October 12th, 2021

TLP White

This week, *Hacking Healthcare* begins by breaking down some of the latest government actions related to ransomware. Specifically, we look at two European countries readying their offensive capabilities and how the United States government's latest actions include targeting cryptocurrency. We then wrap up this week's edition with a look at how a ransomware-related malpractice lawsuit against a hospital highlights some legal dangers that may not be particularly obvious.

But first, if you are an H-ISAC member, this is the last call for participating in H-ISAC's upcoming Hobby Exercise. See the details below. Welcome back to *Hacking Healthcare*.

1. **H-ISAC Hobby Exercise Call for Participation**

   The Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the sector and its partners on significant security and resilience challenges to inform improvements to planning and response. The second iteration of the Hobby Exercise is scheduled for November 2, 2021, at Venable LLP in Washington, DC. We anticipate 30-50 participants, in person, from the public and private sector. This all-day exercise features keynote speakers, large group discussion, breakout room discussions, lunch, and ample breaks to network. The exercise will be held at TLP Amber to facilitate open discussion on these important matters.

   Participant details: An inclusive, holistic, multidisciplinary approach provides value to this exercise, and we are looking for diverse representation across the sector. This diversity extends to organization type (e.g., MDM, HDO, etc.), role (IT/Security, HR, Legal, Comms, etc.), and individual experience level.

   Purpose: The Hobby Exercise educates participants on the issues within healthcare and how H-ISAC and its members can address, and are addressing, them. This exercise builds enduring relationships within and across the public and private sector that help to strengthen understanding, response, and recovery plans and activities.

   To participate in the Hobby Exercise or to learn more, please email jbanghart@h-isac.org.

2. Governments Look to Expand Ransomware Responses

The seemingly unabating waves of ransomware attacks have continued to confound government and private sector efforts to counter them. As the threat that ransomware attacks pose continues to create tangible harm across all sectors, governments are increasingly incentivized to invest more resources in ramping up new approaches to combating it. Multifaceted approaches across various countries are looking to simultaneously build resilience, disincentivize ransom payments, degrade ransomware supporting infrastructure, and even take offensive actions against perpetrators themselves. In recent weeks, the United States (U.S.), the United Kingdom (U.K.), and the Netherlands have either put forth new policies or committed new resources to tackling ransomware and other cyberthreats.

Netherlands: In a letter written in response to a parliamentary inquiry, Dutch Minister of Foreign Affairs Ben Knapen outlined that the Netherlands is willing to "use its intelligence or military services to counter cyber-attacks, including ransomware attacks, that threaten its national security."[1] Knapen specifically called out the threat to critical infrastructure sectors as an example that may "cross the threshold" and justify offensive actions by either the intelligence service or armed forces.[2] In such instances, Knapen explained, the process would include investigating an attack, attributing the attack to a specific entity, and then taking appropriate action.

However, the letter makes clear that legal and diplomatic avenues remain the preferred response to cyber incidents and that the Netherlands has yet to face a ransomware attack or other cyber threat that would require the intelligence service or armed forces to become involved. The Netherlands will likely be ready should that change. As Recorded Future notes, the Dutch previously hacked back an Advanced Persistent Threat (APT) in 2014 when they went after APT29.[3]

U.S.: The Treasury Department and the Department of Justice (DOJ) have both taken actions recently with an eye toward cracking down on ransomware. Among the more notable are:

- The Treasury Department's Office of Foreign Assets Control (OFAC) has released new guidance reiterating the government's stance that paying ransoms carries regulatory enforcement risk and should be avoided.[4] However, it also specifically incentivizes organizations to implement cybersecurity best practices by suggesting that doing so may reduce the likelihood of penalties in the event of a violation.
- OFAC also designated its first virtual currency exchange "for its part in facilitating financial transactions for ransomware actors."[5] This designation means that

"[t]heir assets are blocked, and U.S. persons are generally prohibited from dealing with them."[6] According to a Treasury Department press release, they plan to "continue to disrupt and hold accountable [virtual currency exchanges] to reduce the incentive for cybercriminals to continue to conduct these attacks."

- On October 6th, Deputy Attorney General Lisa O. Monaco announced "the creation of a National Cryptocurrency Enforcement Team (NCET), to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors."[7] The NCET's activities will include "[assisting] in tracing and [recovering] of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups."[8]

U.K. The U.K.'s Defence Secretary, Ben Wallace, recently outlined plans to permanently house their National Cyber Force (NCF) in Lancashire and to provide it with £5 billion in investment by 2030.[9] The NCF, whose existence was formally disclosed to the public in November 2020, has been described as "the new home of offensive cyber operations," with the goal of disrupting "hostile state activities, terrorists and criminals threatening the UK's national security."[10, 11] In a recent interview with The Telegraph, Wallace stated that the NCF could target servers being used to carry out ransomware attacks as an example of potential offensive cyber operations.[12] While noting that the U.K. had yet to experience a "tier-one" cyberattack, Wallace described the 2017 WannaCry attack, which crippled parts of the National Health System (NHS), as an incident that would qualify for an NCF response.[13]

Action & Analysis
Included with H-ISAC Membership

3. Hospital Ransomware Lawsuit Highlights Less Visible Risks

Last week we referenced a malpractice lawsuit involving a newborn who suffered health complications during a ransomware attack on a hospital. While the focus of that article was on the way the media often unnecessarily sensationalize healthcare cyberattacks, the lawsuit also highlighted some of the less visible risks that often accompany cyberattacks against healthcare delivery organizations (HDOs).

For context, the lawsuit stems from 2019, when the Springhill Medical Center in Alabama was victimized by a ransomware attack that severely affected IT systems for several days. During the incident, a patient was admitted to give birth, and the newborn suffered health complications that eventually led to death. The lawsuit alleges that Springhill Medical Center "failed to inform the plaintiff about the cyberattack and outage," and that "physicians and nurses at Springhill Medical Center failed to conduct

multiple tests prior to the birth … and that those tests were not conducted due to the distraction caused by the ransomware attack."[14]

The lawsuit and subsequent reporting highlighted a number of activities and processes that may prove to be important to the outcome of the case. One such example is the text exchanges between hospital staff members that were submitted as evidence. In one exchange, a hospital employee appears to give the impression that the health complications suffered by the newborn were "preventable."[15] Other communication exchanges between hospital staff appear to imply that that under normal operating procedures, this tragic outcome would likely have been avoided, and that staff were more stressed than usual.[16] While the case has yet to be decided, these communications appear difficult to easily dismiss.

Action & Analysis
Included with H-ISAC Membership

Congress -

Tuesday, October 12th:
- No relevant hearings

Wednesday, October 13th:
- House of Representatives – Committee on Financial Services: Task Force on Artificial Intelligence: Beyond I, Robot: Ethics, Artificial Intelligence, and the Digital Age

Thursday, October 14th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Monday, October 11th
- EU Parliament - Committee on the Environment, Public Health and Food Safety

Conferences, Webinars, and Summits –

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

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

October 12th, 2021

---

[1] https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

[2] https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

[3] https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

[4] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[5] https://home.treasury.gov/news/press-releases/jy0364

[6] https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

[7] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team

[8] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team

[9] https://www.bbc.com/news/uk-england-lancashire-58779337

[10] https://www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced

[11] https://www.gchq.gov.uk/news/national-cyber-force

[12] https://www.telegraph.co.uk/politics/2021/10/02/britain-capable-launching-offensive-cyber-attacks-against-russia/

[13] https://www.telegraph.co.uk/politics/2021/10/02/britain-capable-launching-offensive-cyber-attacks-against-russia/

[14] https://www.hipaajournal.com/lawsuit-alleges-ransomware-attack-resulted-in-hospital-baby-death/

[15] https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

[16] https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116