October 27th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining a new report published by the Financial Crimes Enforcement Network (FinCEN) that provides some interesting findings related to the scale and complexity of the ransomware ecosystem. Next, we break down some of the differing perspectives in the debate over cyber incident liability and why a lack of consensus could lead to a less than ideal result for the private sector. Finally, we wrap up with a short explanation of the Commerce Department's new interim rule that limits the sale of hacking tools to foreign entities.

Welcome back to *Hacking Healthcare*.

1. **Government Report Sheds Light on Scale and Complexity of Ransomware**

   With all the attention ransomware has received in recent memory, you could be forgiven for thinking there is nothing new worth reporting. However, a newly released U.S. government report helps to illustrate the scale of the ransomware problem while also helping to contextualize some of the Biden administration's recent anti-ransomware actions.

   The FinCEN *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* was released last week and the fairly technical report provides a number of interesting ransomware data points from the first half of this year.[1] FinCen concluded that "ransomware is an increasing threat to the U.S. financial sector, businesses, and the public."[2] Some of the more notable findings include:[3]

   - Bitcoin was the most common ransomware-related payment method, with Monero increasing slightly over the previous year

- In some cases, attackers accepted either Bitcoin or Monero, but added an extra fee if it was paid in Bitcoin

- If current trends continue, suspicious activity reports (SARs) filed by banks in 2021 are projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined

- FinCEN identified approximately $5.2 billion in outgoing BTC transactions potentially tied to ransomware payments associated with the 10 most common variants of ransomware

- FinCen noted that there are at least 68 different ransomware variants – with REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos being the most common

- Ransomware threat actors use a handful of methods to attempt to shield their activity from law enforcement agencies, such as requesting payments in Anonymity-enhanced Cryptocurrencies (AECs)[e.g. Monero], avoiding reusing wallet addresses, "chain hopping," cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds

Action & Analysis
Membership required

2. Cybersecurity Incident Liability Protections Up for Debate

Is it more beneficial to punish poor cybersecurity practices as an incentive to improve them or would leniency and protection encourage entities to be more open and share needed information about cyber incidents? That is the core of the current debate around the extent to which organizations should be granted liability protection in the aftermath of a cyber incident. It is also a topic that is likely to grow in importance as legislators look to pass cyber incident reporting bills, and as the Biden administration pushes to create baseline cybersecurity expectations for the private sector and critical infrastructure.

While there are certainly those who don't believe liability protections should exist at all, the conversation on this topic generally appears to center around how extensive liability protections should be and where exceptions should be made.

One perspective is that liability protections should not be extended to entities who fail to take cybersecurity seriously and who have not implemented any best practices that could mitigate an incident altogether. This perspective may view an offer of protection as a disincentive to making the types of cybersecurity improvements that are widely

needed across the country, especially in critical infrastructure sectors. New National Cyber Director Chris Inglis appears to endorse a similar line of thinking when he recently stated, “at the end of the day, if you've not performed well in this space, there will be consequences. There should be liability.”[4]

Others argue that without extensive liability protections victims of cyberattacks are less likely to come forward and provide the kind of information that would help the government understand the cyber threat environment and counter malicious actors. Organizations victimized by a cyberattack are unlikely to feel good about disclosing an incident to law enforcement if they face the prospect of immediately adding new legal and regulatory risks. This is something that Deputy Attorney General Lisa Monaco recently appeared to acknowledge when she stated that, “those companies that stand with us and work with us will see that we’ll stand with them in the aftermath of an incident.”[5]

While there are numerous proposals about exactly how this issue could be addressed, with some taking inspiration from the Cyberspace Solarium Commission’s final report, there does not appear to be a consensus among lawmakers on the issue.[6]

Action & Analysis
Membership required

3. Department of Commerce Announces Rule to Limit Sale of Hacking Tools

Under the rather unassuming title of *Information Security Controls: Cybersecurity Items*, the Department of Commerce has published an interim final rule with the goal of curtailing the sale of cybersecurity tools that could be used for hacking or surveillance to certain foreign governments and entities.[7] While that may sound like a fairly straight-forward and laudable achievement that you might have assumed would have already been accomplished, the potential implications of the rule have made this a long drawn out process.

The interim rule was published on October 21st and will take effect in 90 days. It essentially “would require U.S. firms to secure a license to export select cyber technologies to countries “of national security or weapons of mass destruction concern,” including Russia and China.”[8] Additionally, it introduces “license requirements for companies that wish to sell cyber technologies to companies under U.S. arms embargo, or users who could intentionally misuse products.”[9]

The rule effectively puts the United States into alignment with 41 other countries who are members of the Wassenaar Arrangement, an export control regime for conventional arms and dual-use goods and technologies that added "intrusion software" in 2013. Since then, there has been significant debate over how common cybersecurity tools used by researchers could potentially be classified as "intrusion software" which would make their export to other countries a violation. The Commerce Department is requesting public comments to understand how well this revised attempt at rulemaking manages to avoid those concerns.

Action & Analysis
Membership required

Congress

Tuesday, October 26th:
- No relevant hearings

Wednesday, October 27th:
- No relevant hearings

Thursday, October 28th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits –

October 27th, 2021

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

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

---

[1] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

[2] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

[3] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

[4] https://www.nextgov.com/cybersecurity/2021/10/national-cyber-director-liability-should-be-part-equation-public-private-collaboration/186218/

[5] https://www.nextgov.com/cybersecurity/2021/10/justice-official-dangles-liability-protections-encourage-private-sector-breach-reports/186253/

[6] https://www.solarium.gov/

[7] https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items

[8] https://www.nextgov.com/cybersecurity/2021/10/commerce-announces-rule-selling-hacking-tools-foreign-governments/186248/

[9] https://www.nextgov.com/cybersecurity/2021/10/commerce-announces-rule-selling-hacking-tools-foreign-governments/186248/