June 24th, 2020

Hacking Healthcare

TLP White

This week, Hacking Healthcare revisits digital contact-tracing to keep you updated on the latest developments around the world. Additionally, we briefly remind you about the ingenuity of malicious actors by recounting how LinkedIn was weaponized to compromise European aerospace and defense firms. Lastly, we recap the alarming release of a redacted report on the Central Intelligence Agency's (CIA) deeply regrettable cybersecurity practices.   Welcome back to *Hacking Healthcare*.

1. **Digital Contact-tracing Update.** From our "We're Still Watching" department, we bring you the latest in contact-tracing efforts around the world.

    Ireland: On Monday of this week, Ireland's health authority announced that its contact-tracing strategy was set to go forward pending final governmental approval.[1] Based on Apple and Google's framework, Ireland's contact-tracing application has critics concerned about the app's accuracy. Some of their concern stems from research conducted by scientists at Trinity College, who have called into question how reliable the app will be at identifying individuals in proximity in everyday environments.[2] Follow-on research is being conducted by Science Foundation Ireland to provide an independent assessment of the app's shortfalls.[3]

    United States: The varied patchwork of U.S.-based digital contact-tracing applications continues. Unfortunately, American attitudes toward contact-tracing applications have fallen sharply according to an Avira study conducted by polling company Opinion Matters. A resounding 71% of respondents to their online survey said they would not download a contact-tracing application.[4] Worryingly, the age group most likely to resist using a contact-tracing app is the 55 and older demographic, a group that is most at risk. Among all respondents who said they would not use a contact-tracing app, privacy and "creating a false sense of security" were the top two concerns.[5]

    Additionally, there are those who believe that a focus on digital contact-tracing is an impediment to more practical uses of time and money. Dr. Karen Smith, former director of the California Department of Public Health has called into question whether funds spent on digitizing contact-tracing efforts would be better spent if they were sent to underfunded local health departments who lack data entry systems.[6]

Kuwait, Bahrain, and…Norway? These three countries may not appear to have much in common, but Amnesty international's Security Lab reports that "Bahrain's 'BeAware Bahrain', Kuwait's 'Shlonik' and Norway's 'Smittestopp' apps stood out as among the most alarming mass surveillance tools assessed by Amnesty."[7] The Security Lab's research elaborated that "all three actively [carry] out live or near-live tracking of users' locations by frequently uploading GPS coordinates to a central server."[8] Just prior to the release of the Amnesty report, Norway promised to reassess its strategy.

France: France will be a country to monitor when it comes to contact-tracing effectiveness. Their centralized program, which does not make use of the Apple and Google framework, has seen nearly two million downloads thus far. Recent reporting suggests that despite that fairly large number, only 14 notifications of "an at-risk encounter" have been sent, and only 68 individuals have self-reported a positive COVID-19 result.[9] While France has drastically reduced the amount of new COVID-19 cases per-day, the low notifications may call into question either the efficacy of the technology, or the usefulness at such a low adoption rate. Furthermore, French officials have also publicly stated that they regret their own state designed approach is incompatible with the Apple and Google based approaches found throughout much of Europe.

The Private Sector: State governments are not alone in the race to develop and deploy digital contact-tracing solutions. According to Wired, there has been a rapid growth in demand for contact-tracing apps and wearables by private sector organizations.[10] While governments try to develop largely voluntary applications that can work on a multitude of devices for the broadest coverage possible, private sector initiatives are moving forward that promise increased accuracy due to uniform deployment and tailoring for each circumstance. There is allegedly significant interest from global construction and engineering groups, as well as from various manufacturing and industrial sectors.[11] The legality of these efforts will almost certainly be called into question sooner rather than later.

Action & Analysis
H-ISAC Membership Required

2. **LinkedIn Weaponized to Hack European Aerospace and Defense Firms.** Reports surfaced last week that over a four-month period in late 2019, at least two European aerospace and defense firms were targeted and compromised via LinkedIn by an unknown advanced persistent threat ("APT") actor with the primary intent to conduct espionage operations.[12] The attacks are notable for the usage of LinkedIn as the means to social engineer a foothold in the targeted entities' networks. Researchers from ESET

documented their findings in a 28-page report which comprehensively analyzes the attack and is freely available for review.[13]

The attacks showcased the ingenuity of malicious actors in finding an attack vector that allowed their actions a strong façade of legitimacy while also targeting what tends to be the weakest part of any organization's cybersecurity system: people. The openness of social media allowed the malicious actors to quickly ascertain individuals worth targeting, while also making it easy to pass themselves off as credible representatives of other well-known industry organizations. Furthermore, by appealing to the targeted individuals own self-interest with lucrative job offers, the malicious actors were able to get enough interest and responses to compromise at least some of their targeted organizations.

Action & Analysis
H-ISAC Membership Required

3. **CIA Security Failures Highlighted by Newly Released Wikileaks Task Force Report.** In 2016 the CIA suffered a major breach of its internal systems that resulted in "[a]t least 180 gigabytes" of information being stolen.[14] The breach culminated in an information dump on WikiLeaks that included the CIA's sophisticated hacking tools and contained enough data to allow security researchers to attribute a well-known threat group to the CIA.[15] Shortly thereafter, the CIA formed a WikiLeaks Task Force to investigate the breach. Last Tuesday, Sen. Ron Wyden (D-OR) released a partially redacted copy of that report alongside a letter to John Ratcliffe, Director of the Office of the Director of National Intelligence (ODNI), which summarized a number of intelligence community cybersecurity failings.

   The report alleges that "[t]he CIA's [Center for Cyber Intelligence (CCI)] had prioritized building cyber weapons at the expense of securing their own systems. Day-to-day security practices had become woefully lax…."[16] Furthermore, the report cited that "most of our sensitive cyber weapons were not compartmented, users shared systems administrator level passwords, there was no effective removable media controls, and historical data was available to users indefinitely."[17] Troublingly, Sen. Wyden notes that a culture of lax cybersecurity practices appears to be widespread within the intelligence community.

   Action & Analysis
   H-ISAC Membership Required

Congress –

<u>Tuesday, June 23rd</u>:
- Senate – Committee on Health, Education, Labor, and Pensions: Hearings to examine COVID-19, focusing on lessons learned to prepare for the next pandemic.

<u>Wednesday, June 24th</u>:

- Senate – Committee on Homeland Security and Governmental Affairs: Hearings to examine the role of the strategic national stockpile in pandemic response.

- House - Committee on Energy and Commerce - Subcommittee on Consumer Protection and Commerce: Joint Hearing - "A Country in Crisis: How Disinformation Online Is Dividing the Nation" (Virtual Hearing)

Thursday, June 25th:

- House - Committee on the Judiciary - Subcommittee on Courts, Intellectual Property, and the Internet: Hearing - Federal Courts During the Covid-19 Pandemic: Best Practices, Opportunities for Innovation, and Lessons for the Future

International Hearings/Meetings –

EU – No relevant hearings

Conferences, Webinars, and Summits –

--GRF Summit Digital Series - The Ultimate Incident Response Readiness Exercise: Are you remotely ready? – Webinar (6/25/2020)
https://h-isac.org/hisacevents/grf-summit-digital-series-the-ultimate-incident-response-readiness-exercise-are-you-remotely-ready/
--H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--How Authentication Attacks Threaten your Healthcare Environment by Qomplx – Webinar (7/1/2020)
https://h-isac.org/hisacevents/authentication-attacks-qomplx/
--COVID-19 and its Cybersecurity Challenge – Webinar (7/9/2020)
https://h-isac.org/hisacevents/covid-19-and-its-cybersecurity-challenge/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (7/17/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--H-ISAC Virtual Security Workshop – Virtual (7/29/2020)
https://h-isac.org/hisacevents/nz-virtual-workshop/
--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
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Forchheim, Germany
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--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

--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

Sundries –

--Intel will soon bake anti-malware defenses directly into its CPUs

https://arstechnica.com/information-technology/2020/06/intel-will-soon-bake-anti-malware-defenses-directly-into-its-cpus/

--'Vendetta' hackers are posing as Taiwan's CDC in data-theft campaign

https://www.cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/

--Health Sector Most Targeted by Hackers, Breach Costs Rise to $17.76B

https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

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

[1] https://www.bbc.com/news/technology-53137816
[2] https://www.bbc.com/news/technology-53137816
[3] https://www.irishtimes.com/news/ireland/irish-news/covid-19-state-s-contact-tracing-app-to-be-tested-for-accuracy-1.4268079
[4] https://www.avira.com/en/covid-contact-tracing-app-report
[5] https://arstechnica.com/science/2020/06/more-than-7-in-10-americans-dont-want-contact-tracing-data-shows/
[6] https://www.cnbc.com/2020/06/22/coronavirus-contact-tracing-will-save-lives-if-officials-build-it.html
[7] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
[8] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
[9] https://subscriber.politicopro.com/article/2020/06/french-contact-tracing-app-sent-just-14-notifications-after-2m-downloads-3981814?source=email
[10] https://www.wired.co.uk/article/contact-tracing-offices-coronavirus
[11] https://www.wired.co.uk/article/contact-tracing-offices-coronavirus
[12] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf
[13] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf
[14] https://www.wyden.senate.gov/imo/media/doc/wyden-cybersecurity-lapses-letter-to-dni.pdf
[15] https://arstechnica.com/information-technology/2020/06/theft-of-top-secret-cia-hacking-tools-was-result-of-woefully-lax-security/

June 24th, 2020

[16] https://www.wyden.senate.gov/imo/media/doc/wyden-cybersecurity-lapses-letter-to-dni.pdf
[17] https://www.wyden.senate.gov/imo/media/doc/wyden-cybersecurity-lapses-letter-to-dni.pdf