January 7th, 2020

TLP White

In this edition of Hacking Healthcare, we begin the new year with a brief explanation of the increased nation state threat stemming from the killing of Iranian Gen. Soleimani. We then briefly review Mastercard's most recent cybersecurity acquisition and what it might mean for them and their franchisees. Finally, we delve into Russia's announcement that they have successfully tested their own "internal internet". Hope you had a great holiday, and welcome back to *Hacking Healthcare*.

Targeted Killing of Iranian General Increases Nation State Threat Risk. The killing of Iranian Gen. Soleimani, and the subsequent outpouring of promises by both Iranian government and non-government sources to retaliate against the United States, has many experts saying that the likelihood of offensive cyber operations targeting U.S. organizations has increased. Christopher Krebs, head of the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), has since re-iterated CISA's guidance on Iran from this past summer by tweeting "Bottom line: time to brush up on Iranian TTPs and pay close attention to your critical systems, particularly ICS."[1]

While significant attention has been given to the possible targets of a more traditional kinetic attack, Iran will almost certainly consider making use of its cyber capabilities as part of its response. This is especially true if it wishes to directly impact the United States while attempting to avoid direct attribution and not look like an aggressor. Iran has showcased significant offensive cyber capabilities in the recent past, with numerous intrusions and attacks in the Middle East and the United States being attributed to one of several Iranian linked Advanced Persistent Threat ("APT") groups.[2, 3]

Healthcare and Public Health ("HPH") sector organizations should recognize the increased risk associated with the heightened tensions between the United States and Iran and assess the necessity of any changes to their cybersecurity posture. At a minimum, make sure you are paying close attention to threat intelligence via the H-ISAC and other sources.

Mastercard Looks to Purchase Supply Chain Monitoring Organization. Last week, Mastercard announced that it had agreed to acquire supply chain monitoring company RiskRecon.[4] This would be yet another cybersecurity acquisition that Mastercard has made in 2019, and it draws

further attention to the seriousness that organizations are paying to supply chain risk management.

Mastercard is being tight lipped about its long-term plans for the company, but with the growth of awareness around supply chain attacks and the proliferation of Magecart malware, such an investment would seem prudent. Mastercard's official press release also states that RiskRecon will "continue to provide cyber security solutions across a broader set of industries, including healthcare and manufacturing."[5]

Russia Claims Internal Internet Success. As we outlined previously, Russia began taking steps months ago to implement the technical infrastructure necessary to effectively disconnect the country from the global internet and operate an insulated Russian alternative. While there have been doubts as to the feasibility of the endeavor, the Russian government announced a successful trial of the technology on December 24th.[6] There are reportedly few details as to the exact parameters of the test, but the Ministry of Communications declared that users did not notice the change and results are being delivered to President Putin for review.[7]

The technical aspects of the project include the cooperation of domestic ISPs and regulation of global internet access points into Russia. The cooperation of these firms has been made easier by the fact that many are state-owned or heavily state-linked. Professor Alan Woodward of the University of Surrey explained that Russia is attempting to create a giant intranet, which is akin to creating a larger version of what a large corporation or business entity does.[8]

Congress –

Tuesday, January 7th:
- No relevant hearings

Wednesday, January 8th:
- No relevant hearings

Thursday, January 9th:
- No relevant hearings

International Hearings/Meetings –

EU –

-No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Navigator Webinar from Valimail – A Sign of the Times: Automated communications fraud and what you can do to stop it (1/22/2020 at Noon ET)
--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 –

--Not so IDLE hands: FBI program offers companies data protection via deception
https://arstechnica.com/information-technology/2019/12/not-so-idle-hands-fbi-program-offers-companies-data-protection-via-deception/
Coast Guard says Ryuk ransomware hit systems that monitor cargo transfers at maritime facility
https://www.cyberscoop.com/ryuk-coast-guard-ransomware/
--The Apple Watch Is Smart, but It Can't Replace Your Doctor
https://www.nytimes.com/2019/12/26/upshot/apple-watch-atrial-fibrillation.html
--Hackers steal data for 15 million patients, then sell it back to lab that lost it
https://arstechnica.com/information-technology/2019/12/clinical-lab-pays-hackers-for-the-return-of-data-of-15-million-patients/
--'Serious cyber-attack' on Austria's foreign ministry
https://www.bbc.com/news/world-europe-50997773

January 7th, 2020

[1] https://twitter.com/CISAKrebs/status/1212959127003111424
[2] https://www.wired.com/story/iran-apt33-industrial-control-systems/
[3] https://arstechnica.com/information-technology/2020/01/pick-your-poison-the-potential-iranian-responses-to-us-drone-strike/
[4] https://newsroom.mastercard.com/press-releases/mastercard-acquires-riskrecon-to-enhance-cybersecurity-capabilities/
[5] https://newsroom.mastercard.com/press-releases/mastercard-acquires-riskrecon-to-enhance-cybersecurity-capabilities/
[6] https://www.bbc.com/news/technology-50902496
[7] https://www.bbc.com/news/technology-50902496
[8] https://www.bbc.com/news/technology-50902496