November 6, 2018

TLP White: This week we start by examining the impact of the EU's General Data Protection Regulation and U.S. companies' initial responses to the law. We also discuss new vulnerabilities that have been discovered in Bluetooth-enabled devices. We end by shedding some light on ever-worsening threats of Chinese hacking and conclude that the problem has escalated in some new and alarming ways.

Welcome back to *Hacking Healthcare*.

Hot Links –

1. ***U.S. Businesses are Slow to React to the GDPR.*** Approximately 150 days ago, the EU passed sweeping privacy legislation called the General Data Protection Regulation (the "GDPR").[1] Since the law went into effect this May, U.S. businesses have struggled to grapple with how to comply with its directives.[2] In fact, partially due to the GDPR's nebulous wording and its far-reaching commands, the compliance efforts of many U.S.-based businesses have been sorely lacking. For example, the law requires companies to provide a "reasonable" level of protection for individuals' personal data, but U.S. companies have not reached an agreement regarding what is and is not "reasonable" in this space. As a result, companies have suffered from a certain amount of inertia with respect to their GDPR compliance obligations, as the law's unclear standards do not provide businesses with safe harbors or clear commands for meeting its requirements.

   While U.S. industry has largely adopted a "wait-and-see" approach, European companies have made major efforts to comply with the GDPR even in the face of its unclear mandates. European data protection regulators have been inundated with consumer complaints, but they have so far doled out fines to only a few entities. For instance, Portugal-based Barreiro Hospital was charged just $400,000 euro for mishandling patient records, but Canada-based AggregateIQ was threatened with a 20 *million* euro fine for failing to bring itself into compliance with the GDPR. It seems probable that European regulators may soon begin to increase enforcement against U.S. companies who fail to comply with its rules. In any event, given the lack of consensus

[1] https://gdpr-info.eu/
[2] https://threatpost.com/gdprs-first-150-days-impact-on-the-u-s/138739/

regarding what the law actually means, European privacy authorities will need to clarify their expectations through their future enforcement actions and adjudicatory decisions.

2. ***Another Day, Another Vulnerability: This Time It's Bluetooth Chips.*** Researchers at Armis recently discovered flaws in Texas Instruments Bluetooth chips that provide access points to WiFi services. These flaws, affectionately named BLEEDINGBIT, allow unauthorized actors to infiltrate internet-connected devices such as smart locks, insulin pumps, and pacemakers.[3] One of the BLEEDINGBIT flaws allows hackers to gain access to WiFi networks merely by being near a device that has enabled a certain type of Bluetooth technology to communicate. A second flaw sends fraudulent firmware updates to Bluetooth-enabled devices that use an "over-the-air download" feature. Some have stressed the pervasiveness of these flaws, but others have questioned how likely they are to be exploited on any substantial scale.

   BLEEDINGBIT has affected WiFi network equipment tied to large companies such as Aruba Networks, Cisco, and Meraki.[4] In the wake of these corporate network vulnerabilities, Texas Instruments has recommended disabling the "over-the-air download" feature in software production environments. The company has also created a patch to fix the flaws that has been made available to affected entities.

3. ***Hackers from China Show No Signs of Letting Up.*** Security software provider Carbon Black recently reported that China is now the world's preeminent perpetrator of cyberattacks.[5] Much of the world (and particularly the U.S.) had been hoping that China was planning to crack down on its citizens' cyber spying and intellectual property theft. However, it appears quite the opposite: Chinese hacks have only become more sophisticated, crafty, and frequent over time. Hacks from Chinese actors actually surpassed Russian hackers' overall productivity in Q3 of 2018.[6]

   The U.S. Department of Homeland Security ("DHS") recently issued an alert about an alarming hacking campaign called "Cloud Hopper" that has surfaced out of China.[7] The Cloud Hopper campaign was tied to the Chinese Ministry of State Security and took the form of an "island hopping" scheme: a tactic where cyber hackers target large organizations in order to access an affiliate's network. Carbon Black's report highlighted the fact that IoT devices can provide a useful access point for hackers to engage in this "island hopping" technique. DHS's alert listed loss of proprietary information, financial losses to restore systems and data, and reputational harm as some of the impacts of the campaign.

---

[3] https://www.bleepingcomputer.com/news/security/new-bleedingbit-vulnerabilities-affect-widely-used-bluetooth-chips/
[4] *Id*.
[5] https://www.carbonblack.com/quarterly-incident-response-threat-report/november-2018/
[6] https://arstechnica.com/information-technology/2018/11/new-data-shows-china-has-taken-the-gloves-off-in-hacking-attacks-on-us/
[7] https://www.us-cert.gov/ncas/alerts/TA18-276B

China's hacking efforts are alarming on their own, but hackers from other corners of the globe are improving their tactics in a similar manner. Ill-intentioned actors from Brazil, North Korea, and Iran have also upgraded their efforts in order to thwart companies' internal procedures to combat hacks. It appears that the problem is on course to get worse before it gets better.

Congress –

Tuesday, November 6:
--No relevant hearings.

Wednesday, November 7:
--No relevant hearings.

Thursday, November 8:
--No relevant hearings.

International Hearings/Meetings –

EU –

Tuesday, November 13:
--Hearing entitled, "Assessing the impact of digital transformation of health services" (EU Commission's Expert Panel on Health).[8]

Conferences, Webinars, and Summits –

--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall "Never Stand Alone" Summit – San Antonio, TX (11/26-30) <https://nhisac.org/summits/2018-fall-summit/>
--Medical Device Security 101 Conference – Orlando, FL (1/21/19-1/22/19) <https://nhisac.org/events/nhisac-events/medical-device-security-101-conference/>
--FIRST Symposium 2019 – London, UK (3/18/19) <https://nhisac.org/events/nhisac-events/first-symposium-2019/>
--2019 NH-ISAC Spring Summit – Ponte Vedra Beach, FL (5/13/19-5/17/19) <https://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

Sundries –

[8] https://ec.europa.eu/health/expert_panel/events_en

November 6, 2018

--**Senator's data privacy law draft could put CEOs in jail for lying**
<https://www.cnet.com/news/senator-introduces-privacy-law-draft-that-could-put-ceos-in-jail-for-data-breaches/#ftag=CAD590a51e>
--**Midterm elections: How politicians know exactly how you're going to vote**
<https://www.cnet.com/news/how-your-personal-data-is-used-to-create-a-perfect-midterm-election-ad/#ftag=CAD590a51e>
--**Satya Nadella: The cloud is going to move underwater**
<https://arstechnica.com/gadgets/2018/11/satya-nadella-the-cloud-is-going-to-move-underwater/>
--**OVH: the open source public cloud alternative from Paris**
<https://www.itworldcanada.com/article/ovh-the-open-source-public-cloud-alternative-from-paris/411215>
--**FDA Steps Up Its Focus On Medical Device Cybersecurity**
<https://www.law360.com/lifesciences/articles/1097808/fda-steps-up-its-focus-on-medical-device-cybersecurity>
--**Radisson Rewards Program Targeted in Data Breach**
<https://www.darkreading.com/attacks-breaches/radisson-rewards-program-targeted-in-data-breach/d/d-id/1333176?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>
--**The privacy battle to save Google from itself**
<https://www.wired.com/story/google-privacy-data/>

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