June 23, 2022

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by examining new telehealth guidance from HHS that looks to address how HIPAA-covered entities can continue to provide certain telehealth services while remaining compliant with the HIPAA privacy and security requirements. Specifically, we analyze what the guidance might portend for HHS's current enforcement discretion, which alleviates covered-entity compliance, as well as what Health-ISAC members should start to think about doing in response. Next, we briefly cover news of two large-scale international operations to take down malicious botnets. We investigate how the benefits of these actions go far beyond the short-term disruptions caused and how international law enforcement capacity building in relation to cyber is on the rise. Welcome back to *Hacking Healthcare*.

1. HHS Issues New HIPAA Guidance for Telehealth

On June 13th, the U.S. Department of Health and Human Services (HHS) issued guidance on "how covered health care providers and health plans can use remote communication technologies to provide audio-only telehealth services" while remaining compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules once certain enforcement relaxations are no longer in place.[1] The guidance comes as some COVID-19-era policies implemented by HHS to ease the use of telehealth services and technologies during the pandemic are headed toward being phased out.

The guidance is specific to audio-only telehealth service and is intended to specifically address how to improve "public confidence that covered entities are protecting the privacy and security of their health information."[2] HHS's notification acknowledges that audio-only telehealth carries with it advantages for populations who "may have difficulty accessing or be unable to access technologies used for audio-video telehealth because of various factors." In particular, HHS cites financial impediments and a lack of sufficient broadband access to enable video streaming at a necessary quality.[3]

HIPAA-covered entities can use the guidance to find detailed answers to the following questions:

- Does the HIPAA Privacy Rule permit covered health care providers and health plans to use remote communication technologies to provide audio-only telehealth services?
- Do covered health care providers and health plans have to meet the requirements of the HIPAA Security Rule in order to use remote communication technologies to provide audio-only telehealth services?
- Do the HIPAA Rules permit a covered health care provider or a health plan to conduct audio-only telehealth using remote communication technologies without a business associate agreement in place with the vendor?
- Do the HIPAA Rules allow covered health care providers to use remote communication technologies to provide audio-only telehealth if an individual's health plan does not provide coverage or payment for those services?

Action & Analysis

Included with H-ISAC Membership

2. Botnet Takedowns Highlight International Law Enforcement Collaboration

The U.S. Department of Justice (DOJ) and international law enforcement partners successfully disrupted a Russian-linked botnet, according to a new DOJ press release, making it the second high-profile multinational operation this month to do so. The operations highlight the continued collaboration between Western allies in combating malicious cyber actors and reinforce the potential benefits of expanding those capabilities even further.

According to the DOJ post, U.S. authorities worked with law enforcement partners in Germany, the Netherlands, and the United Kingdom to disrupt the RSOCKS botnet, which had grown to incorporate several million hacked devices globally.[4] The post also provided insight into how complex and time-consuming these types of operations can be. The initial FBI investigation into RSOCKS began in 2016, and access to the botnet occurred back in 2017 in an attempt to better identify RSOCKS' "backend infrastructure and its victims."[5]

The DOJ's press release comes several weeks after Europol, the European Union's law enforcement agency, led an operation to disrupt FluBot.[6] That operation involved 10 countries, including "law enforcement authorities of Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands and the United States."[7] Europol reiterated that "international police cooperation was central in taking down

FluBot infrastructure as it began to spread across Europe and Australia."[8] Close collaboration meant that all of the involved actors were able to establish a coordinated strategy, exchange needed operational information, and provide digital forensic support.[9]

Unfortunately, none of the individuals behind the botnets have been apprehended at this time, even though some of them have allegedly been unmasked.[10]

Action & Analysis

Included with H-ISAC Membership

Congress -

Tuesday, June 21st:

- No relevant hearings

Wednesday, June 22nd:

- House of Representatives - Committee on Homeland Security: Hearing: "Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks"

Thursday, June 23rd:

- No relevant hearings

International Hearings/Meetings -

- No relevant meetings

EU –

Wednesday, June 22nd:

- European Commission: Conference on the new Regulation on Health Technology Assessment (HTA)

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.

June 23, 2022

[1] https://www.hhs.gov/about/news/2022/06/13/hhs-issues-guidance-hipaa-audio-telehealth.html

[2] https://www.hhs.gov/about/news/2022/06/13/hhs-issues-guidance-hipaa-audio-telehealth.html

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html

[4] https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

[5] https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

[6] https://www.cyberscoop.com/europol-disabled-botnet-infecting-devices/

[7] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

[8] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

[9] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

[10] https://krebsonsecurity.com/2022/06/meet-the-administrators-of-the-rsocks-proxy-botnet/