February 23, 2022

# Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by highlighting the National Institute for Standards and Technology's (NIST) request for public comment on a potential update to their cybersecurity framework. Next, we dive into a number of new developments outlined by the U.S. Department of Justice that should hopefully make a noticeable dent in cybercrime in 2022. Finally, we provide an update on the hack that hit the International Committee of the Red Cross (ICRC) and offer our thoughts on what it might mean for the healthcare industry in general.

Welcome back to *Hacking Healthcare*.

1. **NIST Cybersecurity Framework RFI**

   On February 22, the National Institute for Standards and Technology (NIST) published a request for information related to "evaluating and improving its cybersecurity resources, including the 'Framework for Improving Critical Infrastructure Cybersecurity' and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains."[1] NIST's cybersecurity resources, including the Cybersecurity Framework, are invaluable, freely available tools that are used widely across many sectors. We encourage members in the healthcare sector to consider providing input to help shape any revisions. The comment period closes on 4/25/2022.[2]

   Those who participated in the initial efforts to develop the NIST Framework know that this input and the subsequent discussions matter a great deal, and now is the time to think about how the Framework and other NIST resources can be most effective in helping the sector improve its security and resiliency.

### 2. DOJ Outlines Cyber Activities at Munich Security Conference

Last week, Lisa Monaco, Deputy Attorney General, spoke at length about the department's approach to tackling cyberthreats. Monaco outlined the department's increased investigative and deterrent capabilities, international partnerships, and how they were "prioritizing cyber disruption."[3] Her remarks help to broadly summarize how the DOJ is attempting to make progress towards countering cyberthreats.

Speaking at the Munich Security Conference on February 17th, Monaco reiterated the challenge of confronting cybercrime when numerous authoritarian governments continue to provide them with safe haven.[4] However, she did share a number of successes that included the first ever use of "a traditional search warrant to execute code and erase digital backdoors," the dismantling of the Emotet botnet, and the takedown of "the world's largest illegal marketplace on the darknet" alongside the arrests of 150 darknet traffickers.[5]

Monaco stated that these actions were only the beginning and explained that "the FBI is investigating more than 100 different ransomware variants, and prosecutors and law enforcement are targeting dozens of ransomware groups."[6] She noted that the DOJ recognizes that disrupting the cybercriminal business model is key to clamping down on ransomware, and doubled down on the DOJ's ability to follow cryptocurrency payments, stating that "the message to companies is concrete: if you report to us, we can follow the money and not only help you, but hopefully prevent the next victim."[7]

Elaborating on what was still to come, Monaco announced that the FBI is "forming a specialized team dedicated to cryptocurrency: the Virtual Asset Exploitation Unit (VAXU)." This unit will apparently "combine cryptocurrency experts into one nerve center that can provide equipment, blockchain analysis, virtual asset seizure and training to the rest of the FBI." The VAXU will collaborate with the National Cryptocurrency Enforcement Team (NCET) which was announced last year. The NCET is also growing with the appointment of Eun Young Choi to be its director.[8]

Regarding international partnerships, Monaco announced the creation of a new position, the Cyber Operations International Liaison, whose responsibility will be to "work with U.S. prosecutors and European partners to up the tempo of international operations against top-tier cyber actors."[9] Additionally, she announced the creation of the International Virtual Currency Initiative, which will "combat the abuse of virtual currency… [and will] allow for more joint, international law enforcement operations… to track money through the blockchain."[10]

Finally, Monaco announced that going forward, "prosecutors, agents and analysts will now assess — at each stage of a cyber investigation — whether to use disruptive actions against cyberthreats, even if they might otherwise tip the cybercriminals off and jeopardize the potential for charges and arrests." This may include "providing decryptor keys or seizing servers."

Monaco ended with a warning for cybercriminals, "the long arm of the law can — and now will — stretch much farther into cyberspace than you think. If you continue to come for us, we will come for you."

*Action & Analysis*
***Membership required***

### 3. International Committee of the Red Cross Hack Update

In mid-January, it was reported that the International Committee of the Red Cross (ICRC) had been victimized by a cyberattack that had exposed sensitive data on hundreds of thousands of vulnerable people. Since then, there have been some new and conflicting updates about exactly what happened and who might be behind it.

The ICRC describes itself as "an impartial, neutral and independent organization," that operates globally on a mission to "[help] people affected by conflict and armed violence" while also "promoting the laws that protect victims of war."[11] Those that the ICRC aids are among the most vulnerable groups of people worldwide. ICRC's status and mission made it all the more unfortunate when it was revealed that a sophisticated cyberattack had "compromised personal data and confidential information on more than 515,000 highly vulnerable people."[12] The U.S. State Department commented that the attack was a "dangerous development" that "has harmed the global humanitarian network's ability to locate missing people and reconnect families."[13]

The ICRC provided some details at the time of the attack, alleging that the hackers "targeted an external company in Switzerland that the ICRC contracts to store data," which forced the ICRC to shutdown computer systems necessary for some of their operations. Since then, the ICRC has put out an update that suggests the attackers used tools and techniques consistent with advanced persistent threat groups (APTs).[14] Furthermore, the operation made use of obfuscation techniques and used tools specifically made to target the ICRC's servers.[15]

The ICRC publicly stated that they have no idea who might have carried out the attack and that they "have not had any contact with the hackers and no ransom ask has been made."[16] They also stated that they "do not have any conclusive evidence that this information from the data breach has been published or is being traded."[17]

Interestingly, a report from Krebs on Security differs from the ICRCs official account. Published the same day as the ICRC's update, Krebs' posting suggests that a criminal actor with apparent ties to an Iranian media influencing operation did appear on cybercriminal forums advertising the sale of the ICRC data, and that it appeared to suggest that a ransom demand had been made.[18]

*Action & Analysis*
***Membership required***

***Congress***

<u>Tuesday, February 22nd:</u>
- No relevant hearings

<u>Wednesday, February 23rd</u>:
- No relevant hearings

<u>Thursday, February 24th:</u>
- 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**

February 23, 2022

*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.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

[2] https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

[3] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[4] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[5] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[6] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[7] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[8] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[9] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[10] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security

[11] https://www.icrc.org/en/who-we-are

[12] https://www.theguardian.com/world/2022/jan/20/hacking-attack-on-red-cross-exposes-data-of-515000-vulnerable-people

[13] https://www.state.gov/u-s-statement-on-the-hack-of-the-icrc/

[14] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

[15] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

[16] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

[17] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

[18] https://krebsonsecurity.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/