May 6th, 2020

TLP White

In this edition of Hacking Healthcare, we begin by examining how COVID-19 led the United Kingdom's (UK) National Health Service (NHS) to give the country's intelligence and security agency emergency powers over its networks. We then brief you on a recent letter from Congressional lawmakers and discuss its illustration of the unique challenge of implementing digital contact tracing in the United States. Finally, we take a brief look at why foreign intelligence services are targeting parts of the healthcare sector, and when it might be expected to stop. Welcome back to *Hacking Healthcare*.

1. **COVID-19's Cyber Threat Leads to More GCHQ-NHS Cooperation.** It has been well documented that, even in the midst of COVID-19, malicious cyber actors continue to target the healthcare sector. These attacks appear to be perpetrated by both state and non-state actors and have targeted everything from hospitals and research labs to national health agencies and global health organizations.[1, 2, 3] In an effort to help ensure that these cyber-attacks do not inhibit the ability of the United Kingdom's National Health Service to respond to COVID-19, Health Secretary Matt Hancock has employed emergency powers to give the Government Communications Headquarters (GCHQ) access to "information relating to the security of any network and information system held by or on behalf of the NHS or a public health body."[4]

   The GCHQ is the UK's national intelligence and security organization and is the organization that houses the UK's National Cyber Security Centre (NCSC). By allowing GCHQ to review the cybersecurity of NHS's networks and systems, NHS would likely receive feedback from the NCSC on which systems and networks may be at risk as well as how to improve cybersecurity more generally.

   The NCSC has attempted to ease any concerns individuals may have over the cooperation of an intelligence organization and the NHS by reiterating that this new power does not allow them to receive patient data, and that the NCSC has no interest in acquiring it.[5] Furthermore, the emergency power, which stems from the NHS Act of 2006, will automatically expire on December 31st unless it is amended. While this particular effort may be justifiable and appears limited in scope, some NHS-GCHQ cooperation on COVID-19 efforts have received pushback.

For example, the NCSC's involvement in the creation of the NHS's centralized contact tracing application has sparked debate. Privacy advocates are wary of their involvement, worrying that a combination of centralization and mission creep will ultimately lead to unintended and dangerous uses of the data collected.[6] However, some advocates do admit that the NCSC possess the capabilities to improve the protection of data collected during the usage of the tracing app.[7]

Analysis & Action

H-ISAC Membership Required

2. **Lawmakers Want Answers on Contact Tracing Efforts.** Lawmakers in the United States House of Representatives wrote to Health and Human Services (HHS) Secretary Alex Azar last week to better understand the Trump Administration's approach to contact tracing efforts. Specifically, they cited their concerns that a comprehensive nation-wide strategy is lacking, and that states have been left to forge ahead with digital contact tracing approaches that raise privacy, efficiency, and interoperability concerns.[8]

   The letter helps to illustrate a hurdle in the United States in rolling out a secure national digital contact tracing program. In other countries, the national government has simply opted in or out of creating a digital contact tracing program and has ultimately determined how one would be implemented. As the letter to Secretary Azar notes, in the absence of a clear federal strategy, states are beginning to take it upon themselves to investigate and develop contact tracing programs and related digital applications.[9]

   The House lawmakers highlighted that such an approach risks creating disjointed, inefficient efforts to track COVID-19 that lack interoperability and exacerbate privacy and security concerns.[10] Even if the Trump Administration does provide clear guidance and support for a nationwide contact tracing program, it may create multiple irreconcilable efforts if support comes after some states have poured resources into creating their own programs.

   Those in the European Union (EU) may be able sympathize with this issue to an extent. The EU would undoubtably prefer a single, interoperable contact tracing scheme across its many member countries, but differences in opinions over privacy, security, and technical details are driving them apart.[11] Germany, Italy, Austria and others appear keen on a effort put forward by Apple and Google that will ease privacy fears, while France, the United Kingdom, and Norway have leaned towards more centralized efforts.[12] How this plays out in the EU may give us a glimpse of what the United States is in for without a coherent national strategy.

   Analysis & Action

   H-ISAC Membership Required

3. **National Spy Agencies Seek COVID-19 Vaccine Research.** According to the director of the United States' National Counterintelligence and Security Center, foreign intelligence agencies are using their cyber capabilities to access data related to COVID-19 vaccine research.[13]

   Warnings over this type of activity, corroborated by the FBI and intelligence sources within the UK and Canada, indicate that it has been occurring since March in some cases.[14] Furthermore, healthcare organizations that proudly state they are working on a COVID-19 vaccine or treatment aren't doing themselves any favors. According to FBI Deputy Assistant Director Tonya Ugoretz, those healthcare organizations that are publicly identified as being involved in COVID-19 research appear to mark themselves for targeting.[15]

   The incentive for stealing COVID-19 research is substantial. Any data that could be used to create a COVID-19 vaccine would almost certainly provide prestige and a political boost to the government that announced it. Furthermore, while a vaccine would almost certainly be immediately shared, whichever country manages it first will likely get a leg up on its regional or global partners in economic recovery.

   Analysis & Action

   H-ISAC Membership Required

Congress –

Tuesday, May 5th:
- No relevant hearings

Wednesday, May 6th:
- No relevant hearings

Thursday, May 7th:
- No relevant hearings

International Hearings/Meetings –

EU –

Tuesday, May 12th:
-European Parliament - Environment, Public Health, and Food Safety meeting

Conferences, Webinars, and Summits –

--Cybersecurity for the 21st Century by IronNet – Webinar (5/14/2020)
https://h-isac.org/hisacevents/byironnet/
--H-ISAC Monthly Member Threat Briefing – Webinar (5/26/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-8/
--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)

May 6th, 2020

https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020) (POSTPONED)
https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/
--H-ISAC Security Workshop - Buffalo, NY (6/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/
H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--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
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--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 –

--How Cybercriminals are Weathering COVID-19
https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/
--COVID-19 Remote Work Causes Spike in Brute-Force RDP Cyberattacks
https://healthitsecurity.com/news/covid-19-remote-work-causes-spike-in-brute-force-rdp-cyberattacks

May 6th, 2020

--Citing hacking threats, Trump limits foreign-sourced equipment in U.S. electric sector
https://www.cyberscoop.com/executive-order-bulk-power-system-hacking-threats/
--How well can algorithms recognize your masked face?
https://arstechnica.com/tech-policy/2020/05/how-well-can-algorithms-recognize-your-masked-face/

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

---

[1] https://securityboulevard.com/2020/04/fbi-warns-of-major-spike-in-cyber-attacks/
[2] https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
[3] https://www.reuters.com/article/us-czech-cyber/prague-airport-says-thwarted-several-cyber-attacks-hospitals-also-targeted-idUSKBN2200GW
[4]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/879049/Security_of_NHS_and_Public_Health_Services_Digital_Systems__Coronavirus__Directions_2020.pdf
[5] https://www.hsj.co.uk/technology-and-innovation/hancock-grants-gchq-powers-over-nhs-it-systems/7027528.article
[6] https://thecyberwire.com/stories/d2c4f4e3e511425e87b4714c68e44e2e/contact-tracing-and-exposure-notification-a-look-at-the-underworld
[7] https://thecyberwire.com/stories/d2c4f4e3e511425e87b4714c68e44e2e/contact-tracing-and-exposure-notification-a-look-at-the-underworld
[8]https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/HHS.2020.4.30.pdf
[9] https://www.nga.org/wp-content/uploads/2020/04/NGA-Report.pdf
[10]https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/HHS.2020.4.30.pdf
[11] https://www.ft.com/content/10f87eb3-87f9-46ea-88ab-8706adefe72d
[12] https://www.ft.com/content/10f87eb3-87f9-46ea-88ab-8706adefe72d
[13] https://www.bbc.com/news/technology-52490432
[14] https://www.bbc.com/news/technology-52490432
[15] https://www.reuters.com/article/us-health-coronavirus-cyber/fbi-official-says-foreign-hackers-have-targeted-covid-19-research-idUSKBN21Y3GL