September 29th, 2021

TLP White

This week, *Hacking Healthcare* begins with a quick overview of the Department of Justice's (DOJ) national healthcare enforcement action that has called out $1.1B in telemedicine fraud. Next, we examine the Treasury Department's newest actions in their fight against ransomware. Finally, we wrap up with some questions about the recent allegation that the FBI didn't disclose the Kaseya decryption key to victims for three weeks.

Welcome back to *Hacking Healthcare*.

1. **The Department of Justice Alleges $1.1B in Telemedicine Fraud**

   On Friday, September 17th, the DOJ released a notice on results from their national health care fraud enforcement action. In total, the enforcement action charged more than 130 individuals and alleged $1.4 billion in losses. Notably, the majority of those losses were attributed to telemedicine fraud.[1]

   Telemedicine has raised its profile considerably since the beginning of the pandemic. Since then, a number of rules and regulations were relaxed to more easily enable a wide range of in-person services to be converted to various online solutions. Unfortunately, although not surprisingly, it appears that the explosion of telehealth in general has resulted in a rise in unscrupulous behavior. The notice states that $1.1 billion of the alleged losses are tied to "fraud committed using telemedicine."[2]

   This enormous sum covers cases in 11 different judicial districts and includes more than 40 individuals.[3] One example of the fraudulent behavior involves the allegation that some telemedicine executives paid doctors and nurses to order unnecessary testing and medications either without any patient interaction or based on only a brief phone call with patients they had never met or seen.[4] Medical equipment companies and testing labs then purchased those orders in exchange for illegal kickbacks and bribes.[5] Other allegations include medical professionals billing Medicare for "sham telehealth

consultations that did not occur as represented" in order to fund luxury shopping sprees.[6]

The notice included a statement from Assistant Attorney General Kenneth Polite, President Biden's relatively newly confirmed head of the DOJ's Criminal Division, stating "The charges announced today send a clear deterrent message and should leave no doubt about the department's ongoing commitment to ensuring the safety of patients and the integrity of health care benefit programs."[7]

Action & Analysis

2. New Treasury Department Ransomware Guidance and Cryptocurrency Crackdown

Tamping down on the scourge of ransomware has been an uphill battle for governments and the private sector alike. Government guidance to the private sector, as well as their offensive actions against malicious cyber criminals, are part of a multifaceted approach to making the problem manageable. Last week, The United States Treasury Department took two actions that may help by issuing an update to their ransomware guidance and by targeting cryptocurrency.

<u>Ransomware Advisory</u>

One of the many stressful considerations that ransomware victims often contend with is the potential threat of legal and regulatory action. Within the United States, the Treasury Department's Office of Foreign Assets Control (OFAC) is one entity that enforces regulations pertaining to ransomware via payments that health care organizations should be aware of. Recently, OFAC released an advisory to update their guidance on the "sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities," and provide information on what steps health care organizations could take to minimize potential punishment for a violation.[8]

On September 21st, OFAC released their *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.* The 6-page document is largely a restatement of the earlier October 2020 Advisory, including reiterating that paying ransoms is discouraged. However, there are notable changes. The most significant may be an elaboration on how organizations can mitigate any enforcement action through cybersecurity.

Whereas the October 2020 advisory was short on mitigation strategies, emphasizing contacting and cooperating with law enforcement in the event of an incident and having a compliance program in place, the update encourages proactively engaging in cybersecurity best practices. The document states that, "meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and

Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide will be considered a significant mitigating factor in any OFAC enforcement response."

The advisory goes on to provide some examples, stating, "such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols." In addition, there is an expanded section on contacting the relevant government departments and agencies.

Cryptocurrency

In addition to the advisory, the Treasury Department took the step of targeting its first ever virtual currency exchange for its role in laundering cyber ransoms. As the Treasury Department's statement explains, "Some virtual currency exchanges are a critical element of this [ransomware/cybercrime ecosystem], as virtual currency is the principal means of facilitating ransomware payments and associated money laundering activities."[9]

The Treasury Department's targeting led to the virtual currency exchange SUEX OTC, S.R.O. (SUEX) being added to its designated entities list. The move came in light of evidence that SUEX "facilitated transactions involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors."

For those not as familiar, the designation by Treasury means that "all property and interests in property of the designated target that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them."

Action & Analysis

3. **FBI withheld decryption key for Kaseya ransomware attack for three weeks: report**

A report from the Washington Post claims that the FBI acquired decryption keys for Kaseya ransomware but did not disclose them to victims for three weeks. [10] Predictably, this has caused some tension between the public and private sectors, as well as between government agencies. It also raises long-standing questions around the processes by which government makes decisions on when and how to share information.

According to reporting, the decryption keys were obtained by infiltrating the cyber infrastructure of the perpetrators REvil.[11] However, rather than immediately disseminating the key to victims, it was decided to hold off in order to maintain

operational surprise and launch an attack against the group's infrastructure.[12] This attack never came to fruition as the group went dark before it could be carried out.

In congressional testimony, differing perspectives on the decision appeared to emerge. FBI Director Wray reportedly blamed "the delay on other law enforcement agencies and allies who they said asked them not to disseminate the keys."[13] In a different hearing, National Cyber Director Chris Inglis appeared to suggest that the article itself was more nuanced than its title suggested and that there was no undue delay.[14] However, he did clarify that in such situations no decision is likely to be optimal.[15]

Action & Analysis

Congress

Tuesday, September 28th:
- No relevant hearings

Wednesday, September 29th:
- Senate – Committee on Commerce, Science, and Transportation: Hearings to examine protecting consumer privacy.

Thursday, September 30th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits –

September 29th, 2021

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

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

---

[1] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[2] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[3] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[4] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[5] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[6] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[7] https://www.justice.gov/opa/pr/national-health-care-fraud-enforcement-action-results-charges-involving-over-14-billion

[8] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921

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

[10] https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html

[11] https://www.zdnet.com/article/fbi-decision-to-withhold-kaseya-ransomware-decryption-keys-stirs-debate/

[12] https://www.zdnet.com/article/fbi-decision-to-withhold-kaseya-ransomware-decryption-keys-stirs-debate/

[13] https://www.zdnet.com/article/fbi-decision-to-withhold-kaseya-ransomware-decryption-keys-stirs-debate/

[14] https://www.hsgac.senate.gov/hearings/national-cybersecurity-strategy-protection-of-federal-and-critical-infrastructure-systems

[15] https://www.hsgac.senate.gov/hearings/national-cybersecurity-strategy-protection-of-federal-and-critical-infrastructure-systems