Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

APRIL 2023

VIA WEBFORM

The Hon Clare O'Neil MP
Minister for Home Affairs
Minister for Cyber Security

and

The Cyber Security Strategy Expert Advisory Board

Australian Government

About TRM Labs

TRM Labs Inc. (“TRM”) provides blockchain intelligence to help financial institutions, cryptocurrency businesses and public sector agencies detect and investigate crypto-related fraud and financial crime. TRM's risk management platform includes solutions for cryptocurrency anti-money laundering (AML), transaction monitoring and wallet screening, entity risk scoring including Know-Your-VASP, and transaction tracing for investigations.

Founded in California in 2018, TRM currently operates in more than 20 countries worldwide, including Australia. More information on our products and services is available on our website at www.trmlabs.com.

Executive Summary

A strong cyber security strategy is integral to safeguarding Australia's digital economy, critical infrastructure, and national security. Aside from the five priority areas outlined in the discussion paper, the financial dimension is also crucial to address in Australia's fight against cybercrime.

The nexus between cyber and financial crime cannot be understated. Cyber criminals are often financially motivated and are constantly finding more sophisticated ways to collect and move their illicit funds. In recent years, virtual assets, which offer decentralised, permissionless, cross border value transfer at the speed of the internet, have increasingly become the payment rails of choice for cyber criminals. Cyber criminals are also using an increasingly sophisticated array of virtual asset-specific technologies and techniques to launder and obfuscate the flow of their illicit funds.

However, the traceability and immutability of the blockchain on which these virtual assets move offers unique opportunities to disrupt the flow of these ill-gotten gains. Blockchain intelligence demystifies the wealth of information on the blockchain and enables regulators, law enforcement and the crypto asset industry to identify and stop bad actors.

Australia can leverage the power of blockchain intelligence to fight cyber crime through public-private partnerships in the following three areas:

1. Sharing information through international platforms
2. Building blockchain intelligence expertise as part of a broader suite cyber intelligence and forensics capabilities
3. Partnering specialist experts to achieve timely incident response

As Australia continues onward to its goal of becoming the world’s most cyber secure nation by 2030, TRM looks forward to further engaging and collaborating with various public and private stakeholders to hit cyber criminals where it hurts - their pockets.

Our Response

TRM is grateful for the opportunity to respond to this Discussion Paper.

A comprehensive and robust cyber security strategy is crucial to address the ever-evolving cyber threats that impact Australia's digital economy, critical infrastructure, and national security. We appreciate the Government's proactive approach in seeking input from a diverse range of stakeholders, and look forward to contributing our perspectives.

The five priorities of securing critical infrastructure, developing standards and best practices, investing in research and development, improving awareness and literacy and strengthening international cooperation are integral to enhancing Australia's cyber security posture.

That said, we would like to highlight one more critical area to decisively address in Australia's fight against cyber crime - the financial dimension.

Financial motivations for cyber crime

Educator and author Anthony D'Angelo said: "When solving problems, dig at the roots." There is no more common root for crime than one that has been called the root of all evil - money.

The flip side to the financial losses suffered by victims of cyber crime is the financial motivation of said crime. In its previous Threat Reports, the Australia Cyber Security Centre (ACSC) has noted that: "Financially motivated criminals that exploit and access systems for financial gain are a substantial threat to Australia,"[1] highlighting "ransomware and business email compromise"[2] as particularly common.

Indeed, nowhere is the financial motivation for cyber crime more evident than in the most destructive of cyber threats - ransomware. In recent years, ransomware itself has become an opportunity for financial gain. As observed by the ACSC in its most recent Threat Report, there has been a rise in organised syndicates offering ransomware as a service (RaaS), usually on the dark web, thus providing "actors who may not have the technical skill to develop their own ransomware with an opportunity to launch highly profitable attacks" and "offering cybercriminals a choice about the tools they can use."

[1] ACSC 2015 Threat Report
[2] ACSC Annual Cyber Threat Report 2021

We are also seeing more "big game hunting," with cybercriminals targeting high-earning organizations to maximise their illicit profits - the recent Optus and Medibank hacks, which came with ransom demands, are evidence of this.

With the ACSC estimating financial losses from cyber crime in the tens of billions, it is clear that there is a huge financial motivation for cyber crime. By disrupting the flow of cyber crime proceeds and denying cyber criminals access to their ill-gotten gains, Australia can strike an offensive blow at the root of the problem.

The financial anatomy of cyber crime

Through our work in blockchain intelligence, TRM has gleaned significant insight into the use of cryptocurrency, also known as virtual assets, to support the laundering of cyber crime proceeds. Unfortunately, the same qualities that make virtual assets a force for good - decentralised, permissionless, cross border value transfer at the speed of the internet - also make them attractive to illicit actors who seek to move funds across the globe at unprecedented speed and scale.

What is a virtual asset?

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. The most commonly used virtual assets are a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology that relies on cryptography, such as a blockchain. Many popular virtual assets operate on public blockchains, where pseudonymous transaction information is viewable.

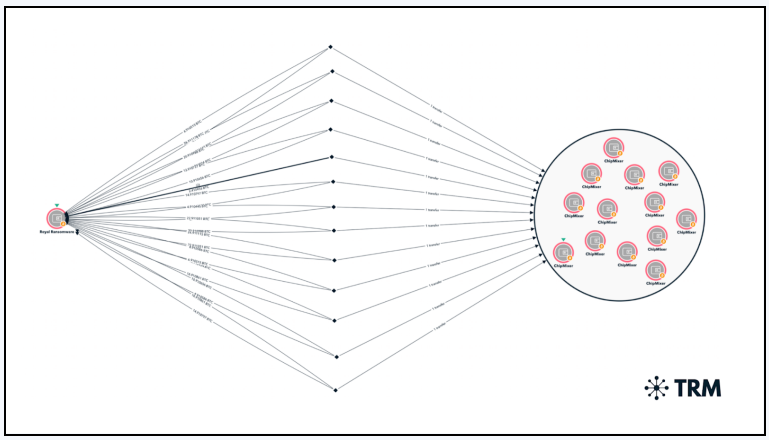
Source: FATF

While the percentage of illicit flows in the broader virtual asset universe is small, the percentage of cryptocurrency flows in illicit finance is significant. General industry consensus is that illicit finance makes up no more than 2% of virtual asset activity. However, the Financial Action Task Force (FATF)'s recent report on ransomware found that "payments and subsequent laundering of ransomware proceeds are almost exclusively conducted through virtual assets." In Australia, the Optus hacker had also demanded for a million dollar ransom to be paid in cryptocurrency.

The growing use of virtual assets by cyber criminals presents an unique opportunity to understand and disrupt their funds flows. As the FATF astutely notes, "pseudonymous transaction information" is permanently and transparently stored on the blockchain, making it available to all for posterity. With the right tools, this information can be decrypted to expose the financial anatomy of crypto-enabled cyber crime.

Case Study: ChipMixer Takedown

In March 2023, German and US authorities, with assistance from Europol, shut down ChipMixer, a crypto mixer allegedly run by Vietnamese Minh Quoc Nguyen, for its role in laundering over US$3bn in crypto. Four servers and approx USD44m in crypto were seized.



TRM's blockchain intelligence confirms that ChipMixer was widely used by prominent ransomware syndicates to launder illicit proceeds. Among them were Karakurt, SunCrypt, REvil, Conti, LockBit, Ragnar Locker, and Royal.

Royal in particular is believed to be the main successor of Conti, one of the most notorious and sophisticated groups in the history of ransomware. It has targeted numerous critical infrastructure sectors including, manufacturing, communications, healthcare, and education, with ransom demands from USD1m to USD11m, payable in bitcoin.

Royal frequently relied on ChipMixer to launder extorted funds. The graph above shows one instance when actors affiliated with Royal laundered nearly USD500k from a ransom payment they received in November 2022.

These findings underscore the significance of the ChipMixer takedown in disrupting illicit actors and their funds flows through virtual assets.

More information is available on our website.

Combating crypto-enabled cyber crime

There is significant potential for blockchain intelligence to disrupt crypto-enabled cyber crime through public-private partnerships. In particular, we urge the Government and the Expert Advisory Board to consider blockchain intelligence partnerships as part of the following three pillars outlined in the discussion paper.

1. Information sharing

The paper calls out the importance of public-private information sharing, including internationally. Especially in a space as borderless as virtual assets, timely and relevant information sharing is critical to successful disruption of illicit activity. Australia's leadership and participation forums such as the International Counter Ransomware Taskforce, as well as the FATF, will help shape global thinking constructively. Such forums are also essential for jurisdictions to share emerging typologies and red flags they are observing, so as to enhance international awareness and knowledge of how bad actors are operating.

Public-private information sharing on a global scale will help to further enhance efforts to counter cyber crime. TRM has invested in platforms such as Chainabuse and Beacon Network to facilitate such information sharing:

- Chainabuse is a free fraud and scam reporting platform where members of the public can increase visibility of notable schemes and limit further victims by reporting the scams they come across. Victims can also choose to report scams and fraud directly to law enforcement and opt in for free personalised support on their case. Since its launch in May 2022, Chainabuse has received close to 350,000 reports, including approximately 55,000 ransomware related reports.

- Beacon Network is TRM's public-private communication network that enables law enforcement and virtual asset service providers to more rapidly collaborate during critical incidents, such as a hack, and accelerate the funds recovery process. Launched last November, the Beacon Network enables faster, secure communication between incident response teams by providing verified points of contact directly through the TRM interface.

We are actively working with law enforcement around the world, including in Australia, to enhance the use of these capabilities in bringing bad actors to task, and look forward to deepening these partnerships to support better cyber security outcomes globally.

2. Capacity building

The paper identifies the development of a skilled cyber security workforce in Australia as an area for potential action. The FATF echoes the importance of such specialist capabilities, particularly in the public sector, in its ransomware report:

"Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-specific techniques, to conduct ransomware-related money laundering investigations. Competent authorities should have the necessary specialised skills and expertise for successful financial investigations relating to ransomware. This includes development, access and training relating to blockchain analytics and monitoring tools."

We are heartened that the Australian Signals Directorate (ASD)'s REDSPICE Blueprint similarly demonstrates a keen awareness of the importance of intelligence capabilities, including a sizeable analytic workforce, to "help prevent strategic surprise, inform decisions of consequence and minimise miscalculation" as well as increase "understanding of adversaries' capabilities, intent and decision-making." This is further buttressed by the development of similar capabilities in other Australian law enforcement and regulatory agencies.

Given the prevalent use of virtual assets by cyber criminals, blockchain intelligence is a key area for capacity building in cyber intelligence and forensics. Blockchain intelligence demystifies the wealth of information on the blockchain and enables authorities to identify and stop bad actors from laundering illicit funds using virtual assets. At TRM, we increasingly see both public and private sector clients leveraging blockchain intelligence. TRM enables real-time monitoring of on-chain funds flow across more than 1m virtual assets and 27 blockchains, including many commonly exploited by cyber criminals, which our clients can use to identify and take timely action on suspicious transactions.

We believe that capacity building is very much a partnership. Our approach to blockchain intelligence extends beyond provision of tools, but training and working with our clients to enhance their understanding and effective use of these tools, including where necessary, direct partnerships for rapid incident response.

3. Incident response

In cyber attacks, time is of the essence and there may be instances where additional support is necessary to respond effectively to an incident, such as a ransomware attack on critical systems. TRM's globally-distributed Crypto Incident Response team, consisting of highly experienced former law enforcement officers including in Australia, can provide investigative assistance from case initiation through to case closure. Investigators assist customers in tracing stolen funds

(leading in some cases to asset recovery) and provide concierge services to connect victims to a global network of law enforcement agencies, cybersecurity firms and specialised law firms. Real-time information sharing between our investigative team and our clients also ensures the most timely and accurate approach to following the money, and increases the probability of asset recovery. Such incident response partnerships can also facilitate knowledge transfer to enable clients to better respond to any future incidents.

As Australia looks to strengthen its incident response functions, we stand ready to partner with private and public agencies to reinforce and strengthen incident response capabilities against crypto-enabled cyber crime.

In conclusion, the financial motivations driving cyber crime, along with the increasing use of virtual assets by cyber criminals, underline the importance of addressing these challenges as part of Australia's cyber security strategy. By leveraging blockchain intelligence, Australia can effectively trace and disrupt illicit flows through virtual assets, and deal an offensive blow to the pockets of cyber criminals. Strong public-private partnerships in areas such as information sharing, capacity building and incident response are crucial to maximise the effectiveness of these efforts. TRM looks forward to further engaging and collaborating with the Government to build a secure, resilient, and trustworthy digital environment for Australia.