting COVID-19 research to the Canadian Parliament last week.[6] Jones explained that policy makers often overlook how many small and medium sized organizations that are critical to the COVID-19 effort lack the cybersecurity resources to adequately defend against the types of threats they are seeing. This has lead individuals like Paul-Émile Cloutier, CEO of HealthcareCAN, to publicly

lament the state of healthcare sector cybersecurity, with some calling for the imposition of national cybersecurity standards for the sector.[7]

Action & Analysis

H-ISAC Membership Required

2. **States Take the Lead in Making COVID-19 Related Telehealth Changes.** While Congress and the federal government assess changes to national telehealth rules and regulations, several states have started taking the initiative.

   Massachusetts: At the end of June, the Massachusetts Board of Registration in Medicine approved a permanent policy on telemedicine that states: "The practice of medicine shall not require a face-to-face encounter between the physician and the patient prior to health care delivery via telemedicine." The policy also affirms that the "standard of care applicable to the physician is the same whether the patient is seen in-person or through telemedicine. "[8] This is considered by many to be a significant step for a state that has avoided making any detailed telehealth policies for decades.[9]

   Colorado: Last week, Colorado Governor Jared Polis signed SB20-212 into law. The bill "[concerns] reimbursement for health care services provided through telehealth" and "bars health plans from imposing specific requirements or limitations on the technologies used to deliver telehealth services as long as those technologies comply with the Health Insurance Portability and Accountability Act."[10, 11] The bill passed the Colorado House and Senate with strong bi-partisan support, receiving only one dissenting vote. Governor Polis specifically called out COVID-19 as the driving force for advancing telemedicine.

   Idaho: In late June, Idaho Governor Brad Little signed an executive order that made a number of temporary telehealth waivers permanent, including easing restrictions on the applications healthcare providers may use for telehealth. The easing of those restrictions came as part of a broader package that made over 150 COVID-19 related emergency rules permanent. Governor Little asserted that these changes "make healthcare more accessible and affordable for Idaho families and businesses."[12]

Action & Analysis

H-ISAC Membership Required

3. **Smartwatch Health App Reiterates IoT HealthCare Security Dangers.** From our "In Case You Forgot Department" we note that excitement over the potential for smartphones, smartwatches, and IoT devices to expand healthcare options and services continues to grow. However, recent reports have reiterated the dangers associated with connected healthcare devices when security is not top of mind during development and when devices with the potential for healthcare applications aren't produced and supported by healthcare entities.

   Last week, security researchers took an in-depth look at a tracker service application and accompanying smartwatch that appears designed specifically for the elderly and those with cognitive impairments. Among the various options included in the watch and accompanying application is a tracking feature to help caregivers locate disoriented wearers, and a triggered

reminder that it is time to take medications. As the researchers note, "If a carer couldn't visit for reasons of isolation during CV-19, a remote alert to a wearer who wasn't able to remember for themselves would be very helpful."[13]

In terms of utility and intention, these device applications are all well and good. In terms of security, the device unfortunately posed undeniable risks. Researchers noted that it only took "basic" hacking skills to allow anyone to track someone using the device, that the audio could be compromised to enable eavesdropping, and that the medication notification could be triggered at will.[14] One of the primary criticisms the researchers have raised is that "[n]o one has looked at the underlying code. No one has looked at how many servers are publicly available and what can be done server side to your children, elderly relatives or even your car."[15]

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, July 14th:
- No relevant hearings

Wednesday, July 15th:
- House – Committee on Oversight and Reform: Hearing on H.R. 7331, the National Cyber Director Act

Thursday, July 16th:
- No relevant hearings

International Hearings/Meetings –

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

--Healthcare Cybersecurity Forum - Mid-Atlantic – Virtual (7/16/2020)
https://endeavor.swoogo.com/summer_virtual_healthcare_innovation_cybersecurity_forum/About
-- H-ISAC Monthly Member Threat Briefing – Webinar (7/28/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-10/
--H-ISAC Virtual Security Workshop – Virtual (7/29/2020)
https://h-isac.org/hisacevents/nz-virtual-workshop/
-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--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 Virtual Security Workshop - Forchheim, Germany (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/

--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/
--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 –

--Secret Service merging electronic and financial crime task forces to combat cybercrime
https://www.cyberscoop.com/secret-service-reorganization-task-force-cybercrime-financial-crime/

-- Microsoft Shuts Down COVID-19 Phishing Campaign and Warns of Malicious OAuth Apps
https://www.hipaajournal.com/microsoft-shuts-down-covid-19-phishing-campaign-and-warns-of-malicious-oauth-apps/

--Home router warning: They're riddled with known flaws and run ancient, unpatched Linux
https://www.zdnet.com/article/home-router-warning-theyre-riddled-with-known-flaws-and-run-ancient-unpatched-linux/

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

---

[1] https://www.nextgov.com/cybersecurity/2020/07/fbi-opens-new-china-related-counterintelligence-investigation-every-10-hours-director-says/166706/
[2] https://www.nextgov.com/cybersecurity/2020/07/fbi-opens-new-china-related-counterintelligence-investigation-every-10-hours-director-says/166706/
[3] https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020
[4] https://www.nextgov.com/cybersecurity/2020/07/fbi-opens-new-china-related-counterintelligence-investigation-every-10-hours-director-says/166706/
[5] https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020
[6] https://subscriber.politicopro.com/article/2020/07/canadas-cyber-czar-hackers-hit-institutions-conducting-coronavirus-research-1964659
[7] https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422
[8] https://www.mass.gov/news/board-of-registration-in-medicine-approves-policy-on-telemedicine
[9] https://www.natlawreview.com/article/massachusetts-adopts-permanent-telehealth-policy-first-time
[10] http://leg.colorado.gov/bills/sb20-212
[11] https://news.bloomberglaw.com/coronavirus/telehealth-barriers-smoothed-under-new-colorado-law
[12] https://mhealthintelligence.com/news/idaho-governor-makes-covid-19-telehealth-expansion-permanent
[13] https://www.pentestpartners.com/security-blog/hacking-smart-devices-to-convince-dementia-sufferers-to-overdose/

[14] https://www.pentestpartners.com/security-blog/hacking-smart-devices-to-convince-dementia-sufferers-to-overdose/
[15] https://www.pentestpartners.com/security-blog/hacking-smart-devices-to-convince-dementia-sufferers-to-overdose/