May 15, 2018

TLP White

We start with a Governor's veto of a bill that would have criminalized unauthorized computer access and permitted companies to engage in hack-back activity. We then highlight a recently issued NIST request for input on improving the cybersecurity of healthcare imaging systems and discuss a new report that claims the DHS plans to take on new initiatives to curb systemic cyber risk and supply chain threats. We also address a new zero-day vulnerability discovered in Microsoft Office 365 and conclude with a discussion about the effect a US government's ban on vendors would have on businesses. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***A Governor's Veto.*** Georgia's Governor Nathan Deal (R) recently vetoed a bill that would have criminalized "unauthorized computer access" and permitted companies to engage in hack-back activity ("hack-back" refers to the idea that an entity, after being hacked, will return a hack of its own against the initial actor). [1] The veto is believed to have been a response to concerns throughout the security community. In issuing the veto, Governor Deal said, "[W]hile intended to protect against online breaches and hacks, [the bill] may inadvertently hinder the ability of government and private industries to do so…[and] [a]fter careful review…I have concluded more discussion is required before enacting this cyber security legislation."

   Specifically, there was concern that the bill's "unauthorized computer access" language – which stated, "any person who accesses a computer or computer network with knowledge that such access is without authority shall be guilty of…[a] crime"[2] – would have penalized white hat hackers and security researches. For example, had the bill been in effect, a researcher could have received jail time and a hefty fine, despite the FBI determining the researcher had done nothing wrong, after discovering and reporting an election systems' flaw that left 6.7 million Georgia voters vulnerable.

   There was also concern surrounding the bill's hack-back provision, which permitted "cybersecurity active defense measures… designed to prevent or detect unauthorized

[1] https://arstechnica.com/tech-policy/2018/05/georgia-governor-vetoes-cyber-bill-that-would-criminalize-unauthorized-access/
[2] https://www.documentcloud.org/documents/4345203-SB-315.html

computer access." For example, companies like Microsoft and Google feared that the provision would cause more harm than good and issued a letter to the Governor, noting the lack of any statutory criteria for the provision and stating that the bill "could easily lead to abuse and be deployed for anticompetitive, not protective purposes."

2. ***NIST's Request for Improving Imaging System Cybersecurity.*** Through its National Cybersecurity Center of Excellence (NCCoE), NIST has issued a request soliciting input from the public on ways to improve the cybersecurity of healthcare imaging systems such as MRIs, X-rays, and CT scanners.[3] Specifically, the request calls on "organizations to provide products and technical expertise to support and demonstrate security platforms for the Securing Picture Archiving and Communication System (PACS) Cybersecurity for the healthcare sector." NIST notes that the goal of the request is to provide the public guidance, reference points, and concrete examples on ways to secure PACS. The request is particularly ripe given Symantec's report from a few weeks ago addressing malware targeting machines like MRIs and X-Rays.[4]

   For those members interested in participating, NIST requires that the responding organization issue a letter of interest to NIST that includes, among other things, (1) which security platforms or components the organization is offering – e.g., PAC Servers, data storage, radiology information systems, data encryption, or web services – and (2) how the organization's products address specific security characteristics from NIST's Cybersecurity Framework – e.g., Identify, Protect, Detect, Respond, and Recover. However, NIST notes that responding organizations should not include proprietary information in their letter of interests.

   Given the rise of the IoT in healthcare and the constant flow of electronic health information throughout the healthcare industry, it is important that machines like MRIs, X-Rays, CT Scanners, and other healthcare imagining systems remain secure from cybersecurity threats. For those not familiar, the NCCoE is a special arm of NIST that focuses on practical solutions to difficult security challenges across multiple industries. They focus heavily on collaboration to ensure that the best ideas are captured and presented.

3. ***DHS's New Plans?*** According to documents obtained by Politico, the Department of Homeland Security ("DHS") has two new initiatives regarding systemic cyber risk and supply-chain threats.[5] Although the DHS has not publicly released the plans yet, Politico's report falls in line with previous comments made by Secretary Nielsen. For example, at RSA she noted, "[DHS] recently launched a voluntary initiative to identify

[3] https://www.federalregister.gov/documents/2018/05/09/2018-09897/national-cybersecurity-center-of-excellence-nccoe-securing-picture-archiving-and-communication

[4] http://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine

[5] https://www.politico.com/newsletters/morning-cybersecurity/2018/05/07/dhs-tackles-systemic-cyber-risk-supply-chain-threats-205953

and mitigate systemic risk in supply chains…[which] includes identifying companies in the supply chain whose risks might go unnoticed…[and] [w]e ask you to work with us to identify systemic risks, to flag emerging ones, and to work with us to fix them."[6]

If Politico's Report is true, then the initiatives will surely impact the healthcare industry given the vast overlap between the healthcare industry and the other industries the Secretary is currently soliciting feedback from. We'll keep you posted on this, folks, and will review the plans when they are released.

4. ***Office 365 Zero Day***: Last week researchers discovered a zero-day vulnerability, formally known as baseStriker that allows attackers to send malicious emails which can bypass security systems on Office 365 accounts. A blog post by Avanan, the company responsible for discovering the attack, suggests that baseStriker may be the largest security flaw in Office 365 since the service was created.

   Avanan reported that there is no fix for the problem, and recommends that users implement two-factor authentication to help resist attempts at credential harvesting by malicious actors. Microsoft had this to say on the matter: "Microsoft has a customer commitment to investigate reported security issues and provide resolution as soon as possible. We encourage customers to practice safe computing habits by avoiding opening links in emails from senders they don't recognize."

5. ***Trust Issues - The Government's Vendor Bans:*** At the end of 2017, President Donald Trump signed legislation banning the use of Kaspersky anti-virus products within the U.S. government.[7] Senator Jeanne Shaheen (D-NH) led the charge, making the case that the Moscow-based antivirus firm was a "grave risk" to national security. In a similar act of distrust, Congressman Mike Conaway (R-TX) introduced a bill in January prohibiting federal agencies from contracting with entities that uses any system from Huawei Technologies, ZTE Corporation, or an entity reasonably believed to be owned or controlled by China.[8] In advocating for the bill, Congressman Conaway stated that "[a]llowing Huawei, ZTE, and other related entities access to U.S. government communications would be inviting Chinese surveillance into all aspects of our lives."[9]

   Beyond the air of distrust and the national security concerns with respect to Russia and China, these bans are ultimately the symptom of a larger, very complex supply chain problem. A top DHS cybersecurity official recently went as far as to describe supply chain vulnerabilities as a "digital public health crisis."[10] While the federal government has several initiatives moving simultaneously to address these issues (such as DHS's plan

[6] https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference
[7] https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4
[8] https://www.congress.gov/bill/115th-congress/house-bill/4747
[9] https://conaway.house.gov/news/documentsingle.aspx?DocumentID=398326
[10] https://www.cyberscoop.com/jeanette-manfra-sf-cybertalks-supply-chain/

to address systemic cyber risk and supply-chain threats as mentioned above as well as NIST's recent update to the Cybersecurity Framework to address supply chain threats) the reality is that the government is struggling to keep up with a quickly evolving, global threat landscape that impacts all types of entities and industry sectors, including healthcare.

Congress –

Tuesday, May 15:
--No relevant hearings

Wednesday, May 16:
--Hearing to examine trends in mobile technologies (Senate Subcommittee on Communications, Technology, Innovation, and the Internet)[11]
--Hearing to examine Cambridge Analytica and the future of data privacy (Senate Judiciary Committee)[12]
--Hearing to examine telecommunications, global competitiveness, and National Security (House Subcommittee on Communications and Technology)[13]

Thursday, May 17:
--Hearing to examine proposed budget estimates and justification for fiscal year 2019 for the National Institutes of Health (Senate Subcommittee on Department of Labor, Health and Human Services, and Education, and Related Agencies) [14]
--Hearing titled, "Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe" (House Committee on Education and Workforce)[15]

Conferences and Webinars –

<https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--Medical Device and Pharmaceutical Security Workshop – London
<https://nhisac.org/events/nhisac-events/security-workshops-london/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17)
<http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>

[11] https://www.senate.gov/committees/committee_hearings.htm
[12] https://www.senate.gov/committees/committee_hearings.htm
[13] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108301
[14] https://www.senate.gov/committees/committee_hearings.htm
[15] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108295

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21)
<https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--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/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Hackers find "official," usable PSP emulator hidden in PS4's PaRappa**
<https://arstechnica.com/gaming/2018/05/hackers-find-official-usable-psp-emulator-hidden-in-ps4s-parappa/>
--**Google and The Rise of 'Digital Well-being'**
<https://www.wired.com/story/google-and-the-rise-of-digital-wellbeing>
-- Multiple OS Vendors Release Security Patches After Misinterpreting Intel Docs
< https://www.bleepingcomputer.com/news/security/multiple-os-vendors-release-security-patches-after-misinterpreting-intel-docs/>
--**AI Isn't a Crystal Ball, But It Might Be a Mirror**
<https://www.wired.com/story/ideas-ai-as-mirror-not-crystal-ball>
-- **Think You've Got Your Credit Freezes Covered? Think Again.**
<https://krebsonsecurity.com/2018/05/another-credit-freeze-target-nctue-com/>
-- **Microsoft Patch Tuesday, May 2018 Edition**
<https://krebsonsecurity.com/2018/05/microsoft-patch-tuesday-may-2018-edition/>
-- **Microsoft Adding "Search with Bing" Feature to Notepad in Windows 10**
<https://www.bleepingcomputer.com/news/microsoft/microsoft-adding-search-with-bing-feature-to-notepad-in-windows-10/>
-- **Firefox 60 Released With Support for an Enterprise-Friendly Policy Engine**
<https://www.bleepingcomputer.com/news/software/firefox-60-released-with-support-for-an-enterprise-friendly-policy-engine/>
-- **Script Kiddies, Criminals Hacking Video Streams for Fun & Profit**
<https://www.darkreading.com/endpoint/privacy/script-kiddies-criminals-hacking-video-streams-for-fun-and-profit/d/d-id/1331770>

May 15, 2018

-- **Email Security Tools Try to Keep Up with Threats**
< https://www.darkreading.com/endpoint/email-security-tools-try-to-keep-up-with-threats/d/d-id/1331769>

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