May 24, 2022

TLP White

This week, Hacking Healthcare begins with a reminder that the Health-ISAC is looking to hear from members interested in participating in this year's Hobby Exercise. Next, we breakdown the recent Department of Justice policy change that states they will no longer attempt to prosecute good-faith cybersecurity researchers. Finally, we wrap up with a quick breakdown of two government cyberattacks that have impacted healthcare services and discuss what warning it might serve to other smaller and less well-resourced countries.

Welcome back to *Hacking Healthcare*.

1. **Hobby Exercise 2022**

   The third iteration of the Health-ISAC Hobby Exercise is on the horizon. This tabletop exercise is an annual Healthcare and Public Health (HPH) event designed to engage the sector and strategic partners, including those in government, on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing healthcare sector resiliency. It is named for Oveta Culp Hobby, the first U.S. Secretary of Health, Education, and Welfare.

   Health-ISAC members interested in learning more or wishing to participate should email yours truly, John Banghart (jbanghart@h-isac.org).

2. **Department of Justice Signals Policy Change on Cybersecurity Research**

   Cybersecurity research in the United States often falls into a gray area of legality, where independent researchers risk severe penalties for their actions despite having good intentions. A recent policy change by the Department of Justice (DOJ) signals a positive step toward acknowledging the benefits of security researchers by stating that "good-faith security research" should no longer be charged.[1]

In a change specifically related to the DOJ's application of the Computer Fraud and Abuse Act (CFAA), the press release states that DOJ policy will, for the first time, "[direct] that good-faith security research should not be charged," as long as it is conducted:[2]

- Solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability; and
- Where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

For those not as familiar with the CFAA, it is a decades-old law that is used to address a variety of cyber-based crimes, including the unauthorized access or use of "protected computers." It is this provision that most often applies to the work of cybersecurity researchers. Since its enactment, the CFAA has undergone several congressional amendments that have expanded and revised its scope, and DOJ policy on its application has adjusted as well.

The policy change was announced on Thursday, May 19, through an official press release and an accompanying five-page policy document.[3] The release quoted Deputy Attorney General Lisa Monaco as saying, "Computer security research is a key driver of improved cybersecurity," and that while "[t]he department has never been interested in prosecuting good-faith computer security research as a crime," the change "provides clarity for good-faith security researchers who root out vulnerabilities for the common good."[4]

This approach has led some to question the potential for unintended consequences, such as bad actors extorting organizations after finding vulnerabilities to effectively receive a "free pass" as long as they claimed their actions were for research purposes. The DOJ acknowledged those concerns, but it highlighted that actions assessed to have been made in bad faith will still be covered.

The policy change is effective as of May 19 and it will require "[a]ll federal prosecutors who wish to charge cases under the [CFAA]" to "follow the new policy, and to consult with [DOJ's] Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) before bringing any charges."[5]

Action & Analysis

3. Greenland Health System Hit by Cyberattack and Costa Rica Is at "War" With Conti

The government of Greenland confirmed last week that it was the victim of a cyberattack that severely impacted the island's national health system. The incident follows in the wake of last year's significant cyberattack against Ireland's Health Service Executive (HSE). Meanwhile, the government of Costa Rica is "at war" with Conti as a cyber incident that started in April has now impacted 27 institutions. These recent events shine a spotlight on the risks that cyberattacks pose to national healthcare services of smaller, less well-resourced countries.

Greenland: According to reports, the attack began on May 9 and is the fourth such incident suffered by Greenland's government in the last six months that has targeted government services. Greenland's government officials did not elaborate on the exact nature of this particular incident but noted that IT systems and servers needed to be restarted and that the island's health services were severely limited.[6]

The impacts to the country's healthcare system included patient records being made unavailable, the healthcare system email was offline, appointments were delayed, and there were disruptions to online prescription renewal.[7, 8] As of May 20, restoration operations were still underway. While details of the attack are not yet clear, there are echoes of Ireland's HSE incident from last year. That particular ransomware event affected services across the country for weeks, and the total cost of recovery has been estimated by some to exceed $100 million.[9]

Costa Rica: Newly elected Costa Rican President Rodrigo Chaves has been on a crisis footing since assuming the presidency as a Conti ransomware attack that began under his predecessor stretches on. What appears to have begun as an incident at the Finance Ministry has since spread to 26 other government institutions and led President Chaves to declare a national emergency.[10]

The escalation and length of the attack are largely a product of Costa Rica's refusal to pay the ransom but may also be indicative of what President Chaves describes as a failure by his predecessor to take the cyber threat seriously.[11] The attack has left the country's public health agency scrambling to conduct "a perimeter security review ... to verify and prevent possible attacks."

Action & Analysis

Congress

Tuesday, May 24th:

May 24, 2022

- No relevant hearings

Wednesday, May 25th:
- No relevant hearings

Thursday, May 26th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

https://h-isac.org/events/

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

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness, and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

[2] https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

[3] https://www.justice.gov/opa/press-release/file/1507126/download

[4] https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

---

[5] https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

[6] https://therecord.media/greenland-cyberattack-healthcare-systems/

[7] https://therecord.media/greenland-cyberattack-healthcare-systems/

[8] https://www.govinfosecurity.com/cyberattack-affects-greenlands-healthcare-services-a-19120

[9] https://therecord.media/greenland-cyberattack-healthcare-systems/

[10] https://www.bbc.com/news/technology-61323402

[11] https://www.bbc.com/news/technology-61323402