July 24, 2018

Hacking Healthcare

TLP White

We start with a look at an effort to make moving user data easier and then take a look at a recent healthcare data breach in Singapore. We conclude with a new entry in what seems like a regular feature on IoT security. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Tech Giants Working Together.*** Coming out of our "Wait. What?" department, we report that four of the largest IT companies recently announced the Data Transfer Project (DTP)[1], the purpose of which is to "…create an open-source, service-to-service data portability platform so that all individuals across the web [can] easily move their data between online service providers whenever they want." Microsoft, Facebook, Google, and Twitter formed the effort in 2017, and released a scientific paper[2] with details this past Friday, July 20th.

   The paper describes the architecture and provides some example of how DTP can be used, all while meeting a core set of agreed-upon principles, summarized here:

   - **Build for users**: Data portability tools should be easy to find, intuitive to use, and readily available for users.
   - **Privacy and Security**: Providers on each side of the portability transaction should have strong privacy and security measures—such as encryption in transit—to guard again unauthorized access, diversion of data, or other types of fraud.
   - **Reciprocity**: A user's decision to move data to another service should not result in any loss of transparency or control over that data.
   - **Focus on user's data**: Portability efforts should emphasize data and use cases that support the individual user.
   - **Respect Everyone**: Data portability tools should focus only on providing data that is directly tied to the person requesting the transfer.

[1] https://datatransferproject.dev/

[2] https://datatransferproject.dev/dtp-overview.pdf

As users, we have all been faced with the challenge of changing service providers, whether it is for email, pictures, documents, or the myriad other forms of data that we create and manage about and for ourselves. That these competitors would want to come together to make switching between them easier may initially seem counter-intuitive, but as the DTP says: "[We] believe that portability and interoperability are central to innovation. Making it easier for individuals to choose among services facilitates competition, empowers individuals to try new services and enables them to choose the offering that best suits their needs." Sounds reasonable enough. However, we'll note that while not called out explicitly, it seems fairly obvious that at least part of the motivation here is the GDPR, which you will recall requires that users be able to access, move, and delete their data.

Notably missing from the list of companies at the moment are Apple and Amazon. Whether or not they come on board is yet to be seen, but we imagine it will be difficult to avoid if users come to expect portability from their service providers and see it as a market differentiator.

We think that this all makes perfect sense when you consider that data has become a commodity. And like all commodities, standardizing its storage, transfer, and use is ultimately the best solution for everyone.

2. ***Healthcare Breach in Singapore.*** This past Friday, Singapore's Ministry of Health (MOH) revealed that "a hacker had breached its IT systems and stolen personal and health-related data on roughly 1.5 million citizens."[3] Some facts about what was and wasn't taken:

- 1.5 million patients (about 1/3rd of all possible records) who visited SingHealth's specialist outpatient clinics and policy clinics.
- Data included records created between May 1, 2015 and July 4, 2018. Yes, that is over 3 years' worth.
- Data included name, address, gender, race, and data of birth.
- For 160,000 patients, the data also included information about medicines they had been given.
- Data was exfiltrated for roughly 8 days before the breach was discovered and stopped.
- The attack vector appears to have been malware placed on a computer with access to the database.
- Not in the trove were diagnosis details, test results, and doctor's notes.
- Nothing was apparently deleted or changed.

[3] https://www.bleepingcomputer.com/news/security/hackers-stole-a-third-of-singapores-healthcare-data-including-prime-ministers/

We have heard most of this before. It wasn't so long ago that Anthem and Premera[4] got hit in the United States, and plenty of other healthcare breaches have occurred over the years.

While the resulting loss of data isn't great, we would be remiss if we didn't point out a few positives. Eric Hoh, President of Asia Pacific at FireEye, noted that on average, Asia Pacific Organizations usually take 498 days (versus the 8 days in this case) before they detect intruders in their networks, and that "Against those metrics, this is a relatively fast response."[5]

We also like the fact that the Singapore government moved quickly to publicly disclose the breach and to begin reaching out to impacted individuals. They were decisive, and as far as we can tell from our vantage point on this side of the world, they took all the right steps in a difficult situation.

3. ***Oh IoT, What Are We Going to Do With You?*** Among the many changes that IoT has brought with it into the world is the notion of what we consider "a lot of devices" to be. Case in point this week is the DNS rebinding vulnerability found to be present in half a billion smart devices connected today.[6] The types of devices cover the waterfront, from smart TVs, routers, printers, surveillance cameras, IP phones, and..well you get the idea.

   In short, a DNS rebinding attack "trick's a user's browser or device into binding to a malicious DNS server and then make[s] the device access unintended domains." For example, let's say you want to access your companies online email portal. If your device has been compromised, your browser can be tricked into accessing a different site via DNS that looks like what you are expecting, but in fact has been set up by an attacker to get your credentials. If that sounds familiar, it should, because this type of attack has been around for a long time. For most enterprises, stopping it is relatively straightforward through some DNS filtering at the firewall level, preventing certain kinds of scripts from running in the browser, and a handful of other methods.

   But as with other IoT challenges, much of the problem lies with the ever-proliferating devices outside more mature enterprises. Home and small businesses are less able to protect against this attack and the sheer number of devices means that even if 90% are patched or otherwise mitigated (they aren't), that is still millions of devices that could

[4] https://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html

[5] https://www.bleepingcomputer.com/news/security/hackers-stole-a-third-of-singapores-healthcare-data-including-prime-ministers/

[6] https://www.bleepingcomputer.com/news/security/half-a-billion-iot-devices-vulnerable-to-dns-rebinding-attacks/

be used in DDoS attacks (like the Mirai botnet[7]), collecting information, or negatively impacting critical infrastructure.

This won't be last time we talk about IoT.

Congress –

Tuesday, July 24:
--Hearing entitled, "Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System" (House Committee on Oversight and Government Reform).[8]
--Joint Hearing entitled, "Shielding Sources: Safeguarding the Public's Right to Know" (House Subcommittees on Healthcare, Benefits, and Administrative Rules & Intergovernmental Affairs).[9]

Wednesday, July 25:
--Hearing to examine the race to 5G, focusing on exploring spectrum needs to maintain United States global leadership (Senate Committee on Commerce, Science, and Transportation).[10]
--Hearing entitled, "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response"). [11]

Thursday, July 26:
--No relevant hearings

Conferences, Webinars, and Summits –

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--NH-ISAC & Boston Scientific Medical Device Security Workshop – Maple Grove, MN (7/24) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-maplegrove-mn/>
--NH-ISAC Blended Threats Exercise Series – MN (7/25) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--CSS-Healthcare System Management of Medical Devices – TBD (7/26) <https://nhisac.org/events/nhisac-events/css-2/>
--Basic Best Practices in Cybersecurity – Abilene, TX (7/31) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas-2/>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>

[7] https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
[8] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108594
[9] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108595
[10] https://www.senate.gov/committees/hearings_meetings.htm
[11] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=107999

--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 Demployment 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 –

--**Vaccine Available for GrandCrab Ransomware v4.1.2**
<https://www.bleepingcomputer.com/news/security/vaccine-available-for-gandcrab-ransomware-v412/>
-- **PayPal's Venmo App Exposes Most Transactions via Its API**

<https://www.bleepingcomputer.com/news/security/paypals-venmo-app-exposes-most-transactions-via-its-api/>
--**EU Fines Google $5 Billion for Breaching Antitrust Rules in Android**
<https://www.bleepingcomputer.com/news/google/eu-fines-google-5-billion-for-breaching-antitrust-rules-in-android/>
--**Voting machine vendor says it installed remote software connections in a 'small number' of systems**
<https://www.cyberscoop.com/es-s-voting-machine-remote-access-ron-wyden/>
--**Former U.S. officials call for transparency in cybersecurity of 2020 Census**
<https://www.cyberscoop.com/former-officials-open-letter-census-cybersecurity/>
--**McCaul: U.S. should go on the cyber offensive if Russia hacks midterms**
<https://www.cyberscoop.com/mccaul-u-s-go-cyber-offensive-russia-hacks-midterms/>
--**10 Ways to Protect Protocols That Aren't DNS**
<https://www.darkreading.com/operations/10-ways-to-protect-protocols-that-arent-dns/d/d-id/1332298>
--**What We Talk About When We Talk About Risk**
<https://www.darkreading.com/attacks-breaches/what-we-talk-about-when-we-talk-about-risk/a/d-id/1332192>
--**Microsoft Identity Bounty Program Pays $500 to $100,000 for Bugs**
<https://www.darkreading.com/endpoint/microsoft-identity-bounty-program-pays-$500-to-$100000-for-bugs/d/d-id/1332325>
--**The Space Force Should Improve the Cybersecurity of Space Assets**
<https://www.lawfareblog.com/space-force-should-improve-cybersecurity-space-assets>

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