January 14th, 2020

Hacking Healthcare

TLP White

In this edition of Hacking Healthcare, we begin with a reminder that increased digitization in healthcare brings many benefits, but also requires contingency planning. Next, we briefly outline the Trump Administration's guidance on Artificial Intelligence ("AI") regulation. Finally, we breakdown an International Criminal Police Organization ("INTERPOL") operation that they claim has led to a 78% drop in cryptojacking in the Association of Southeast Asian Nations ("ASEAN") region. Welcome back to *Hacking Healthcare*.

1. **Australian Wildfires Illustrate the Perils of Digital Economy.** As the wildfires continue to rage across large portions of Australia, one of the lesser highlighted issues has been the impact on contactless payments. As reported in the Washington Post earlier this month, "With even landlines down, and banks closed and ATMs empty, the cashless economy in some areas seized up."[1] While a disaster on the scale of the current wildfire outbreak in Australia is not a common occurrence, the impact it has had on the cashless economy was not unforeseeable. This ongoing disaster, and its impact on payment technologies, should serve as a reminder to the healthcare sector at large that contingency planning is a necessity and not a luxury.

   The growing popularity of cashless payment options and the seemingly inexorable march towards a truly digital global economy, are not trends that can be significantly influenced by the healthcare sector alone. In light of this, it is imperative that healthcare organizations understand the inherent weaknesses in such systems and spend time developing viable mitigations in the case of disasters, criminal acts, or other emergencies.

   This type of contingency planning is obviously not limited to payments. The healthcare sector is becoming more and more digitized and connected for convenience and enhanced patient care. Serious consideration must be given to how healthcare organizations can continue to provide essential services despite a sudden inaccessibility of health data, communications, and other technological dependencies. As our reliance on technology increases, we must adequately assess and implement back-up plans that can keep essential services operational regardless of environmental circumstances.

2. **White House Provides Guidance on AI Regulations.** Last week, The White House released a draft memorandum outlining the Trump Administration's policy considerations "that should guide, to the extent permitted by law, regulatory and non-regulatory oversight of AI applications developed and deployed outside of the Federal government."[2] The guidance leans towards a lighter regulatory touch, asking regulators to not "Needlessly hamper AI innovation and growth."[3] The draft memorandum further outlined 10 "principles for the stewardship of AI applications."[4]

   A quick summary of the ten principles can be found below:

   1) Public Trust in AI – Ensuring that AI applications are carefully assessed for their impacts to privacy, individual rights, autonomy, and civil liberties in order to maintain public trust.

   2) Public Participation – The public should be involved in the rulemaking process, and agencies should be transparent in their actions.

   3) Scientific Integrity and Information Quality – Ensuring that the data used is held to a high standard, and further that AI application best practices should include transparency in articulating the strengths, weaknesses, intended optimizations or outcomes, bias mitigation, and appropriate uses of the AI application's results.

   4) Risk Assessment and Management – "Regulatory and non-regulatory approaches to AI should be based on a consistent application of risk assessment and risk management across various agencies and various technologies."[5]

   5) Benefits and Costs – When formulating regulatory and non-regulatory approaches to AI, Agencies should consider the "full societal costs, benefits, and distributional effects before considering regulations related to the development and deployment of AI applications."[6]

   6) Flexibility – Regulatory and non-regulatory approaches should be flexible and able to respond to the rapid changes and evolution of technology.

   7) Fairness and Non-Discrimination – Agencies should consider the impact of AI applications on fairness and discrimination.

   8) Disclosure and Transparency – "Agencies should carefully consider the sufficiency of existing or evolving legal, policy, and regulatory environments before contemplating additional measures for disclosure and transparency."

   9) Safety and Security – "Agencies should promote the development of AI systems that are safe, secure, and operate as intended, and encourage the consideration of safety and security issues throughout the AI design, development, deployment, and operation process." This includes special attention to ensuring confidentiality, integrity, and availability. Additionally, it should promote the consideration to a system's resiliency and cybersecurity.

10) Interagency Coordination – The government, as a whole, should have a coherent approach that promotes coordination between agencies.

The draft memorandum further illustrates that that agencies should look to non-regulatory approaches such as creating sector-specific policy guidance or frameworks, pilot programs and experiments, and voluntary consensus standards. The Trump Administration's approach will likely further incentivize organizations to push forward AI enabled/integrated projects across all sectors, including healthcare.

3. **INTERPOL Action Reduces ASEAN Cryptojacking.** An INTERPOL coordinated operation involving 10 ASEAN states has reportedly struck a significant blow to malicious actors engaging in cryptojacking. The operation, dubbed "Goldfish Alpha", began in June of last year and identified over 20,000 hacked routers in the ASEAN region.[7] By working with national police, CERTs ("Computer Emergency Response Team"), and private sector organizations, INTERPOL was able to help coordinate widescale notifications and patching that reportedly led to a 78% drop in cryptojacking in the ASEAN region.[8]

   Cryptojacking is the infection of a victim's device by a malicious actor wanting to use its computing power to mine for cryptocurrency. This particular category of malware can be easy to miss, as it often runs quietly in the background without necessarily impacting a device's performance in a significantly noticeable way.[9] Cryptojacking remains a significant and profitable threat that doesn't require significant technical skill to operate.

Congress –

Tuesday, January 14th:
- No relevant hearings

Wednesday, January 15th:
- Hearing: "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy" – House Committee on Oversight and Reform

Thursday, January 16th:
- No relevant hearing

International Hearings/Meetings –

EU –

-No relevant hearings

January 14th, 2020

Conferences, Webinars, and Summits –

--A sign of the times: Automated communications fraud and what you can do to stop it by Valimail
https://h-isac.org/hisacevents/a-sign-of-the-times-by-valimail/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
--Healthcare Cybersecurity Forum - Southern California – San Diego, CA (2/5/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/Southern_California
--Global Cyber Security in Healthcare & Pharma Summit - London, UK (2/6/2020)
http://www.global-engage.com/event/cybsec-health-summit/
--H-ISAC Analysts Security Workshop - Titusville, FL (3/4/2020)
https://h-isac.org/hisacevents/h-isac-analysts-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Chennai, India (3/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-india/
--2020 APAC Summit – Singapore (3/31/2020-4/2/2020)
https://h-isac.org/summits/apac-summit-2020/
--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 (4/14/2020)
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 Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--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
--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 –

--TrickBot developers have spun up a new backdoor for high-value targets
https://www.cyberscoop.com/trickbot-backdoor-banking-trojan-financial/
--Lawmakers Prod FCC to Act on SIM Swapping
https://krebsonsecurity.com/2020/01/senators-prod-fcc-to-act-on-sim-swapping/
--SNAKE Ransomware Is the Next Threat Targeting Business Networks
https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/
--DHS tells U.S. organizations to clamp down on cybersecurity in wake of Soleimani killing
https://www.cyberscoop.com/dhs-iran-advisory-cybersecurity-soleimani/

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

[1] https://www.washingtonpost.com/world/asia_pacific/thousands-flee-australias-coastal-towns-as-raging-wildfires-close-in/2020/01/02/c33d2250-2d0a-11ea-bffe-020c88b3f120_story.html

[2] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[3] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[4] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[5] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[6] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[7] https://www.bleepingcomputer.com/news/security/cryptojacking-drops-by-78-percent-in-southeast-asia-after-interpol-action/

[8] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia

[9] https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html