FATF

FATF REPORT

Countering Ransomware Financing

March 2023

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2023), *Countering Ransomware Financing,* FATF, Paris,
http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.html

Table of contents

See also:

Countering Ransomware Financing: Potential Risk Indicators

This list of potential risk indicators complements the FATF report *Countering Ransomware Financing* and can help public and private sector entities identify suspicious activities related to ransomware.

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

Acronyms

AEC	Anonymity-enhanced cryptocurrency
AML/CFT	Anti-money laundering/Countering the financing of terrorism
CERT	Computer Emergency Response Teams
DeFi	Decentralised finance
DNFBP	Designated non-financial business and profession
FIU	Financial Intelligence Unit
IP	Internet protocol
LEA	Law enforcement agency
ML	Money laundering
OTC	Over-the-counter
PPP	Public-private partnership
RaaS	Ransomware as a service
STR	Suspicious transaction reports
VACG	Virtual Asset Contact Group
VASP	Virtual Asset Service Provider
VPN	Virtual private network

Executive Summary

The global scale of financial flows related to ransomware attacks has grown dramatically in recent years. Industry estimates report up to a fourfold increase in ransomware payments in 2020 and 2021, compared to 2019. New techniques have increased the profitability of attacks and the likelihood of success. These include the targeting of large, high-value entities as well as ransomware as a service, where ransomware criminals sell user-friendly software kits to affiliates. The consequences from ransomware attacks can be dire and pose national security threats, including damaging and disrupting critical infrastructure and services.

Through this study, the FATF aims to improve global understanding of the financial flows linked to ransomware and highlight good practices to address this threat. The report also provides a list of potential risk indicators that will help authorities and the private sector detect such financial flows. The findings of this report draw upon experience and expertise from across the public and private sectors, including inputs and case studies from more than 40 delegations across the FATF Global Network.

A ransomware attack is a form of extortion and the FATF Standards require that it be criminalised as a predicate offence for money laundering. This report finds that payments and subsequent laundering of ransomware proceeds are almost exclusively conducted through virtual assets. Ransomware criminals exploit the international nature of virtual assets to facilitate large-scale, nearly instantaneous cross-border transactions, sometimes without the involvement of traditional financial institutions that have anti-money laundering and counter terrorist financing (AML/CFT) programs. Criminals further complicate their transactions by using anonymity-enhancing technologies, techniques, and tokens in the laundering process, such as anonymity enhanced cryptocurrencies and mixers.

The near-exclusive use of virtual assets in ransomware-related laundering further reinforces the importance of accelerating the implementation of FATF Recommendation 15, which requires jurisdictions to put in place measures to mitigate risks linked to virtual assets and to regulate the virtual asset service provider (VASP) sector. These efforts are critical to prevent criminals from easily accessing VASPs located in jurisdictions with weak or non-existent AML/CFT controls to launder the profit from their crimes.

This report also finds that ransomware attacks are generally underreported, whether due to challenges in detection by the private sector, negative impacts to the victim's business or a fear of retaliation from criminals if a victim reports an attack. This partly explains the lack of experience in investigating money laundering related to ransomware. Jurisdictions need to carry out further work to increase and enhance sources of detection and reporting. Authorities need to move quickly to collect key information and should have the necessary tools and skills to effectively trace and recover virtual assets.

Ransomware cuts across a wide range of areas and investigations may involve actors outside the traditional AML/CFT authorities, including cybersecurity and data protection agencies. As such, a multi-disciplinary approach is required to effectively tackle ransomware and associated money laundering. Due to the inherently decentralised and transnational nature of virtual assets, building and leveraging existing international co-operation mechanisms is imperative to successfully tackling ransomware-related laundering.

To strengthen the global response against ransomware and related laundering, the FATF proposes that jurisdictions take the following actions.

Proposed Actions

The information gathered for this study provided some practical examples of actions that countries can take to improve their ability to counter illicit financial flows related to ransomware. This section summarises these good practices and makes suggestions for how jurisdictions could more effectively disrupt ransomware-related money laundering.

Implement relevant FATF Standards, including on VASPs, and enhance detection

- Jurisdictions should accelerate compliance with the relevant FATF Standards on the VASP sector by implementing Recommendation 15 (including the Travel Rule[1]) as soon as possible. This ensures that VASPs are complying with the necessary AML/CFT obligations to capture critical financial information and report suspicious transactions.
- Jurisdictions should ensure that ransomware is criminalised as a predicate money laundering offence in line with FATF Recommendation 3 (e.g., as a type of extortion).
- Jurisdictions should enhance detection of ransomware by:
  - Supporting regulated entities to detect ransomware and related money laundering and report suspicious transactions, including by sharing trends, detection guides, and red flag indicators (like those contained in *Countering Ransomware Financing: Potential Risk Indicators*[2]) with the relevant reporting entities.
  - Encouraging victims to voluntarily report incidents, such as by raising awareness of available support and resources or creating safe channels for reporting.
- Jurisdictions should also consider establishing channels of communications with non-traditional actors that may not be subject to AML/CFT requirements (such as cyber insurance and incident response companies) to increase sources of detection.

Promote financial investigations and asset recovery efforts

- Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-

1 The 'Travel Rule' is a key AML/CFT measure, which mandates that VASPs obtain, hold, and exchange information about the originators and beneficiaries of virtual asset transfers. This enables financial institutions and VASPs to conduct sanctions screening and to detect suspicious transactions.

2 Available at https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

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.

- Jurisdictions should ensure that law enforcement has, and maintains, the necessary abilities and powers to swiftly and effectively seize and confiscate assets, particularly for virtual assets. Jurisdictions should ensure that specialised mechanisms are in place to properly manage seized virtual assets.

Adopt a multi-disciplinary approach to tackle ransomware

- Jurisdictions should ensure that they identify and assess the money laundering risks posed by ransomware in their national risk assessments. Given the decentralised nature of virtual assets and ransomware criminal groups, this includes jurisdictions with virtual asset sectors where ransomware is not currently a domestic threat. Such findings can further help support national cyber strategies by achieving a holistic national overview of ransomware risks.
- Jurisdictions should develop co-ordination mechanisms across relevant competent authorities, ranging from law enforcement, AML/CFT and cyber-crime authorities, to non-traditional partners such as cyber-security or data protection agencies. This promotes information and intelligence sharing and provides a useful platform for cross-sharing of various technical expertise.

Support partnerships with the private sector

- Jurisdictions should identify and establish mechanisms that support public-private co-operation. Jurisdictions should consider the inclusion of VASPs and other non-traditional partners in such co-operation mechanisms. This creates useful platforms to raise awareness, exchange expertise and insights, as well as support law enforcement objectives.

Improve international co-operation

- Jurisdictions should establish and actively participate in bilateral, regional, and multilateral mechanisms, such as by using liaison offices and establishing clear 24/7 contact points, to facilitate rapid international co-operation and information exchange. This helps effectively support rapid cross-border funds tracing and effective asset recovery and helps authorities to successfully dismantle transnational networks engaging in ransomware and associated money laundering.

Introduction

Focus and scope

1. Ransomware is a type of malicious software (malware) that criminals develop and/or use to deny access to data, systems, or networks while demanding a ransom payment in exchange. Common attack methods include data encryption, data exfiltration, and disruption of victim operations. Attacks often involve more than one method and may include a threat to publish the victim's data.[3]

2. Ransomware incidents have grown significantly in recent years[4], both in number and scale. Ransomware is primarily a profit-seeking endeavour, and the growth in attacks has led to a consequent increase in ransomware proceeds and related money laundering. Industry estimates indicate that ransomware payments increased at least fourfold in 2020 and 2021 as compared to 2019.[5] While latest industry data suggest a downward trend in 2022 (potentially due to victims' refusal to pay), the value of virtual assets received by ransomware attackers remains significantly higher than prior to 2019.[6] The actual total number of attacks and related losses are likely to significantly higher as ransomware attacks often go unreported.

3. Attacks have caused major disruption and damage for governments, public institutions, businesses, and citizens, in some cases impacting healthcare and threatening national security, including requiring the stoppage of critical infrastructure and services or compromising sensitive data.[7] Ransomware criminals have developed techniques to increase the profitability of their attacks and likelihood of success. As a result, the threat of illicit financial flows related to ransomware will likely continue to grow.

4. Criminals demand ransomware payments almost exclusively in virtual assets. Victims, or related third parties acting on a victim, often use virtual asset service providers (VASPs)[8] to pay ransoms. Ransomware criminals also use VASPs to

---

3 FBI "Scams and Safety: Ransomware" (accessed September 2022), available at: www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; Australian Cyber Security Centre "Ransomware" (accessed September 2022), available at: www.cyber.gov.au/ransomware.

4. ENISA Threat Landscape 2022 (October 2022), available at www.enisa.europa.eu/publications/enisa-threat-landscape-2022

5 Chainalysis, "Chainalysis Crypto Crime Report 2022" (February 2022), available at: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

6 Chainalysis, "Ransomware Revenue Down As More Victims Refuse to Pay" (January 2023), available at: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

7 Attacks on hospitals, for instance, have jeopardized care for patients and attacks on police departments have impacted security.

8 Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer1 of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

launder illicit funds and exchange proceeds for fiat currency, which can be more easily exchanged for goods and services and is a more stable store of value.

5. In 2018, the FATF amended its Recommendations to cover virtual assets and VASPs. Since then, the FATF has issued various guidance to help jurisdictions and the private sector monitor and mitigate the risks in this sector, including red flag indicators of money laundering (ML) and terrorist-financing (TF).[9] While this work has often touched on ransomware, this report is the first time the FATF has focused specifically on laundering trends and techniques linked to ransomware attacks.

6. Under the Singaporean Presidency, the FATF is leveraging its experience on financial investigations involving virtual assets, to identify challenges and share good practices for countering ransomware financing and related ML. This report focuses on: how to identify and report ransomware-related payments; how to prevent, detect, and investigate ransomware financial flows; and how such proceeds are laundered. This report does not focus on the use of ransomware for terrorist financing given the lack of significant or notable use of ransomware for this purpose in the Information and case studies submitted for this report

7. As a ransomware attack is a form of extortion, the FATF Recommendations require all jurisdictions to criminalise ML related to ransomware (R.3). The FATF also requires jurisdictions to identify, assess and take steps to mitigate their ML risks (R.1-2); ensure the private sector, including VASPs, applies adequate preventive measures, such as reporting suspicious transactions (R.9-23); ensure law enforcement investigates, traces, and confiscates criminal proceeds (R.4, 29-31); and co-operate internationally to pursue ML and predicate offences, and associated proceeds (R.36-40).

8. While ransomware is one type of cybercrime, the information in this report is focused on ransomware and may or may not be applicable to other types of cybercrime, such as malware, phishing business email compromise or the compromise and sale of financial information.

Objectives and structure

9. Part I of this report demonstrates how ransomware criminals receive, launder, and cash out their illicit proceeds. It aims to raise global awareness and understanding of the scale of the global ransomware threat, how payments for or related to ransomware are made and how the proceeds related to ransomware attacks are made available to cybercriminals.

10. Part II identifies challenges and good practices in identifying, investigating, and disrupting ransomware-related financial flows.

11. This report intends to help **operational authorities** produce high quality financial intelligence, conduct financial investigations, and identify, trace, and seize illicit proceeds. **National regulators** and **policymakers** can use the information in this report to identify vulnerabilities and mitigate risks. It will also

[9] See: FATF (June 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers*; (September 2020) *Virtual Assets Red Flag Indicators*; and (August 2019) *Confidential FATF Guidance on Financial Investigations Involving Virtual Assets.*

help **financial institutions**, **VASPs**, and **designated non-financial businesses and professions (DNFBPs)** to design and implement controls to detect, report and prevent the illicit movement of ransomware-related proceeds.

Methodology

12. Experts from Israel and the United States co-led this project. In addition, the following jurisdictions and entities contributed to the work as part of the project team: Australia, Canada, the European Commission, France, Germany, Japan, Luxembourg, Mexico, Philippines, Singapore, South Africa, Spain, Switzerland, Türkiye, the United Kingdom, the Asia Pacific Group on ML, and the Egmont Group of Financial Intelligence Units.

13. The findings in this report are based on:

- A review of existing literature and open-source material on this topic.
- A request to the FATF's Global Network of over 200 jurisdictions for information on jurisdictions' perceptions of risk, national laws and powers, challenges and good practices, and case studies related to ransomware. In total, the project team received inputs from over 40 delegations.
- Discussions in the FATF's Virtual Assets Contact Group (VACG).[10]
- Targeted engagement with the private sector though the VACG.

[10] In June 2019, the Policy Development Group agreed to set up the Virtual Assets Contact Group to communicate the FATF's requirements to the private sector, and to ensure that the industry promptly develops appropriate technology solutions to implement them.

PART I. FINANCIAL FLOWS FROM RANSOMWARE

Scale of Financial Flows

14. The scale of ransomware attacks and related financial flows has grown dramatically across the globe. Many jurisdictions have seen an increase in the frequency of ransomware attacks in recent years, ranging from 10% growth to several hundred percent, depending on the jurisdiction. There has been a corresponding increase in reports by victims and a rise in suspicious transaction reports (STRs) related to ransomware across various jurisdictions. In one jurisdiction, STRs filed in the first six months of 2021 identified the equivalent of USD 590 million (EUR 552 million) in ransomware-related transactions, a 42% increase compared to 2020 when the total reached USD 416 million (EUR 389 million).[11] Recent annual reports by law enforcement organisations show substantial growth in ransomware activity[12], and industry estimates show similar growth in terms of the number of attacks and active ransomware strains. In 2021, the estimated number of ransomware attacks was around 623.3 million, more than double the 304.6 million estimated attacks in 2020.[13] Similarly, the estimated number of active ransomware strains is reported to have doubled from the number in 2019.[14]

15. While some jurisdictions reported low levels of ransomware attacks, the information gathered for this report shows that ransomware attacks remain underreported even though the number of STRs and reports by victims have increased in some jurisdictions. This makes it difficult to accurately estimate the total number of incidents and amounts paid in ransoms. Case studies submitted for this report showed that ransomware can be a risk for developed and developing jurisdictions, regardless of the region.

16. Several jurisdictions identified that the increase in ransomware attacks and related financial flows was associated with the development of techniques by ransomware criminals like **big game hunting**, **ransomware as a service (RaaS)**, **double/triple/multiple-extortion** tactics to maximise efficacy of attacks and the resulting profitability (See Box 1).

---

11 FINCEN, "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021" (June 2021), available at: www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis Ransomware 508 FINAL.pdf

12 FBI, "Internet Crime Report 2021" (accessed 1 December 2022), available at: www.ic3.gov/Home/AnnualReports; EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA) 2021" (accessed 1 December 2022), available at: www.europol.europa.eu/publications-events/main-reports/iocta-report

13 SonicWall, "2022 SonicWall Cyber Threat Report" (2022), available at: www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

14 Chainalysis, "Chainalysis Crypto Crime Report 2022" (February 2022), available at: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Box 1. Development of ransomware techniques

With **big game hunting**, ransomware criminals target large, high-value organisations or high-profile entities that they think are more likely to pay a ransom in order to resume business operations or avoid public scrutiny. Ransomware criminals also selectively target organisations operating in just-in-time supply chains, which are more likely to have higher costs of downtime, as well as critical infrastructure, and organisations holding sensitive or valuable information. Attackers may assess that these organisations have a higher propensity to pay ransoms compared to other victims.

RaaS refers to a criminal business model in which ransomware criminals provide ransomware software kits on the Dark Web or outsource elements of ransomware attacks, including distribution of malware, initial compromise of a victim's network, the exfiltration of data, or ransom negotiation for affiliates in exchange for a fee and/or a percentage of the ransom. Criminals can also purchase stolen credentials to access and exploit victim's systems which enable the distribution of ransomware and can obtain intelligence regarding specific industries in specific jurisdictions to inform their targeting and to maximise the effectiveness of their attack. The RaaS model has reduced the cost and necessary technical expertise to conduct ransomware attacks, lowering the barriers of entry and allowing less sophisticated criminals to conduct ransomware attacks.

Double-Extortion refers to a practice in which ransomware operators exfiltrate a victim's data before encrypting it and then threaten to publish the stolen data if ransom demands are not met. This threat of publication is in addition to the threat relating to the disrupted system. This tactic may put additional pressure on victims to pay ransom demands even if they are able to restore operations.

Triple-Extortion refers to a practice in which ransomware operators seek money not only from the victim that was first targeted, but also from a victim who might be impacted by the disclosure of the original targeted victim's data, such as protected health information, personally identifiable information, account credentials, and intellectual property.

Multiple-Extortion refers to a practice which involves more than two extortion methods. It is based on double-extortion using encryption and exfiltration but includes additional pressure tactics such as distributed denial-of-service (DDoS), contacting victims' customers, short selling victims' stocks, and disrupting infrastructure systems.

17. Over half of all reported ransomware attacks are against victims in the government/public sector, healthcare, and industrial goods and services sector, according to public information [15,16]. This is likely in part due to big game hunting, which may account for large pay-outs and an overall increase in ransomware payments. Ransomware criminals have also targeted energy, financial, communication, and education institutions in recent years. While ransomware criminals employing big game hunting tactics may focus on large victims, medium and small organisations and industries are also heavily targeted by ransomware attacks. In fact, ransomware attacks still predominantly target small and medium-sized enterprises. These smaller targets may have a more consistent risk to reward ratio compared to higher profile attacks against larger victims. In the second quarter of 2020, nearly 55% of total attacks took place against companies with fewer than 100 employees, and about 75% of attacks occurred on companies with less than USD 50 million (EUR 47 million) in revenue[17].

18. Ransom amounts range from hundreds of dollars or euros worth of virtual assets in small-scale cases targeting individuals, to the equivalent of millions of dollars or euros in cases targeting large corporations, especially critical infrastructure or organisations holding sensitive or valuable information. Jurisdictions' experiences indicate that the ransom amount requested by criminals has also grown in recent years. In 2021, the average ransom payment was around the equivalent of USD 800 000 (EUR 748 000) worth of virtual assets, nearly five times higher than in 2020[15]. This increase is likely related to the use of big game hunting techniques, noted above. In some cases, ransom demands have reached tens of millions of dollars or euros worth of virtual assets; for example, according to press reports, in 2021, a US-based insurance company was attacked by a 'Phoenix CryptoLocker' (reportedly the third biggest RaaS by revenue in 2021 after Conti and DarkSide)[18] and reportedly paid USD 40 million (EUR 37 million) to regain control of its network[19].

---

15 Sophos, "The State of Ransomware in State and Local Government" (September 2022), available at: https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state-of-ransomware-government-2022-wp.pdf.

16 Digital Shadows, "Ransomware: Analyzing The Data From 2020" (January2021), available at: www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/.

17 Coveware, "Q2 Quarterly Report" (August 2020), available at: www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

18 Chainalysis, "Chainalysis Crypto Crime Report 2022" (February 2022), available at: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

19 Mehrotra, Kartikay and Turton, William, "CNA Financial Paid $40 Million in Ransom After March Cyberattack," Bloomberg, 20 May 2021 (accessed 1 December 2022), available at: www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

Characteristics and Geographic Trends

19. Ransomware is generally an international phenomenon, due in part to the nature of both cybercrime and virtual assets. Information from the FATF Global Network, case studies, and industry data point to certain characteristics and geographic trends in ransomware attacks. Numerous ransomware networks have been linked to jurisdictions with higher ML risks (see Box 2). In many instances, ransomware criminals deposit or cash out their proceeds in these jurisdictions. In other cases, ransomware attacks were conducted from or potentially sponsored by these jurisdictions.[20]

Box 2. Jurisdictions with higher money laundering risks

While there is no universally agreed upon definition or methodology for determining whether a jurisdiction represents a higher risk for ML/TF, the consideration of country-specific risks, in conjunction with other risk factors, provides useful information for further determining potential ML/TF risks. Indicators of higher risk include: (a) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them; (b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling; (c) Countries that are subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations; and (d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, especially for VASPs, and for which VASPs and other obliged entities should give special attention to business relationships and transactions.

Source: FATF (2021) Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs, para.154

20. The scale of ransomware attacks differs by geography. Industry reports from 2022 indicate that the Middle East and Africa region was the least targeted by ransomware attacks (4%), followed by Latin America (6%), Asia-Pacific (10%), Europe (28%), and North America (52%).[21] The variation in scale across geographic regions has had an impact on how these regions perceive the risk they face from ransomware. Information provided by the FATF Global Network shows that jurisdictions witnessing increased big game hunting and associated

[20] See Alert (AA22-187A) from the U.S. Cybersecurity & Infrastructure Security Agency (July 2022), available at: www.cisa.gov/uscert/ncas/alerts/aa22-187a.

[21] Group-IB, "Ransomware Uncovered Report. Group-IB" (May 2022), available at: https://spiresolutions.com/wp-content/uploads/2021/07/ransomware_uncovered_2020.pdf.

high value ransoms are more likely to assess the risks of ML related to ransomware as high.

21. Many large ransomware groups operate a version of RaaS called the affiliate-model, in which they outsource elements of the ransomware attack in exchange for a fee and/or a percentage share of the ransom. In such cases, these criminals are often geographically dispersed, and it may be difficult to identify and locate involved parties in ransomware attacks. For example, as illustrated by the EMOTET case study below, ransomware criminals can co-operate on conducting attacks or use shared infrastructure while operating from different jurisdictions. The variety of criminals involved across various jurisdictions can also complicate the tracing of money flows associated with the key ransomware criminals.

Box 3. EMOTET case study[1]

EMOTET is one of the most significant malware campaigns in recent years. It was first discovered as a banking Trojan[2] in 2014, developing into a key tool for other malwares and ransomware. By the time of the takedown of the network in January 2021, EMOTET was enabling up to 70 per cent of the world's malwares, including RYUK and DoppelPaymer, which have had a significant economic impact on UK businesses. The takedown involved close work between LEAs of Canada, France, Germany, Lithuania, the Netherlands, Ukraine, the UK, and the US, with international activity co-ordinated by Europol and Eurojust. Through this collaborative partnership, domestic LEAs were able to pinpoint and analyse data linking payment and registration details to criminals who used EMOTET. The case exemplifies the scale and nature of cybercrime, proving how key international co-operation is to tackle the threat.

Source: United Kingdom

Notes:
1. See also Europol's press release on EMOTET, available at: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
2. A banking Trojan refers to a piece of malware that attempts to steal credentials from a financial institution's clients or gain access to their financial information.

22. The laundering of ransomware payments is also transnational given the cross-border nature of virtual assets, in which ransomware payments are almost always made. Users of virtual assets can transact peer-to-peer – transacting directly with each other, using only their private key and an internet connection, regardless of geographic borders and without the involvement of institutions with AML/CFT obligations. Criminals, including ransomware criminals with access to the internet can exploit these characteristics of virtual assets to facilitate large-scale, nearly instantaneous cross-border transactions without traditional financial intermediaries that have AML/CFT programs. They also have access to VASPs based around the world in jurisdictions with weak or non-existent AML/CFT controls, which ransomware criminals use to cash out their illicit proceeds in fiat currency.

Box 4. 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. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

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. As discussed below, many popular virtual assets operate on public blockchains, where pseudonymous transaction information is viewable.

Source: FATF

Common Methods and Trends

23. Conducting a successful financial investigation into a ransomware attack requires a sound understanding of the methods and techniques used to launder funds. As ransomware attacks are generally underreported, this report further gathered information from a variety of open sources as well as experiences from jurisdictions to obtain a better understanding on how ransom payments are made, laundered, received, and in some cases exchanged for fiat currency.

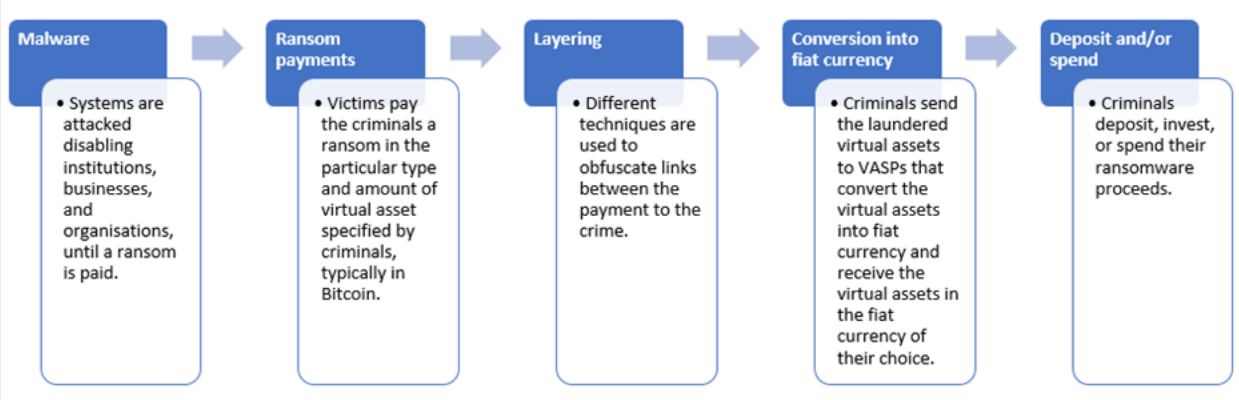
24. The financial flows related to ransomware often involve multiple traditional financial institutions as well as VASPs. Other third parties, such as cyber insurance companies, incident response companies, or cybersecurity companies may also be involved in the response to a ransomware attack, including the victim payment process.

25. While virtual assets are the primary method for ransomware payments, the overall financial flows related to ransomware involve multiple traditional financial institutions as well as VASPs and additional third parties.

Table 1. Types of sectors that may be involved in ransomware financial flows

Financial Institutions	Financial institutions usually act as intermediaries that ransomware victims (or a third party operating on the victim's behalf) use for transmitting funds to a VASP for the purchasing of virtual assets.
VASPs	Ransomware victims (or a third party operating on the victim's behalf) use VASPs to purchase and transfer the particular type and amount of virtual asset specified by the ransomware criminal.
Insurance Companies	Insurance companies may cover and sometimes pay ransom as part of the cyber insurance coverage.
Incident Response Companies	Incident response companies contracted by ransomware victims often negotiate the ransom payment with attackers. As part of their service, these companies may purchase the virtual assets from VASPs for the ransom payment and transfer them to the attackers on behalf of the victims.
Cybersecurity Companies	Companies that are responsible for safeguarding the client's data, systems, networks, and connected devices from any unauthorized and illegal access

Box 5. Typical financial flows related to ransomware payments:



Following a victim's receipt of the ransom demand, a victim or a third party operating on the victim's behalf will typically transmit funds via wire transfer, automated clearinghouse, or credit card payment to a VASP to purchase the type and amount of virtual asset specified by the ransomware criminal. Third parties, operating on the victim's behalf can include incident response or cyber insurance companies.

Next, the victim or third party will send the ransom payment, often from a wallet hosted at a VASP, to the perpetrator's virtual asset address. This is usually an unhosted wallet (a software or hardware that allows users to hold, store and transfer virtual assets outside a third party, such as a VASP; also referred to as a non-custodial wallet) controlled by ransomware criminal or a mule or a wallet hosted by a VASP situated outside of the jurisdiction where the attack occurred and that does not typically co-operate with LEAs or FIUs.

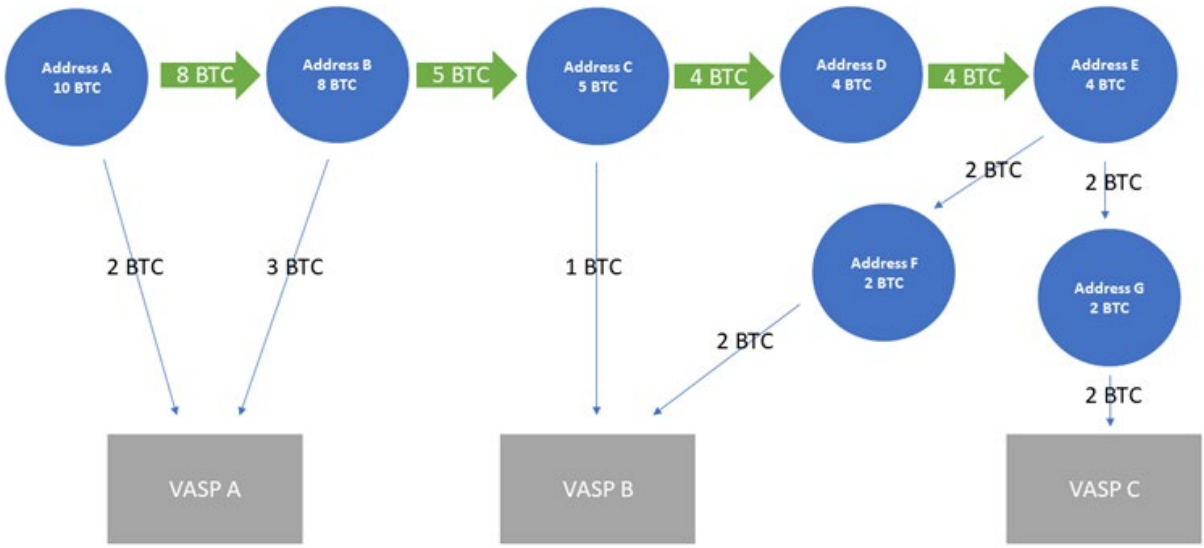
In many cases, the ransomware criminal will then use different techniques that can facilitate layering (described in more detail below). Finally, ransomware criminals often use VASPs located in jurisdictions outside of where they are based to exchange virtual assets for fiat currency, although they may also leave funds in unhosted wallets for long periods of time or use virtual assets to pay third parties involved in the attacks.

26. Ransomware criminals often use anonymity enhancing technologies, techniques, and tokens in the laundering process, including one or more of the below. Ransomware criminals may not use the same elements each time or follow the same order when laundering their proceeds.

- Ransomware attackers often demand that victim payments in virtual assets be sent to wallet addresses they control, and often **different wallet addresses** to receive illicit proceeds from each attack.
- After attackers receive funds, they can use multiple intermediate addresses to move the virtual assets from one wallet address using a series of transactions that transfer small amounts of virtual assets to new addresses in succession. The funds are often sent to wallet addresses hosted at more than one VASP. These transaction patterns are referred to as **peel chains** which are not

exclusively used to obscure the movement of virtual assets.[22] However, they may also be exploited by criminals to launder a large amount of virtual assets through a series of minor transactions with the aim to decrease the opportunity for this behaviour to be traced. In particular, the trail of the virtual assets can be obscured if the transactions are executed with a high speed and frequency of transactions.

Figure 1. Illustration of peel chains



- Ransomware criminals also often launder virtual assets through **mixers or tumblers** (e.g., Wasabi), which use various methods to conceal the connection between the address sending virtual assets and the addresses receiving virtual assets, either as an alternative or in addition to moving virtual assets through peel chains. In some cases, cybercriminals use CoinJoin transactions, in which multiple senders and recipients of funds combine their payments in a single aggregated transaction. This often requires a dedicated service such as JoinMarket that matches interested users and supports them in creating such transaction.
- Additionally, ransomware attackers also use **anonymity-enhanced cryptocurrencies (AECs; also called privacy coins)** even though most demand payment in Bitcoin. Jurisdictions' experiences and industry reports indicate that AECs are used to pay ransomware attackers, as they can obfuscate sending and receiving wallets. For example, AECs can use a combination of privacy-enhancing technologies such as mixers, ring signatures, stealth address, and ring confidential transactions all of which can obfuscate sending and receiving wallets. Increasing numbers of ransomware attackers ask for payments exclusively in Monero, although the most

[22] Peel chains are frequently observed and may occur naturally due to how virtual asset wallets are designed.

commonly used virtual asset in ransomware cases is Bitcoin (99%).[23] Some jurisdictions have seen cases where attackers accepted payments in both Bitcoin and Monero. However, they would charge an additional fee ranging from 10-20% of the demanded ransom for Bitcoin payments on the basis that such transactions are more easily traceable. As such, criminals will pay additional fees to use anonymity-enhancing technologies, like mixing services, to make it more difficult for authorities to trace or attribute transactions.

- Several jurisdictions also noted that cybercriminals often convert the ransom payment from Bitcoin to other virtual assets through VASPs or DeFi protocols.[24,25] This action is often referred to as **chain-hopping**, which refers to moving from one virtual asset into another different blockchain, often in rapid succession and with the aim of evading attempts to track these movements. One jurisdiction reported that ransomware criminals are increasingly using DeFi protocols to chain-hop into so-called stablecoins.[26] prior to exchanging funds into fiat currency. DeFi platforms are attractive to criminals because many do not implement AML/CFT controls, even though they may be subject to AML/CFT obligations depending on the facts and circumstances of their business models. One jurisdiction reported seeing the consistent use of DeFi protocols and mixers by ransomware criminals, sometimes used in succession multiple times in the ML process.
- During the laundering process, ransomware criminals often use centralised VASPs, including over-the-counter (OTC) traders to cash out of their proceeds. Ransomware criminals often send the virtual assets to a VASP in high-risk jurisdictions or a VASP with weak or non-existent AML/CFT controls for conversion into fiat currency. Criminals based in high-risk jurisdictions may be able to use local centralised VASPs for these purposes, as in the cases of U.S-designated VASPs, Suex,[27] Chatex,[28] Garantex[29] and Bitzlato Limited (see Box 6

23 Coveware, "Q3 Ransomware Marketplace Report" (November 2019), available at: www.coveware.com/blog/q3-ransomware-marketplace-report.

24 The term decentralised finance (DeFi) is used when decentralised or distributed Apps, enabled by a smart-contract provisioned blockchain, offer financial services, such as those offered by VASPs. A DeFi application (i.e., software programme) is not a VASP under FATF Standards, as the Standards do not apply to underlying software or technology. However, creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services.

25 In addition to being used to launder ransomware payments, DeFi protocols themselves, particularly cross-chain bridges, have been increasingly targeted by cybercriminals who seek to exploit security gaps and steal virtual assets.

26 Note on terminology: The FATF considers that the term "stablecoin" is not a clear legal or technical category but is primarily a marketing term used by promoters of such coins. In order to avoid unintentionally endorsing their claims, this report therefore refers to them as "so-called stablecoins".

27 See U.S. Treasury's press release, available at: https://home.treasury.gov/news/press-releases/jy0364

28 See U.S. Treasury's press release, available at: https://home.treasury.gov/news/press-releases/jy0471

29 See U.S. Treasury's press release, available at: https://home.treasury.gov/news/press-releases/jy0701

below).[30] Several jurisdictions reported that cash-out facilities are heavily concentrated in urban, central locations. In some cases, ransomware criminals from various groups used the same VASPs to receive or launder their virtual assets.

- In cases where multiple parties are involved, ransomware criminals typically have to pay criminal partners and infrastructure hosts. Increasingly, criminal infrastructure operators are willing to accept payment in virtual assets, and ransomware criminals frequently make these payments using proceeds from their attacks. In numerous cases, blockchain analytics firms have observed direct diversions of ransomware payments to virtual asset addresses associated with malicious criminal "infrastructure as a service" operators.

Box 6. Bitzlato Limited[1]

In January 2023, a transnational operation determined that Bitzlato Limited, a virtual currency exchange with significant operations in Russia, played a critical role in laundering Convertible Virtual Currency (CVC). The operation was led by the French and U.S. authorities, with the support of Europol, and the involvement of authorities from Belgium, Cyprus, Portugal, Spain, and the Netherlands. Bitzlato was suspected of facilitating various illicit transactions including for ransomware criminals such as Conti, a Russia-affiliated Ransomware-as-a-Service group. The U.S. Department of Justice also alleged that Bitzlato received more than $15 million in ransomware proceeds. In parallel, the U.S. FIU (Financial Enforcement Network) issued an order identifying the platform as a "primary money laundering concern".

These investigations allowed the dismantling of the exchange platform, including the seizure of digital infrastructure and criminal assets of EUR 18 million in crypto wallets in France, as well as the arrest of key individuals across various jurisdictions.

Bitzlato has marketed itself as requiring minimal identification from its users, and as a result of these deficient know-your-customer (KYC) procedures, Bitzlato allegedly became a haven for criminal proceeds and funds intended for use in criminal activity.

Source: France and United States

1. See also French National Gendarmerie's press release, available at: www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d-une-plateforme-de-cryptomonnaies-servant-au-blanchiment; as well as Europol's press release, available at: www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. Some jurisdictions also noted that ransomware criminals used **money mules** with accounts at VASPs to convert proceeds back into fiat currency by using off-

[30] See U.S. Department of Justice's press release, available at: www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million

ramps which are services/platforms that allow for the exchange of virtual assets for fiat currency (sometimes referred to as "cashing out"). Such accounts can be created using a stolen or fake identity or can be a legitimate account held by another party complicit in the account use. Money mules are typically un-associated third parties involved in the final stage of the ML process and are responsible for a portion of the overall funds flowing through a laundering process. Their disassociation from the criminal entity and their smaller value transfers can make them harder to identify.

Box 7. Example of money mule recruitment

Ransomware criminals recruit money mules and provide them with mobile devices. In most instances, these money mules have no Internet presence and little Internet literacy. Email accounts are then created at anonymous email service providers outside the jurisdiction, thus making it difficult to identify the users of the email accounts. Money mules utilise a mobile device provided by the criminal "handler" for the on-boarding processes and to create an account at the financial institution or VASP. After successful onboarding, money mules return the device to the criminal "handler". Criminal "handlers" use these devices on behalf of the money mule to conduct online transactions. In some instances, criminals take advantage of virtual private network (VPN) services, which anonymizes the Internet Protocol (IP) address of the device being used. As a result, the actual geographical location of the criminal who is conducting transactions remains hidden.

Source: South Africa

PART II. CHALLENGES AND GOOD PRACTICES IN DISRUPTING ML FROM RANSOMWARE

Legal Framework

28. A robust legal framework serves as a basis to enable competent authorities to develop effective ransomware risk mitigation policies. This section analyses the relevance of the FATF Standards to (i) the criminalisation of ransomware for ML and (ii) applying preventive measures to relevant regulated sectors.

Ransomware as a predicate offence to ML

29. While most jurisdictions do not have ransomware-specific criminal legislation, this generally does not prevent jurisdictions from criminally pursuing ransomware attacks as a predicate offence.[31]

30. Based on input from project participants, jurisdictions tend to pursue the predicate offence of ransomware either through extortion charges or, more commonly, as a computer-related crime, such as damage to data, intrusion or damage to computer programs and systems. FATF Recommendation 3 requires jurisdictions to criminalise ML related to extortion-related offences. Extortion offences typically have the benefit of being technologically neutral, meaning they can capture ransomware attacks regardless of the method or form. Jurisdictions using extortion offences should ensure that their laws remain relevant to allow competent authorities to effectively investigate and recover illicit virtual assets flows (see Section 6).

31. Unlike extortion, computer crimes are not included in the FATF's minimum list of predicate offences.[32] However, it does not appear that this has led to gaps in pursuing ML arising from ransomware activity in practice. Based on a sample of jurisdictions, those using computer crimes to pursue ransomware capture these offences as a predicate offence (either in the designated list of predicate offences, or via an 'all-crimes approach'). During this study, no jurisdiction reported problems pursuing ML related to ransomware. Nonetheless, jurisdictions should ensure that their choice of predicate offence charge does not inhibit their ability to pursue ML related to ransomware.

Applying preventive measures to relevant actors

32. The FATF Standards require jurisdictions to apply measures to prevent ML, including through financial institutions, DNFBPs, and VASPs. These measures ensure that these entities understand and mitigate their ML risks; apply

[31] Jurisdictions also mostly reported that they did not criminalise victims making ransom payments to the perpetrators of ransomware attacks, although some jurisdictions strongly discourage ransomware payments by victims

[32] See Designated categories of offences defined in the Glossary of the FATF Recommendations

appropriate controls, including identifying their customers; and detect and report suspicious transactions in line with FATF Recommendations 9 to 23.

33. Given the relationship between ransomware and virtual assets, the 2018 amendment to the FATF Standards to apply these measures to VASPs was an important step in enhancing the global AML/CFT regime against the risks posed by ransomware. However, as of January 2023,[33] of 86 jurisdictions that have been assessed against the revised Standards (Recommendation 15), 63 (73%) are partly or non-compliant with these requirements.[34] Only one of the 86 jurisdictions have been assessed as fully compliant.

34. Given the range of jurisdictions assessed against the revised Recommendation 15, it is likely that these figures are largely representative of the situation across the FATF Global Network. This assessment is further supported by findings from a March 2022 FATF survey, which found that in 2022 less than half of respondents had a licensing or registration regime for virtual assets and VASPs. As such, there are likely gaps in the application of AML/CFT obligations by VASPs, including identifying customers or reporting suspicious transactions, in majority of jurisdictions. Given the cross-border nature of virtual assets, it is important that jurisdictions across the Global Network accelerate compliance with Recommendation 15 (including the Travel Rule).

Proposed Actions

- Jurisdictions should accelerate compliance with the relevant FATF Standards on the VASP sector by implementing Recommendation 15 (including the Travel Rule) as soon as possible. This ensures that VASPs are complying with the necessary AML/CFT obligations to capture critical financial information and report suspicious transactions.
- Jurisdictions should ensure that ransomware is criminalised as a predicate ML offence in line with FATF Recommendation 3 (e.g., as a type of extortion).

[33] See consolidated assessment ratings, available at: www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Please note that not all jurisdictions have been assessed against the revised methodology on Recommendation 15.

[34] This analysis is based on mutual evaluation and follow-up reports of jurisdictions that have been assessed according to the revised methodology on Recommendation 15.

Detection and reporting

35. Due to the geographic distribution of ransomware criminals, their use of ML techniques and current characteristics of ransomware attacks (as discussed in Part I above), it is difficult to estimate the scale of financial flows derived from this phenomenon. In most jurisdictions, ransomware attacks remain underreported, making it difficult to develop a full picture of financial gains and financial flows relating to ransomware.

36. Robust detection and reporting provide a foundation for successful financial investigations (see Section 6 below). Based on jurisdictions' experience and case studies submitted, there are two primary sources for detecting ransomware-related financial flows: STRs and victim reporting. This section explores challenges and good practices in relation to the scope of STR reporting requirements; identifying suspicious transactions; encouraging victim reporting; and other sources of detections.

Scope of STR reporting obligations

37. Competent authorities commonly use STRs to detect ransomware attacks, and as a source of information during investigations. To date, the vast majority of STRs relating to ransomware payments are filed by VASPs and banks.

38. A small number of jurisdictions have identified sectors that are not typically subjected to AML/CFT obligations as additional potential sources for detection of illicit ransomware-related proceeds. Encouraging or requiring these non-traditional sectors to report suspicious transactions may be useful particularly when these sectors are directly involved in the resolution of ransomware attacks on behalf of clients.

39. For example, the broader insurance sector, particularly institutions involved in ransomware and cyber-insurance, may possess direct information on ransomware attacks involving cyber-insured clients making reimbursement claims. These entities are not captured by the FATF definition of "financial institution", which covers the underwriting and placement of life insurance and other investment-related insurance. However, by engaging with the sector to encourage or require reporting, some jurisdictions have seen an initial positive impact on ransomware related reporting.

Box 8. Targeted outreach to insurance sector to enhance ransomware filing

The non-life insurance sector is subject to AML/CFT requirements in France. In 2021, outreach was done to this sector through dedicated working groups, which gathered representatives across the public and private sectors. These working groups aimed to study the insurability of cyber risks and strengthened the resilience of companies against cyber-attacks. A key product that arose out of these working groups was a published report[1] which covers, among others, ransomware-related ML risk developments, as well as AML/CFT obligations and good practices relating to payment and reimbursement of ransoms made.

There was further specific supervisory scrutiny by the Prudential Supervision and Resolution Authority (ACPR) on insurance companies, including during on-site examinations. The ACPR subsequently reminded regulated entities of their AML/CFT requirements when engaging such services, including the need to monitor and obtain any relevant financial information (especially for payment tracing).

Since then, TRACFIN has observed an increased in STRs linked to ransomware payments filed by the insurance sector, from 28 in 2020 and 19 in 2019, to 66 in 2021. The increase in 2021 is partially due to a single insurance company and the volumes are not significant enough yet to draw any conclusions or outcomes.

Source: France

1. Available in French at www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. Incident response companies also have access to pertinent information related to ransomware attacks and payments. These companies, such as digital forensic incident response companies and law firms, help victims respond to ransomware attacks. They may facilitate ransomware payments to cybercriminals by negotiating ransomware payment amounts, converting customer fiat currency into virtual assets, and transferring the funds to criminal-controlled accounts. Encouraging or requiring reporting from this sector allows for the timely detection and reporting of ransomware attacks, especially as clients are likely to inform these entities of the attack at first instance (in some case before law enforcement). Depending on the business model and the services they are providing, these companies may also fall under the VASP definition (and consequently be subjected to AML/CFT and STR filing obligations) if they operate as a business for or on behalf of another natural or legal person exchange virtual assets for other virtual assets or fiat currency, transfer virtual assets, or safekeep or administer virtual assets.

Box 9. Regulating digital forensic and incident response (DFIR) companies

DFIR companies and cyber insurance companies (CICs) may assist ransomware attack victims in the course of providing services by facilitating ransomware payments. In 2020 and 2021, FinCEN (the U.S.' FIU) clarified in ransomware advisories[1] that, depending on facts and circumstances, this activity could constitute money transmission. Entities engaged in money transmission are required to register as a money services business and are subject to AML/CFT obligations. The advisories also included financial red flag indicators or ransomware and associated payments for DFIRs and CICs to support identification of suspicious activity and the filing of suspicious activity reports (SARs).

During the first-six months of 2021, filings submitted by U.S. based DFIR firms accounted for approximately 63 percent of ransomware-related SARs filed[2]. Overall ransomware-related filings received by FinCEN in 2021 also increased by 188 percent. These filings enabled FinCEN to analyse and uncover patterns and trend information to support whole-of-government efforts to prevent and combat ransomware attacks. For example, for all of 2021, FinCEN analysis found that ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, businesses, and the public. Moreover, the analysis highlighted that Russia-related ransomware variants were responsible for the majority of ransomware activity reported, accounting for 69 percent of ransomware incident value and 75 percent of ransomware-related incidents during the second half of 2021[3].

Source: United States

Notes
1. Available in French at www.banque-france.fr/sites/default/files/rapport_45_f.pdf
2. See FinCEN's Financial Trend Analysis, available at: www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
3. See FinCEN's Financial Trend Analysis, available at: www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. The above illustrates the utility of encouraging or requiring reporting from a broad range of non-traditional reporting entities, in line with risk and context. This allows suspicious activity to be reported and captured across different sectors' perspectives, which enhances authorities' abilities to uncover and detect otherwise unknown incidents by piecing together information across different sectors.

Measures to improve detection of suspicious transactions

42. Jurisdictions recognise that ransomware-related suspicious activities are likely generally underreported across sectors. Detection challenges may arise due to the geographically decentralised nature of ransomware criminal groups, the variety of criminals involved, and the use of different ML techniques. No one sector may be able to see the entire picture.

43. To improve the frequency and quality of reporting by regulated entities, and detection more broadly, jurisdictions have relied on varying methods such as private sector engagement as well as the development and sharing of red flag indicators and detection guides (see also Section 8.3 below).

Box 10. Israel Money Laundering and Terror Financing Prohibition Authority (IMPA)'s ransomware guidance paper

The IMPA, Israel's FIU, conducted a strategic analysis of unusual activity reports to identify characteristics of ransomware payments. This included information on the frequency and type of entities attacked, sums paid, type of virtual assets used and involvement of third parties. This resulted in the publication of a ransomware focused guidance paper which included red flags and case studies. The paper was published on IMPA's website[1], forwarded to all relevant reporting entities and was accompanied by an official press release.

Research findings were also presented on various occasions at public forums and professional conferences. The publication promoted, among other things, engagement with the Israeli incident response sector, thus paving the way to further expand such relationships and explore opportunities for future co-operation and information sharing.

Source: Israel

1. Only available in Hebrew at www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. In most cases where a VASP files a ransomware-related STR, it is filed based on a suspicion that virtual assets have been purchased to pay a ransom demand. Useful indicators that VASPs rely on include the victim's own statements to the VASP, purchases made by a known incident response company, as well as payments made that are linked directly or indirectly to a virtual asset address with exposure to ransomware likely identified through blockchain analytics. As VASPs act as a direct intermediary in many ransom payments, they are a key source of STRs on illicit financial flows related to ransomware. Please refer to *Countering Ransomware Financing: Potential Risk Indicators* for a compilation of relevant risk indicators on which VASPs may rely.

Box 11. Involvement of a crisis management company

IMPA received a STR via an Israeli VASP regarding a crisis management (incident response) company that purchased virtual assets (valued at tens of thousands of dollars at the time) intended to be used for a ransomware payment, on behalf of an undisclosed victim of attack. According to the STR, an additional amount of cryptocurrency was also purchased independently by a representative of the suspected target of attack from the same Israeli VASP.

IMPA's financial investigation discovered that the wallet address that received most of the funds had links to other ransomware attacks and received funds from other addresses. The accumulated funds were then transferred to a VASP located in a high-risk jurisdiction. In addition, the funds that were independently purchased by the company were transferred through several addresses, with a large portion ultimately funnelled through a mixer. An intelligence report was shared with relevant LEAs for further investigation.

Source: Israel

45. Unlike VASPs, banks and other financial and payment institutions may observe a victim transferring fiat currency to a VASP or a third party acting on the victim's behalf related to a ransom payment and can file a corresponding STR. However, they may not have direct insight into ransomware-related payments or related ML because most payments are made in virtual assets and not fiat currency. As a result, these financial and payment institutions may have very limited information on virtual asset addresses or source of funds, which makes the use of blockchain analytics difficult for them. To mitigate these challenges, these institutions in many cases require proxy indicators to identify potential ransomware payments. Based on case studies, common indicators include unusual transfers to VASPs (especially when the company does not typically deal in virtual assets), the purchase of virtual assets by cyber-security, insurance and incident response firms, clients' own statements that a bank funds transfer is being used to pay a ransom demand, as well as open-source information corroborating attack (e.g., news releases, reports of incidents, etc.). A detailed list of relevant risk indicators can be found in *Countering Ransomware Financing: Potential Risk Indicators*.

Victim reporting

46. Due to the low levels of suspicious transaction reporting on ransomware payments in most jurisdictions, STRs remain an insufficient source of detection or to understand the full scope of ransomware attacks and related ML, and support investigations. Hence, victim reporting is also an important source of information for detecting and investigating ransomware-related financial flows. Timely victim reporting is important to enable LEAs to act quickly to trace the financial flows and increases the likelihood for successful enforcement outcomes.

47. Incident reporting requirements vary by jurisdiction and are dependent on the legal framework of each jurisdiction. In most cases, incident reporting is voluntary. When victims report, they typically make them to the police, cyber security agencies or special cyber incident reporting units or to the local Computer Emergency Response Teams (CERT).

48. However, victim reporting is also found to be limited as attacks are underreported. There are a variety of reasons that may deter victims from voluntarily coming forward to report ransomware attacks due to perceptions of potential conflicts against their own business interests. This includes concerns over reputational damage, a desire to quickly restore operations, or fear of retaliation from the ransomware criminals. The nature of ransomware typically involves illicit access to personal and sensitive customer data. An admission of security or data lapses to LEAs or the public is perceived to negatively affect businesses and may result in civil lawsuits. Victims may also be threatened with public data leaks by criminals if LEAs are notified.

49. Additionally, victims may not have incentives to voluntarily report incidents post-ransom payment. In cases where victims have cyber-insurance, the victim may lack financial motivation to report an attack as the insurance firm may cover the cost of the payment. In some jurisdictions, victims may also not come forward after paying ransoms for fear of breaching national regulations (e.g., payments made to a sanctioned entity) or being deemed complicit to the criminal groups.

50. Jurisdictions have adopted a range of methods to encourage victims to report attacks. For example, some jurisdictions have implemented policies or conducted activities such as public campaigns to raise awareness on ransomware attacks and encourage reporting. These policies and activities typically also involve the private sector and serve to emphasise how authorities may be able to help mitigate the impact of ransomware attacks. This includes returning assets to victims and sharing decryption keys to recover data where available.

Box 12. No More Ransom[1]

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, and two industry partners with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals. The website contains a repository of keys and applications that can decrypt data locked by different types of ransomware. This helps victims to restore their access to their encrypted files or locked systems without having to pay.

The initiative pulls together numerous partners from the public and private sector across multiple jurisdictions, including law enforcement and IT security companies. It aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. The website further encourages victims to not pay any ransom and provides links to redirect victims to the reporting website of their country to lodge an incident complaint.

Source: No More Ransom

1. For more information, see www.nomoreransom.org/en/index.html

51. To counteract concerns about the reputational risk associated with reporting, some jurisdictions have sought to create safe environments for companies that are victim of a ransomware attack to come forward without fear of reputational harm, e.g., through regular engagements and attending business conferences. Another good practice is the creation of "one-stop" website portals as a singular source for victims to report incidents while serving as a resource hub for expert advice and remediation action. While these efforts often focus on detecting the ransomware attack itself, the information obtained from a victim report is vital to financial investigations, including tracing the associated financial flows and ML.

Box 13. Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (Cyber Centre) opened in 2018 as a key initiative under Canada's National Cyber Security Strategy. The Cyber Centre is the single unified source of expert advice, guidance, services, and support on cyber security for government, critical infrastructure owners and operations, the private sector, and the Canadian public. It offers resources to individuals and businesses including guidance on how to prevent and recover from ransomware incidents and reports on the threat landscape for ransomware. The Cyber Centre collects cyber incident reports from government and private sector stakeholders, both national and international. Reports can be made online, via email, or by phone. The Centre encourages reporting to the police if they believe a cyber incident is an imminent threat to life or of a criminal nature.

Source: Canada

52. Some jurisdictions have taken the approach of identifying certain industries or instances in which victim reporting is mandatory, e.g., for attacks on critical infrastructure (such as energy, communications, healthcare, etc.) or data leaks. In many jurisdictions, these industries may also include financial sectors subject to AML/CFT requirements (e.g., banking), where regulated entities are required to report significant incidents to competent authorities such as supervisors as part of the regulatory framework. Data protection frameworks may also encourage or require mandatory reporting for data breaches involving personal information, which may support timely detection. To enhance detection of illicit financial flows, it is a good practice to capture relevant financial information during such reporting (such as wallet address, type of virtual asset).

Other detection sources

53. As discussed above, exchanges and collaboration with stakeholders outside the financial institutions, DNFBP and VASP sectors, e.g., Internet Service Providers and the cyber-security sector, can be a potential valuable source of information. However, these sectors may not be subject to AML/CFT regulatory requirements, including STR reporting. In some cases, there may be a potential conflict of interest (e.g., cyber security firms acting on behalf of victims), which could limit proactive reporting. In such circumstances, information may be obtained through informal mechanisms such as public/private partnerships involving these entities, or via direct engagement.

Box 14. Collaboration with cybersecurity firm

A victim company contracted a cybersecurity company after suffering an attack from a ransomware group. A ransom was demanded either in Bitcoin or in Monero. The victim eventually paid the ransom to the criminal group through the cybersecurity firm.

The cybersecurity company subsequently informed the law enforcement office of this incident, which allowed authorities to trace the illicit flows. The office frequently collaborates with cybersecurity firms. The collaboration aims at minimal interference with the cybersecurity firms' recovery work for their clients but ensure that key elements such as IP and crypto addresses are provided for criminal investigations.

For this case, law enforcement observed the use of anonymization techniques such as the use of mixers and the use of numerous unhosted wallet addresses. At the time of the investigation, a significant part of the assets was kept into unhosted wallets and could therefore not be traced further. A significant part of the funds is reported to have been channelled through two VASPs in foreign jurisdictions.

Source: Switzerland

54. Competent authorities also detect ransomware attacks and payments through independent financial investigations using blockchain analysis on wallets known to have links to ransomware. This also includes monitoring of known attacks, blogs, and open-source analysis shared by blockchain analytics firms, as well as proactive contact with potential victims after analysis.

55. These efforts may reveal additional leads to previous ransomware attacks. It may also reveal insights on the magnitude of an attack attributable to a ransomware criminal as well as trends, typologies, and infrastructure that the criminals use to launder, receive, and use their illicit proceeds.

Box 15. Analysing open sources to identify RaaS criminals

FIU Türkiye received an STR from a VASP relating to a virtual asset wallet address linked to a person recorded as 'Name 1' by the VASP. An online search of the name found that there is a website in the same name. Further investigation showed that the website was carrying out activities related to Darknet and was serving as an intermediary in the sale of ransomware software and other malicious software.

Further analysis via open sources found that:

- The person involved in the transaction mentioned in the STR used a different nickname ('Name 2'). This led to the identification of the real name of the person ('Person X'). This person was previously a person of interest of the Police Department's Anti-Cyber Crime Branch.
- The suspect (Person X) was offering services and products such as unauthorised access, access to confidential information, fake identity credentials, hacking of social media accounts, sale of hacklinks and phishing pages.
- Payments for these illegal products/services were made with Bitcoin and other virtual assets.

Additional information was subsequently requested by FIU Türkiye from the VASP related to the person included in the STR, especially virtual asset wallet addresses, financial transactions (both virtual assets and fiat currency), and other personal information. An analytical report was prepared and submitted to the Cyber Crime Departments of Turkish National Police, suspecting that the person included in the STR was an intermediary in the sale of ransomware and other malicious software. Investigations are ongoing.

Source: Türkiye

56. Jurisdictions can also be alerted to ransomware attacks and payments through information shared by other jurisdictions. International co-operation, mutual legal assistance and informal information exchange with foreign jurisdictions may provide information on funds layered through domestic exchanges linked to foreign attacks/victims.

Proposed Actions

- Jurisdictions should support regulated entities to detect ransomware and related ML and report suspicious transactions, including by sharing trends, detection guides, and red flag indicators (like those contained in *Countering Ransomware Financing: Potential Risk Indicators*) with the relevant reporting entities.
- Jurisdictions should encourage victims to voluntarily report incidents, such as by raising awareness of available support and resources or creating safe channels for reporting.
- Jurisdictions should consider establishing channels of communications with non-traditional actors that may not be subject to AML/CFT requirements (such as cyber insurance and incident response companies) to increase sources of detection.

Financial investigation strategies

57. The goal of almost all ransomware attacks is to generate profit. Most jurisdictions recognise that ransomware investigations have a significant financial component. Case studies show that virtual asset tracing is a key part of ransomware investigations. In jurisdictions that reported investigating ransomware attacks, there is typically a parallel financial investigation tracing the ransom payment.

58. Globally, there is an observable lack of experience in investigations of ML related to ransomware. Very few jurisdictions have brought ML charges in ransomware cases. This may in part be attributable to the challenges in detection and reporting as discussed in Section 5 above.

59. This section explores specific challenges and good practices in successful financial investigations of ransomware and related ML, including (i) working with victims to access information; (ii) investigative techniques and mechanisms; and (iii) asset recovery.

Acting rapidly and working with victims to access information

60. Given the nature of cybercrimes like ransomware, successful law enforcement outcomes hinge on the ability to move quickly and collect key information related to the ransomware attack and payment. This includes virtual asset addresses, total amount of the ransom and type of virtual asset used, dates of transfers, types of services involved, identity of the victim, communications between victim and ransomware criminals, as well as any third parties involved with the ransom payment.

61. In many cases, the collection of such information depends on the co-operation of victims, or third parties involved in the incident response and/or ransom payment process. However, as discussed earlier, victims may be reluctant to

report incidents to law enforcement (see Section 5.3 above). Victims may also be reluctant to co-operate due to perceived competing interests with law enforcement; victims often want to resume commercial operations as soon as possible and may prefer to pay the ransom. They may also fear retaliation from criminals for involving law enforcement. Law enforcement on the other hand may require time to secure forensic evidence, develop controlled operations and take other investigative steps, which may delay the resumption of services.

62. Late or incomplete reporting, as well as the lack of co-operation from victims may compromise the quality of information available to successfully pursue and further investigations. The absence of a clear action plan for victims to undertake post-attack and/or payment may compromise available evidence due to the lack of data preservation. The good practices discussed in section 5.3, such as public campaigns and other efforts to encourage victim engagement are important to mitigate these challenges.

63. Some jurisdictions further highlighted the importance of sharing information between cyber (predicate) investigators and ML investigators. In the course of gathering forensic evidence for the predicate investigation of ransomware, law enforcement will inevitably gather information that is relevant to the ML investigation. Such information allows law enforcement to draw connections between different groups and affiliates of ransomware attackers, and provide follow-up leads to support a broader financial investigation. See Section 8.2 below for more information on how various domestic competent authorities can co-operate effectively.

Box 16. Relevant sources of evidence for financial investigations obtained during predicate investigations

Forensic evidence: Examples of forensic evidence include – Attack vectors (i.e., how criminals achieve unauthorised access); information on the ransomware strain; IP addresses; names or nicknames used; and the devices of the attacker. Such information may be gathered directly from victims, Internet Service Providers, cyber-security and incident response firms and the use of forensic technology.

Direct evidence from private sector: Relevant private sector companies include those that own the technology or infrastructure that was misused in a ransomware attack. Investigators may obtain subscriber information from email or social media companies with which the perpetrator may have held accounts for communications with the victim.

Open-source information: Review of open-source information, including social media, online forums, Darknet markets, and communications by ransomware criminals can help identify potential perpetrators.

Investigative techniques and mechanisms

Relevance of traditional investigative techniques

64. The technologies used by ransomware criminals to hide their locations, identities and financial flows can hamper investigations. Particular challenges include the use of VPNs, 'The Onion Router'[35] or encrypted email to allow increased privacy and security, and anonymous activity as traffic moves through a network. Such challenges can be further compounded due to the speed at which such technologies evolve.

65. FATF Recommendation 31 lays the foundation to provide LEAs the necessary powers for effective financial investigations. These traditional investigative techniques remain relevant to overcome these challenges to enable the collection and analysis of key information related to ransomware financial flows. This includes surveillance, intercepting communications as well as undercover operations. However, these traditional techniques will need to be adapted in the context of financial investigations involving virtual assets. Examples of how this can be done to achieve successful investigative outcomes include:

- *Surveillance*: Determining the types of electronic devices that a suspect is using; to detect any virtual wallets being used as well as their preferred methods of electronic communication.
- *Intercepting communications and undercover operations*: Developing insights into the subject's activities and workings of a criminal organisation, identifying individuals associated with the subject and relevant financial information and assets, as well as infiltrating criminal communities (like Darknet forums) to de-anonymise ultimate perpetrators and beneficiaries.
- *Production Orders:* Obtaining information from VASPs or other financial institutions involved in ransom payments, etc.

66. The use of these tools in financial investigations can be further informed by details obtained through STRs or victim reporting (see Section 5 above). Law enforcement may identify relevant financial institutions and VASPs through STRs and blockchain analytics (see section 6.2.2 below), to obtain the necessary evidence via production orders. VASPs can provide useful identifying information to support financial investigations related to ransomware to obtain basic and beneficial ownership and transaction information (e.g., user identity and related information, IP addresses, credit cards or bank accounts etc.).

67. However, as discussed in Section 3 above, some ransomware networks have also been linked to high-risk jurisdictions where there are weak or non-existent AML/CFT requirements for VASPs, or where VASPs often fail to meet the requirements. Hence, investigations may face complications if the funds move through or are held at these VASPs. In such instances, the VASPs may not collect relevant information at all or may be unresponsive to law enforcement requests.

68. Investigators face similar challenges when criminals use unhosted wallets. This provides users control of virtual assets without the involvement of a VASP, thereby presenting challenges to detecting and preventing ML activity. The lack

[35] Also known as TOR, it is an open-source software that allows users to surf the Internet anonymously.

of a connection to a third-party entity (and one that should be registered/licensed under the FATF Standards) can complicate authorities' ability to identify the owner of the wallet as there is no external party from which to seek information.

69. The limited implementation of the FATF 'Travel Rule' by VASPs also provides opportunities for cyber criminals to avoid detection and hinder investigations. The Travel Rule requires VASPs and other financial institutions engaging in virtual asset transfers to share information on the sender (originator) and the recipient (beneficiary) alongside any transfer. This increases transparency in transactions to prevent criminal misuse and is a source of information that law enforcement can access to identify the parties involved in a given transaction. However, a FATF report from 2022 found that only one third of jurisdictions report having passed legislation to implement the Travel Rule for VASPs, and even fewer are actually enforcing these requirements.[36] This lack of consistent regulation reduces the amount of information available to law enforcement from VASPs in jurisdictions without Travel Rule obligations. It also means that VASPs in compliant jurisdictions transacting with VASPs in non-compliant jurisdictions will not likely be able to obtain this information, limiting the information available to investigators even in jurisdictions that implement the Travel Rule.

[36] FATF (June 2022) *Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers.* The Targeted Update only covers countries whose MERs/FURs published from June 2021 and May 2022

Box 17. Traditional and financial investigative techniques against ransomware group

An Italian victim company lodged a police complaint after making a Bitcoin ransom payment and successfully unlocking their data that was infected by a ransomware attack. The payment was performed through a VASP mentioned in the ransom request.

Police investigations against the VASP found its website to be formally registered in Italy. An Italian subject was subsequently identified and was discovered to have facilitated the Bitcoin flows linked to the ransom payment. The police subsequently searched his apartment and seized payment cards, mobile phones, as well as hardware items such as hard disks, USB drives and tablets. Phone tapping and analysis of mobile phone messages exchanged resulted in the identification of a group of further Italian subjects (the "Group") who played similar roles in facilitating ransomware-related Bitcoin flows. Financial investigations found that the fiat funds sent by the ransomware victims were transferred by the Group to foreign bank accounts maintained by foreign VASPs, including those located in high-risk jurisdictions.

Based on the financial investigations, as well as forensic analysis of the phones and the hardware items, the authorities concluded that the Group was spreading ransomware to victims, with ransom amounts of several hundred euros for each attack. The Group has been charged for ransomware-related extortion and the subsequent laundering of proceeds, which were estimated to total around EUR 300 000 across various victims. Investigations are currently still ongoing.

Source: Italy

Virtual asset-specific techniques

70. In addition to traditional techniques, law enforcement should rely on virtual asset-specific techniques to conduct ransomware-related financial investigations. Most virtual assets operate on a public blockchain, which acts as a viewable database through which pseudonymous information associated with virtual asset transactions can be traced, using open-source or subscription blockchain analysis tools (see Section 7 below). Blockchain analysis, combined with traditional investigative techniques, may allow investigators to obtain the information necessary to identify online ransomware criminals and their affiliates, as well as trace the movement of illicit proceeds.

71. Tracing proceeds using blockchain analytics usually requires identifying an initial wallet address, which makes detection and collection of ransom payment information a critical first step. Once an initial wallet address is provided, investigators can identify payments made from and received by that wallet address, among other capabilities. However, the information available may depend on the service being used. While the public blockchain does contain useful information for financial investigations, some virtual asset transactions also occur off-chain. Certain blockchain analytics further rely on clustering

algorithms and other techniques to group wallet addresses or transactions that may be associated with criminality, such as ransomware.

72. Information from blockchain analytics can further inform the use of traditional investigative techniques. For example, blockchain analytics could help identify a VASP hosting a wallet address that received a payment sent to or from ransomware criminals, which could prompt LEAs to use compulsory methods to request information on the wallet address from the VASP in question.

Box 18. Investigations into known ransomware wallets revealing additional unknown victims

Online blockchain threat analysis had been ongoing relating to a Bitcoin address, which was known to receive approximately 20 Bitcoin between 12 May 2017 and 27 May 2021. It was discovered that the said Bitcoin address could be directly linked to ransomware that infected several business entities and government departments in South Africa. Analysis revealed that a separate local Bitcoin address, which belonged to a VASP in South Africa, provided 0.06 Bitcoin to the aforementioned address under investigation in February 2018.

A victim was identified after obtaining subscriber information from the VASP, who acknowledged that he suffered financial loss. He preferred not to report the incident to local investigative authorities as he feared public embarrassment for poorly securing customer data. The matter was referred by FIU South Africa to local investigative authorities. Because the identified victim did not want to lay any criminal charges, the case was withdrawn and closed by local law enforcement.

Source: South Africa

73. The anonymity enhancing laundering methods used by ransomware criminals (discussed in Section 3 above) also present challenges to law enforcement authorities to trace and attribute transactions using blockchain analytics, although some blockchain analytic companies have developed technology to mitigate some of these measures. Affiliate models or RaaS providers, as well as the involvement of money mules also increase the complexity of financial investigations related to ransomware. Since the payments cannot always be traced to the victim, it becomes difficult to identify the addresses used for the initial payment of virtual assets which typically serves as a lead for the blockchain analysis.

74. Beyond using blockchain analytics to trace the payment from the ransomware attack and its subsequent laundering, investigators should also trace the prior transactions associated with the ransomware group. This additional step allows law enforcement to identify potential trends and typologies, and/or additional criminality.

75. As a good practice, law enforcement authorities in some jurisdictions have developed databases of key information on mules or wallet addresses involved in ransomware cases. These databases typically include data on incidents,

identifying information of mules, damage amount, and ransomware criminals (e.g., account number, wallet addresses, usernames). Such databases help identify and trace ransomware payments and related ML by providing a repository to match prior investigative leads (including payment information) to existing and future incidents. This allows law enforcement to understand the wider laundering network that may cut across various regulated entities and sectors.

Asset recovery

76. In addition to enhancing detection and financial investigative capabilities, law enforcement authorities also need the legislative powers and capacity to seize and confiscate virtual assets. Virtual assets transactions are near-instantaneous. This means that as soon as competent authorities are made aware of a ransomware attack and ransom payment, they must be able to quickly trace the ransom payment and have access to rapid freezing powers, ideally within a matter of hours, to prevent dissipation. In line with FATF Recommendation 4, such powers should already exist in many jurisdictions and can vary in form.

77. Several jurisdictions also highlighted the usefulness of alternative tools for intercepting illicit proceeds, such as FIU postponement powers, in dealing with suspected criminal assets identified in STRs. To keep pace with the dynamic nature of virtual assets, there may also be a need to consider updating existing asset forfeiture legislation, regulations, and policies and procedures.

Box 19. Colonial Pipeline

In June 2021, the U.S. Department of Justice announced that it had seized 63.7 bitcoins valued at approximately $2.3 million. These funds allegedly represented the proceeds of 8 May 2021 ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation. The seizure warrant was authorized by a judge in California earlier that day.

On or about May 7, 2021, Colonial Pipeline was the victim of a highly publicized ransomware attack resulting in the company taking portions of its infrastructure out of operation. Colonial Pipeline reported to the Federal Bureau of Investigation that its computer network was accessed by an organization named DarkSide and that it had received and paid a ransom demand for approximately 75 bitcoins. As alleged in the supporting affidavit, by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address. This bitcoin represents proceeds traceable to a computer intrusion and property involved in ML and may be seized pursuant to criminal and civil forfeiture statutes.

Source: United States

Proposed Actions

- Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-specific techniques, to conduct ransomware-related ML investigations.
- Jurisdictions should ensure that law enforcement has, and maintains, the necessary abilities and powers to swiftly and effectively seize and confiscate assets, particularly for virtual assets.

Skills and expertise

78. As discussed in Section 6.2, while traditional law enforcement techniques remain critical for ransomware-related ML investigations, specialised technical expertise is also required for successful ML investigations and prosecutions as well as asset recovery relating to virtual assets. This includes technological and legal knowledge of the virtual assets' ecosystem.

79. Additionally, investigative teams working on ML cases or asset recovery related to ransomware should include personnel with technical skills in cybersecurity, computer forensics, online intelligence, and open-source platforms. This should include a focus on online reconnaissance to gather financial information pertaining to virtual asset transactions within the public domain, including information that can be identified from blockchain analytics, the scanning of websites, social media, on-line forums, the Darknet and dark markets, as well as online abuse reports.

80. Particularly where virtual assets are involved, competent authorities may need new skills and expertise to interpret and access information. Specifically, authorities need to develop familiarity with blockchain analytics and monitoring capabilities, such as the use of blockchain analytic tools, including free software to view the public blockchain, and analytics to trace funds. Additionally, different tools provide varying and complimentary capabilities (analysis of different types of virtual assets, ability to analyse chain hopping, open-source intelligence, etc.).

81. Specialised training and technical expertise are required to develop these various tools and use them during investigations and some jurisdictions have identified ways to integrate specialists into relevant investigations (see Section 8.2). Access to the required resources can be expensive and some jurisdictions may lack the resources necessary to support the development of these skills, which can hamper authorities' ability to pursue ML related to ransomware.

82. If in-house expertise is unavailable or insufficient, jurisdictions may consider using tools created by private sector companies. Third-party tools can help authorities to identify, trace, and attribute virtual asset transactions on all major and most minor virtual asset blockchains. Currently, these tools support hundreds of tokens and use methods such as clustering algorithms, web

scraping, and scam database monitoring that enable an investigator to link and attribute a wide range of transactions to real-world individuals and entities. The tools generate transaction graphs and enable network analysis, which allow agencies to understand and then present the complex associations to juries and courts in subsequent prosecutions and asset recovery actions. These tools can also help authorities identify VASPs that may have been used to launder or exchange illicit proceeds for fiat currency and that could have relevant information to support the investigation.

83. In terms of asset recovery, the seizure and management of virtual assets require additional technical and legal expertise. Authorities must be prepared to take appropriate steps and implement procedures to ensure proper seizure and storage. It is a good practice to establish specialised mechanisms to seize, confiscate and dispose of virtual assets. This may include proper seizure planning, managing seed phrases[37] and cold storage of seized virtual assets (i.e., storing them in an offline unhosted wallet), as well as chain-of-custody issues.

Proposed Actions

- 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.
- Jurisdictions should ensure that specialised mechanisms are in place to properly manage seized virtual assets.

National Policies and Co-ordination

National assessment and strategy

84. FATF Recommendation 1 requires jurisdictions to identify and assess their ML risks and apply a risk-based approach to mitigate those risks. This approach should also serve as the foundation for jurisdictions to efficiently allocate resources across their AML/CFT regime.

85. Ransomware is often approached from a cyber-security threat assessment perspective. For instance, at the national level, some jurisdictions have enacted national strategies on cybersecurity or cybercrime, which support domestic co-ordination and provide the political commitment to actively pursue ransomware and associated illicit financial flows. National strategies typically involve various governmental agencies,[38] and may include relevant AML/CFT authorities such as the justice, finance, and interior ministries as well as the private sector. It is important to note, however, that the purpose of many of these strategies is not

[37] A set of words randomly generated by a wallet application and listed in a specific order that can be used to recover or gain access to a its private key(s) bypassing additional (e.g.: password) protection.

[38] These agencies include those focused on law enforcement, defence, security, and information communication given the national security threat posed by ransomware.

necessarily focused on illicit finance risks, which should be considered in detail through a risk assessment.

Box 20. National Cybersecurity Strategy of Spain

The National Cybersecurity Strategy of Spain (last updated in 2019) aims to strengthen skills to fight cyber threats. It lays out the priorities, objectives, and appropriate measures to achieve and maintain a high level of security for networks and information systems. Some of the key action lines of the Strategy seek to strengthen skills to fight cyber threats and reinforce capabilities to investigate and prosecute cybercrimes.

The Strategy established the need to strengthen legal and police co-operation, with sufficient resources assigned to competent bodies and professional skills training. This is also linked to the creation of an institutional framework for cybersecurity, which established the National Cybersecurity Council. This Council is led by Spain's Prime Minister with the aim to co-ordinate the national Security policy on cybersecurity and to promote the co-ordination, collaboration, and co-operation among public administrations bodies[1] and the private sector[2], which plays a relevant role for a multi-disciplinary approach.

Source: Spain

Notes
1. Ministries of Foreign Affairs, Justice, Defense, Home Affairs, Treasury, Presidency; the National Intelligence Centre, the National Security Department, and others.
2. Private sector experts include those from professional associations, companies, and academia.

86. Jurisdictions should ensure that they also consider the threat posed by ransomware as part of their national ML risk assessment in line with FATF Recommendation 1. This assessment provides the basis on which jurisdictions can build mitigating measures – including implementing the suggested actions contained in this report. By understanding the ML risks associated with ransomware, jurisdictions will be able to allocate resources in line with a risk-based approach, including to develop virtual asset technical skills and expertise and acquire blockchain analytic tools for relevant AML/CFT competent authorities.

87. Jurisdictions where ransomware and related ML does not currently pose a significant domestic threat should also consider the illicit financing risks posed by ransomware, particularly due to the unique relationship between ransomware and virtual assets. Jurisdictions should consider not only the threat of ransomware attacks on domestic victims, but also the potential that ransomware criminals are based in their jurisdictions or that VASPs in their jurisdiction are being used to launder or cash out ransomware proceeds. For example, many VASPs may have distributed architectures across several jurisdictions, such as registering in one jurisdiction, having personnel located in another jurisdiction, and hosting technical infrastructure or private keys in

separate jurisdictions. This means that such jurisdictions could still be exposed to the illicit financial movements linked to ransomware, particularly through the VASP sector.

Box 21. Assessment of ransomware in national ML risk assessments

The United States in March 2022 published its third National Money Laundering Risk Assessment (NMLRA), which highlights the most significant illicit finance threats to include cybercrime as well as vulnerabilities related to virtual assets. The NMLRA identified that incidents of cybercrime significantly increased since 2018, and that ransomware presents a particularly significant illicit finance threat. For example, the NMLRA found that the severity and sophistication of ransomware attacks rose through the COVID-19 pandemic. The NMLRA provides substantive information about ransomware attack trends, including the use of ransomware as a service model and double extortion tactics. The NMLRA also highlights numerous ML typologies, such as the use of foreign VASPs with weak or non-existent AML/CFT controls for ransomware-related deposits. The NMLRA findings informed the United States 2022 National Strategy for Combatting Terrorist and Other Illicit Finance, which provides recommendations for addressing illicit finance risks, and the Action Plan to Address Illicit Financing Risks of Digital Assets.

Source: United States

National co-operation and co-ordination

88. FATF Recommendation 2 requires jurisdictions to have domestic mechanisms for policy makers, the FIU, LEAs, and other competent authorities to co-operate, co-ordinate and exchange information. Ransomware cuts across a wide range of areas and investigations may involve actors outside the traditional AML/CFT authorities, including cyber-security and data protection agencies. Effective domestic co-ordination mechanisms are vital to bring together relevant information and different experts, including from the private sector, to ensure a holistic response to mitigate the threat posed by ransomware and associated ML. This further allows the critical exchange of information between enforcement authorities conducting forensic predicate investigations and parallel financing investigations.

89. A good practice is the creation of law enforcement teams or multi-disciplinary bodies dedicated to cybercrime (or even ransomware specifically). These bodies can co-ordinate investigations into ransomware and related ML that require a broad range of expertise (e.g., FIU or LEA experts, prosecutors, technical engineers, negotiators, etc.). This approach typically includes law enforcement officials with expertise in virtual assets tracing and may be a useful way to centralise specialised technical expertise, particularly in the face of limited resource or capabilities.

Box 22. Co-ordination mechanisms to centralise intelligence and investigative expertise

To address the evolving cyber challenge, the U.S. Government established the National Cyber Investigative Joint Task Force (NCIJTF) in 2008. The NCIJTF is comprised of over 30 partnering agencies across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organisation's mission from a whole-of-government perspective.

As a unique multi-agency cyber centre, the NCIJTF has the primary responsibility to co-ordinate, integrate, and share information to support cyber threat investigations, supply, and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation.

In late 2014, the NCIJTF created the Virtual Currency Team (VCT) which focused its efforts on tracing cryptocurrency transactions related to cybercrimes. This team provide cryptocurrency tracing to all members of the NCIJTF. As a part of their own investigative efforts, NCIJTF members such as the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) established their own individual teams to trace virtual assets as their use increased in various types of crimes.

In early 2022, the FBI created the Virtual Assets Unit (VAU), a nerve centre for the FBI's virtual currency programs where intelligence, technology, and operational support will flow to other divisions. In the VAU, virtual asset experts and cross-divisional resources are embedded in a task force setting to seamlessly integrate intelligence and operations across the FBI.

Source: United States

Co-operation with and guidance for the private sector

90. As discussed in Section 5.2, engagement with the private sector is useful to mitigate some of the challenges identified in this report. For example, regulated entities may face difficulties in detecting and identifying ransomware-related suspicious transactions. Some jurisdictions have seen success in enhancing the frequency and quality of ransomware-related STR reporting by engaging and providing guidance to reporting entities, including red flag indicators (see Countering Ransomware Financing: Potential Risk Indicators, FATF, 2023) and detection guides.

Box 23. Australia's Financial Crime Guides

Australia's Fintel Alliance[1] publishes a range of resources, including financial crime guides, to help businesses understand, identify and report suspicious financial activity to detect and prevent criminal activities.

Financial crime guides provide detailed information about the financial aspects of different crime types. They include case studies and indicators to help the financial services sector identify and detect suspicious transactions.

To assist the fight against ransomware, in April 2022 AUSTRAC released financial crime guides focused on the criminal abuse of digital currencies and detecting and stopping ransomware. These two guides provide practical information and key risk indicators to help detect and respond where someone could be the target of a ransomware payment or trying to profit from a ransomware payment. Both financial crime guides are available on the AUSTRAC website:

- Detecting and stopping ransomware payments | AUSTRAC
- Preventing the criminal abuse of digital currencies | AUSTRAC

Source: Australia

1. Fintel Alliance is Australia's public-private partnership and brings together experts from a range of organisations involved in the fight against money laundering, terrorism financing and other serious crime. Fintel Alliance partners include major banks, remittance service providers and gambling operators, as well as law enforcement and security agencies from Australia and overseas.

91. The form and degree of collaboration with the private sector to combat ransomware varies between jurisdictions. Public-private partnerships (PPPs) are a useful and commonly understood model, although in many jurisdictions these remain focused on traditional stakeholders (particularly banks and other financial institutions, although there is increasing involvement of DNFBPs). The specific composition will differ depending on the aims and objectives of the PPP but may include non-traditional stakeholders. In the context of effectively preventing and detecting ransomware, PPPs should be used to bring together law enforcement authorities, the local CERT, the FIU, and VASPs, in addition to cyber security companies, telecommunication providers, and blockchain analytics companies (for example, as a sub-group or operational arm of an existing PPP).

92. Common objectives of such PPPs include raising participants' awareness of ransomware and related ML, sharing information on current trends, and exploring new and existing threats. These mechanisms can also foster stronger relationships with the private sector and can encourage reporting.

93. Jurisdictions have also leveraged PPPs to achieve various law enforcement objectives. PPPs provide a useful platform to share tactical leads to generate

intelligence, allow information-sharing to enhance detection of mule and laundering networks across various regulated sectors, and advance investigations.

94. As VASPs hold information vital for successful law enforcement outcomes (including wallet ownerships and withdrawals in fiat currencies), developing co-operative relationships with this sector can also enable authorities to quickly access information for virtual asset tracing as well as effective asset seizure and confiscation.

Box 24. INTERPOL's Project GATEWAY and Operation Cyclone

Project GATEWAY is a framework for data sharing with private entities which commenced in 2016 for information exchange in relation to cybercrime. The project boosts law enforcement and private industry partnerships to generate threat data from multiple sources and enable police authorities to prevent attacks. The entities that form part of Project GATEWAY are players relevant in the cybercrime ecosystem. These include cybersecurity companies, threat intelligence companies, VASPs, and banks.

The framework enables the provision and receipt of cybercrime information between INTERPOL and the private sector and allows the private sector to provide assistance to INTERPOL for cybercrime analysis. Private sector partners are used for their technical expertise to help to determine the type of ransomware infection, if unknown, as well as analysis on any of the potential attribution leads.

Operation Cyclone[1] follows global police investigations into attacks against Korean companies and US academic institutions by the Cl0p ransomware threat group. The global operation in June 2021 resulted in arrests of six members of the notorious ransomware family, and was co-ordinated by INTERPOL with Korean, Ukrainian and US law enforcement authorities. The suspects are thought to have facilitated the transfer and cash-out of assets of more than USD 500 million on behalf of the ransomware group. INTERPOL deployed Operation Cyclone with the assistance of information provided by its private partners through INTERPOL's Gateway project.

Source: INTERPOL

1. For more information, see: www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring

Proposed Actions

- Jurisdictions should ensure that they identify and assess the ML risks posed by ransomware in their national risk assessments. Given the decentralised nature of virtual assets and ransomware criminal groups, this includes jurisdictions with virtual asset sectors where ransomware is not currently a domestic threat. Such findings can further help support national cyber strategies by achieving a holistic national overview of ransomware risks.
- Jurisdictions should develop co-ordination mechanisms across relevant competent authorities, ranging from law enforcement, AML/CFT and cyber-crime authorities, to non-traditional partners such as cyber-security or data protection agencies. This promotes information and intelligence sharing and provides a useful platform for cross-sharing of various technical expertise.
- Jurisdictions should identify and establish mechanisms that support public-private co-operation. Jurisdictions should consider the inclusion of VASPs and other non-traditional partners in such co-operation mechanisms.

International co-operation

95. Ransomware attacks and the related financial flows are often transnational and multinational. Ransomware criminals are generally based in a different jurisdiction than the multiple jurisdictions through which funds (particularly virtual assets) are laundered and ultimately 'cashed-out'. The complexity and challenges of ML schemes related to ransomware require ongoing cross-border co-operation between law enforcement authorities with relevant information, tools, and expertise. Building and leveraging existing mechanisms for international co-operation is imperative for successful financial investigations and asset recovery particularly for ransomware.

Box 25. Joint international investigation against Lockergoga strain

A ransomware attack occurred on January 2019 against a major French company. Lockergoga malware was identified as the ransomware strain used to encrypt several files and internal servers of the company. While a ransom of 410 Bitcoin was requested after negotiation, the company did not pay the ransom. However, the Lockergoga strain was also found to have been employed by hackers in numerous other attacks.

A joint investigation team was formed under Eurojust/Europol together with several European jurisdiction. This resulted in the efficient sharing of information, including juridical co-operation through European

Investigative Orders (EIO) and Mutual Legal Agreement Treaty (MLAT), which helped to expedite investigations. Europol/Eurojust also provided technical support with large capacity of hardware and funding. A criminal command and control infrastructure was subsequently identified, with messaging flows of the hackers decrypted and the group was finally found to be located in an eastern jurisdiction. This allowed for several arrests to be made in the said jurisdiction.

Investigations are ongoing. Through blockchain analysis, investigators unravelled the various peel chain techniques used. This resulted in the arrest of one of the main money launderers in Switzerland. Several other mules were also apprehended in different jurisdictions. Investigations further found that ransoms paid were not dedicated for the sole benefit of the hacker. For example, illicit payments had to be made to various criminal partners and used for infrastructure (software engineers and developers, bullet proof- hosts for secure servers, bullet proof VPN services to hide communication or connection to the command-and-control servers, ML services to organize peel chain movements etc.), and to find mules and cash-out facilities.

Source: France

96. Information sought in international requests typically relates to both forensic evidence required for predicate investigations and financial data needed for ML investigations. This includes IP addresses located abroad, names and nicknames used, subscriber information, as well as beneficial ownership information, transaction details and counterparty information relating to wallets hosted by foreign VASPs.

Specific challenges posed by the use of virtual assets

97. The involvement of virtual assets in ransomware-related laundering can create new difficulties in co-operating across borders. Differences in the substantive treatment or regulation of virtual assets across legal systems—and limited or a lack of government involvement in or supervision of the sector in some jurisdictions—may complicate the ability or willingness of authorities to engage in international co-operation.

98. For example, jurisdictions that do not register or supervise VASPs may struggle to identify companies from which to request information. Even if the appropriate entity is located, authorities may then only have access to coercive investigative techniques to execute an international co-operation request. This may limit the information that can be obtained through informal co-operation processes.

99. This challenge is exacerbated by the reality that many jurisdictions where either the ransomware criminals and their money mules are located, or where the VASPs used to launder and cash out their proceeds are based or operate in, are tolerant of this activity and may be unresponsive to foreign law enforcement requests. Where VASPs are in jurisdictions without AML/CFT obligations, they may simply not have the relevant records available to law enforcement. This ultimately frustrates ongoing financial investigations and asset recovery

attempts. These challenges again reinforce the importance of accelerating the global implementation of FATF Recommendation 15 (including the Travel Rule).

Box 26. Investigative challenges arising from non-cooperative overseas VASP

Company X was a victim of a ransomware attack, believed to be the Caley ransomware strain. After negotiation, the victim paid 0.25 bitcoin to the ransomware criminal, and received an email with the decryption key, allowing the victim's operations to return to normal after decryption.

Authorities were belatedly made aware of the case through a police report lodged by the victim several days after paying the ransom, which resulted in the payment trail turning cold. Based on blockchain analysis, the ransom payment trail went to a VASP based overseas, and it was noted that a balance of 0.0081 Bitcoin went into a virtual wallet hosted by the overseas VASP, which has since remained reticent despite multiple requests for information. Investigations were further complicated by the perpetrator's use of a mixer to obfuscate transactions. Based on the circumstances of this case, the perpetrator remains unknown, and no asset recovery or arrest could be made.

Source: Singapore

100. The distributed architectures of some VASPs (with operations spanning across multiple jurisdictions) may also pose a significant investigative burden for law enforcement to identify the proper entity to approach with requests for information, or the proper jurisdiction to which to send a request for assistance. For example, one jurisdiction cited challenges in identifying the relevant jurisdiction to seek assistance from based on an IBAN that presumably belongs to a bank account managed by a VASP at a foreign financial institution. Another jurisdiction noted that some VASPs appear to have no physical presence, which can make it difficult to identify the correct jurisdictions to co-operate with.

The need for rapid co-operation

101. Since ransomware criminals can be widely distributed across the globe and virtual assets can be transferred nearly instantaneously, law enforcement needs to act quickly to trace and prevent the cross-border dissipation of ransomware related proceeds. To do so, formal international co-operation mechanisms (like mutual legal assistance) are typically required to obtain evidence and secure seizures in the context of criminal proceedings. However, such formal co-operation mechanisms are not always conducive to speed, which may significantly slow, stall or even thwart investigations. The complexity of ransomware-related investigations, in terms of the number of jurisdictions and companies involved, aggravates these challenges, with international co-operation taking more time and resources for ransomware than other criminal activities.

102. Leveraging informal co-operation can be useful to overcome these challenges and may help to streamline and expedite mutual legal assistance requests. To facilitate timely co-operation, some jurisdictions noted the importance of existing contacts and established informal channels for contacting and engaging with foreign counterparts. This helps facilitate swift information exchange necessary to advance criminal proceedings, while abiding by the necessary processes in place to protect such information. Such informal information exchange can occur between FIUs through the Egmont Secure Web, while police-to-police co-operation can occur through INTERPOL's I-24/7 as well as other informal networks including the Camden Asset Recovery Inter-Agency Network (CARIN) and regional Asset Recovery Inter-Agency Networks (ARINs). Authorities should have established processes and points of contact for available international and regional co-operation channels to support rapid funds tracing and effective asset recovery.

103. Some jurisdictions have seen success co-operating through established bilateral relationships. The use of dedicated cybercrime liaison officers posted internationally can significantly facilitate information and intelligence sharing between the liaison's host and home jurisdiction, as well as allow authorities to collect and provide evidence from abroad in investigations related to ransomware. To promote bilateral co-operation, authorities should consider publicising processes and points of contact for co-operation, particularly to support rapid fund tracing and asset recovery.

Box 27. Project CODA

A Canadian cyber-criminal tied to ransomware campaigns and cyber compromise of Alaskan government departments and medical facilities was arrested in November 2021 and charged with multiple cybercrime-related offences. Prior to contacting international partners, the FBI was investigating several related criminal cyber intrusions. Once the subject was identified and located, the FBI engaged with their bilateral contact at the Ontario Provincial Police (OPP).

Parallel investigations commenced in both jurisdictions, with support to the OPP and FBI provided by the Canadian National Cybercrime Coordination Centre (NC3), Europol, and Dutch law enforcement authorities. The NC3 provided operational support, data and behavioural analysis, intelligence briefs and reports, cryptocurrency tracing services and analysis over the course of 23 months as part of the international investigation. These efforts aided in confirming the identification of the subject of interest leading to his subsequent arrest. The use of advanced analytical technical techniques and specialized tools, such as cryptocurrency tracing, is key in these types of cybercrime investigations.

Source: Canada and the United States

The importance of multilateral co-ordination

104. Case studies featuring successful enforcement action typically involve competent authorities across multiple jurisdictions. This reflects the international and decentralised nature of ransomware attacks and associated ML. A prominent ingredient for success is the need for international co-ordination across affected jurisdictions to simultaneously uproot and disrupt cyber-syndicates and their affiliates. This also mitigates risk displacement, where these criminal organisations can easily relocate their digital operations to another safe haven.

105. There are several international law enforcement co-ordination mechanisms that can be used for this purpose, such as Europol/Eurojust or INTERPOL. These organisations host databases and provide logistics and expertise to co-ordinate stakeholders from several jurisdictions. Such multilateral mechanisms can be helpful, especially in accelerating critical information sharing for financial investigations and asset recovery.

Box 28. Operation GoldDust[1]

In November 2021, Romanian authorities arrested two individuals suspected of cyber-attacks deploying the Sodinokibi/REvil ransomware. They are allegedly responsible for 5 000 infections, which in total pocketed half a million euros in ransom payments. Since February 2021, law enforcement authorities have also arrested three other affiliates of Sodinokibi/REvil and two suspects connected to GandCrab. These are some of the results of operation GoldDust, which involved 17 jurisdictions[2], Europol, Eurojust and INTERPOL. All of the arrests followed the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family, which is seen as the successor of GandCrab.

Operation GoldDust was developed from leads related to previous investigations targeting GandCrab, a Romania-led investigation with support from Europol and law enforcement authorities from several jurisdictions, including the United Kingdom and the United States.

Europol facilitated the information exchange, supported the co-ordination of operation GoldDust and provided operational analytical support, as well as cryptocurrency, malware, and forensic analysis. Europol also deployed experts to each location and activated a Virtual Command Post to co-ordinate the activities on the ground. The international co-operation enabled Europol to streamline victim mitigation efforts with other EU jurisdictions. These activities prevented private companies from falling victim to Sodinokibi/REvil ransomware.

The Joint Cybercrime Action Taskforce (J-CAT) at Europol supported the operation. This standing operational team consists of cyber liaison

officers from different jurisdictions who work from the same office on high profile cybercrime investigations.

Source: Europol

Notes
1. For more information, please refer to: www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
2. Participant jurisdictions: Australia, Belgium, Canada, France, Germany, the Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom, the United States.

Proposed Actions

- Jurisdictions should establish and actively participate in bilateral, regional, and multilateral mechanisms, such as by using liaison offices and establishing clear 24/7 contact points, to facilitate rapid international co-operation and information exchange.

Conclusion

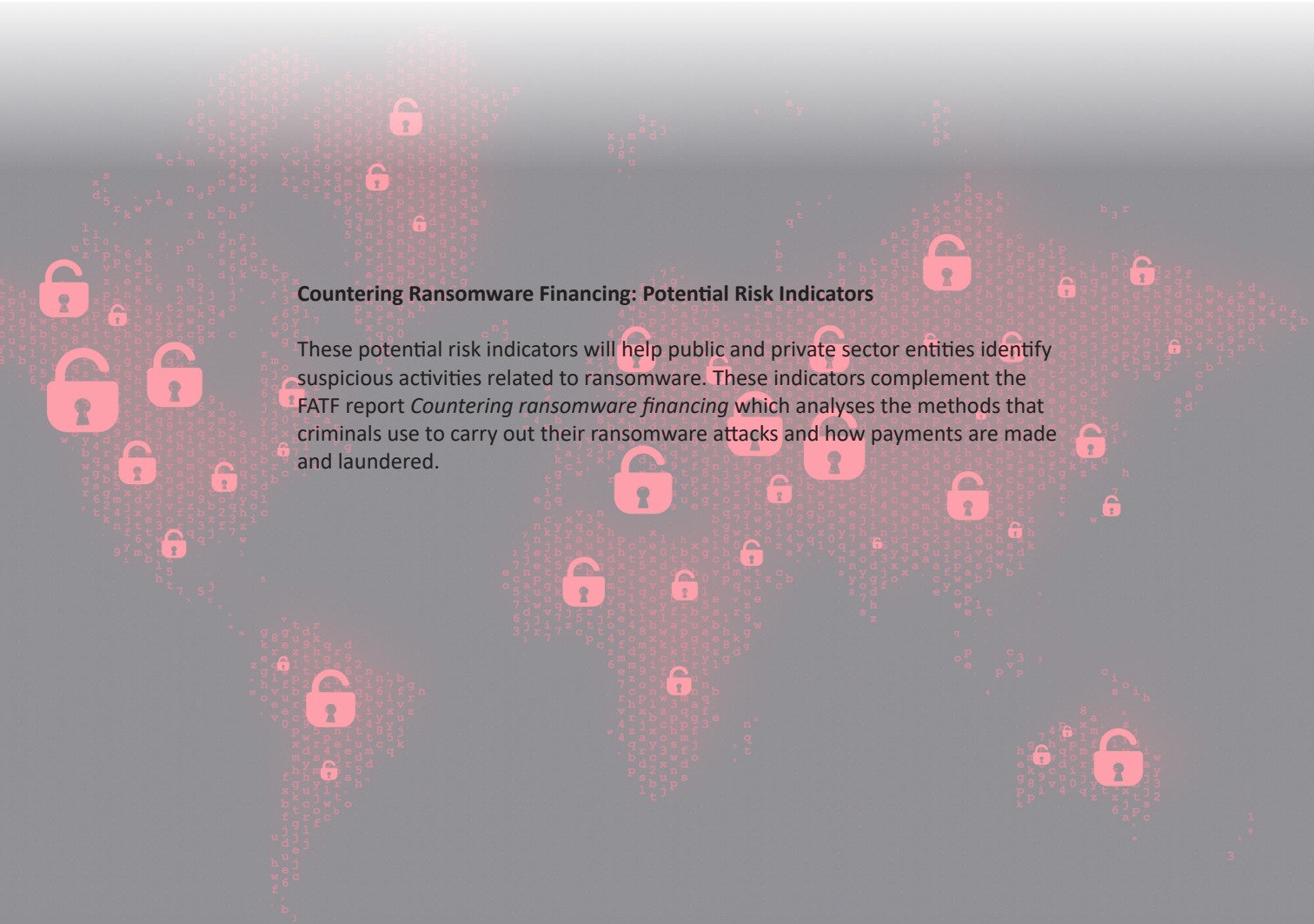
106. Despite the recent growth in global ransomware financial flows, there is still an observable lack of investigations for related ML. This study has shown that ransomware is a multi-disciplinary and international problem. This requires a co-ordinated approach for an effective response against this threat. To achieve this, jurisdictions should leverage partnerships at three levels: public-public; public-private; and with foreign jurisdictions and multilateral organisations.

107. This study further illustrates the importance of an accelerated implementation of the FATF Standards to provide an effective framework to tackle illicit proceeds derived from ransomware, particularly in relation to virtual assets and the VASP sector. FATF will continue to promote the implementation of the FATF Standards in this sector.

108. Finally, the role of virtual assets in the laundering of ransomware proceeds, as well as the evolving techniques employed by ransomware criminal groups, further present challenges. Competent authorities should ensure that their laws remain relevant and are equipped with the skills and capabilities required to be nimble in the face of a dynamic digital criminal environment.

www.fatf-gafi.org

March 2023



Countering Ransomware Financing: Potential Risk Indicators

These potential risk indicators will help public and private sector entities identify suspicious activities related to ransomware. These indicators complement the FATF report *Countering ransomware financing* which analyses the methods that criminals use to carry out their ransomware attacks and how payments are made and laundered.