ACAMS

Written Evidence

Joint Committee on the National Security Strategy: Ransomware Inquiry

Submitted: December 16, 2022

Introduction

1. The ACAMS global community continues to monitor the worldwide evolution of transnational criminal organizations, including those involved in cybercrime. The financial crime threats from such groups highlight their ability to evolve and adapt. Capitalizing on new payment channels and the rise of digitalization, they continue to exploit existing governance arrangements and acclimatize to a wave of new technology. Their operating environment is growing increasingly complex and reining it in will be a significant challenge, requiring agile and dynamic cooperation from both the public and private sectors. In support of this, the purpose of our response is to highlight the importance and challenges of 'following the money', a key pillar of countering the ransomware ecosystem.

About ACAMS

2. ACAMS is a leading international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 100,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. ACAMS' 60+ Chapters globally further amplify the association's mission through training and networking initiatives.

ACAMS Response

3. The ransomware threat is both multifaceted and constantly evolving. Much of government and industry efforts are rightly focused on prevention (i.e. enhancing cybersecurity systems, updating firmware and training employees to identify phishing attempts). However, attacks cannot be prevented in all instances. It is important for both governments and private organizations to prepare incident responses, considering questions such as whether to pay a ransom and – if they do – what risks to be aware of. Furthermore, disrupting the illicit proceeds is a critical component in countering the ransomware ecosystem. Our response will be focused on these areas, where financial crime and ransomware intersect. Specifically:

    - Ransomware threat landscape indicators
    - Money laundering's role in enabling ransomware
    - The nexus of sanctions and ransomware and related victim considerations
    - Government efforts to tackle ransomware and lessons learned from other countries

The Ransomware Threat

4. A systemic challenge in understanding and mapping ransomware's threat lies in a lack of clear and reliable data. This makes ascertaining an accurate picture of the trends challenging. As **reported** by the **Ransomware Task Force**, which brings together cyber experts from across industry and governments, the patchwork of data available likely fails to capture the scope, scale, and impact of ransomware attacks. Therefore, it is difficult to render accurate interpretations and assessments. A contributing factor to this is victims' reluctance to report incidents to law enforcement. However, despite these informational challenges, the data available can provide some helpful indicators.

5. The **2022 Crypto Crime Report** published by blockchain analytics firm Chainalysis in February 2022 found that US$692 million (and counting) in ransomware payments from 2020 had been identified - much of which was only detected relatively recently. Furthermore, the report notes that this sum is expected to be surpassed once the 2021 data is fully tabulated.

6. Over the past couple of years, US government data has indicated that the number of ransomware attacks, along with their costs, has grown. The most recent **Financial Trend Analysis** published by FinCEN on ransomware-related Bank Secrecy Act filings for 2021 suggested that the number of ransomware incidents increased significantly compared to 2020, with a far higher total dollar value - US$1.2 billion in ransomware-related filings compared to US$418 million. Moreover, from January 2021 to July 21, 2021, the FBI's Internet Crime Complaint Center **reported** 2,084 ransomware complaints, a 62% increase from the previous year. Also, in February 2022, the Cybersecurity and Infrastructure Security Agency **reported** that it was aware of ransomware incidents at 14 of the 16 critical sectors of US infrastructure. While this data is specific to the US, it likely indicates wider trends.

7. While these statistics indicate increasing ransomware incidents, it should be kept in mind that these figures may also reflect an improved willingness by private industry to report ransomware incidents. Notably, these numbers do not include data for 2022. Some analysts believe that the frequency of ransomware attacks may have reduced this year. Possible reasons for a decrease may include the rising trend of hackers demanding pay-outs in difficult-to-trace cryptocurrencies, as well as a slump in price this year rendering the business of ransomware less lucrative. Ultimately, due to the 'lag time' of ransomware data, statistical indicators for 2022 may take some time to materialize.

8. Alongside this data, there appears to be growing concern for ransomware within industry. In a **Global Ransomware Risks survey** conducted by ACAMS at the end of 2020, which surveyed nearly 400 individuals from the international compliance community, respondents indicated their growing concern of ransomware's threat. The key aspects of this included:

    - Just under a third of respondents viewed the threat of ransomware to their organization as high.
    - Two-thirds see ransomware as a growing threat - with over half viewing it as a cybersecurity priority.
    - Just under half felt it was likely that their organization would suffer a ransomware attack in the next 12 months.
    - Nearly one in ten stated that their organization had suffered a successful ransomware attack.

Ransomware's Nexus with Financial Crime: Money Laundering

9. Detection and prevention are clearly essential pillars in effectively countering ransomware. However, it is impossible to prevent a breach in all cases, particularly as ransomware actors continue to evolve and find new methods of attack. Following a successful attack, ransomware actors will utilize financial networks to conceal their funds. Accordingly, understanding and countering this process is critical, particularly since ransomware funds are often reinvested to support further attacks. Therefore, perpetrators' abilities to obtain ransom payments and launder them into fiat currency is a key factor in enabling ransomware activity. 'Following the money' and interrupting these financial networks is an essential component in countering the ransomware ecosystem.

10. As a relatively new phenomena in the financial crime space, work is still being undertaken to map the ransomware payment ecosystem. Understanding the actors and processes within this ecosystem is central to combatting the illicit proceeds of ransomware.

11. A recent **paper** issued by the Institute for Security and Technology's Ransomware Task Force, building upon information included in FinCEN's 2021 Advisory (updated in 2022), seeks to set out the various different elements of a ransomware payment. Essentially, when a victim decides to pay a ransomware actor, they need to obtain the amount of cryptocurrency required. They may choose to engage with a specialist firm to do so. The victim's funds are then moved from their fiat currency depository institution via wire transfer, automated clearing house, or credit card, either to a third party that specializes in ransomware payments or to a crypto business directly. Then, the receiver of the funds exchanges fiat currency for crypto and deposits it into a wallet owned by the victim or the organization paying on their behalf. Subsequently, the victim or organization directs the payment to a wallet (or wallets) owned by the ransomware actors and/or their associates.

12. The ransomware actors will then seek to move and conceal their illicit proceeds. To do this, they often acquire assistance from third-party money launderers. This complex process contains many options, often utilizing or targeting cryptocurrency businesses with weak financial crime controls, as well as jurisdictions with inadequate financial crime regulations. To do this, ransomware actors will likely utilize tumblers and mixers, whereby a service provider mixes several individual's coin deposits, holding the funds before returning them to participants at random times and values. This process makes it much harder to trace the original transactions and conceals the illegality of the proceeds.

13. There are several other techniques used by perpetrators of ransomware, such as CoinJoin transactions: in which multiple payments from different users are combined into a single transaction, whereby addresses are mixed but totals remain the same. Chain hopping is another method: this involves moving different cryptocurrencies in rapid succession to reduce their traceability. Furthermore, to launder illicit funds, ransomware actors may employ merchant services, darknet markets, high-risk and centralized exchanges, and peer-to-peer exchanges. Over-the-counter trading desks – where actors trade cryptocurrency without an exchange acting as a facilitator or mediator – can also provide cryptocurrency laundering services to ransomware perpetrators.

14. These techniques make it harder, or in some cases impossible, to trace the origin of the assets – making them ideal for obscuring the flow of value. That is why these kinds of features are chosen for cybercrime and the proceeds from ransomware attacks.

15. An additional challenge is that cybercriminals have turned to using anonymity-enhanced cryptocurrencies (AECs), such as Monero, Dash, and Zcash. These AECs (also known as privacy coins) have a specific focus on encryption and use an obfuscated public ledger, offering a higher level of anonymity to cybercriminals.

16. Given the role of cryptocurrency in these processes, crypto businesses, as well as traditional financial institutions, play a vital role in enabling the government to disrupt and trace the proceeds of ransomware.

17. The European Union Agency for Cybersecurity's (ENISA) 2021 **Cyber Threat Landscape Report** identified that only a small number of money launderers control the process of cleaning ransom payments received by multiple ransomware groups. According to the report, 199 crypto addresses received 80% of all funds sent by ransomware addresses in 2020. Moreover, an even smaller group of 25 addresses accounted for approximately 46%.

18. While recent law enforcement efforts have made considerable gains – partly through the use of blockchain analytics/forensics – for example through making **arrests**, **seizing ransom payments** (millions of dollars have been recovered in the past 12 months) and removing infrastructure associated with ransomware, much more needs to be done to target ransomware actors' financiers.

19. In summary, to disrupt the illicit proceeds of ransomware, which are used to enable more attacks and fund further distribution, it is essential to follow the money as well as target the funds and those who facilitate them. In doing so, it is critical that the UK government engages in public-private and cross-industry dialogue, both with financial institutions and crypto-businesses, as these organizations are able to provide expertise and context on the way this money is moving, as well as being on the front-line of stymying these proceeds through implementation of anti-money laundering regulations.

Ransomware's Nexus with Financial Crime: Financial Sanctions & Impact on Victims

20. Another key touchpoint between ransomware and financial crime is the use of sanctions. These are financial restrictions that compel freezing of assets and other measures. A number of jurisdictions have used sanctions as tools to combat cybercrime groups and cyber-enabled crime, including ransomware.

21. The **US**, the **UK** and the EU have cyber sanction programs in place. These enable the relevant authorities to designate cyber-actors who perpetrate illicit and malicious cyber activity, which results in the persons/entities being added to the respective sanctions list and restrictions imposed. While the UK and EU have not currently designated many actors or groups under their regimes, the US has made over 300 cyber-related designations, including for several persons/entities engaged in recent ransomware-focused actions.

22. For victims of ransomware attacks, these sanctioning systems and the actors on their lists are extremely relevant. While ransomware payments are not legally prohibited generally (though often strongly discouraged), they do run the risk of potentially violating economic sanctions and causing both the victim and other involved parties to face additional legal, financial, and reputational risks.

23. This is particularly relevant in the US context, given the large number of cyber actors designated, the number of US touchpoints in the global financial system, and the extent of US jurisdiction. Should an organization within the US's jurisdiction (US persons or

those within US territory) facilitate - in any part of a ransomware payment's chain - a ransom payment involving a sanctioned person, they may face civil or criminal penalties. Furthermore, under US sanctions, it is prohibited to make a ransomware payment to cyber actors based in or linked to a comprehensively sanctioned jurisdiction (e.g. Iran, North Korea, Cuba). It is important to remember that many individuals and organizations in the UK may be subject to US jurisdiction and will need to consider the risks of paying a ransom to a US designated party.

24. Therefore, victims need to consider their exposure to sanctions and the risks of making a ransomware payment. To mitigate these risks, it is important for organizations to take several steps to protect themselves, such as creating a cyber incident response plan, identifying decision-makers regarding whether to pay or not, understanding the risk-appetite within their organization's risk-based approach, applying ransomware policies and procedures, engaging with reputable cyber incident response firms and – critically – undertaking due diligence before making payments.

25. Several resources have been produced by ACAMS that outline compliance best practices and provide further information on mitigating the risk of sanctions:

- **Sanctions Masterclass - Exploring the Intersection of Ransomware, Crypto, and Sanctions Risks**
- **Sanctions Masterclass: Nexus of Cyber, Ransomware, and Sanctions Compliance**
- **Sanctions Masterclass Follow-Up Briefing Paper**

26. To add context to the risks presented here, Chainalysis **estimated** that 15% of ransomware payments in 2020 had a sanctions nexus. This will likely have increased since, as sanctions are being used to combat the ransomware ecosystem more frequently. Furthermore, while the UK and the EU cyber sanctions lists are presently limited, they are likely to be expanded over time.

27. At present, industry is generally unfamiliar with these risks. This unawareness even exists among the global compliance community, which can be seen from our Global Ransomware Risks survey:

- Of non-financial institution (FI) respondents, 28% were familiar with the sanctions risks posed from making ransomware payments. 44% were either not at all familiar or quite unfamiliar. By comparison, 24% of FI respondents were familiar and 50% were unfamiliar.
- Of private sector respondents outside the financial sector, 38% stated that they had factored ransomware into their sanctions compliance programs and 34% said they had not. Of the FI respondents, 42% answered that they had and 23% answered that they had not. In both cases, large numbers of respondents did not know.

28. It should be remembered that these were global responses. However, the results are evidence that more work could be undertaken to raise awareness of the risk of sanctions posed by ransomware and that the UK government should provide more support and assistance to industry.

29. Given these sanctions risks, and the lack of knowledge and understanding surrounding them, the UK government should endeavor to raise awareness, provide guidance and collaborate with the private sector to strengthen victims' capacities for managing and mitigating them, particularly if the UK chooses to utilize sanctions against ransomware actors more frequently. The **OFAC's** and **FinCEN's** guidance are both examples of useful advice, both for victims and financial institutions.

Government Efforts to Tackle Ransomware & Lessons Learned from Other Countries

30. In our Global Ransomware Risks survey, respondents indicated a desire for more effective government response. When asked about their national government's efforts on combating ransomware, 29% felt that their government had done very little to protect businesses from attacks. 38% answered that some steps had been taken but much more is needed, 15% stated that an adequate job was being done, and only 5% stated an exceptional job had been undertaken.

31. Respondents were asked what would be most useful for them in dealing with ransomware attacks moving forward and were presented with a series of options. Greater access to specific information on current and emerging threats and the issuance of guidance on how to best prevent attacks were the options most respondents selected as being useful.

32. Respondents were also asked what government actions would be most useful in the global fight against ransomware, and they were given several options. The three selected as most useful were:

- Stronger government efforts to identify and penalize ransomware groups
- Greater flexibility within the public and private sectors in sharing relevant intelligence
- Stronger training throughout the private sector on how to shield firms from attacks

33. To ensure that responses are not being siloed, it is essential for different government departments (e.g. the NCSC, the NCA, the OFSI, the UK Treasury, the GCHQ, the MOD, the Home Office) to collaborate on this issue. Work should be undertaken by cyber agencies to enhance organizational resilience to ransomware attacks; however, guidance must also be provided to victims who are considering whether to process a ransomware payment, including on the financial crime risks.

34. Looking to other countries' approaches, the US has taken a vigorous **whole-of-government** approach to countering ransomware under the Biden administration. This has included significant efforts in raising awareness, encouraging the adoption of cyber-hygiene principles, frequent updates on the ransomware threat landscape (**CISA advisories**), creating resources to help industry (e.g. **StopRansomware**), and moving to enhance public-private information sharing (Illicit Virtual Asset Notification [IVAN] information sharing partnership).

35. OFAC has also issued guidance on **sanctions for the cryptocurrency industry** that sets out the sanctions risks and responsibilities for these organizations. Sanctions engagement with this sector, some of whom may not have mature compliance functions, is a welcome step.

36. A recent US legislative development is the passing of the **Cyber Incident Reporting Act**, which introduced mandatory incident reporting for critical infrastructure within 72 hours of a cyberattack and 24 hours of paying a ransomware payment. With time, this law may provide clearer information on ransomware trends, and other jurisdictions may look to implement similar legislation.

37. The Biden-Harris strategy includes using financial tools, such as sanctions, as a critical pillar to dismantle payment ecosystems. Recent examples, such as the targeting of Hydra, SUEX and Tornado Cash (see **ACAMS Infographic**), appear to be having an effect in disrupting ransomware proceeds.

38. As with many areas of criminality, international cooperation is critical in opposing the ransomware ecosystem, and this is not least the case with ransomware. Given the nature of the payment ecosystem, actors will seek to 'cash out' their cryptocurrency in jurisdictions with more relaxed controls. Continued engagement with the US-led International Counter Ransomware Initiative is an important step in strengthening this cooperation.

Conclusion & Recommendations

39. A holistic, robust, and effective effort to counter the ransomware ecosystem must include identifying and disrupting the financial proceeds.

40. To support this, the UK government should consider deepening public-private partnerships as it seeks to implement ransomware policies. This is because financial institutions and cryptocurrency businesses are well positioned to provide practical perspectives and intelligence and ensure that regulations are effectively operationalized.

41. A core element of this is sharing information on key aspects of cybercrime, including identification of trends (e.g. the growing use of AECs) and threat intelligence.

42. Additionally, the UK government should ensure it supports increased awareness of the financial crime risks tied to ransomware, particularly for crypto businesses, and encourages victims to report their experiences to law enforcement.

43. Cyber-sanctions regulations can present complex challenges for ransomware victims. If these measures are increasingly utilized by the UK government, it is important that guidance and clarity is provided to industry to ensure they understand the related sanctions risks.

This written evidence was submitted to the Joint Committee on the National Security Strategy on December 16, 2022, as part of its Ransomware Inquiry. You can view other written evidence **here**.