March 3rd, 2020

TLP White

In this edition of Hacking Healthcare, we begin by exploring the German Patient Data Protection Act that is under criticism for its approach to cybersecurity and privacy. Next, we briefly examine the interesting effect the United States' naming and shaming of Chinese state hackers is having. Finally, we break down why DNS over HTTPS might come with considerable tradeoffs.

Welcome back to *Hacking Healthcare*.

1. **German Patient Data Protection Act Draft Under Review.** Germany appears to be on its way towards realizing the benefits that can come with adopting greater digitization of health data. Federal Health Minister Jens Spahn made a draft of the German Patient Data Act available toward the end of last month, and the bill is now under review by the government.[1] If passed without major revisions, the bill would create numerous opportunities for German patients to easily access and use their patient data electronically while allegedly adding protections to prevent its misuse.

   The current draft for the German Data Protection Act sets out how electronic patient records will be regulated and accessible to German patients. While still open to revisions, the current draft allows for "the possibility of data donation without personal reference for scientific research, the regulation of electronic patient record access rights for physicians under patient sovereignty, the right of insured persons to have their treatment data made available, and also their one-time instruction in EPR use."[2]

   However, not everyone is happy with the current iteration of the bill. The Association of Independent Doctors criticized the level of security outlined in the bill and stated that it would lead to sensitive patient data being "stored centrally at IT companies via insecure mobile phone apps."[3] Further concern comes from the Association of Research-based Pharmaceutical Companies. The association believes that the bill would significantly hamper industrial research by unnecessarily limiting access to health data.

2. **The Results of Naming and Shaming Chinese Hackers.** China's use of its sophisticated cyber capabilities to steal valuable commercial IP and gather useful political and military intelligence is well known. The United States' public naming and shaming of Chinese hackers that are linked to cyberattacks or intrusions through federal indictments has had an interesting effect on their operations.

Speaking during the RSA conference, co-founder of CrowdStrike Dmitri Alperovitch stated that specific groups named in these public pronouncements seem to disappear after being outed.[4] This isn't to say that those groups no longer exist or that the individuals behind them have stopped cyber operations. Alperovitch suggested that the personnel associated with these groups could have been reassigned to groups that have not yet been publicly identified as their operations under their original groups appear to have ceased.[5] He continued that this type of behavior is at odds with Russian and Iranian actors who tend to continue their operations regardless of public scrutiny.[6]

It is impossible to know for certain why China appears to make these tactical adjustments. It could be that the move is useful in adding an additional layer of deniability and obfuscation, but Alperovitch noted that it may partially coincide with a restructuring of Chinese cyber operations.[7] He noted that the People's Liberation Army significantly drew down its operations in the wake of the agreement President Obama and Xi Jingping struck with regards to commercial IP hacking, and the Chinese Ministry of State Security ended up becoming much more active in the aftermath.[8]

3. **DNS over HTTPS is a Double-edged Sword.** Prominent web browser company Mozilla announced last week it will begin to migrate US users of their web browser Firefox over to Cloudflare's encrypted DNS service. The change will make DNS over HTTPS (DoH) the default setting for Firefox users barring the discovery of any major issues during the rollout. The move is intended to make browsing more secure by keeping 3rd parties from seeing what DNS lookups the browser is performing, and it comes at least partially in response to concerns over internet service provider (ISP) monitoring.

   Interest in DoH rose significantly in the wake of increased awareness of ISP's selling customer data to third parties, and Mozilla has been among the more aggressive in making the change despite pushback from ISPs. However, the ISPs are not the only ones pushing back on DoH implementation. Many cybersecurity experts feel DoH is potentially more harmful than helpful outside specific circumstances and that the benefits of DoH adoption have been greatly exaggerated.

   Among the criticisms levied at DoH are that it doesn't actually prevent ISPs from tracking you if they really want to. There are numerous other types of data that are not encrypted by DoH from which an ISP can infer what a user is doing.[9] DoH also centralizes DNS traffic into a few DoH resolvers, which essentially gives them all the information that previously would have just been seen by the ISP.

   As significant as those criticisms are, the biggest is that DoH has the potential to drastically reduce the effectiveness of a plethora of cybersecurity tools by blinding them to what users are doing. Notable voices including the SANS Institute and the Netherlands National Cyber Security Centrum have already been sounding the alarm on how DoH will negatively impact monitoring solutions.[10] These fears are warranted, as malware has already been discovered using DoH to mask its actions and go undetected by traditional cybersecurity tools.[11]

March 3rd, 2020

Congress –

Tuesday, March 3rd:

- Senate - Committee on Health, Education, Labor, and Pensions - Hearings to examine an emerging disease threat, focusing on how the United States is responding to COVID-19, the Novel Coronavirus.

Wednesday, March 4th:

- Senate – Committee on Commerce, Science, and Transportation - Hearings to examine 5G supply chain security, focusing on threats and solutions.

- House - Committee on Homeland Security - Confronting the Coronavirus: Perspectives on the Response to a Pandemic Threat

- House - Committee on Appropriations - National Institutes of Health Budget Request for FY 2021

Thursday, March 5th:

- Senate – Committee on Homeland Security and Governmental Affairs - Hearings to examine the Federal interagency response to the Coronavirus and preparing for future global pandemics.

International Hearings/Meetings –

EU – No relevant hearings/meetings

Conferences, Webinars, and Summits –

--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Member Meet-Up at HIMSS Global Conference – Location TBA (3/11/2020)
https://h-isac.org/hisacevents/h-isac-member-meet-up-at-himss/
-- Smart IoT – London – ExCeL London, UK (3/11/2020)
https://www.smartiotlondon.com/
--H-ISAC Monthly Member Threat Briefing – Webinar (3/31/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-6/
--H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/
--H-ISAC Security Workshop - Atlanta, GA (4/13/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-atlanta/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (4/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--H-ISAC 2020 Spring Summit – Tampa, FL (5/11/2020-5/15/2020)
https://h-isac.org/summits/apac-summit-2020/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--2020 APAC Summit – Singapore (6/23/2020-6/25/2020)
https://h-isac.org/summits/apac-summit-2020/

--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--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
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/

Sundries –

--Healthcare should approach consumer-generated data cautiously, expert says
https://www.healthcareitnews.com/news/healthcare-should-approach-consumer-generated-data-cautiously-expert-says
--Coronavirus: Fake news is spreading fast
https://www.bbc.com/news/technology-51646309
--Google's acquisition of Fitbit could pose 'high level of risk to privacy and data protection'
https://www.healthcareitnews.com/news/europe/google-s-acquisition-fitbit-could-pose-high-level-risk-privacy-and-data-protection
--Clearview AI: Face-collecting company database hacked
https://www.bbc.com/news/technology-51658111

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

[1] https://www.healthcareitnews.com/news/europe/german-health-minister-jens-spahn-presents-draft-law-patient-data-protection
[2] https://www.healthcareitnews.com/news/europe/german-health-minister-jens-spahn-presents-draft-law-patient-data-protection
[3] https://www.healthcareitnews.com/news/europe/german-health-minister-jens-spahn-presents-draft-law-patient-data-protection
[4] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/
[5] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/
[6] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/
[7] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/
[8] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/
[9] https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/
[10] https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/
[11] https://www.zdnet.com/article/first-ever-malware-strain-spotted-abusing-new-doh-dns-over-https-protocol/