BGIN SR 006

Study Report for Ransomware Reaction

Part 1: General

Introduction

Ransomware attacks have grown in frequency and sophistication to become an epidemic that has warranted the attention of government officials at the highest level. Ransomware not only attacks private businesses and individuals but also increasingly, critical infrastructure and government agencies. Leaders on a global scale have signaled Ransomware to be of critical concern requiring a coordinated response to this ever-growing threat.

There is a significant body of literature online, including the U.S.'s Ransomware resource hub, that provides a slew of best practices, recommendations, and other resources to both help individuals and businesses prevent Ransomware attacks on themselves, and how to respond to them.

Ransomware is operated much like a business requiring Governments to approach their Ransomware policies and plans by disrupting these business models. For those wondering how Ransomware is like a business, worry not, we address this here as well.

The Product **-** Ransomware is essentially a sophisticated form of Malware that encrypts files on a device and blocks the victim from accessing those files until the ransom is paid. The locked data can either prevent other systems from working or can be private information that can have devastating results for the victim should it be released. Ransomware attackers generally threaten to release this information unless the ransom is paid.[1]

The Revenue **-** Ransomware payments are usually made in cryptocurrency, with Monero being the most rapidly rising type of crypto used by threat actors. "We've seen Ransomware groups specifically shifting to Monero," said Bryce Webster-Jacobsen, Director of Intelligence at GroupSense, a cyber security group that has helped a growing number of victims payout ransoms in Monero. "[Cyber criminals] have recognized the ability for mistakes to be made using bitcoin that allow blockchain transactions to reveal their identity."[2] However, due to the wider availability and high liquidity, BTC continues to be a popular choice.[3]

As soon as the cryptocurrency is paid, the funds are transferred across several exchanges and frequently converted to other cryptocurrencies as the payment makes its way to its final destination. In many cases, only a portion of the funds remain with the hacker(s), while the remaining portion is frequently funneled into research and development (R&D) and re-invested into their business model e.g. purchasing more stolen identities on the darknet.[4]

[1] FBI. (2020, April 3). Ransomware. FBI. Retrieved December 29, 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/Ransomware

[2] Murphy, H. (2021, June 22). Monero emerges as crypto of choice for Cybercriminals. Financial Times. Retrieved December 31, 2021, from https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6

[3] Crowe. (2021, October 25). The Wild World of crypto Ransomware payments. FEI. Retrieved December 31, 2021, from https://www.financialexecutives.org/FEI-Daily/October-2021/The-Wild-World-of-Crypto-Ransomware-Payments.aspx

[4] Waldman, A. (2021, April 27). Rise in ransom payments may fuel more dangerous attacks. Search

In addition to striving for profitability, these transnational criminal “businesses” focus on developing ever more sophisticated forms of Ransomware to stay one step ahead of law enforcement and cyber security specialists. Ransomware organizations also compete against other Ransomware-as-a-Service platforms. Many popular forms of Ransomware have an “antidote” developed by cyber security experts to decrypt the files and return access to the victim. Eventually these tools make the current form of Ransomware ineffective. The cyber criminal organizations R&D funds are then used to create more sophisticated Ransomware to continue the business model. What results is a constant back and forth battle between the Ransomware threat actors and cyber security providers to develop more sophisticated Ransomware and Ransomware mitigation tools. In other cases, Ransomware attacks can act as a cash cow for other areas of organized crime such as drug, human, and weapons trafficking. Finally, once a ransom is paid by the victim, the encrypted/ransomed data does not always return to the victim. As mentioned in this document, in many cases, this data is sold to other criminals on the darknet.[5]

The Organizational Structure- There are many types of structures within the world of Ransomware. Some have organized themselves while others purchase the Ransomware technology (called “White Labeling”) to launch it themselves. With the ever-increasing popularity and success of Ransomware attacks, businesses have evolved to provide Ransomware-as-a-Service (RaaS) - In a nutshell, the RaaS model operates much like many other Software-as-a-Service vendors. The RaaS provider develops and sells time and space on their Ransomware platforms to other “ransomhackers”. This has greatly increased the number of Ransomware attacks and attackers as little technical skill is required to add a link to an email and send it across several staff in a targeted organization (phishing).

In any event, the model can either be subscription based, affiliate or one time sale.

a. Subscription - User pays the provider a periodic fee in cryptocurrency for the duration of usage
b. Purchase - User purchases a Ransomware package from the Provider
c. Affiliate - User pays a subscription fee and a percentage of a successful Ransomware attack to the provider[6]

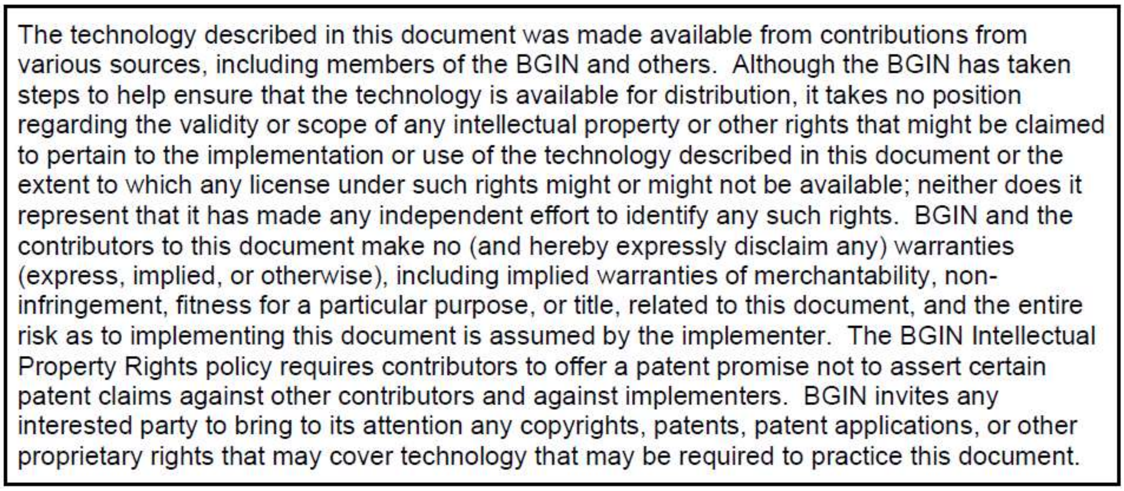
Security. Retrieved December 31, 2021, from https://www.techtarget.com/searchsecurity/news/252499899/Rise-in-ransom-payments-may-fuel-more-dangerous-attacks

[5] CISO MAG. (2020, November 13). Ransomware: A lucrative business model for hackers, says FS- ISAC. Cyber Security Magazine (CISO MAG). Retrieved December 31, 2021, from https://cisomag.eccouncil.org/Ransomware-a-lucrative-business-model-for-hackers-says-fs-isac/

[6] Ransomware-as-a-service: A new business model for Cybercriminals. Hylant. Retrieved December 31, 2021, from https://www.hylant.com/2021/10/Ransomware-as-a-service-a-new-business-model-for-cybercriminals/

According to Forbes, 33% of Ransomware attack victims paid the ransom, 22% of those never regained access to their data.[7] In fact, the most common result whether access is regained or not, is that the “ransomhacker" then sells or provides access to the data to another hacker to extort or publish. Additionally, 80% of businesses that paid the ransom were attacked again. In 66%, victims believed it was the same actor as the previous attack. In the remaining cases (34%), the attacker was likely different than the previous time (this 34% varies depending on the source). In those cases, once a payment has been provided, it signaled to other hackers that this company was willing to pay large sums of money to resolve this issue in the short term.[8]

In summary, Ransomware-as-a-Service is a transnational, sophisticated criminal enterprise with a profitable business model. A model which re-invests in itself, funds R&D, and develops tools that can be deployed easily by any individual purchasing RaaS on the darknet. Our document provides further analysis from a policy perspective including specific recommendations with a view towards how privacy is an important tool in this fight and how balancing with compliance - including via cutting-edge technological developments - we can more effectively gain ground against this epidemic when privacy is fundamentally included.



The technology described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

[7] Wilson, M. (2021, July 12). Council post: Why paying Ransomware is typically a bad idea and what you can do instead. Forbes. Retrieved December 31, 2021, from https://www.forbes.com/sites/forbestechcouncil/2021/07/12/why-paying-Ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/?sh=68eb65581503

[8] Panduru, D. (2021, July 13). 80% of Ransomware victims hit by repeat attacks, a new report reveals. ATTACK Simulator. Retrieved December 31, 2021, from https://attacksimulator.com/blog/Ransomware-victims-hit-by-repeatattacks/

Table of contents

1. Scope

The target audience of this document are policymakers, regulators, and law enforcement (hereinafter “Government(s)”) directly working to stem the growth of Ransomware domestically or internationally.

This document is not intended to be a comprehensive Ransomware preparedness or reaction plan for end-users. Instead, this document focuses on providing targeted recommendations for consideration that mitigate the risk of Ransomware including by prioritizing removal of the business incentive (profitability) while maintaining privacy for citizens and continuing to foster innovation within both the financial and technology sectors.

The document specifically considers:

- How privacy can help mitigate the effectiveness of the Ransomware epidemic
- Removing the business incentive of Ransomware without overregulating the payments or cryptocurrency industries
- Recommended policies for governments and international bodies that will help increase the risks to threat actors and lower the number of attacks

This document does not focus on the following items:

- Best practice Ransomware prevention or reaction plans for individuals and businesses (Cyber Hygiene)

2. Normative reference

This document has no normative reference.

3. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

AML/CFT	Anti Money Laundering/Countering the Financing of Terrorism
AI/MIL	Artificial Intelligence/Machine Learning
BGIN	Blockchain Governance Initiative Network
BTC	Bitcoin
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLP	Data Loss Protection
EDD	Enhanced Due Diligence

FI	Financial Institution
LE	Law Enforcement
ML/TF	Money Laundering/Terrorist Financing
R&D	Research and Development
RaaS	Ransomware-as-a-service
RCTF	Ransomware Crimes Task Force
XMR	Monero
VASP	Virtual Asset Service Provider
ZKP	Zero Knowledge Proof

NOTE: All the abbreviations SHALL appear in this clause.

4. Areas of Exploration on a Policy level

Given geo-political sensitivities when discussing policy options, the following suggestions are meant to be country agnostic to allow for a global concerted effort - as effectively and realistically as is possible. Ransomware is a cutting-edge multinational criminal industry that can only be addressed with a sophisticated multinational response.

Below are suggested areas in which to focus policy considerations and are driven by the overarching philosophy of:

1. Prioritizing privacy as a critical tool to protect individuals from becoming Ransomware targets with the effect of reducing the highly lucrative model of Ransomware.
2. Smart Regulation which builds on existing frameworks; and
3. Encouraging a mission to fund and create necessary frameworks for governments (domestic and international) to be leaders in developing and using cutting-edge technologies to disrupt Ransomware's highly lucrative business model.

4.1 Proposed Government Policies and Processes

Without delving into the logistical details of building an interagency task force (e.g., Ransomware Crimes Task Force (RCTF)) on a domestic government level or building an international task force (or leveraging existing frameworks domestically or internationally like INTERPOL), this section focuses on a non-exhaustive set of proposed measures to more effectively counter transnational Ransomware attacks.

1. An ideal is not to "reinvent the wheel" but rather to improve or leverage existing procedures - in an accelerated fashion - to combat this Ransomware epidemic. Speed is critical.

    a. Leverage or create an interagency group on a domestic government level to focus on combating Ransomware within.

    b. Leverage, create or join an international task force (potentially through INTERPOL[9] or a similar organization) of cyber security Law Enforcement (LE) officials, intelligence agencies, and private sector businesses.

    c. Leverage existing frameworks including treaties (e.g., the Budapest Convention on Cybercrime).

    d. Assist LE (domestic and international) through existing and improved resources and/or specialized trainings to more effectively combat transnational Ransomware crimes. Prioritize sharing of data and transnational cooperation.

2. Create a system of clear incentives and guidelines for entities to report Ransomware attacks and/or payments to LE.

    a. Consider promoting a grant process for industry participation in minimizing Ransomware attacks.

    b. Consider a decentralized autonomous organization (DAO) composed of entities (private and public) and individuals on a secure protocol. These parties anonymously will be connected to this DAO and must follow a set of conditions (rules) related to minimum cyber hygiene practices relating to protection from current Ransomware threats. The protocol can periodically check that these conditions are met in a non-invasive manner. Should one of the members of the DAO be attacked through a current condition, an alarm (issued in real-time) will notify other members of the DAO anonymously that one of the members has been attacked through this condition. This could signal a new vulnerability in an area that will notify members to add additional protections in this area. If a member is attacked through a condition not currently covered by the protocol, this alerts members of a potentially new type of Ransomware. This would ultimately "democratize" the response to these bad actors – thereby reducing their impacts while also lowering costs to companies. In effect you create a Worldwide standard for cybersecurity but also an instantaneous early warning system operating in real-time (analogous to sirens that go off in extreme societal distress e.g. war). Entailed is a system of incentives available to anyone (generic large-scale way) in order to motivate the democratic response to eliminating threats as well as penalties for failure to follow conditions.

        i. The responses/solutions should be completely democratic (i.e. open source, peer reviewable; anyone can check) but the author of those

[9] INTERPOL. (2021, July 12). Immediate action required to avoid Ransomware pandemic. INTERPOL. Retrieved December 31, 2021, from https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL

responses/solutions should be protected (personal identifying information not disclosed; ensuring privacy/protection from bad actors).

   ii. The above is intentionally abstract as this is beyond the scope of this document. However, the authors see the DAO model as a potential framework to collaborate globally in a decentralized manner, with real-time information being shared between participating entities.

3. Invest in technological expertise on Government teams (to include blockchain/cutting-edge technology experts). Prioritize technology that allows for traceability while protecting privacy.

   a. One overlooked factor in this equation is the Government's over reliance on the private sector to steer the development of LE tools such as blockchain analytics and decryption tools. By prioritizing funding into research and development of these tools, the Government can more proactively steer the outcomes such as achieving traceability with privacy.

   b. Approach the technology as an innovative business with the goal of outdoing the competition i.e. a shift in the mindset of how a technology taskforce can combat this issue (e.g. ANOM private messaging platform; created by law enforcement with very successful results.[10])

4. Prioritize funding mechanisms - including at international level - to support poorly resourced countries.

   a. Domestically - amend/pass laws as necessary to ensure Asset Forfeiture and Seizure funds can be redirected to fight transnational cybercrimes and support funding to poorly resourced countries.

   b. Internationally - consider possible funding streams/costs: structured similarly to an intergovernmental organization, where member countries provide funding to the institution and may add stipulations on what their funds would be used for (development of new tech to trace transactions, coordination tools, etc). Included would be a pool focused on supporting resource-strapped countries.

4.2 Leveraging Privacy in the Battle Against Ransomware

To proactively address top Ransomware attack vectors within the above overarching philosophy, it is essential to improve "track & trace" technology while allowing for privacy. It is also essential to prioritize privacy in any conversation about regulation and technology-driven solutions; thereby more effectively reducing individuals/entities' vulnerabilities to being targeted for Ransomware

[10] U.S. Attorney's Office Southern District of California. (2021, June 8). FBI, encrypted phone platform infiltrated hundreds of criminal syndicates; result is massive worldwide takedown. The United States Department of Justice. Retrieved December 31, 2021, from https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

attacks.

To that end, there are various key matters:

1. Consider whether regulation of payment rails is the most effective way to address Ransomware attacks. Although we generally welcome smart regulation of cryptocurrency, attempting to over-regulate cryptocurrency to stem Ransomware will be a monumental task and likely ineffective in stopping Ransomware for a number of reasons. Some of these are:

    a. There exists an unequal application of cryptocurrency regulations across the globe. Although most major cryptocurrency markets have implemented some form of the FATF travel rules, Ransomware attacks that stem from state actors will unlikely be affected by these regulations as they can bypass them.[11]

    b. With the advent of DeFi (i.e. true DeFi with no centralized responsible entity), regulation and enforcement is difficult. For example, given the open-source, peer-to-peer nature, who does Law Enforcement (LE) charge should the platform break the law?

    c. Over-regulating or relying on traditional regulatory philosophies/frameworks to oversee cutting-edge technologies may have the unintended consequence of pushing a significant portion of this industry “underground” or “offshore”.

2. Consider disrupting the Ransomware business model which in many cases operates like a multinational business. A portion of a successful Ransomware payment goes to the individual or team involved with the hack, while a sizable remaining portion of the payout is funneled back into development of more sophisticated Ransomware tools. This cycle has largely fueled the significant increase in number and sophistication of Ransomware attacks in recent years.[12] To disrupt, the key is to understand and focus on what the attackers are seeking – data – and then ask how that can be protected or made less appealing such that attackers will no longer invest in this business model. Remove the business incentive and you remove the appeal. This can include greater regulations on the protection of data and other cyber hygiene mandates for a wider set of industries than what is required today (e.g., further regulating large retailers’ loyalty point programs), or exploring the benefits of encryption and/or decentralization as it applies to traditional businesses and what/how data is collected and maintained.

3. Understand how privacy is an important tool to protect individuals from becoming Ransomware targets; thereby reducing the financial (or other) appeal of Ransomware. Employees are a common attack vector at institutions. To break out of this vicious cycle, in addition to encryption, here we focus on Ransomware and the unintended consequence of transparency in crypto payments:

[11] TRM Insights (2021, July). FATF’s Crypto Sequel: It’s time to implement Standards. TRM Labs. Retrieved March 1, 2022 from https://www.trmlabs.com/post/fatfs-crypto-sequel-its-time-to-implement-standards

[12], Lemnitzer, Jan, Copenhagen Business School, February 17, 2021. Ransomware Gangs are Running Riot - Paying Them Doesn’t Help. The Conversation. Retrieved March 1, 2022 from https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254

a. Ransomware proliferates in diverse ways, including through exploitation of vulnerabilities, as well as social engineering tactics. These tactics, such as "phishing" emails, deceive employees within an organization to open attachments that launch the malware that then infects their networks. Compromised employee credentials continue to be a preferred attack vector, comprising 20% of Ransomware attacks.[13] On average, a typical Ransomware attack can take up to 287 days to identify and contain a breach.[14]

b. Phishing emails are ever more sophisticated. Based on the authors' experience in Law Enforcement (LE) and business, we have seen a progression in the quality of the phishing emails resulting in more effective Ransomware attacks and identity theft. Bad actors have access to a plethora of resources to create these sophisticated profiles of targeted individuals - via data leakages, data breaches, data harvesting, data bought on Darknet marketplaces, open-source data – i.e. the monumental amounts of data collected on us (where we are the commodity). Adding more disclosure with unprotected financial information on a public permissionless blockchain is an accelerant that further exacerbates a vicious cycle already overwhelming LE and Regulators.

c. The belief that transparency in tracing cryptocurrencies "will help us catch criminals" – if not balanced with the need for privacy – does not risk manage the consequence that it also exponentially increases everyone's vulnerabilities to attacks. It is analogous to having your bank balance/transactional history available for public consumption (which leads to security issues for the wallet holder).

d. It is also important to consider the vulnerabilities of "companies, institutions and critical infrastructure" (i.e. entities) and their interplay with privacy and Ransomware attacks. These types of prospective victims are often too well known so privacy in cryptocurrency transactions is less effective in protecting them from becoming targets. However, entities still have an economic interest in maintaining their crypto payments private to protect their commercial activity/financial information. Plus, in the context of Ransomware, an entity being known to pay is likely to trigger additional attacks. 80% of businesses that paid the ransom were attacked again. In 66%, victims believed it was the same actor as the previous attack. In the remaining cases (34%), the attacker was likely different than the previous time (this 34% varies depending on the source). In those cases, once a payment has been provided, it signaled to other hackers that this company was willing to pay large sums of money to resolve this issue in the short term.[15]

4. Understand that privacy serves as a critical element in traditional financial transactions, and

[13] IBM (2021). Cost of a Data Breach Report 2021. IBM. Pg 20. Retrieved December 31, 2021 from https://www.ibm.com/security/data-breach

[14] IBM (2021). Cost of a Data Breach Report 2021. IBM. Pg 6. Retrieved December 31, 2021 from https://www.ibm.com/security/data-breach

[15] CyberSeason. Ransomware: The True Cost to Business. June 2021. TechTarget. Retrieved March 1, 2022 from https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

cryptocurrency transactions should be no different. Privacy prevents sensitive data such as wallet balances from being seen by threat actors, lowering the risk of an individual being targeted. We do not minimize anonymity enhancing tools that - while granting privacy to people not engaged in criminal activity i.e. the majority of the users - can also make illicit transactions more difficult to track and trace. That is why a balanced technology-driven policy/regulatory solution should prioritize traceability while protecting individuals' privacy which is essential including for day-to-day financial transactions (unless required to be disclosed through legal processes). Without prioritizing development of traceability technology (to enforce AML/CTF regulations) for Ransomware payments, balanced with privacy rights, unintended consequences will continue to result.

5. Consider that privacy and AML/CFT compliance is/does not have to be mutually exclusive. Based on the authors' knowledge of cryptocurrencies and privacy, there are examples of privacy protecting technologies that allow for compliance under current AML/CFT reporting requirements for VASPs. VASPs own the relationship with their user/account holder which – based on their internal risk appetite – may trigger enhanced due diligence (EDD). For enforcement purposes, traceability is still critical and a concern when moving beyond the control of the VASP. Yet reverting to transparency for cryptocurrency payments as the holy grail is inefficient given the ever increasing development of privacy as Web3 advances (i.e. there is a significant portion of the ecosystem that is organically moving away from this type of transparency) as well as the previously discussed unintended consequence of transparency increasing vulnerabilities of individuals/entities.
    a. Although outside the scope of this document, it is worth mentioning that the risk appetite of an FI or VASP may be so low as to stifle legitimate business when there is an automatic perception that privacy in cryptocurrency equals criminal activity.

4.3 Technology to Combat Ransomware

Because privacy is not binary, even when considering traceability after an attack has been deployed, it remains critical to focus on developing technology that allows tracking and tracing through current and future privacy enhancing tools. Funding for research and development of cutting-edge technologies that can combat Ransomware and protect PII data/privacy interests, should be prioritized.

Some examples of possible technologies or areas for further research include:

1. Artificial Intelligence/Machine Learning (AI/MIL)
    a. Artificial intelligence and Machine Learning (AI/MIL) is currently being utilized to detect patterns/vulnerabilities to mitigate against Ransomware attacks.[16] Its effectiveness depends on access to data which raises concerns regarding how

[16] Cooper, Tim.FATF Report: New Tech Set to Boost Financial Crime Fighting Efforts." *AML RightSource*, 30 August 2021, Retrieved 30 March 2022. from https://www.amlrightsource.com/news/fatf-report-new-tech-set-to-boost-financial-crime-fighting-efforts.

privacy interests are being protected.

2. Encryption

   a. Valuable tool in Data Loss Prevention (DLP).[17] - Encryption can be highly effective because, although it may not prevent the entity's data from being stolen/encrypted by the "ransomhacker", the files will already be unreadable (if encrypted). It counters the "double extortion" tactic - i.e. data seized in Ransomware attack, victim extorted to release the data back to them, and victim extorted a second time by threatening to publicly release the data stolen during the attack. Encryption removes the business incentive of re-selling the data on a Darknet marketplace.

3. Watermarking - Traditionally, watermarking has been used as a method to track counterfeit paper currency and other government documents. Watermarking has been more recently applied to the media industry (copyright issues) and watermarking of non-media data has become a possibility. This could improve the effectiveness of using privacy-enhancing tools with additional deterrent effects.

   a. Watermarking the non-media data - As this is cutting-edge technology, watermarking sensitive non-media data is still being researched. There are many considerations to work through with watermarking non-media data; e.g. "...embedding of hidden multipurpose information sequences into transmitted and stored digital data...methods of digital steganography and methods of digital watermarking. Methods of digital **steganography** are designed for establishing hidden channels of confidential information transmission in digital objects. Methods of digital watermarking are used for authentication of digital objects and their owners."[18]

   b. Watermarking the crypto payment - presumably, this technology would also allow for watermarking the payment itself. Although cryptocurrency payments have unique identifiers, watermarking non-media data through a blockchain can act as a method of authentication as well as tracing in a more robust manner with the goal of also balancing privacy.

4. Applicability of ZKPs balancing privacy with compliance - Key is to consider what is possible?

   a. Including how to incorporate Data Encryption to reduce the destructive effect of a Ransomware attack plus the added threat of a common double extortion during said attack (see Section 4.3(2)(a) above).

   b. Consider decentralized data as a means of reducing the effectiveness of Ransomware attacks, including in combination with ZKPs.

[17] Cipher, Sept 2020. Why Data Loss Prevention Matters to Your Security Strategy. Cipher Retrieved March 1st 2002 from https://cipher.com/blog/why-data-loss-prevention-dlp-matters-to-your-security-strategy/

[18] Evsutin, O.,& Meshcheryakov, Y. (2020). The use of the blockchain technology and digital watermarking to provide data authenticity on a mining enterprise. Sensors, 20(12), 3443. https://doi.org/10.3390/s20123443

c. Privacy in DeFI context and reducing ML/TF risks via cutting-edge technological track and tracing capabilities. How would this work?

d. Applicability of Steganography - Hash the code/secret message so that identity of the author of the message is protected. Can it be used to enhance privacy while permitting tracking and tracing of Ransomware payment?

5. Conclusions

This Ransomware epidemic requires an innovative, proactive, and collaborative transnational strategy from Governments (and industry). The default narrative that privacy enhancing tools across the board are not trustworthy - or automatically equate criminal intent - is neither pragmatic nor accurate. Privacy allows for innovation, economic opportunity, and protects national security interests. Even the traditional financial system permits privacy balanced with compliance. And Web3 projects substantially prioritize giving users the option of privacy.

Achieving innovative technology driven policy solutions requires a paradigm shift in how regulation is viewed and how governmental processes are leveraged/streamlined, and funding is prioritized. Governments should be leading these initiatives, leveraging existing governmental frameworks (domestic and international) to maximize existing (as well as encouraging more specialized) skills, teams, networks while driving the direction of innovation. We believe Governments are driven by constituents' interests (as well as, national security and economic interests) and thus, are willing to discuss the critical importance of privacy to fight Ransomware and ancillary crimes.

Ransomware targets data. Adding full financial transaction transparency on a blockchain - to the already monumental amounts of data existing on any one individual - has unintended and very dangerous consequences. Full transparency on a blockchain inadvertently strengthens the attackers' abilities to build ever more sophisticated profiles with ever increasing success at baiting or identifying one of the weakest and easiest vectors of Ransomware attacks - people.

Instead of fighting the privacy wave with unintended and more harmful consequences, Governments should embrace technology driven solutions that protect privacy.

Solutions should include developing advanced technologies that balance privacy with compliance and leverage privacy. For example, incorporating privacy within our proposed DAO that seeks to create a Worldwide standard for cybersecurity and instantaneous early Ransomware warning system (operating in real-time).

Finally, and in reaching the above conclusions, additional questions arose:

1. What technologies are - or should be - under development that will allow for tracking and tracing (pursuant to proper legal process) through privacy enhancing tools? And within the DeFI space?
2. What role can decentralized data have, including for governments and how critical

infrastructures are managed?

3. How can regulation evolve faster given the speed of technological developments? Is there a place for decentralized regulation? Can Governance mechanisms help or shape regulation?
4. Who should be driving the direction of tracking and tracing innovation? Governments or the Private Sector? And what checks and balances exist to protect people's civil liberties?

There is no turning back from technology. Therefore, it is imperative that we control its influence for good as a superset, not a subset, of the work we undertake herein. And to ensure it is used for good, we believe privacy is a critical component of any discussion on combating the Ransomware epidemic.

Appendix A – Acknowledgement

(Informative)

A.1 Co-Editors

- Jessica Mila Schutzman
- Omar Hamwi

A.2 Contributors

- Roman Pavlov
- Tomonori Yuyama

Appendix B – Informative reference

- CISO MAG. (2020, November 13). Ransomware: A lucrative business model for hackers, says FS-ISAC. Cyber Security Magazine (CISO MAG). Retrieved December 31, 2021, from https://cisomag.eccouncil.org/Ransomware-a-lucrative-business-model-for-hackers-says-fs-isac/
- Crowe. (2021, October 25). The Wild World of crypto Ransomware payments. FEI. Retrieved December 31, 2021, from https://www.financialexecutives.org/FEI-Daily/October-2021/The-Wild-World-of-Crypto-Ransomware-Payments.aspx
- FBI. (2020, April 3). Ransomware. FBI. Retrieved December 29, 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/Ransomware
- IBM. (2021). Cost of a data breach report 2021. IBM. Retrieved December 31, 2021, from https://www.ibm.com/security/data-breach
- INTERPOL. (2021, July 12). Immediate action required to avoid Ransomware pandemic. INTERPOL. Retrieved December 31, 2021, from https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL
- Murphy, H. (2021, June 22). Monero emerges as crypto of choice for Cybercriminals. Financial Times. Retrieved December 31, 2021, from https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6.
- Panduru, D. (2021, July 13). 80% of Ransomware victims hit by repeat attacks, a new report reveals. ATTACK Simulator. Retrieved December 31, 2021, from https://attacksimulator.com/blog/Ransomware-victims-hit-by-repeat-attacks/
- Ransomware-as-a-service: A new business model for Cybercriminals. Hylant. Retrieved December 31, 2021, from https://www.hylant.com/2021/10/Ransomware-as-a-service-a-new-business-model-for-cybercriminals/
- U.S. Attorney's Office Southern District of California. (2021, June 8). FBI&#39;s encrypted phone platform infiltrated hundreds of criminal syndicates; result is massive worldwide takedown. The United States Department of Justice. Retrieved December 31, 2021, from https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive
- Waldman, A. (2021, April 27). Rise in ransom payments may fuel more dangerous attacks. Search Security. Retrieved December 31, 2021, from https://www.techtarget.com/searchsecurity/news/252499899/Rise-in-ransom-payments-may-fuel-more-dangerous-attacks
- Wilson, M. (2021, July 12). Council post: Why paying Ransomware is typically a bad idea and what you can do instead. Forbes. Retrieved December 31, 2021, from https://www.forbes.com/sites/forbestechcouncil/2021/07/12/why-paying-Ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/?sh=68eb65581503

- Evsutin, O., & Meshcheryakov, Y. (2020). The use of the blockchain technology and digital watermarking to provide data authenticity on a mining enterprise. Sensors, 20(12), 3443. https://doi.org/10.3390/s20123443
- Chainalysis. (2021). Ransomware 2021: Critical Mid-year update. Chainalysis. Retrieved December 31, 2021, from https://go.chainalysis.com/Ransomware-2021-update.html
- Institute for Security and Technology (IST). (n.d.). Ransomware Task Force report: Combatting Ransomware. Institute for Security and Technology (IST). Retrieved December 31, 2021, from https://securityandtechnology.org/Ransomwaretaskforce/report/
- Panah, A. S. (2017, June). (thesis). Digital Watermarking of Non-media data stream (applications). BMIT University. Retrieved December 31, 2021, from https://www.researchgate.net/publication/317956069_Digital_watermarking_of_non-media_data_stream_applications
- Perimeter 81. (2021, August 26). What is Zero trust? Perimeter 81. Retrieved December 31, 2021, from https://www.perimeter81.com/glossary/zero-trust RSM US LLP. (2021, October 25).
- TRM Insights (2021, July). FATF's Crypto Sequel: It's time to implement Standards. TRM Labs. Retrieved March 1, 2022 from https://www.trmlabs.com/post/fatfs-crypto-sequel-its-time-to-implement-standards
- Lemnitzer, Jan, Copenhagen Business School, February 17, 2021. Ransomware Gangs are Running Riot - Paying Them Doesn't Help. The Conversation. Retrieved March 1, 2022 from https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254
- CyberSeason. Ransomware: The True Cost to Business. June 2021. TechTarget. Retrieved March 1, 2022 from https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business
- Cooper, Tim.FATF Report: New Tech Set to Boost Financial Crime Fighting Efforts." *AML RightSource*, 30 August 2021, Retrieved 30 March 2022. from https://www.amlrightsource.com/news/fatf-report-new-tech-set-to-boost-financial-crime-fighting-efforts.
- Cipher, Sept 2020. Why Data Loss Prevention Matters to Your Security Strategy. Cipher Retrieved March 1st 2002 from https://cipher.com/blog/why-data-loss-prevention-dlp-matters-to-your-security-strategy/