November 9, 2022

TLP White

This week, Hacking Healthcare examines what to make of the White House's second annual summit on combating ransomware. We briefly recount why the summit came to be, what it accomplished in year one, and how commitments in year two might positively impact the healthcare sector. Welcome back to *Hacking Healthcare*.

1. **International Summit Builds Coalition to Tackle Ransomware and Illicit Cryptocurrency Use**

   In October of 2021, the Biden administration held a virtual meeting with representatives of 30 countries and the European Union (EU) to address the growing threat of ransomware. That summit resulted in the creation of the Counter Ransomware Initiative (CRI), a multinational group of governments who would pursue several workstreams over the following year.

   The goal of the initial CRI meeting was to "rally allies and partners to counter the shared threat of ransomware," a problem that transcends borders and any one government's attempt to crack down on it.[1] That first summit led to several lines of effort, including building resilience, countering illicit finance, the use of law enforcement efforts to disrupt and degrade criminal operations, and a diplomatic approach to spread rules-based behavior, encourage responsible cyber norms, and promote capacity building. These workstreams tended to have vague strategic goals rather than specific action items by which success could be measured. As such, it isn't easy to decipher the impact that the CRI had in its first year, but the group met again last week to see what had been accomplished and discuss what to do next.

   Expanding by roughly a half-dozen members, the CRI reconvened last week (October 2022) and published a statement re-affirming their "joint commitment to building our collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat."[2]

As opposed to the inaugural meeting, 2022's summit concluded with more specific action items and commitments. Those actions that are likely to more directly impact the HPH sector include:[3]

- **Establish an International Counter Ransomware Task Force (ICRTF)** - Members committed to contribute to the joint work of the coalition through information and capability sharing as well as joint action in the fields of resilience, disruption, and countering illicit finance.
- **Create a fusion cell at the Regional Cyber Defense Centre (RCDC)[4]** - The RCDC will publish semiannual public reports on ransomware trends and mitigation measures. Technical information about ransomware (i.e. tools, tactics, and procedures) will be shared with a wide spectrum of stakeholders.
- **Institute active and enduring private-sector engagement** – To be based on trusted information sharing and coordinated action to improve joint work toward operational disruption. To also include sharing information "through new platforms, on actors and tradecraft." Additionally, "CRI members will also share information about ransomware strains on an active and enduring basis."
- **Hold a second counter-illicit finance ransomware workshop** – Which would "build capacity on blockchain tracing and analytics, which would include a tabletop ransomware exercise, coordinated with law enforcement."
- **Take joint steps to stop ransomware actors from being able to use the cryptocurrency ecosystem** - This will include sharing information about cryptocurrency "wallets" used for laundering extorted funds and the development and implementation of the international anti-money laundering/combating the financing of terrorism (AML/CFT) standards for cryptocurrency and related service providers, including "know your customer" rules to mitigate their misuse by cyber criminals.
- **Pursue the development of aligned frameworks and guidelines** -These are to prevent and respond to ransomware, with particular regard to the provision of essential services and critical infrastructure. Members are also committed to mapping inter-jurisdictional issues.

Congress -

Tuesday, November 8th:

- No relevant hearings

Wednesday, November 9th:

- No relevant hearings

Thursday, November 10th:

- No relevant hearings

International Hearings/Meetings -

- No relevant meetings

EU –

- No relevant meetings

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, 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.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/

[4] The Regional Cyber Defence Center (RCDC) is "a subsidiary of the National Cyber Security Centre under the Ministry of National Defence of the Republic of Lithuania (NCSC)." As one of the members of the CRI, Lithuania is co-leading the resiliency working group alongside India. For more information please see: https://www.nksc.lt/rkgc/en.html