Addressing The Intelligence Applications of Bitcoin Payments Related to Ransomware

Adam Brian Turner

B.Eng. UTS, DipEngPrac UTS, MPICT Macq

Principal Supervisor: Dr Alex Simpson, Senior Lecturer, Department of Security Studies and Criminology, Macquarie University, Sydney, Australia.

Associate Supervisors: Dr. Allon Uhlmann, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands.

Stephen McCombie, Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands.

Dr. Muhammad Ikram, Lecturer, Department of Computing, Macquarie University, Sydney, Australia.

Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy

Department of Security Studies and Criminology, Faculty of Arts

Keywords

Ransomware, Cryptocurrency, Financial Crime, Cyber Threat Intelligence, Machine Learning, Graph Analysis, Structured Threat Information Expression (STIX).

Abstract

This thesis addresses the evolving threat of the use of cryptocurrency in ransomware attacks. These attacks are a form of cyber extortion in which malicious software (malware) is used to infect, encrypt, and render systems unusable unless the victims pay a ransom. Such attacks can cripple the capabilities of business-critical systems as well as critical infrastructure. Increasingly, ransom payments are being demanded in hard-to-trace cryptocurrency formats such as Bitcoin.

This thesis by publication, comprising four published research papers, a published conference proceeding paper, and two research papers submitted for journal publication, demonstrates the utility of taking a target centric approach to intelligence collection and analysis of a ransomware-cryptocurrency network. Utilising graph analysis techniques applied to data gathered from the Bitcoin blockchain, this research addresses challenges security researchers face in preventing the propagation of ransomware payments throughout cryptocurrency networks as well as determining the accountability of such payments.

The first paper provides a general perspective on analysis techniques relating to illicit Bitcoin transactions and ransomware incidents, and the second paper develops a target-centric intelligence approach to a specific Bitcoin ransomware incident (WannaCry 2.0). The third study explores the possibility of using a common sharing standard such as STIX to share ransomware payment related cyber intelligence, while the fourth paper discerns Bitcoin payment patterns from well-known ransomware attacks (WannaCry, CryptoDefense, and NotPetya). The fifth paper examines graph embeddings in more

detail to reveal risky nodes in a ransomware-Bitcoin network, and the sixth paper develops a novel methodology to systematically identify ransomware transactions within cryptocurrency payment networks.

By undertaking target network modelling and analysis, this research provides a basis for analysing payment patterns generated by ransomware-Bitcoin transactions as a graph. Furthermore, to enhance the understanding of the ransomware-Bitcoin environment and any points of vulnerability, blockchain data collection is used to populate the target network model. This allows for the development of a knowledge graph for understanding the relationship between data assets in the ransomware-Bitcoin payment network and provides context to the machine learning systems used in this research.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACH	Automated Clearing House
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
AUSTRAC	Australian Transaction Reports and Analysis Centre
BTC	Bitcoin
C2	Command and Control
CDD	Customer Due Diligence
CDN	Content Delivery Network
CIA	Central Intelligence Agency
CKC	Cyber Kill Chain
CSV	Comma Separated Values
CTF	Counter-terrorism Financing
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities & Exposures
DAG	Directed Acyclic Graph
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force

FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FN	False Negative
FP	False Positive
FSI	Financial Services Institute
GCN	Graph Convolutional Network
GDS	Graph Data Science
IC	Intelligence Community
ICO	Initial Coin Offerings
ICP	Intelligence Collection Plan
IOC	Indicators Of Compromise
ISR	Intelligence, Surveillance & Reconnaissance
JSON	JavaScript Object Notation
KYC	Know Your Customer
LEA	Law Enforcement Agencies
ML	Machine Learning
MSB	Money Services Business
PCA	Principal Component Analysis
PII	Personal Identifiable Information

PDM	Problem Definition Model
RaaS	Ransomware as a Service
ROI	Return On Infections
RPPI	Ransom Payments per Infection
SEC	Securities and Exchange Commission
SDO	STIX Data Object
SRO	STIX Relationship Object
SCO	STIX Cyber Observable
STIX	Structured Threat Information eXpression
STR	Suspicious Transaction Reporting
SRBF	STIX-Ransomware-Bitcoin Framework
TN	Ture Negative
TNM	Target Network Model
TP	True Positive
TOR	The Onion Router
U.S DOJ	United States Department of Justice
VA	Virtual Assets
VASP	Virtual Asset Service Providers

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: _____

Date: _____28th October 2022____

Authorship Contribution Statement

Chapter 2

1. Details of publication and corresponding author

Title of Publication		**Publication status**
Analysis Techniques for Illicit Bitcoin Transactions.		Published
Name of corresponding author	**Department/Faculty**	**Publication details** (Submission required in American English)
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner A. B.**, McCombie, S., and Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science*, 2: 600596. doi: 10.3389/fcomp.2020.600596

2. Student Declaration

Name of HDR thesis author	**Department/Faculty**	**Thesis title**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware
Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors		
This publication draws from my experience, as the main author, combined with the expertise of the co-authors, Stephen McCombie and Allon Uhlmann. I contributed to the assessment of both the technical and non-technical aspects of cryptocurrency analysis. Specifically, I developed the examination of the current scope of analysis in place for illicit cryptocurrency transactions, articulated the gaps, and recommended additional graph data science approaches which are elaborated on during the course of the whole thesis. The secondary authors, McCombie and Uhlmann, contributed theoretical observation and methodological approaches relevant to cybersecurity. Specifically, McCombie contributed insight into ransomware tactics, techniques, and procedures. Uhlmann contributed methodological insights into the construction of intelligence analysis, and how to translate specific insight into ransomware into actionable intelligence. I, as the main author, took responsibility for integrating the different contributions into a coherent analysis, in consultation with the other two authors.		
I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022	

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Allon Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Analysis and interpretation Writing the paper
Stephen McCombie (Associate Supervisor and Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

i. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

ii. that there are no other authors according to these criteria,

iii. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

iv. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	Authorised * By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)	Date
Allon Uhlmann	Authorised by email	1/5/2022
Stephen McCombie	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	Storage Location or DOI	Name of custodian if other than the corresponding author

Chapter 3

1. Details of publication and corresponding author

Title of Publication		**Publication status**
A target-centric intelligence approach to WannaCry 2.0		Published
Name of corresponding author	**Department/Faculty**	**Publication details**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner, A.B.**, McCombie, S. and Uhlmann, A. J. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control*, 22(4): 646-665. https://doi.org/10.1108/JMLC-01-2019-0005

2. Student Declaration

Name of HDR thesis author	**Department/Faculty**	**Thesis title**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware

Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors

This publication draws from my experience, as the main author, combined with the expertise of the co-authors, Stephen McCombie and Allon Uhlmann. I suggested the application of a Target Network Model (TNM) to the intelligence collection and analysis of a ransomware-Bitcoin problem definition. The co-author, Allon Uhlmann, proposed taking a target centric intelligence approach to the problem. From there, I mapped out the Problem Definition Model (PDM) followed by the design and development of a generic TNM and system model that can be used for any ransomware-Bitcoin data collection and situation analysis. Furthermore, co-author Stephen McCombie proposed the examination of the Cyber Kill Chain (CKC) with respect to the WannaCry 2.0 ransomware attack. I then recommended focusing on the Command and Control (C2) and Actions on Objectives steps in the CKC to derive the intelligence needed on the cryptocurrency elements of a ransomware attack. Owing to this focus, a classification model was also proposed using the WannaCry 2.0 attack data to determine the modus operandi of the ransomware attackers.

I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Dr. Allon J Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper
Stephen J McCombie (Associate Supervisor and Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

v. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

vi. that there are no other authors according to these criteria,

vii. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

viii. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	Authorised * By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)	Date
Allon Uhlmann	Authorised by email	1/5/2022
Stephen McCombie	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	Storage Location or DOI	Name of custodian if other than the corresponding author

Chapter 4

1. Details of publication and corresponding author

Title of Publication		**Publication status**
Ransomware-Bitcoin threat intelligence sharing using Structured Threat Information Expression (STIX)		Submitted for publication
Name of corresponding author	**Department/Faculty**	**Publication details** (Submission required in American English)
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner, A.B.**, McCombie, S. and Uhlmann, A. J. (2022). Ransomware-Bitcoin threat intelligence sharing using Structured Threat Information Expression (STIX), *IEEE Security & Privacy*. DOI: 10.1109/MSEC.2022.3166282 Manuscript Number: SP-2021-07-0157

2. Student Declaration

Name of HDR thesis author	**Department/Faculty**	**Thesis title**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware
Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors		
As the main author of this publication, I explore the application of the STIX framework to Cyber Threat Intelligence collected and shared relating to cryptocurrency transaction data of ransomware. Stephen McCombie as a co-author provided guidance and application of the traditional STIX framework with MITRE ATTCK patterns. Allon Uhlmann as the other co-author guided the discussion on intelligence collection and how to approach the disruption of a suspicious cryptocurrency payment network. As a result I developed the STIX Ransomware-Bitcoin Framework (SRBF) as a model of Cyber Threat Intelligence using STIX for a Ransomware-Bitcoin scenario. This publication also collected a volume of data to populate the SRBF. This data was collected by me as the main author and also made available at IEEE Dataport, doi: https://dx.doi.org/10.21227/1amp-n662.		
I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022	

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Dr. Allon J Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper
Stephen J McCombie (Associate Supervisor and Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

ix. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

x. that there are no other authors according to these criteria,

xi. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

xii. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	**Authorised *** **By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)**	**Date**
Allon Uhlmann	Authorised by email	1/5/2022
Stephen McCombie	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	Storage Location or DOI	Name of custodian if other than the corresponding author
Turner, A. December 22, 2021, "Bitcoin blockchain data of address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"	IEEE Dataport, doi: https://dx.doi.org/10.21227/1amp-n662.	

Chapter 5

1. Details of publication and corresponding author

Title of Publication		Publication status
Discerning payment patterns in Bitcoin from ransomware attacks		Published
Name of corresponding author	**Department/Faculty**	**Publication details**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner, A. B**., McCombie, S. and Uhlmann, A. J. (2020). Discerning payment patterns in Bitcoin from ransomware attacks, *Journal of Money Laundering Control*, 23(3): 545-589. https://doi.org/10.1108/JMLC-02-2020-0012

2. Student Declaration

Name of HDR thesis author	Department/Faculty	Thesis title
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware
Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors		
As the main author of this paper I investigate the available forensic data on the Bitcoin blockchain to identify typical transaction patterns of ransomware attacks. I specifically created the Ransomware–Bitcoin Intelligence–Forensic Continuum framework to search for transaction patterns in the blockchain records from actual ransomware attacks. I performed the data analysis of a number of		

different ransomware Bitcoin addresses that were extracted to populate the framework, via the WalletExplorer.com programming interface. I explored the idea of assembling the data in a representation of the target network for pattern analysis on the transaction input (cash-in) and transaction output (cash-out) side of the ransomware seed addresses. Allon Uhlmann as a co-author guided the exploration and analysis of how distinct these patterns are and their potential value for intelligence exploitation in support of countering ransomware attacks. Stephen McCombie provided the concepts of examining the data over a transient period spanning the the moments before and after a ransomware attack. Furthermore, Stephen suggested the use of a control case where the ransomware results were compared to a "control" network derived from a Bitcoin charity. This allows the reader to discern between ransomware payment patterns opposed to other types of payments made on the Bitcoin network.	
I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Dr. Allon J Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper
Stephen J McCombie (Associate Supervisor and Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

xiii. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

xiv. that there are no other authors according to these criteria,

xv. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

xvi. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	Authorised * By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)	Date
Allon Uhlmann	Authorised by email	1/5/2022
Stephen McCombie	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	Storage Location or DOI	Name of custodian if other than the corresponding author

Chapter 6

1. Details of publication and corresponding author

Title of Publication		Publication status
Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network.		Published
Name of corresponding author	**Department/Faculty**	**Publication details**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner, A.**, McCombie, S. and Uhlmann, A. (2021). Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network. In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 1560). http://hdl.handle.net/10125/70801

2. Student Declaration

Name of HDR thesis author	Department/Faculty	Thesis title
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware

Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors

As the main author of this paper, I used a number of data science techniques, (Graph Embeddings, clustering and Cosine Similarity), to develop a relative risk score of nodes (Bitcoin addresses and transactions) on a Bitcoin payment network related to a ransomware campaign. The co-authors, Stephen and Allon provided editorial review and guidance on how best to develop the continuity of my findings. Building on the data already collected, the application of these techniques to this type of scenario allowed me to construct the scope and logic of what role an individual node and a community of nodes represents relative to the ransomware-seed address. The utility of this approach can be applied to other cryptocurrency payment networks that need a representation of risk.

I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Dr. Allon J Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper
Stephen J McCombie (Associate Supervisor and Professor of Maritime IT Security, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

xvii. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

xviii. that there are no other authors according to these criteria,

xix. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

xx. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	Authorised * By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)	Date
Allon Uhlmann	Authorised by email	1/5/2022
Stephen McCombie	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	Storage Location or DOI	Name of custodian if other than the corresponding author

Chapter 7

1. Details of publication and corresponding author

Title of Publication		Publication status
Classifying ransomware-Bitcoin nodes using graph embeddings.		Submitted for publication
Name of corresponding author	**Department/Faculty**	**Publication details**
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	**Turner, A.**, Muhammad, I., and Uhlmann, A. (TBD). Classifying ransomware-Bitcoin nodes using graph embeddings. Submitted to Journal of Online Trust and Safety (April 21, 2022), https://tsjournal.org/index.php/jots/authorDashboard/submission/52)

2. Student Declaration

Name of HDR thesis author	Department/Faculty	Thesis title
Adam Turner	Department of Security Studies and Criminology, Faculty of Arts, Macquarie University	Addressing the intelligence applications of Bitcoin payments related to ransomware

Description of HDR thesis author's contribution to planning, execution, and preparation of the work if there are multiple authors

As the main author of this publication, I apply the GraphSage embedding algorithm in a semi-supervised method to derive a classification of nodes on a ransomware-Bitcoin payment network. I created the classification labels (small_tx_cluster, seed_target_cluster and large_tx_cluster) and the system for the multi-classifier to be able to use data collected and learn the context of these labels. In addition, an auxiliary feature, exposure, is developed to describe the amount of exposure nodes on this network have to the facilitation of ransomware payments. Co-author Muhammed, provides assistance with the data science techniques to help me represent what the False Positives and True Positives are from my dataset. Allon as a co-author helped me interpret what the results actually mean in the context of intelligence collection, where experts might be able to use such data and how it integrates into an investigation process.

I declare that the above is an accurate description of my contribution to this publication, and the contributions of other authors are as described below.	Student signature: Date: 30 April, 2022

3. Description of all other author contributions

Name and affiliation of author	Intellectual contribution(s)
Adam Turner (PhD candidate and corresponding author, Macquarie University, Australia)	Concept and design Planning and implementation Data collection Analysis and interpretation Writing the paper Overall project responsibility
Dr. Allon J Uhlmann (Associate Supervisor, Visiting Professor of Intelligence Studies, Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands)	Concept and design Planning and implementation Analysis and interpretation Writing the paper
Dr. Muhammad Ikram (Associate Supervisor and Lecturer, Department of Computing, Macquarie University, Australia)	Concept and design Planning and implementation Analysis and interpretation Writing the paper

4. Author Declarations

I agree to be named as one of the authors of this work, and confirm:

xxi. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,

xxii. that there are no other authors according to these criteria,

xxiii. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,

xxiv. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	**Authorised *** **By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)**	**Date**
Allon Uhlmann	Authorised by email	1/5/2022
Muhammad Ikram	Authorised by email	1/5/2022

5. Data Storage

The original data for this project are stored in the following location, in accordance with the Research Data Management Standard accompanying the Macquarie University Research Code.

Data description/format	**Storage Location or DOI**	**Name of custodian if other than the corresponding author**

MACQUARIE University

ADAM TURNER <adam.turner@students.mq.edu.au>

Author Declarations for Final PhD Report

Stephen McCombie Sun, May 1, 2022 at 6:08 PM
To: Allon Uhlmann <allon.uhlmann@mq.edu.au>
Cc: Adam Turner <adam.turner@students.mq.edu.au>

Adam,
Likewise I confirm the declaration below as requested. Let me know if you need anything else.

Regards
Stephen

Sent from my iPhone

> On 1 May 2022, at 7:49 am, Allon Uhlmann <allon.uhlmann@mq.edu.au> wrote:
>
> Adam,
>
> With this email I confirm the declaration below as requested.
>
> All the best,
>
> Allon
>
> **Allon J Uhlmann, PhD**
> Intelligence Studies and Cyber Security
>
> **T:** +61 (0)2 9850 1449 | **F:** +61 (0)2 9850 1440
> **E:** allon.uhlmann@mq.edu.au | **Academic Profile**
>
> **From:** ADAM TURNER <adam.turner@students.mq.edu.au>
> **Sent:** Sunday, 1 May 2022 00:30
> **To:** Stephen McCombie ; Allon Uhlmann <allon.uhlmann@mq.edu.au>
> **Subject:** Author Declarations for Final PhD Report
>
> Hi Stephen and Allon,
>
> Just doing some formalities on the final report and realise I need to obtain your authorisations for the following work we published. If you just confirm via reply to this email, I believe it satisfies the authorisation requirements below.
>
> **Turner A. B.**, McCombie, S., and Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science,* 2: 600596. doi: 10.3389/fcomp.2020.600596

Turner, A.B., McCombie, S. and Uhlmann, A. J. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control*, 22(4): 646-665. https://doi.org/10.1108/JMLC-01-2019-0005

Turner, A.B., McCombie, S. and Uhlmann, A. J. (TBD). Ransomware-Bitcoin threat intelligence sharing using Structured Threat Information Expression (STIX), *IEEE Security & Privacy* Digital Object Identifier: 10.1109/MSEC.2022.3166282 Manuscript Number: SP-2021-07-0157

Turner, A. B., McCombie, S. and Uhlmann, A. J. (2020). Discerning payment patterns in Bitcoin from ransomware attacks, *Journal of Money Laundering Control*, 23(3): 545-589. https://doi.org/10.1108/JMLC-02-2020-0012

Turner, A., McCombie, S. and Uhlmann, A. (2021). Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network. In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 1560). http://hdl.handle.net/10125/70801

Author Declarations

I agree to be named as one of the authors of this work, and confirm:

i. that I have met the authorship criteria set out in the Authorship Standard, accompanying the Macquarie University Research Code,
ii. that there are no other authors according to these criteria,
iii. that the description in Section 3 or 4 of my contribution(s) to this publication is accurate,
iv. that I have agreed to the planned authorship order following the Authorship Standard.

Name of author	Authorised * By Signature or refer to other written record of approval (e.g., pdf of a signed agreement or an email record)	Date
Allon Uhlmann		
Stephen McCombie		

Kind Regards,

Adam

MACQUARIE University

ADAM TURNER <adam.turner@students.mq.edu.au>

Author Declarations for Final PhD Report

Muhammad Ikram <muhammad.ikram@mq.edu.au> Sat, Apr 30, 2022 at 5:40 PM
To: Adam Turner <adam.turner@students.mq.edu.au>, Ikram Muhammad Allon Uhlmann <allon.uhlmann@mq.edu.au>

Hi Adam,

Thank for your email.

I confirm the submission to TS journal.

With bests,
Ikram

From: ADAM TURNER <adam.turner@students.mq.edu.au>
Sent: Sunday, May 1, 2022 12:33 AM
To: Muhammad Ikram <muhammad.ikram@mq.edu.au>; Ikram Muhammad Allon Uhlmann <allon.uhlmann@mq.edu.au>;
Subject: Fwd: Author Declarations for Final PhD Report

Hi Ikram and Allon,

Just doing some formalities on the final report and realise I need to obtain your authorisations for the following work we published. If you just confirm via reply to this email, I believe it satisfies the authorisation requirements below.

Turner,
A., Muhammad, I., and Uhlmann, A.
(TBD). Classifying ransomware-Bitcoin nodes using graph embeddings. Submitted to Journal of Online Trust and Safety (April 21, 2022).

https://tsjournal.org/index.php/jots/authorDashboard/submission/52

Acknowledgments

This research is supported by an Australian Government Research Training Program (RTP) Scholarship.

When I was younger my father used to whistle and sing to me the tune made famous by Monty Python's *The Life of Brian: ♪Always look on the bright side of life♪* (Jones et al, 1999). In addition, a good friend of mine would always encourage me to keep a "*stiff upper lip.*" Reflecting over the course of this PhD project, whether consciously or subconsciously, these two pieces of sage advice have enabled me to keep my spirits high and my head down when needed. Sadly, my father will not be around to share in the pride and jubilation of completing my thesis; however, he remains a pillar of my strength beyond the physical world and for that I would like to dedicate this body of work to him. I would also like to acknowledge and dedicate this work to my wife and two daughters. The love, support, and encouragement they have shown me beyond this project is immense. And Mum, without a doubt I thank you for the sacrifices you have made to get me where I am today.

Having worked on the entirety of this project remotely from Munich, Germany, it is only befitting to acknowledge the inspiration taken from my surroundings. There were many long days sitting in the Bavarian State Library (Bayerische Staatsbibliothek), an

architectural marvel to be inspired by. I'll never forget the German words of wisdom I picked up along the way: "*Anfangen ist leicht, Beharren eine Kunst*" (Literal: Starting is easy, persistence is an art) and "*Alles hat ein Ende, nur die Wurst hat zwei*" (Literal: Everything has an end, only the sausage has two). Thank you also to those who have helped me over the course of this project, including Aleš Jander for providing Application Programming Interface (API) access to the Bitcoin tracing tool wallertexplorer.com (which allowed me to collect the data I needed for this project) and Ravi Nayar for always popping up with a link to some very poignant research relating to ransomware and cyber security.

Finally, I would like to thank my supervisor Dr. Allon Uhlmann and associate supervisors Stephen McCombie and Dr. Muhammad Ikram. They gave me the unrelenting support I needed whilst being a long way from home base. They always made themselves available at weird and wonderful hours of the day, maintaining the discipline and cadence for our regular meetings. Above all they provided the guidance and feedback needed for me to correct my course whilst running down many different rabbit holes.

Chapter 1: Introduction

"*Genesis*." – The term given to the first ever Bitcoin transaction[1].

1.1 Chapter Overview

This chapter presents the research background (Section 1.2), the development of a lucrative ransomware-cryptocurrency nexus (Section 1.3), and the transparency of cryptocurrency systems (Section 1.4). Section 1.5 details the escalating threat of ransomware attacks, Section 1.6 describes attempts to combat these attacks, and Section 1.7 provides an overview of existing strategies and analysis utilised in the investigation process. Section 1.8 presents the aims and scope of this body of research and Section 1.9 provides an overview of the structure of this thesis. Finally, Section 1.10 concludes this chapter.

1.2 Background: Setting the scene

The origins of ransomware can be traced back to 1989 where Joseph L. Popp, a biologist from Harvard, distributed around 20,000 floppy disks labelled *AIDS Information – Introductory Diskettes* to attendees of the World Health Organisation's international AIDS conference (Laffan, 2020). The disks contained the AIDS Trojan, also known as PS Cyborg (Richardson and North, 2017). The malware encrypted user files, locking

[1] The first 'Genesis' Bitcoin transaction can be viewed via a blockchain explorer, for example, blockchain.com: https://www.blockchain.com/btc/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

their access, and crafted a ransom message that indicated the user was in breach of their licensing agreement. The message directed the user to pay via cheque to a post box in Panama the amount of $US 189 to renew their license and decrypt their files (Hampton and Baig, 2015). Malware enthusiasts continued to pursue their hobby throughout the late 1990s. Technical dominance of a computer system was seen as the ultimate status hack to their peer group. This was until the realisation, in the early 2000s, that significant monetary gains were possible by hijacking computer systems to conduct information theft (Bechtel, 2014) and obtain user banking credentials (Condon, 2012). Due to the lack of online payment facilities, this trend continued up until 2005. Victims were instructed to pay ransoms via SMS text messages or by mailing prepaid gift cards and telephone calling cards that enabled the attacker to earn money (Zetter, 2015). These payment methods were deemed risky, since they did not afford the attackers any anonymity and an investigator could easily trace them back to the attacker via postal, retail purchase or telephone records.

In 2008 ransomware hit new heights with the advent of digital currencies such as Bitcoin, which gave cyber criminals a means for extorting their victims for financial gain rather than simply destroying files and dominating computer systems. A first instance of ransomware leveraging digital currency occurred in 2008 using a digital currency known as e-gold. The ransomware variant GPcode.AK encrypted files and asked for ransom payments between $US 100 and $US 200 in e-gold and another digital currency known as Liberty Reserve (Tromer, 2008). Direct end-user extortion could now be facilitated by a cryptocurrency payment facility that granted attackers a cloak of anonymity or pseudonymity, which made attribution of their crime much more convoluted and complex due to the peer-to-peer nature of cryptocurrency and lack of

regulation. Needless to say, the United States (U.S) government became suspicious of these digital currency payment facilities and in the case of both e-gold and Liberty Reserve, the U.S government found legal means to shut the operators of these businesses down. In the case of e-gold, plea deals were made with the company and the directors, Douglas L. Jackson and Barry K. Downey, where they were found guilty of the "operation of an unlicensed money transmitting business" and "conspiracy to engage in money laundering" (e-gold Legal Update, 2008). Liberty Reserve, who allegedly laundered more than $US 6 billion in criminal proceeds suffered a similar fate (Cloherty, 2013). The U.S. Southern District of New York led an international investigation that charged seven people with operating an unlicensed money transmitting business and money laundering, and consequently shut down the service in May 2013 (UNODC, 2021).

1.3 A Lucrative New Nexus is Formed

The first real usage of Bitcoin in a ransomware attack was CryptoLocker, which was released in September 2013 and infected over 500,000 machines up until May 2014 (Richardson and North, 2017). The delivery mechanism for CryptoLocker was the Gameover Zeus banking Trojan. This bank targeting malware group saw an opportunity in encrypting data for ransom. The threat actors behind the botnet[2] made the link between password stealing malware that targeted financial services institutions (FSIs) through Automated Clearing House (ACH) and wire fraud attacks (Crowdstrike, 2021a). The attackers were now able to augment profits from cybercrime by collecting ransom payments by holding computer systems and data hostage through strong

[2] "A botnet is a network of compromised computers that are supervised by a command and control (C&C) channel" (Crowdstrike, 2021b).

encryption mechanisms. Ultimately, the FBI in coordination with international law enforcement efforts shut down the CryptoLocker Gameover Zeus operation (U.S. Department of Justice (DOJ), 2014). This worldwide collaboration saw the identification and seizure of command and control computers acting as launch hubs for CryptoLocker. Researchers have estimated that more than $US 27 million in ransom payments were made during the early stages of the CryptoLocker ransomware campaign (U.S. DOJ, 2014). However, while Conti et al (2018) identify over 51,000 payments in their analysis of CryptoLocker, only 804 are ransom payments, taking CryptoLocker's economic gain from the attack to 1403.7548 BTC or $US 449,274.97 using the exchange rate of BTC: USD at the time (Conti et al, 2018). This shows a great disparity in the analysis techniques of ransomware related payments. Regardless, CryptoLocker had created a critical inflection point in the world of profiteering from cybercrime. The era of ransomware had kick-started an unstoppable moment.

Perhaps the most infamous example is the WannaCry ransomware attack. This attack is repeatedly used for analysis throughout this research due to its widely reported analysis and investigation. WannaCry infected over 300,000 machines and collected 248 ransom payments from the beginning of the campaign on May 12th to October 2nd 2017 (Europol, 2017). WannaCry is utilised as a case study to determine the targets, vulnerabilities, and cryptocurrency payments evident in a modern-day ransomware attack. The WannaCry ransomware can spread itself to any unpatched computer on the victim's network or the Internet, behaving like a worm. Analysis of the WannaCry ransom payment collection by Bistarelli et al (2018) found 248 ransomware payments totalling 50.14 BTC. Although this attack collected significantly fewer ransom payments than CryptoLocker, WannaCry gained notoriety due to its attribution to state

based hackers from the Democratic People's Republic of Korea (DPRK) (North Korea) (U.S. District Court, Central District of California, 2018). A recent U.S federal indictment identified three military hackers from the DPRK in a scheme committing cyberattacks and financial crimes across the globe (U.S. DOJ, 2021a). This indictment expanded from the 2018 case that detailed the Lazarus group (originating from the DPRK) attack on Sony Pictures and the creation of WannaCry (Park, 2021).

The combination of a malware attack that leverages the highly unregulated world of cryptocurrency poses a new threat to organisations, security researchers, law enforcement, and the intelligence community. The challenges that these stakeholders face revolve around how to protect computer assets from these new threats, how to collect and analyse threat data for situational understanding of the threat, and how to investigate these crimes. Taking a traditional cyber security lens to analyse a ransomware attack may prepare an organisation against the threat of malware, for example by having strong IT security policy, backup and restore facilities, regular application security updates, and other internal controls to mitigate risk to business interruption. However, once systems are infected and ransom payment requests start being made, it is necessary to ask whether it is possible to reclaim these payments, understand who is controlling them, where the transactions are taking place, and how the proceeds of crime are being utilised.

1.4 Transparent System, Dirty Money

The analysis and investigation of financial crimes that ransomware actors knowingly undertake to extort their victims is possible due to the open nature of the Bitcoin network. Each transaction is freely available to analyse as part of the blockchain

technology that enables Bitcoin peer-to-peer payments (Nakamoto, 2008). The transparency of the Bitcoin system can prove advantageous to law enforcement, investigators, and intelligence analysts to understand patterns of payment behaviour by analysing the vast amount of transaction data available on the Bitcoin blockchain. There are sophisticated tools commercially available on the market for investigators and cryptocurrency exchanges to use in order to address the operational risks associated with cryptocurrency as well as provide help to law enforcement in tracking down ransomware payments. For example, Chainalysis supported U.S authorities in disrupting the NetWalker ransomware attack (Chainalysis, 2021b). However, it does not seem to stem the tide of ransomware attacks, even with the transparency of transactions, access to Bitcoin ledger data, and available commercial tooling. The financial gains attackers are making out of this type of cybercrime are compounding every year.

1.5 Ransomware an escalating threat

Across the main cryptocurrencies Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH), and Tether[3] (USDT), in 2016 approximately $US 20 million of ransoms were paid by victims and in 2020 this reached almost $US 350 million worth of ransoms received by ransomware addresses, a 311% increase from 2019 (Chainalysis, 2021a). The 2021 Chainalysis Cryptocrime report further identifies the distribution of ransom payments collected per year by specific ransomware strain. In 2019 and 2020 the dominant ransomware strain was Ryuk, which collected around $US 200 million during

[3] Tether is a stable coin that follows the price of the U.S Dollar. Stablecoins are seen as a cryptocurrency without the pricing volatility. This is achieved by pegging their digital currency to an underlying asset such as a fiat currency (CoinMarketCap, 2021: see: https://coinmarketcap.com/currencies/tether/)).

that period (Chainalysis, 2021a). This could be owing to the large ransom being demanded by the attackers in the range of 15 to 50 BTC ($US 574,690 to $US 1,915,632 at current exchange rates[4]) and the high profile targets they were after, such as EMCOR, UHS hospitals, and Tribune publishing newspapers (Malwarebytes, 2020). Adding to that,Further, cryptocurrencies create a new payment network where traditional techniques for illicit financial investigation, such as Anti-Money Laundering (AML) and Counter Terrorism Financing (CFT), do not apply. Identifying the money laundering infrastructure ransomware attackers use and the strategies they take is key intelligence in the fight against ransomware.

The cryptocurrency funds being cashed out of ransomware wallets have a variety of destinations. For example, from 2015 to date, ransomware attackers moved most of their victims' ransom payments to mainstream exchanges; in fact, a group of five exchanges (unnamed in the Chainalysis Cryptocrime Report) received 82% of all ransomware funds (Chainalysis, 2021a). Other destinations include high-risk exchanges (these are exchanges with minimal to no financial compliance standards and may facilitate exchange into more anonymous cryptocurrencies like Monero), mixers (which are used to obfuscate the origin of a transaction and employing typical money laundering techniques that place and layer the illicit transactions among other legitimate transactions), and other criminally controlled cryptocurrency addresses.

Furthermore, the ransomware threat is constantly evolving. For example, in 2020, security researcher RiskSense identified 223 unique Common Vulnerabilities and Exposures (CVEs) that were attributed to 125 ransomware families. That is nearly four

[4] https://coinmarketcap.com/currencies/bitcoin/ (Accessed on: 30 April, 2022)

times as many CVEs as the prior year and approximately a seven-fold increase in the number of ransomware families (RiskSense, 2021).

1.6 Combating the proliferation of ransomware

New strains of ransomware are continuously emerging. In 2019 and 2020, as previously mentioned, the dominant strain with respect to collected ransom payments was Ryuk. However, new entrants in 2020, namely Netwalker, Maze, and DoppelPaymer, collected an approximately combined amount of $US 100 million (Chainalysis, 2021a). DoppelPaymer in particular dominated the scene in 2020, demanding ransom payments from $US 25,000 to $US 1.2 million (Nair, 2020) and attacking high profile targets such as Pemex (a Mexican state-run oil company), Germany's Düsseldorf University Clinic, and Chile's Ministry of Agriculture (Schwartz, 2020). Investigators and researchers are finding that nation state actors are behind these ransomware strains. RiskSense (2021) identified China behind Maze, North Korea had links to WannaCry, and Russia is said to be behind DoppelPaymer and NotPetya.

These threat actors are also changing their business model, as they are now looking to license their infections, enabling Ransomware as a Service (RaaS). This allows the creators of the ransomware to make money off other attackers using their variants of ransomware without the creators even conducting the attack. Cybercrime intelligence firm Intel 471 (2020) identified the big five players using the RaaS model. These are DoppelPaymer, Egregor/Maze, Netwalker, REvil (aka Sodinokibi), and Ryuk (Intel 471, 2020). All of these strains have emerged since 2019 and have been collectively involved and evident in close to 750 ransomware attacks in 2020 (Intel 471, 2020). Their targets are indiscriminate, yet they widely appear to be attacking critical

infrastructure. For example, a recent attack on the Colonial Pipeline in the United States by the cybercriminal group DarkSide in May 2021 resulted in gas shortages across the U.S East Coast, with Reuters reporting 30% of gas stations in metro Atlanta being without gasoline (Kumar and Sanicola, 2021). Furthermore, the New York Times reported closure of more than 5,500 miles of gas pipeline, stretching from the state of New Jersey to the state of Texas (Sanger and Perlroth, 2021). The FBI attributes DarkSide to a Russia-based cybercrime group (FBI National Press Office, 2021). Whilst DarkSide exhibits the traits of a modern ransomware attack (i.e., using RaaS, being state-backed, and targeting an adversary's critical infrastructure), the attack on the Colonial Pipeline also revealed a success for law enforcement and conviction in their strategies and tactics against ransomware threats.

1.7 Strategies and analysis considerations

Law enforcement seized a total of $US 2.3 million in cryptocurrency paid to DarkSide as a result of the Colonial Pipeline attack (U.S. DOJ, 2021b). This amounted to 63.7 bitcoins and roughly half the $US 4.4 million Colonial paid to the hacker group. This was widely viewed as a significant win for the Ransomware and Digital Extortion Task Force created specifically to disrupt the rise of ransomware attacks (Roney, 2021). Although details are scant on how the FBI obtained the private key and password associated with the Bitcoin wallet that was seized containing the illicit funds, according to Deputy Attorney General Lisa O. Monaco, the strategies and analysis that worked in this case focused on "following the money [as it] remains one of the most basic, yet powerful tools we have" (U.S. DOJ, 2021b). This approach alone will not sustainably yield the prevention of ransomware.

Therefore, there is a need for an emerging branch of cryptocurrency data collection, analysis, and sharing to understand and mitigate the ransomware threat and to combat their money laundering strategies on cryptocurrency networks. The ability to find connections between ransomware strains and common deposit addresses (to which funds are sent by attackers using money laundering services that are frequented by different strains of ransomware) yields important information to intelligence analysts, law enforcement, and security researchers. It provides an opportunity to disrupt an overarching ability of multiple ransomware strains to cash out their illicit proceeds by taking one targeted exchange being used for money laundering offline (Chainalysis, 2021a). Other strategies ransomware attackers employ when it comes to the processing of ransom payments collected include a collect and hold strategy (where the attackers are happy to wait and sit on the cryptocurrency until such time the cryptocurrency value has grown or sufficient time has passed to enable the attackers to utilise the funds without scrutiny) and a pass-through strategy (where ransom payments are collected and immediately moved on, possibly to avoid any detection thresholds that may be triggered due to the accumulation of illicit funds in a certain cryptocurrency address). These strategies are examined in detail in Chapter 4.

Relevant legal and enforcement authorities are harnessing these capabilities to tackle the rise in ransomware attacks. The recent collaboration between the FBI and Chainalysis facilitated "coordinated international law enforcement action to disrupt a sophisticated form of ransomware known as NetWalker" (U.S. DOJ, 2021c). There is movement by regulators and jurisdictions on the policy side to enforce stricter adherence to legal and ethical usage of cryptocurrency. As detailed in Chapter 1, financial governing bodies, regulators, and law enforcement such as the Financial

Action Task Force (FATF), the Financial Crimes Enforcement Network (FINCEN), Australian Transaction Reports and Analysis Centre (AUSTRAC), the European Union's sixth Anti-Money Laundering Directive, U.S Department of Treasury, U.S Security and Exchanges Commission (SEC), Europol, and Interpol are mandating additional data points and reporting requirements for investigators to leverage. For example, the Department of Homeland Security (2014) identified the need for official departments such as the Financial Action Task Force (FATF, 2015) and the Financial Crimes Enforcement Network (FinCEN, 2013) to develop analysis tools for law enforcement to assist them in financial crime investigations using Bitcoin. This provides transparency when it comes to attribution of any illicit activity relating to cryptocurrency services such as exchanges and enforces the application of Know Your Customer (KYC), Customer Due Diligence (CDD), and Suspicious Transaction Reporting (STR) practices.

Policy instruments certainly assist the investigation process from a regulatory or industry partnership approach (Lim, 2015), or through AUSTRAC, FinCEN, and the FATF for traditional financial crimes such as Money Laundering (ML) or Terrorism Financing (TF). However, the effectiveness of these models requires further testing against a wider range of Bitcoin-related cybercrime, specifically ransomware, which is the focus of this thesis.

1.8 Thesis aims and scope

This research addresses the evolving threat of the use of cryptocurrency in ransomware attacks. From 2019 to 2020 a 311% increase in ransomware cryptocurrency payments

occurred, with $US 350 million paid by victims of ransomware attacks in 2020 (Chainalysis, 2021a).

This thesis by publication, comprising four published research papers, a published conference proceeding paper, and two research papers submitted for journal publication, demonstrates the utility of taking a target centric approach to intelligence collection and analysis of a ransomware-cryptocurrency network. Utilising graph analysis techniques applied to data gathered from the Bitcoin blockchain, this research addresses challenges security researchers face in preventing the propagation of ransomware payments throughout cryptocurrency networks as well as determining the accountability of such payments. This cross-disciplinary research explores areas of law and policy development, financial regulation and compliance, computer science, security and intelligence, and behavioural aspects that reveal patterns to criminal payments as they move through the Bitcoin ecosystem.

This thesis primarily focuses on the ransomware campaign WannaCry 2.0 in order to determine the targets and vulnerabilities evident in a modern-day ransomware attack. WannaCry infected over 200,000 machines and collected 238 ransom payments from May 12th to October 2nd, 2014 (Europol, 2017). By breaking down the WannaCry system and ransomware kill chain, a timeline can be formed to understand the key elements from mobilisation to cashing out the ransom payments collected in Bitcoin and the involvement of the actors along the continuum. To complement the WannaCry 2.0 data, this research also uses data collected from the Bitcoin blockchain relating to the respective ransomware seed addresses (Bitcoin addresses that are set up by ransomware attackers to collect ransom payments) for ransomware campaigns, namely

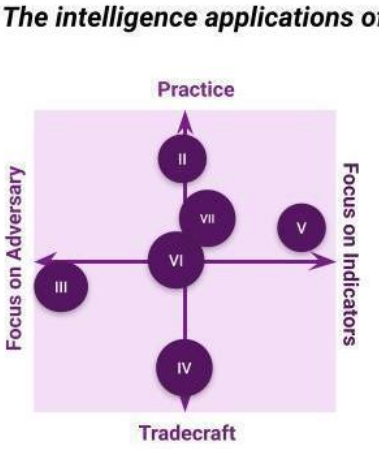
CryptoDefense, NotPetya, and a control subject, The Water Project (a charity set up to collect charity payments via Bitcoin). Ransomware related Bitcoin addresses, payment inflows and outflows, along with the respective payment mechanics are examined to create a graph model of the adversary. Several analyses are undertaken by tracing ransomware-Bitcoin transactions to certain Bitcoin exchanges and anonymising services. This research resulted in the creation of an innovative methodology for modelling a ransomware-Bitcoin attack as a graph. In addition, software has been developed to support the research efforts relating to data collection, analysis, and intelligence sharing.

The fraught nature of intelligence sharing underlines the importance of the need for collaboration between law enforcement agencies. In addition, understanding a common threat perception, building trust in the analysis and use of technology, and context of information provided are all contributing factors to enhancing intelligence cooperation (Seagle, 2015). Extracting threat intelligence for Bitcoin-related cybercrime proves a unique challenge due to the anonymity surrounding identities and transactions of cryptocurrencies (Gross and Acquisiti, 2005; Androulaki et al, 2013; Meiklejohn, 2013; Reid and Harrigan, 2013). Sharing Bitcoin threat intelligence becomes even more difficult unless transaction or address behaviours are mapped through a common understanding of the heuristics being deployed. Furthermore, to analyse these behaviours and profiled information there is a need to transform this data into insights via a common data interface or ontology, such as the Structured Threat and Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). These standards enable "automated cyber threat information exchange across organization and product boundaries" (Barnum, 2012, p.2). Other such models for

threat intelligence sharing are discussed in detail by Choi et al (2006), who also provide features for dimensional analysis as well as sharing. The problems relating to traditional intelligence collection techniques will be relevant for those applied to cryptocurrency investigations. The need for information sharing will be crucial as attackers can utilise the decentralised, transnational, and anonymous nature of Bitcoin.

Both quantitative and qualitative analysis techniques are utilised in this research project. For example, time series analysis on payments being made into and out of certain ransomware-controlled Bitcoin addresses are analysed to determine payment profile patterns. In addition, the study of ransomware-Bitcoin network patterns will allow typologies to be developed and tested, which will benefit the law enforcement community. Furthermore, process analysis and risk rating criteria are developed to enhance existing methods used to investigate ransomware-Bitcoin cybercrime. To support these and other methods, there will be a need to make use of internal and external data as well as utilise advanced machine learning technologies.

This research is collaborative and will create practical and academic outcomes to conceive a new area of study previously unexamined, that of ransomware-Bitcoin analysis. The combination of methodologies, theoretical frameworks, and technology will help counterbalance the weaknesses inherent in existing individual approaches. A meaningful continuum of themes this research elucidates is shown in Table 1.1.



Chapter	Article Title
II	Analysis Techniques for Illicit Bitcoin Transactions.
III	A target-centric intelligence approach to WannaCry 2.0
IV	Ransomware-Bitcoin threat intelligence sharing using Structured Threat Information Expression (STIX)
V	Discerning payment patterns in Bitcoin from ransomware attacks
VI	Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network
VII	Classifying ransomware-Bitcoin nodes using graph embeddings

Figure 1.1: The position of the chapters and their respective papers within the overarching thematic areas.

More specifically, a journey from tradecraft to practice is made with a cross-cutting focus on the adversary and data driven indicators, leading to the following objectives of this research:

O1: Identify the incumbent techniques used for analysis of illicit Bitcoin transactions. Use these techniques to explore the technical (blockchain) and non-technical (regulatory) mechanisms for identifying and preventing ransomware-Bitcoin payments.

O2: Based on the characteristics of a ransomware-Bitcoin network, develop a framework to classify a ransomware attack as destructive or revenue generating.

O3: Develop a ransomware-Bitcoin cyber threat intelligence sharing framework using the Structured Threat Intelligence eXpression (STIX) standard.

O4: Examine patterns of ransomware-Bitcoin transactions that determine common profiles and attacker behaviour on the Bitcoin payment network for deeper graph analysis.

O5: Derive a measure of risk in a ransomware-Bitcoin payment network that reveals nodes and communities that can be targeted for investigation and disruption.

1.9 Thesis structure

This thesis by publication is structured as follows. Chapter 1 sets out the aims and scope of the study, and the structure of the thesis relating to the publications that form the body of this work. The scene is set by introducing the background to ransomware, namely its origins and evolution into a lucrative class of cybercrime. The problem space is further explored by looking at the escalation of the threat and the challenges law enforcement faces in addition to the strategic and analytical considerations that may be deployed to help combat the proliferation of undetected ransomware related Bitcoin payments.

Chapter 2 comprises a paper published in *Frontiers of Computer Science* (Turner et al, 2020a), providing a comprehensive literature review of existing analytical techniques, from both a non-technical and technical perspective. Non-technical areas focus on the policy, regulatory and compliance measures being considered or that already exist in various jurisdictions across the world. The technical analysis techniques, which subsequent chapters of this thesis focus on, look at how to leverage vast amounts of data from a Bitcoin network so machine learning systems can be developed based on these data flows to gain a deeper understanding of ransomware-Bitcoin payment behaviour.

Chapter 3 presents a paper published in the *Journal of Money Laundering Control* (Turner et al, 2019) that develops a target-centric intelligence approach to a specific

Bitcoin ransomware incident (WannaCry 2.0). Here the Target Network Model (TNM) and the Problem Definition Model (PDM) are developed using the target centric approach to intelligence. These two artifacts create an analytical framework that provides a schematic for analysts to test their hypotheses, integrate, and share data for collaborative ransomware-Bitcoin investigations. This chapter uses data from the WannaCry 2.0 ransomware attack to help build this framework. Furthermore, in conjunction with the framework and by looking at the payment statistics for WannaCry 2.0, this chapter classifies ransomware attacks as tools of destruction versus revenue generating campaigns.

Chapter 4, a paper published in *IEEE Security & Privacy* (Turner et al, 2022), explores the possibility of using a common sharing standard such as STIX to share ransomware payment related cyber intelligence. This chapter designs an intelligence collection planning template with reference to the red flag indicators for Money Laundering (ML) and Terrorism Financing (TF) using Virtual Assets (VAs) from the Financial Action Task Force (FATF). This enables a deeper understanding of the ransomware-Bitcoin environment and points of vulnerability on the Bitcoin network. By focusing on data collection efforts, security researchers, law enforcement, and intelligence agencies can turn data into insights and populate Structured Threat Information Expression (STIX) objects for cyber threat intelligence sharing and analysis.

Chapter 5 comprises a paper published in the *Journal of Money Laundering Control* (Turner et al, 2020b) to discern Bitcoin payment patterns from well-known ransomware attacks (WannaCry, CryptoDefense, and NotPetya). Data collected is used to reveal patterns in a ransomware-Bitcoin payment network, with the aim to identify distinctive

patterns that are unique to ransomware attacks. For this reason, the research aims to distinguish ransomware payment patterns from potentially confusing similar charity donation patterns. Ransomware campaigns WannaCry 2.0, CryptoDefense, NotPetya, and a control subject, The Water Project, are examined based on the payments they receive into their collector or seed address (known as the cash-in network) and any payments moving out of these addresses (known as the cash-out network). Time series profiles and generic graph visualisations are used to determine what patterns are evident in the data both on the cash-in and cash-out networks.

The Ransomware–Bitcoin Intelligence–Forensic Continuum framework is created in this chapter to help understand activity taking place on the network prior to a ransomware campaign commencing and after the campaign when the attackers start to move their ransom funds into other networks. Part of the appeal of using cryptocurrency networks is that transactions are well disguised and not easily distinguishable between illicit and legitimate transactions on the network. This makes it difficult to identify bad actors amongst the masses of legitimate users of Bitcoin. However, because of this research, discernible patterns in the network relating to the input and output side of the ransomware graphs are evident. Collection profiles over time for ransomware output patterns differ from those associated with the charity addresses, as the attackers' cash-out tactics are quite different from the way charities mobilise their donations.

Chapter 6, published in the *Proceedings of the 54th Hawaii International Conference on System Sciences* (Turner et al, 2021) examines graph embeddings in more detail to reveal risky nodes in a ransomware-Bitcoin network using machine learning techniques. A system is developed that compares the relative position of different nodes

in a ransomware-Bitcoin network by calculating the similarity between the nodes. A riskiness score is then derived for individual nodes by following the money from the ransomware cash-out graph. In addition, analysing the derived "riskiness" at a community level (groups of nodes in the network) provides an enhanced granularity for identifying and targeting influential nodes. The score is attributed to risk as it identifies those nodes whose targeted removal or disruption from the network would risk the successful completion of the network's objectives. This method ultimately helps identify key nodes on the blockchain that are involved in the execution of a ransomware attack.

Chapter 7, a paper submitted to the *Stanford Journal of Online Trust & Safety*, develops a novel methodology to systematically identify ransomware transactions within cryptocurrency payment networks. This chapter extends the analysis from Chapter 6 by making modifications to the embedding algorithm used. The 'GraphSAGE' algorithm is used, rather than the 'DeepWalk' algorithm. This formalises a machine learning method that can be used for classification and prediction. Additional data is produced because of this analysis. The culmination of research conducted to this point and the additional data from this analysis provide rich context to define a knowledge graph for ransomware-Bitcoin transactions. The findings enhance the methodology originally described in Chapter 6 along with a focused implication on law enforcement investigations, resulting in a reusable model that adds connected context and knowledge discovery into investigation processes.

The appendices summarise the additional effort undertaken in software development required to analyse the large amounts of data used in this thesis.

1.10 Conclusion

This chapter outlined the objectives, scope, and structure of this research. Ransomware is an extremely prevalent threat in our current digitally interconnected world. The extensive research that follows will examine this threat from the perspective of collecting intelligence and building a model to analyse and target Bitcoin payments relating to the money flows from a ransomware attack. A considerable gap was uncovered when examining the literature relating specifically to ransomware-Bitcoin money flows. This research sets out to achieve five objectives to close this gap. Firstly, by understanding the status quo in the current literature. Then by developing, testing, and evaluating frameworks, models and analysis techniques that will support the intelligence community, law enforcement, and researchers in their quest for the detection, prevention, and deterrence of ransomware attacks using cryptocurrency. The next chapter examines some of the existing tools and techniques that are currently used to examine illicit Bitcoin transactions. The chapter reviews techniques that include both technical machine learning approaches as well as non-technical legal and governance considerations, all of which provide a foundation for understanding how to examine ransomware payments on a Bitcoin network.

Chapter 2: Analysis Techniques for Illicit Bitcoin Transactions

"*Analytical strategies are important because they influence the data one attends to. They determine where the analyst shines his or her searchlight, and this inevitably affects the outcome of the analytical process*." – Richards J. Heuer, Jr. (Heuer, 1999)

2.1 Abstract

This comprehensive overview of analysis techniques for illicit Bitcoin transactions addresses both technical, machine learning approaches as well as a non-technical, legal and governance considerations. We focus on the field of ransomware countermeasures to illustrate our points.

2.2 Introduction

This paper examines the current literature on the analysis of illicit Bitcoin transactions and focuses specifically on the analytic techniques that are applied to blockchain data. These illicit Bitcoin transactions could take the form of money laundering, terrorism financing or the movement of proceeds from other crimes such as ransomware attacks. Many of the techniques wrestle with the problem of attribution in the face of the anonymity of sources within the Bitcoin ecosystem. Therefore, we first examine the body of literature relating to regulatory efforts that aim to balance the freedom of an open system with the requirements of crime prevention and law enforcement. Following that is a review of the research into the techniques that exploit heuristics and behaviours inherent in the Bitcoin system. We then highlight the application of graph

analysis techniques to the Bitcoin ecosystem and transaction networks. Furthermore, Machine Learning (ML) and Artificial Intelligence (AI) techniques applied to money laundering, cybercrime and other illicit activities across the Bitcoin ecosystem are reviewed. Moreover, a focus is placed on the application of these techniques to the modern day threat of ransomware, a lucrative branch of contemporary global crime which in 2020 is estimated to cost companies anywhere between $US 42 billion and $US 170 billion worldwide in ransoms paid, lost productivity and other recovery expenses (Emsisoft, 2020).

2.3 Regulatory and Compliance Challenges

The regulatory landscape has continuously evolved since Nakamoto (2008) released the inaugural paper on Bitcoin, *A peer-to-peer electronic cash system.* The decentralized nature of the peer to peer network from which Nakamoto (2008) designed Bitcoin affords the user anonymity and bypasses the central authority used to regulate traditional financial systems.

2.3.1 The regulatory environment

Tsukerman (2015) surveys the state of the Bitcoin regulatory environment from a United States (US) centric position. To help understand this environment they provide a breakdown of the laws into two categories: those laws that protect consumers who use Bitcoin; and those that address the broader societal impacts of people using Bitcoin for illegal purposes such as money laundering and terrorist financing (Tsukerman, 2015). Tu and Meredith (2015) complement the work by Tsukerman (2015) by

considering the impediments to effective regulation of Bitcoin which addresses the issues of ownership, attribution and the susceptibility to theft, that virtual currencies are subject to. Wagstaff and Karpeles (2014) reported on the largest theft of Bitcoin at the Bitcoin exchange Mt Gox in February 2014. This breach saw the exchange lose 850,000 Bitcoins worth $US 450 million at the time. Reclamation of these stolen funds is identified as a major risk to users by Tu and Meredith (2015). Irwin and Turner (2018) argue that cryptocurrency systems, in contrast with traditional money transmission businesses and financial institutions, are relatively unhindered by anti-money laundering and counter-terrorism financing (AML/CTF) regulations. In addition, these systems do not collect the necessary Personal Identifiable Information (PII) that will allow for the implementation of strict financial transaction reporting procedures for the purposes of mitigating illicit financial activity and the misappropriation of funds (Irwin and Turner, 2018). The procedures discussed in Irwin and Turner (2018) aim to examine the atypical business dealings conducted over Bitcoin, along with the use of AML/CTF techniques potentially indicating illicit activity.

In June 2018, The Law Library of Congress (2018) published a paper on '*Regulation of Cryptocurrency in Selected Jurisdictions*'. This report provides a comprehensive review of the cryptocurrency regulation and policy stance of the following jurisdictions: Argentina, Australia, Belarus, Brazil, Canada, China, France, Gibraltar, Iran, Israel, Japan, Jersey, Mexico, Switzerland. For each of these jurisdictions, there is a foreign law specialist assigned to assess the legal conditions within the respective jurisdiction. During the introduction of this report, foreign law specialist Hanibal Goitom identifies the major issues jurisdictions are facing. Namely, the legality of cryptocurrency operations, issues around taxation and AML/CTF implications.

2.3.1.1 Legality of cryptocurrency markets

By revealing how different countries are legally operating cryptocurrency markets in their jurisdictions the report highlights specific laws enacted for cryptocurrency markets to operate and the contrasting jurisdictions that restrict their trade. It identifies the likes of Belarus, Gibraltar[5], Jersey[6], and Mexico have enacted laws specifically recognising cryptocurrency markets. For example, in Belarus The Presidential Decree on the Development of the Digital Economy initiated on March 28, 2018 provides a legal framework for "*buying, selling, exchanging, creating, and mining cryptocurrencies and tokens.*" (Decree of the President of the Republic of Belarus No. 8., 2017). The Decree sets out a specific economic zone for companies to operate cryptocurrency related exchanges and services. In contrast, countries such as China and Iran are excluding financial institutions within their jurisdiction from engaging in cryptocurrency markets. For instance, Pilarowski and Yue (2017) identify eight entities in China providing governance and oversight on the prevention of cryptocurrency usage. These entities are: "*the People's Bank of China (PBOC), the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the China Banking Regulatory Commission (CBRC), the China Securities Regulatory Commission (CSRC), and the China Insurance Regulatory Commission (CIRC).*" (Pilarowski and Yue, 2017). They all announced a ban on Initial Coin Offerings (ICOs)

[5] Financial Services (Distributed Ledger Technology Providers) Regulations 2017, Legal Notice No. 204/2017, Gibraltar Gazette No. 4401 (October 12, 2017), https://gibraltarlawyers.com/uploads/PDF/FinancialServicesDistributedLedgerTechnologyProvidersRegulations-LegalNotice20420170.pdf

[6] Jersey is a Crown Dependency of the United Kingdom. However, it is self-governing and has its own financial and legal systems and own courts of law (gov.je, 2022). Available from: https://www.gov.je/Leisure/Jersey/Pages/Profile.aspx [Accessed 9 October 2022].

on September 4, 2017. The reason sighted was down to investor protection and financial risk prevention (Pilarowski and Yue, 2017).

2.3.1.2 Taxation

Tax evasion is an important but peripheral topic to this paper, however, Goitom, from The Law Library of Congress (2018) highlights the issue of how cryptocurrencies are taxed across various jurisdictions. This is a wide-ranging debate on the application of Tax Law against how cryptocurrencies are treated as a financial instrument. The Tax debate falls outside the scope of this review.

2.3.1.3 Anti-Money Laundering (AML) / Counter Terrorism Financing (CTF)

The spring 2020 Cryptocurrency Crime and Anti-Money Laundering report from blockchain intelligence and forensics company CipherTrace revealed the global amount of Bitcoin crime attributed to fraud and misappropriation as $US 4.5 billion in 2019 (CipherTrace, 2020). A high proportion of these illicit Bitcoin transactions (74%) moved from exchange-to-exchange across jurisdictional borders. The report argues that the nature of these 'cross-border' transactions emphasises the need for cryptocurrency exchanges to adopt and ensure appropriate AML and CTF compliance is achieved. Efforts to regulate this in the Bitcoin context are evident in the AML laws, regulation and compliance instruments such as, The Anti-money Laundering (AML) and Counter-terrorism Financing (CTF) Act 2006 (Cth) in Australia. The Australian AML/CTF Act calls for reporting entities to verify a customer's identity before the provision of a

designated service (see Section 6 of the AML/CTF Act). In addition, risks need to be individually assessed for specific types of services and customers, how these services will be delivered to the customers, any foreign jurisdictions being traversed, and the state of connection of any financial entity performing a service in a foreign jurisdiction. In addition, the 5th Anti-Money Laundering Directive of the European Union (EU, 2018a, 2018b) provides a legislative framework for the prevention and detection of money laundering and terrorism financing in virtual currencies and exchanges. The EU directive (2018a) places an emphasis on the national Financial Intelligence Units (FIUs) to "*combat the risks related to the anonymity*", and that the FIUs "*should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency.*" (EU, 2018a, Section 9). Provisions under these AML/CTF regimes define standards on Know Your Customer (KYC) and Customer Due Diligence (CDD) processes. Financial institutions and FIUs can leverage stringent KYC and CDD practices to enable essential customer identification procedures for a reporting entity. Irwin and Turner (2018) emphasize KYC and CDD as critical for linking the real-world identity of a customer's behaviour and developing an understanding of their expected financial activities. Furthermore, to counter any AML/CTF risks, KYC and CDD ultimately satisfy the legal obligations to protect consumers and society from any misuse of virtual currencies for criminal purposes.

2.4 Financial Intelligence Units

Supporting these legislative frameworks are prominent FIUs such as the Financial Crimes Enforcement Network (FinCEN), The Financial Action Task Force (FATF) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). FinCEN is the

FIU of the US Treasury supporting US and international law enforcement investigations. In addition, FinCEN issues guidance and advisory notices regarding illicit usage of virtual currencies (FinCEN, 2019). For example, FIN-2019-G001 (2019), *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, is a comprehensive guidance to persons engaging with money services businesses (MSBs) that involve the transmission of convertible virtual currencies (CVCs) and how they are subject to the US Bank Secrecy Act. FIN-2019-G001(2019) provides the necessary definitions and applications of the Bank Secrecy Act along with the obligations required when dealing with CVCs.

FATF provides recommendations and standards for over 200 jurisdictions to help prevent money laundering and terrorism financing. The FATF secretariat is located at the OECD Headquarters in Paris. The FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - *the FATF Recommendations* provide a comprehensive and consistent framework of measures allowing countries to implement to fight against money laundering and terrorist financing (FATF, 2012). Within that framework there are provisions explicitly relating to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). The guidance document for a *Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (FATF, 2019) identifies '*risk indicators that should specifically be considered in a VA context, with an emphasis on factors that would further obfuscate transactions or inhibit VASPs' ability to identify customers.*' (FATF, 2019). Furthermore, it enhances the original FATF recommendations (FATF, 2012) amending FATF Recommendation 15 by requiring '*VASPs be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licenced*

or registered, and subject to effective systems for monitoring or supervision.' (FATF, 2019).

AUSTRAC is Australia's primary financial intelligence agency and has primary responsibility for AML/CTF intelligence collection and analysis. In addition, it provides guidance to entities against the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and the Financial Transaction Reports Act 1988. AUSTRAC manages the register for digital currency exchange businesses in Australia, along with a guide to preparing and implementing an AML/CTF program for digital currency exchange businesses (AUSTRAC, 2019).

Clearly, law enforcement agencies lack globally consistent procedures, laws, regulations or standards to police the misuse of cryptocurrencies. The FATF strives to set out global standards to combat money laundering and terrorist financing, and other significant threats that exist to disrupt the integrity of the global financial system. However, in most countries, when it comes to cryptocurrency operators there is no enforcement of the "know your customer" procedures or the intention to validate the identity of customers undertaking cryptocurrency transactions. According to The Law Library of Congress (2018) a number of countries are beginning to look at regulating cryptocurrencies and formulating policy frameworks. Furthermore, CipherTrace (2020), highlight the potential effectiveness of AML measures by indicating a 47% drop in criminal funds being sent directly to exchanges. Albeit a subjective link, CipherTrace suggest that this could be down to the AML controls inhibiting the exchange or cash-out of illicit proceeds.

This along with the EU directive (2018), underlines the significance of enabling authorities to monitor the use of virtual currencies. By authorizing FIUs to monitor the use of cryptocurrencies, the EU directive (2018) provides a step towards a more holistic approach for entities to combat the AML/CFT threat. The directive further states, "*Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship.*" (EU, 2018a, Section 8).

Challenges remain anchored in the international nature of cryptocurrency transactions and any resultant cybercriminal activity. To counter this challenge, it will be essential to prevent offenders from hopping from one jurisdiction to another. To impede such behaviours the enforcement of AML/CTF KYC provisions will act as a deterrent. The application of more stringent provisions could risk stifling the innovative functionality of cryptocurrencies, but at the same time balance out any illicit usage by having the capability to reveal the true identity of those participating in cryptocurrency. However, for the trade-offs to be effective international cooperation, information sharing and monitoring between law enforcement agencies, FIUs and cryptocurrency service providers will be required.

This type of monitoring demands analysis techniques based on graph theory and network analysis which can produce predictive features and a machine learning architecture to manage large datasets. Implementation of machine learning architectures is intended to improve monitoring and investigations over time and would

be less manpower intensive. In the next section we will review the literature pertaining to such techniques.

2.5 Bitcoin analysis

2.5.1 In the beginning

After the release of the Nakamoto (2008) whitepaper, *A peer-to-peer electronic cash system*, the early analysis of Bitcoin revolved around understanding the mechanics of the system. This is evident in Kaminsky (2011) who presented findings on the interaction of the Bitcoin protocol with Internet security protocols. In addition, Rosenfeld (2011) examined how the mining process works in order to reward participants on the Bitcoin network, Karame et al (2012) looked at the 'double spending attack' examining how to take advantage of the early stage Bitcoin transaction processing times and Drainville (2012) looked at the privacy motivations for using Bitcoin along with attack vectors that aim to compromise security and anonymity of the Bitcoin system. Then Stokes (2012), broke ground on the utility of virtual currencies applied to money laundering. However, Reid and Harrigan (2011), Ron and Shamir (2012) and Meiklejohn et al (2013), pioneered the fundamental techniques for analysing Bitcoin transaction behaviour.

2.5.2 Bitcoin heuristics

Investigation into illicit Bitcoin usage creates a mosaic of information that must be forensically reconstructed to provide an accurate view of the target. The information can be technological, behavioural, criminological and regulatory in nature. The

introduction of heuristics into the analysis can help address the difficulties of attribution. This is achieved by grouping similar transactional behaviour and linking ownership to addresses and services on the Bitcoin network.

Meiklejohn et al (2013) produced a seminal paper on analysing the Bitcoin blockchain to reveal identity. The heuristics presented within this paper form the basis of which much of today's Bitcoin analysis is performed. This work makes it possible to cluster activity around a certain user and add context to this user for purposes of identification or grouping similar services on the network. In addition, it introduces the concept of peeling, where smaller amounts of Bitcoin are "peeled" off a larger amount and transferred onto another address with the remainder transferred back to the one-off change address. In addition, they discover, if a user of an input address also controls a one-off change address associated to that transaction, it may be assumed that both addresses are owned by the same user. This common pattern can be used to obfuscate the movement of funds and result in the detection of money laundering on the Bitcoin network. Meiklejohn et al (2013) produce various other time-series analyses along with Bitcoin service breakdown analysis to understand and model the effects of the different services on the Bitcoin network. Meiklejohn et al (2013), apply this type of analysis on aggregated data to help profile and characterize different activity trends on the Bitcoin network. Drilling deeper into the payment trends allows for a more targeted understanding of illicit user activity, especially its source. They also determined that it was only possible to identify ownership after any suspicious activity had occurred. Predicting that suspicious activity is going to take place in the future requires the collection of targeted Bitcoin addresses or transaction IDs to learn and train models for future prediction, investigation and analysis. Therefore, there is a need to look at other

information sources to determine possible fraudulent transactions. This is where Reid and Harrigan (2011) posited cluster analysis as a technique to reveal patterns, associations, structures and relationships emanating from different data sources. Clustering can be used to identify common entities on the Bitcoin network controlling Bitcoin addresses by building up a picture of transaction flows over time. Nakamoto (2008), implies that clustering algorithms can group together multiple input transactions controlled by the same address, potentially identifying the owner of the address (Nakamoto, 2008). This makes it possible to construct a user network identifying mappings between Bitcoin addresses and a cluster of similar users (Reid and Harrigan, 2011). There is also the potential to find connection between Bitcoin addresses, IP addresses and spending patterns through this type of analysis.

2.5.3 Analysing the network layer

To de-anonymize users on the Bitcoin network, Turner and Irwin (2018) look at the openness of the Bitcoin system and some of the defining features seen within the anatomy of a Bitcoin transaction coupled with extensive data collection from packet sniffing software. Using network traffic analyser tools, such as Wireshark, can capture Bitcoin protocol traffic by listening on the network to port 8333 and building a profile of transaction flow between IP addresses and Bitcoin addresses over time. This is known as public key profiling. This method has weaknesses, such as the potential of Bitcoin addresses to change as frequently as every transaction. If this is the case, it will result in weak linkages to any network observations. Due to the peer-to-peer propagation of transactions any observation of an IP address where a transaction is intercepted may not be the original creator of the transaction. This further removes any

ability to reveal identity via Bitcoin address usage analysis on the network (Turner and Irwin, 2018). Furthermore, Irwin and Turner, (2018), highlight the lack of reliability in this analysis approach and the inhibitors of revealing any illicit transaction. They state: "*IP addresses that connect to computers in a library, café, open wireless network, virtual private network or Tor exit relay, used by many people, do not identify the perpetrator and, therefore, is not probable cause that a person was responsible for the communication or illicit activity*" (Turner and Irwin, 2018). Nakamoto (2008) designed the Bitcoin system so that actors are pseudonymous. In addition, the transaction packet moving through the Bitcoin network does not contain the IP address. Only transaction IDs are ultimately stored on the blockchain. The transaction payload is publicly available for anyone to view at any time on the blockchain. Along with the transaction amount and timestamps, this payload reveals a concatenation of public keys. This comprises of the Bitcoin address and cryptographic signatures to provide an index linking the sender to the intended recipient of the Bitcoin (Nakamoto, 2008). Other analysis challenges exist as presented by cyber security researcher Dan Kaminsky in a 2011 Black Hat presentation on Bitcoin security when the Tor application is used. This application ensures anonymity via the Internet protocol stack leveraging the "Darknet" and utilizing a specific cryptocurrency "Dark Wallet" service. IP address obfuscation is achieved using a Tor router (Onion Router). IP address and Bitcoin address mappings are lost, and any investigator will only find the IP address associated to a Tor exit node preventing any meaningful analysis (Kaminsky, 2011).

Considering the limitations observed at the network layer when analysing illicit Bitcoin activity, the next section reviews the literature relating to graph data models and how

nodes and relationships formed on the Bitcoin network can provide insight into illicit activity.

2.6 Graph analysis

This section will look at the techniques used to analyse Bitcoin transactions as a graph. Beginning with modelling the transactions and addresses as a Directed Acyclic Graph (DAG). Then, looking at the behaviours and patterns that emerge from suspicious Bitcoin payments. In addition, understand what automated software tools are available to inspect these patterns and behaviours. Furthermore, delve into the algorithms available for graph analysis.

2.6.1 Directed Acyclic Graph (DAG)

A Directed Acyclic Graph (DAG)[7] is formed by the transactions and addresses on the Bitcoin network. The ability to break the entire Bitcoin graph into two smaller DAGs was researched by Reid and Harrigan (2011) as they investigated the problem of anonymity. A first DAG was constructed with Bitcoin addresses from tracing the flow of Bitcoins between users. A second DAG represented the analysis of transactions over time. The second DAG represented a transaction as a node and the directed edges between Bitcoin source and target were modelled as the output of one transaction to the input of another, creating a transaction chain. The graph may reveal transactions repeatedly performed by identifiable communities (multiple entities) or multiple transactions conducted by a single entity. Breaking the Bitcoin system down into two DAGs enables the ability to map and cluster behaviours of Bitcoin users and transactions over time. Reid and Harrigan (2011) break the Bitcoin system into

[7] DAG – A directed edge (x, y) indicates that activity x must occur before y. They allow for topological sorting which is an important property providing order to process each vertex before any of its successors (Skiena, 2008).

analysable user and transaction graphs and apply their method to reveal identity by using multiple sources of data. These data sources include: Off network information (building a directory of Bitcoin users) which allows monitoring activity, common transaction usage and routing behaviour, using a website called the Bitcoin Faucet[8]. This website uses TCP/IP Network information, matching Bitcoin addresses to IP addresses, in order to build up a map of geographical usage. This could ultimately be flawed due to the Bitcoin propagation protocol where the last routed Bitcoin node IP address is not necessarily where the transaction originated. Examples of where the Bitcoin Faucet system has been applied include, looking at address pattern behaviour attributed to known entities, such as WikiLeaks. In addition, using flow and temporal analyses to build a case study of Bitcoin theft.

2.6.2 Transaction Behaviour

Taking algorithmic network analysis another step further helps the reader understand the evolutionary behaviour of Bitcoin transactions and the way Bitcoin addresses adapt over time. Furthermore, advanced analytical techniques involving machine learning, can be used to determine the identity underneath the pseudonymous nature of Bitcoin addresses.

Ron and Shamir (2012) provide a step in this direction by analysing a graph of the largest transactions in Bitcoin through a series of sub-graphs, identifying multiple characteristic behaviours for the flow of Bitcoin transactions. These are: "*long*

[8] http://freebitcoins.appspot.com/

consecutive chains of transactions, fork-merge patterns that may include self loops, setting aside [Bitcoins] BTC's and final distribution of large sums via a binary tree-like structure." (Ron and Shamir, 2012). These patterns can be used to reflect common practice among users that may lead to suspicious behaviours on the Bitcoin network and these patterns can be re-used and applied to other illicit transaction scenarios. For example, Bartoletti et al (2020) analysed the redistribution of money flows relating to identifying Ponzi schemes in the cryptocurrency Ethereum. They identified several patterns in the money flows. The chain-shaped schemes and tree-shaped schemes are two illicit money-flow patterns that can also be modelled as a graph. To do this at any meaningful scale, automated software and algorithmic techniques are necessary. The following sections examine the literature relating to these techniques.

2.6.3 Automated Software

Spagnuolo et al (2014) provide a framework for forensic analysis of such illicit Bitcoin transactions and subsequently developed graph analysis and automated software called Bitiodine. This software is used to parse the Bitcoin blockchain for transactions and addresses, and then augment that with different data scraped from the web to cluster, contextualize and visualize Bitcoin transaction graphs. An important piece to this literature is the application of their system to various case studies. These include investigating the Silk Road Bitcoin activity and associated trades made on the suspicious exchange, Mt Gox and transactions made by the owner of Silk Road, Dread Pirate Roberts, aka Ross Ulbricht, linking web forum data with blockchain data. Perhaps the most relevant application of Bitiodine is that of the Cryptolocker ransomware investigation. BitIodine is used "*to detect the CryptoLocker cluster(s),*

belonging to the malware authors, and compute some statistics about ransoms paid by the victims." (Spagnuolo et al, 2014). This data results from Google searches related to the ransomware, reddit forums that reveal addresses belonging to the ransomware, then a classifier is run over these addresses clustering the list of extorted addresses and automatically associating usernames from reddit to Bitcoin addresses. Furneaux (2018) also identifies several automated analysis tools that help visualize the Bitcoin graph and forensically investigate suspicious addresses. These tools include Numisight, Maltego, Learnmeabitcoin.com and the commercial enterprise systems available from Chainalysis and Elliptic which provide algorithmic modules to learn, infer and predict patterns in the network.

2.6.4 Algorithmic Analyses

Fleder et al (2015) build on the previous techniques and look to identify suspicious behaviour on the Bitcoin network. Providing context to the blockchain data from external data sources by web scraping forums and social media websites, graph analysis can be applied on the transactions performed to try and match any suspicious use of Bitcoin addresses. The methodology is similar to that found in Spagnuolo et al (2014), however it introduces the use of the PageRank algorithm: "*We use PageRank as a guide to determine the most interesting nodes, or users in our user graph to further investigate their linkage with known forum users.*" (Fleder et al, 2015). The graph analysis techniques used (PageRank and clustering) are fundamental to a deeper behavioural analysis of the Bitcoin due to its inherent data structure, (the blockchain), and activity (transactions between users) forming a graph or network. According to Fleder et al (2015), enriching the blockchain data by looking at external data in the form of security

reports, Indicators of Compromise, malware sites and other cyber security feeds can help reveal identity for intelligence and law enforcement purposes. Particularly significant is the paper's use of the PageRank algorithm which is applied to the communities of transactions being performed by ransomware. This is a key indicator for understanding unusual behaviour in networks, such as anomaly or fraud detection cases (Needham and Hodler, 2019).

As an example, Fleder et al. (2015) provided analysis on funds captured and sent to known Bitcoin addresses owned by the FBI. Nodes highly ranked via their technique were flagged for further investigation. Large clusters of transactions were detected from suspicious sites including WikiLeaks, cryptocurrency gaming service SatoshiDICE and the infamous Silk Road. The algorithmic technique from Fleder et al. (2015) borrows from other financial fraud risk management techniques. By associating an address or transaction coming from, or going to, such nefarious services as the Silk Road, it immediately becomes demarcated as a high-risk transactions or address on the Bitcoin network. Due to the potential risk of exposure to criminal activity a user has now made an illicit reference that can be tagged in the collected data. More advanced graph analysis techniques can be applied to sub-graphs of interest and reveal further intelligence on the Bitcoin network.

Although primarily concerned with the anonymity of Bitcoin, Gaihre et al (2018) provide some important claims for analysis on transaction behaviour, such as reuse frequency of addresses, zero balance addresses and how amounts are split up into smaller transactions with the usage of the change address, revisiting the concept of

peeling introduced by Meikeljohn et al (2013). Additionally, Gaihre et al (2018), apply more advanced graph analysis techniques like the in-degree, which is the number of incoming edges to a node, as well as, connectedness of nodes on the network. Furthermore, they look at the diameter of the graph, which works on discovering the longest of all shortest paths in the network using a Bread First Search (BFS) algorithm. There are also several transaction walks that depict miner behaviours, where the miner accumulates the mined Bitcoin and also where the miner splits the mined Bitcoin. These can be useful payment typologies to build on for other illicit transaction activity.

Maesa et al (2018) go deeper into the detail of the clustering algorithm used to generate a user graph containing nodes with groups of addresses controlling the transactions of interest. The clustering process is outlined step by step. This could be useful when applying a similar process to the population of incoming transactions to a ransomware seed address for example. This analysis yields a clustering coefficient of the user graph. A constant order of magnitude for the coefficient is exhibited over time and it is similar when compared to other complex social networks. Centrality measures provide the computation and interpretation of the results. These measures include PageRank and Eigenvector indexes to see the balance of nodes with respect to incoming and outgoing transactions. The Gini coefficient is also computed on the user graph, as a further measure to analyse the in-degree distribution over time. The Gini coefficient is an economic indicator that gauges economic inequality, measuring income distribution or wealth distribution among a population.

Another aspect Maesa et al (2018) investigate is the analyses on the entire user graph of Bitcoin, as at the end of 2015. These analyses include a time series view of the Bitcoin network, along with economic analysis showing distribution of wealth. Furthermore, using techniques to detect critical nodes of the network where connectivity is strongest. The technique on node criticality is the most pertinent to illicit payment discovery. It is part of a centrality analysis on the graph and identifies the most active nodes in the graph. Nodes with high centrality (i.e. the most influential in a graph), will yield high in degree and/or out degree characteristics and Maesa et al (2018) demonstrate a case that reveals the largest exchanges in the Bitcoin network, which at the time was Mt. Gox. This is also be applied to ransomware-Bitcoin analysis. For example, the centrality measures can reveal the most active nodes in a ransomware graph. Depending on the network depth, this could be the ransom seed address, the originating victim address (i.e. where the victim is getting their Bitcoin from), or the cash out point for where the cash out trail meets an exchange. This can become complex when interpreting whether the node actually has any influence over the movement of ransom payments during a ransomware campaign or simply over standard transactions on the Bitcoin network. That is why more information and context should be collected via machine learning to understand the representation of that node in the graph we are looking at.

2.7 Machine Learning Techniques

Machine learning in its simplest form is the act of teaching machines how to carry out tasks by themselves (Richert and Coelho, 2015). Richert and Coelho (2015) provide this introductory perspective in their book on building machine learning systems with

python. The book provides a practical reference on building machine learning models in python to train a computer program to learn from data fed into a system. Richert and Coelho (2015) dive into the detail of the commonly used python programming language and the respective data science and statistical libraries needed to work through problem sets that required machine learning algorithm development as a solution to these problems. They highlight classification, topic modelling, sentiment analysis, regression, recommendation engines, computer vision and dimensionality reductions as important problem spaces to work on. The learning algorithms applied to these problems can take the form of supervised, unsupervised or reinforcement learning. Kamath (2011) delivered a presentation at the annual python conference in 2011 that neatly summarized the differences in the available learning algorithms. Supervised learning is based on training data that contains correct responses to input data and as such the training data is used to learn a model that can be applied to classify future data items.

Unsupervised learning algorithms have no prior knowledge of the domain or structure of the data they use as inputs to interpret or classify meaningful outputs. It may not be possible to label the input data for the problem space being worked on, and unsupervised algorithms can be a powerful way to detect anomalies or learn features of the dataset being analysed. One unsupervised learning method is clustering. This is the process of grouping objects found in the input data exposing similar and distinctly different attributes which form clusters (Kamath, 2011). Bitcoin systems provide a strong case study for the clustering algorithm. An example of this can be realized with multiple input and multiple output Bitcoin transactions. Meikeljohn et al (2013) found by grouping these types of transactions together it may be possible to find Bitcoin

addresses and the transactions controlled by a common entity. Reinforcement learning provides a supervised and unsupervised hybrid learning approach. The learner runs through many different scenarios, then as a result of reinforcing an engineered policy against these scenarios, a good action is learned if it is a part of the well-engineered policy. Alpaydın, (2020) comments on the goodness of policies, which is determined by a sequence of good actions which attain a desired goal.

Building on these learning techniques, the following literature looks at the analysis of Bitcoin networks using Machine Learning and Artificial Intelligence techniques with application to money laundering and fraud detection.

2.7.1 Supervised Machine Learning techniques

Yin and Vatrapu (2017) analyse the clusters, entities and categories that are used to understand the control over funds in the Bitcoin network along with attributing some form of contextualization to the clusters with respect to the activity they are performing (e.g. Mining, mixing, exchanges). They also categorize based on criminal activity, in total the categories provided are Tor markets, scams, ransomware, mixing, and stolen bitcoins, exchange, gambling, merchant services, hosted wallets, mining pools, personal wallets. A methodology is provided outlining the data required from each cluster for analysis. This data includes: Transactions (hash, timestamp, input address, output address and value), addresses (address, number of transactions with peer address and value), counterparties (counterparty address, value, category and counterparty name) and exposure. Exposure acts as a risk calculation based on the knowledge of the cluster in terms of how many inputs and outputs out of total transactions emanate or

arrive at a particular service category. The pipeline and analysis process diagram summarize the methodology having a big emphasis on data collection, cleansing, preparation and feature extraction. This reflects the high level of effort required to get the data ready to analyse. The second half of the diagram brings forth the machine learning capabilities for training data sets, model selection and validation. The statistical limitations on the machine learning components are identified in terms of the over and under sampling of the various classes, which limits the predictability of the under sampled classes. However, this methodology is something that can be refined with improved data collection, training and classification. This may be able to improve the 0.5 precision achieved on ransomware identification from their experiments.

Harlev et al (2018) follow the same methodology as Yin and Vatrapu (2017) using supervised machine learning to attribute Bitcoin clusters to those predetermined categories. By looking at the anatomy of a Bitcoin cluster and using supervised machine learning to attribute Bitcoin clusters to those predetermined categories they break down the cluster structure to help categorize the controlling entities. Clustering will only take the analysis so far and emerging techniques based on neural networks that apply deep learning of latent representations on a graph or network structure provide an advantage. This is where the fraud team from Logical Clocks (2019) looked at the different machine learning approaches and how traditional AML anomaly detection problems use supervised machine learning against training data which contains an imbalance of ‘good’ and ‘bad’ transactions. They take this so far as saying it is an unviable approach which may only yield one bad transaction in more than a million. Therefore, there is a need to explore other machine learning methods to minimize the occurrence of the false positive and false negative detections and consequences of such detections.

2.7.2 Unsupervised Machine Learning techniques

Whilst Yin and Vatrapu (2017) used supervised learning techniques, Monamo et al (2016) provide a means of looking at the unsupervised learning techniques by giving the machine learning algorithms (trimmed k-means), which can both cluster objects and detect fraud in a multivariate setup to detect fraudulent Bitcoin activity. The k-means algorithm can perform clustering and classification without a training data set leaving the algorithm to establish its own labels as it comes across the data that is fed into it. This is both a limitation and a performance enhancement when it comes to fraud detection. Limitation in that unlabelled data somehow needs to be checked, modified and fed back into the system with context (manually). Performance enhancing as it will execute its machine components quicker. The authors concede that in the criminal detection process comparing known criminal elements would be better served using a neighbourhood-based algorithm. These types of algorithms use classifiers to help the machine understand the context of the data they are processing and thus making the results more easily validated by experts in the field. Turner and Irwin (2018) experimented with the LINGO algorithm. They explain the open source nature of this algorithm and the previous application of the algorithm to web search results clustering by Osinski (2003). Osinski (2003) describes the algorithm as a combination of Latent Semantic Indexing (LSI) and the Vector Space Model (VSM) which use unsupervised and supervised learning techniques respectively. The unsupervised application of LSI discovers abstract context in the data that passes through it. It forms cluster labels to be used as a reference for the supervised VSM algorithm. This is then used to determine cluster contents (Osinski, 2003). Turner and Irwin (2018) then look at applying LINGO to a combination of social media and Bitcoin blockchain data. Their results show a need

to tune the algorithm with the input of subject matter expertise if any meaningful suspicious activity is to be found. Illicit money flows have traditionally been treated as anomaly detection problems. Researchers Graves and Clancy (2019) at DeepMind look to solve anomaly detection using unsupervised learning methods. One such advanced method seeks to train an algorithm to generate its own models of the underlying classification of data it has discovered. These ‘generative’ machine learning models can use common techniques such as k-means clustering and principal component analysis (PCA) to build a model of ‘good’ and ‘illicit’ transaction classes on the Bitcoin network. Such techniques can only be enabled through deep learning which provides a deep understanding of the data being observed in its context.

2.7.3 Deep Learning

Steenfatt et al (2018) introduce an approach that allows deep learning on graph networks to learn the role a node plays in the network. This is based on the ‘struc2vec’ algorithm, where traditionally similar nodes are in the same close proximity as each other, understanding the role a node plays with respect to embedded data yields node and network similarities that may not belong to directly connected components. Learning node representations or ‘node embeddings’ that have meta-data and structural information encoded into them is a powerful way to find new suspicious relationships in the target network. An example given by Steenfatt et al (2018) showed data from the WeChat payment network of 3,000 fraudulent nodes that have role labels from 15,000,000 nodes. The labels identified one of three types of fraud and grouped the transactions accordingly.

As an alternative to graph embedding, Li et al (2019) proposed a Graph Matching Network (GMN), which calculates a graph similarity score by using Graph Neural Networks (GNN). GNNs are used to learn unlabelled graph structures by using the underlying encoded graph structured data (Zhang et al, 2009). Li et al (2019) scale this idea up to work on complete graphs in order to understand their similarities by comparing the input graphs against different graphs to associate nodes and identify any differences in the node and edge features. This technique is related to the field of ransomware and through the application of graphs formed by ransomware - Bitcoin transactions the literature shows it is possible to understand the similarities and differences in a ransomware target network model. In addition, by creating a GNN for ransomware – Bitcoin graphs it is possible to machine train and learn what behaviours and parameters these networks may form in the future.

The collaboration between cryptocurrency forensic analysis firm Elliptic and researchers at IBM and Massachusetts Institute of Technology (MIT) have released a public data set of around 200,000 transactions partially labelled with illicit or non-illicit flags to identify suspicious transactions on the blockchain within the context of Anti-money Laundering (AML) (Weber et al, 2019). Using graph analysis techniques such as Graph Convolutional Networks (GCN) which use neural networks to allow the embedding of relational information between nodes and relationships to be further used in machine learning techniques. The GCN is a similar approach to the one taken by DeepWalk (Perozzi et al, 2014), however the difference is in the feature representations. A GCN aggregates the in and out degrees of a nodes neighbour and propagating these representations as features onto the nodes of the network. The DeepWalk embeds structural information on the graph to learn the typology of the

graph by building up a node's context in the graph through a number of random walks from that node, much the same way a Natural Language Processing (NLP) algorithm learns words in a sentence from a corpus, or vocabulary, of words (Perozzi et al, 2014).

Furthermore, researchers at the CSIRO Data61 unit, produced a report on Bitcoin Ransomware Detection with scalable Graph Machine Learning (Jung, 2019). In this research, GCNs are also used to predict super nodes, those nodes in a Bitcoin network having a large amount of incoming and outgoing edges, which could be indicators of ransomware addresses and activity on the Bitcoin network.

2.7.4 Human and Machine

The techniques for examining the Bitcoin blockchain as a graph require a combination of machine powered analytics combined with human subject matter expertise in order to contextualize the data for intelligence collection and forensic interpretation. The ability to apply high performance computing to large amounts of data in the Bitcoin ecosystem provides efficiencies in analysis. Clustering data around influential nodes in the Bitcoin graph is a common approach undertaken by most of the authors of the literature. It allows for the application of graph algorithms relating to community detection, pageRank and centrality. Adding labels to the data collected and also combining the Bitcoin data with external data sources builds intelligence into the graph model by encoding structural knowledge into the graph such as in, out, or change addresses, timestamps, amount sent and received, service labels, network depth and address reuse frequency. A recent example of this is the open data project by Michalski et al (2020) at the Harvard dataverse. They collected Bitcoin addresses and labelled

them as mining pools, miners, coinjoin services, gambling services, exchanges, other services for training machine learning algorithms to learn and predict future addresses. A targeted application of these techniques is to the case of identifying ransomware payments in Bitcoin. At present there is limited application in this realm, however the intention is to look for similar graph patterns across different ransomware campaigns. Future research will be able to build upon these techniques and apply deep learning and Artificial Intelligence (AI) to further enhance the ransomware-Bitcoin target network model with labelled data and augment the cognitive process for identifying ransomware networks in the Bitcoin ecosystem.

2.8 Ransomware – Bitcoin transaction analysis

Ransomware is a prevailing threat to the mainstream usage of cryptocurrencies and for malware developers and users, cryptocurrencies have enabled cyber criminals to collect their proceeds of crime undetected. Since 2018 the estimated global damage of ransomware has increased 2.5 times. From $US 8bn in 2018 to a projected $US 20bn in 2020 (Purplesec, 2020).

There is an essential need for identification and analysis frameworks. Ahn et al (2016), describe a Ransomware Identification Framework (RIF) for identifying ransom payments from the set of all transactions sent to the ransomware cluster. Using cluster analysis on the total network of the Cryptolocker ransomware campaign, they were able to understand the underlying financial infrastructures and money laundering strategies of the ransomware. Furthermore, the analysis yielded connections to popular services like BitcoinFog and BTC-e. It also speculated connections to criminal activity like the

sheep marketplace, which was used for transacting narcotics, and was the successor to the infamous Silk Road site.

The methodology used by Ahn et al (2016) for the RIF looks at the total number of transactions for each seed address, the total amount of bitcoins sent and received, and the number of ransom payments received. At an individual transaction level, the framework followed the input and output addresses, bitcoins transferred, and timestamps of these transfers. These parameters were used to build the target network model for their research, along with additional labels to indicate the network depth (i.e. how far away from the seed address the activity is taking place) and any service identifiers able to be picked up from a blockchain Application Programming Interface (API) that indicate Bitcoin exchanges.

Bistarelli et al (2018) describe a tool that was created for this purpose. Through their analysis of the WannaCry attack, they were able to visualize the Bitcoin flows of WannaCry. Flows toward the three different ransom seed addresses were analysed in an "in-flow" analysis to show a cluster of payments made to the ransom seed addresses and where they had come from. This revealed certain payments coming from leading crypto exchanges such as poloniex.com and other services like cubits.com. The "in-flow" analysis is one section of the intelligence-forensic continuum introduced as an analysis framework by Turner et al, (2019). It is important to take a full view of the continuum to build out the complete target network model, from mobilization through to actions on the objectives of the collected ransom.

Furthermore, Paquet-Clouston et al, (2018) analyse the collector addresses of the top 15 ransomware families by ransom payments received and by ransomware families. The authors investigate the graph formed by the incoming ransom payments and applied graph analysis techniques, such as centrality, to classify addresses to a particular ransomware. The two ransomware campaigns examined in detail from a graph analysis perspective were Locky and CryptoHitman. Transaction walks were produced showing which nodes in the graph acted as collectors and what services the addresses corresponded to, i.e. Bitcoin exchanges, mixing services, gambling services, etc. A longitudinal (time series) analysis was also conducted which showed the profile of a ransomware address and how it collected ransoms over time. Many of these profiles were similar, i.e. collecting their ransom over a burst of initial payments and then tapering off over the first week or two. Performing the time series analysis looks back at the history of a particular collector address and this is also important to understand the behaviour of the victims and attacker. Paquet-Clouston et al, (2018), find that by moving back and forward through time over the lifespan of a Bitcoin address helps profile the incoming and outgoing relationships, providing a more targeted mechanism for identifying patterns in ransomware – bitcoin transaction graphs.

Patterns are one structure of interest providing a footprint to ransomware-Bitcoin activity. Another is measuring the impact or significance the ransomware attack had by plotting their collection and payment profiles. Conti et al (2018) provide a ‘lightweight framework’ to analyse 24 different types of ransomware from the perspective of their economic significance through the amount of Bitcoin they collected over time. The paper focuses solely on the number of Bitcoins received by the ransomware Bitcoin addresses over the time window for the ransomware campaign. They also look at the

cumulative distribution function (CDF) of the ransomware to show the total amount of ransom collected over the campaign. This is a relatively simplified analysis that provides an approach to deal with some blockchain specifics on multiple input transactions and change addresses.

Huang et al (2018) provide a more detailed insight into 10 ransomware clusters. The paper outlines a robust framework for identifying ransom addresses by scraping reports from real victims, creating synthetic victims under lab control conditions by making micropayments and tracing the flow of bitcoins and via clustering by co-spending which looks at addresses that create a transaction controlled by the ransom seed wallet. In addition, external data sources are looked at for information regarding the ransomware campaign. These include Google search history trends and YARA[9] malware indicators of compromise from a tool called VirusTotal. Once this framework has been set up and the initial detection and collection has been done, payment analysis can be conducted to look at things like estimating revenue of the ransomware, payment mechanics (timing and profile) and potential cash-out behaviour. Cash-out behaviour is one of the more interesting parts of the ransomware – bitcoin analysis as it gives targeted evidence on criminal behaviour relating to ransomware attackers looking to use their proceeds of crime.

The techniques used for ransomware – Bitcoin analysis vary across the intelligence-forensics continuum using the elements discussed and by adding data attributes to nodes and vertices in a graph by labelling, it is possible to aid graph classification using graph machine learning algorithms to find similarity or trends in the graphs (Tiao et al, 2019).

[9] YARA is a tool used in malware detection that creates rules based on hex, binary or string patterns that may be present as malware signatures in malicious files (Li, 2020).

From the aforementioned literature, the importance of populating the target network model with context relevant data and comparing against different graphs from a variety of ransomware campaigns becomes evident.

2.9 Discussion

The enforcement of AML/CTF KYC provisions for cryptocurrency will impede those who would misdirect its innovative functionality towards illicit ends and expose those who choose to do so. However, for law enforcement agencies to benefit, it is imperative that law enforcement agencies, financial intelligence units and cryptocurrency service providers should cooperate and share information. There is precedent for this.

For example, in 2017, a combined research and law enforcement partnership was made in the European Union between agencies and academic institutions from The Netherlands, Germany, Spain, Finland, Austria, and the UK, setting up the "Titanium" project, (Tools for Investigation of Transactions in Underground Markets). This project supported forensic analyses relating to criminal transactions, anomaly detection and machine learning techniques which were developed as a solution for investigations relating to criminal and terrorist acts using cryptocurrencies on the internet. According to Darknetmarkets (2017) Titanium was a platform using data from multiple sources, including "*online forums, P2P networks on dark marketplaces, virtual currencies and data found on electronic equipment that has been seized from suspects*." (Darknetmarkets, 2017). Demonstrating a strong partnership between technology and subject matter experts, Titanium is a model project from which law enforcement can

build upon to strengthen their role alongside technology in the discovery and fight against illicit cryptocurrency usage.

This paper reviewed various techniques that are quite limited on their own. However, in combination these techniques are a formidable arsenal, much greater than the sum of the individual techniques. These techniques range from the simple heuristic approaches that help assume ownership of addresses and transactions, to the graph algorithms that provide essential foundations for community detection, PageRank and connectedness patterns in illicit networks. Moreover, advanced computing power is enabling a resurgent field of Artificial Intelligence (AI). Machine Learning, when applied to graphs and networks, produces rich contextual understanding of graph behaviour and opens new horizons for anomaly detection. It facilitates very detailed and complex benchmarking and pattern detection. Sophisticated algorithms such as, Microcluster-Based Detector of Anomalies in Edge Streams (MIDAS), can detect dynamic behaviours in graphs (Mishra, 2018). This automated simultaneous analysis lends itself well to the Bitcoin - blockchain environment as the graphs formed here are constantly being updated with new addresses and transactions. This capability is particularly useful for ransomware attacks whose first indications are often sudden bursts of activity on the blockchain (Bhatia et al, 2019).

2.10 Conclusion

The literature reviewed in this paper forms a coherent approach to the analysis of the Bitcoin blockchain for illicit money flows. This approach revolves around techniques that seek to reduce the levels of anonymity provided by the Bitcoin system to identify

real world participants. The literature reveals challenges with the regulatory environment. The different applications of laws and compliance controls across jurisdictions can hinder deanonymization and attribution to the real world of virtual identities on the cryptocurrency network. The emergence of machine learning and its application to graphs is providing a powerful analysis capability for disrupting Bitcoin related criminal activity. Particularly important are the practices of graph analysis, clustering, connectedness and GNNs as a form of deep learning applied to graphs. When compared to standard machine learning that employ supervised learning techniques and rules-based anomaly detection, these graph-based techniques dramatically enhance the future-orientated intelligence and real-time analysis of Bitcoin transactions.

Ultimately, the literature shows that there is no lack of available data on the Bitcoin blockchain. By providing open data this allows the community to flag certain behaviour or orientation of Bitcoin addresses and transactions. However, the challenge is to correctly identify and classify the data and link it to off-chain data to provide a richer context. A way to potentially improve the performance of the machine learning algorithms is to take the graph labelling another step further. This would require adding more meta-data to the graph that attributes the addresses and transactions to various classifications, such as ransomware or other illicit purposes. These challenges have precipitated open data efforts such as those conducted by joint research collaborations at Harvard dataverse (Michalski et al, 2020) and between Elliptic, IBM and MIT (Weber et al, 2019) that will support future investigations and enhance intelligence sharing on illicit Bitcoin transactions.

2.11 From theory to practice

Having reviewed the analytical framework that underlies investigations of cryptocurrencies, it is time to pivot towards developing a novel approach to analysing Bitcoin transactions associated with ransomware. In the absence of powerful commercial blockchain analytics platforms, such as Chainalysis Reactor or Palantir Foundry for Crypto, it is important to build up a common open source analysis model to help investigators frame the problem of ransomware-Bitcoin payment analysis. Therefore, by expanding on the application of the aforementioned techniques to analyse ransomware-Bitcoin transactions, Chapter 3 decomposes the WannaCry 2.0 case study to build a model that will enable analysts to develop a common picture of the key interactions taking place during a ransomware campaign with respect to a network of Bitcoin payment activity.

Chapter 3: A Target-Centric Intelligence Approach to WannaCry 2.0

"*One picture is worth ten thousand words*" – Chinese proverb

3.1 Abstract

Purpose: This paper aims to demonstrate the utility of a target centric approach to intelligence collection and analysis in the prevention and investigation of ransomware attacks that involve cryptocurrencies. The paper uses the May 2017 WannaCry ransomware usage of the Bitcoin ecosystem as a case study. The approach proves particularly beneficial in facilitating information sharing and an integrated analysis across intelligence domains.

Design/methodology/approach: We conducted data collection and analysis of the component Bitcoin elements of the WannaCry ransomware attack. We took note both of the technicalities of Bitcoin operations, and current models for sharing cyber intelligence. Our analysis builds on and further develops current definitions and strategies for sharing cyber threat intelligence. It uses Problem Definition Model (PDM) and generic Target Network Model (TNM) to create an analytic framework for the WannaCry ransomware attack scenario allowing analysts the ability to test their hypotheses, integrate and share data for collaborative investigation.

Findings: Using a Target-Centric Intelligence approach to WannaCry 2.0 shows us that it is possible to model the intelligence problem of collecting and analysing data related to inflows and outflows of Bitcoin related ransomware transactions. Bitcoin transactions form graph networks and allow us to build a target network model for collecting, analysing and sharing intelligence with multiple stakeholders. Although attribution and anonymity prevail under cryptocurrency usage, there is a means for

developing transaction walks using this method to target nefarious cryptocurrency exchanges where criminals are inclined to cash out their proceeds of crime.

Originality/value: The application of a target centric intelligence approach to the cryptocurrency components of a ransomware attack, provides a framework for intelligence units to breakdown the problem in the financial domain and model the network behaviour of illicit Bitcoin transactions relating to ransomware.

3.2 Introduction

In May 2017, a ransomware outbreak known as WannaCry, infected more than 300,000 computers across 150 countries worldwide, making it the most prominent ransomware attack involving nation states and cryptocurrencies to date (Irwin and Turner, 2018). The use of cryptocurrencies in ransomware attacks like WannaCry poses challenges for Law Enforcement Agencies (LEAs), the Intelligence Community (IC), regulators and policy makers. These challenges relate to the effective collection and analysis of cryptocurrency intelligence, and ascertaining the identification of criminal behaviour. It is possible to overcome these challenges through a clearly identified target centric intelligence model and move towards a more advanced warning of ransomware mobilisation.

3.2.1 The Crypto-criminal evolution

The largest cryptocurrency by market capitalisation[10] is Bitcoin. At the time of writing, Bitcoin had a market capitalisation of more than five times that of the next largest

[10] Bitcoin market capitalisation is defined as the total number of Bitcoins in circulation multiplied by the Bitcoin price (Statista, 2018).

cryptocurrency, Etherum, US$113.2B versus US$21.3B respectively (CoinMarketCap, 2018). Further to that, on 18th October 2018, the volume of Bitcoin traded in a 24-hour period was approximately three times that of Etherum, US$4B versus US$1.4B respectively (CoinMarketCap, 2018). Bitcoin's leading market position among its peers is a function of its mainstream circulation, strong liquidity and sharp rise in price, peaking at US$19,783.21, per Bitcoin, in December 2017 (Higgins, 2017). However, it is hard to ignore the criminal roots that tarnish Bitcoin and even with its rise in popularity there is still much trepidation surrounding the cryptocurrency due to its association with Darknet marketplaces like "The Silk Road", "Valhalla" and "Alpha Bay" (Irwin and Turner, 2018). According to Europol, approximately US$1B was transacted on AlphaBay (Europol, 2017). The pseudo-anonymous properties of Bitcoin make it particularly attractive to criminal activities. Coupled with the obfuscating network infrastructure of the Darknet using The Onion Router (TOR) protocol[11] Bitcoin transactions make it possible to evade regulators and law enforcers. The use of Bitcoin and other cryptocurrencies for the movement of criminally acquired funds is often attributed to the circumvention of economic and trade sanctions imposed on a country, such as those faced by the DPRK. The DPRK is known to avoid such sanctions by mining Bitcoin and Monero (Guerrero-Saade & Moriuchi, 2018). Not surprisingly, cryptocurrencies have emerged as the currency of choice in ransomware attacks.

Ransomware combines two elements. One is a malware cyber attack that targets and exploits a vulnerability on a computer and encrypts the victim's critical data. The other is the capability to extort a ransom payment from the victim in return for decryption or

[11] The Onion Router (TOR) – User IP addresses and subsequent browsing activity are hidden behind an Onion Proxy (OP) which connects to the Onion Routers (ORs) on the Tor network concealing the data stream behind at least three layers of Tor Relays (ORs) through a persistent Transport Layer Security (TLS) connection between the ORs (Dingledine et al, 2004).

restoration of the hijacked data (Carbon Black, 2018). According to the 2018 Chainalysis report into the changing nature of cryptocurrency crime, a shift is evident in the illicit usage of Bitcoin from Darknet markets to thefts from scams, ransomware and hacks (Chainalysis, 2018). In addition, in 2017, Deputy U.S Attorney General Rod J. Rosenstein, quoted FBI estimates that ransomware payments would reach around US$1B annually (U.S. DOJ, 2017). Influences on that estimate could be seen through the two major ransomware attacks of 2017, NotPetya and WannaCry. With WannaCry driving a 40 percent uptick in infections between 2016 and 2017, according to Symantec's Internet Security Threat Report (ISTR) (2018).

WannaCry executed its ransomware campaign with three hardcoded Bitcoin addresses/wallets. As of 20th June 2017, 335 payments, totalling 51.91182371 Bitcoin (BTC) or US$144,010.54, had been collected from victims into the three Bitcoin wallets (Irwin and Turner, 2018). At the time WannaCry was one of the biggest outbreaks of ransomware (F-Secure, 2017), proving a strong indication of the evolving cryptocurrency threat from ransomware and the need for intelligence services to counter that threat.

3.2.2 Target Centric Intelligence

Back in 2012, the FBI identified the difficulties law enforcement could face when it comes to gaining intelligence from cryptocurrency systems in order to disrupt, prosecute and target illegal cryptocurrency activity (FBI, 2012). The advent of cryptocurrencies has enabled cyber criminals to avoid attribution and to move their proceeds of crime relatively anonymously throughout cryptocurrency ecosystems such as Bitcoin. Traditional institutional structures of intelligence collection, analysis and

dissemination, need to be readjusted to better meet the challenges of ransomware transaction in the Bitcoin ecosystem.

The target centric approach (Clark, 2017) seems to be particularly effective when applied to the cyber domain. This approach differs from the formal, clearly demarcated processes of the traditional intelligence cycle in that it allows all the stakeholders in the intelligence process – collectors, analysts, processers, technicians, and customers – to jointly and simultaneously elaborate a shared understanding of the target.

This paper takes a target centric approach to intelligence collection and analysis of WannaCry's usage of the Bitcoin ecosystem. This case study aims to present a generic model for intelligence collection and analysis against ransomware, a model that facilitates effective data sharing along with integrated, actionable assessment (Clark, 2017). Future research will look to build on the model with a combination of data from different intelligence sources in order to understand how ransomware might evolve in the future. This will, incorporate data from the target model into a Cyber Threat Intelligence (CTI) ontology using the Structured Threat Information Expression (STIX) format.

The paper structure is as follows: Section 3.3 looks at WannaCry and the details that define the attack, including important system components of WannaCry and Bitcoin along the typical malware kill chain. Section 3.4 addresses the problem definition by looking at the implications for intelligence and creates a generic problem definition model. Section 3.5 sketches the implications of the study and charts directions for future research, and Section 3.6 describes the findings in the context of the subsequent chapter.

3.3 Ransomware and Cryptocurrency – The Criminomics

Symantec's Internet Security Threat Report (ISTR) from July 2017, identifies ransomware attacks as the leading cybercrime threat to organisations and individuals worldwide (O'Brien, 2017). This increased concern was driven by the apparent success of the WannaCry and NotPetya attacks in May and June of 2017 respectively. Prior to these two attacks, ransomware comprised mainly of unsophisticated spam email campaigns. WannaCry dramatically changed the ransomware landscape with its ability to self-propagate across computer networks. In fact, there was a 46% rise in variants of ransomware in 2017 compared to 2016, (241,000 in 2016 vs. 350,000 in 2017 – Symantec, 2018). Further, a 2017 Carbon Black report into the ransomware economy shows a 2,502% increase in the sale of ransomware on dark web marketplaces (US$249,287.05 in 2016 to US$6,237,248.90 in 2017 – Carbon Black, 2017). This shows the continuous development and propagation by major ransomware groups to use ransomware diversely as a revenue generating attack, a decoy for further attacks or as a tool of destruction (O'Brien, 2017) that can be executed by skilled cyber criminals or even script kiddies[12]. Identifying where WannaCry fits into this classification helps to understand the mechanics and economics of the ransomware, in turn, helping build up a target picture of threat intelligence and the impact the WannaCry campaign had on its victims.

[12] A "Script Kiddie" is someone who uses existing programming code to hack somebody's computer, because they do not have the skill to write their own code (Oxford Dictionary, 2018).

3.3.1 WannaCry: Targets and Damages

WannaCry affected over 300,000 systems in 150 countries during its campaign beginning on the 12th May 2017 (Europol, 2017). Before breaking down the WannaCry – Bitcoin ecosystem as the target of intelligence collection and analysis, it is important to understand the WannaCry ransomware system in its full cyber domain context. WannaCry targeted vulnerabilities in older versions of the Windows Operating Systems (OS) (CVE-2017-0144) taking advantage of a flaw enabling the Server Message Block (SMB) protocol which enabled the proliferation of the malware using the EternalBlue exploit kit (U.S. District Court, 2018). The ransomware is capable of spreading itself to any unpatched computers on the victim's network or the Internet, behaving like a worm. In fact, a reversed engineered version of the CVE-2017-0144 exploit was made available for download by security researchers, RiskSense, on GitHub for non-malicious purposes days before the campaign struck its victims (U.S. District Court, 2018). According to Kaspersky Labs (2017), the victims ranged in geography and type. Corporations with networked IT systems were particularly vulnerable. Geographically, Russia seemed to be hit hardest and after day one of the attack WannaCry was evident in 74 countries.

Whilst a geographical analysis of Wannacry infections does not pinpoint patient zero[13] an industry or organisational view may help reveal important intelligence on the attackers' motivations and objectives. Mattei (2017, p.1) highlights that:

"…WannaCry also significantly disrupted the routine operation of several large commercial and governmental institutions including Fedex, the National Health

[13] Patient zero is the term given to the first infected machine of a malware attack and can help with containment, eradication, recovery and attribution when managing and investigating of an attack (Holley, 2018).

Service (NHS), Deutsche Bahn, Megafon, Telefónica, the Russian Central Bank, Russian Railways and Russia's Interior Ministry."

Out of those institutions, the NHS was hit hardest with 80 of the 236 its component Trusts, plus a further 603 operations affected (U.S. District Court, 2018). WannaCry did not seem to target any particular type of victim.

3.3.2 Bitcoin: Collection and Analysis

Before analysing the Bitcoin components of the WannaCry ransomware attack, it is important to briefly provide some details on the Bitcoin infrastructure. The Bitcoin infrastructure is made up of six elements: The Bitcoin wallet, the Bitcoin miner, the blockchain, network discovery, transaction structure, Bitcoin exchanges and services (Turner and Irwin, 2018).

Bitcoin is a peer-to-peer network where wallets, addresses, miners, exchanges and services act as nodes and transactions are the links between these nodes.

Transactions are the primary vehicle for exchanging value in the Bitcoin ecosystem. Bitcoin wallets are nodes on the network that contain multiple Bitcoin addresses which perform transactions that are propagated throughout the network and mined into new or existing blocks. A transaction maintains a list of inputs, which contains an index to unspent transactions and the associated signature, and outputs, which contains the receiving address and value to transfer.

The system generates some specific forensic information that could be used to help identify participants (Turner and Irwin, 2018). For example, criminally controlled wallets could leverage the fact that users must spend the entire list of inputs in the one

transaction. If this is not done a change address is setup to pay the user back any unspent inputs. The change address process makes it difficult to trace how many and where Bitcoins are being spent (Farghaly, 2014). Exploitation of the change address can be achieved through a technique called “peeling”. Analysis can be performed by following a large transaction amount and tracking the change address as it “peels” off into smaller amounts and then tracing and aggregating the peels to a meaningful recipient (Meiklejohn et al., 2013). This process can be witnessed in the WannaCry case when the wallets begin to cash-out their criminal proceeds, known as outflows (see Figure 3.6). Bitcoin outflows are movements from the attacker in an attempt to cash out their proceeds, by integrating their illicit funds at an exchange, into fiat currency, or into another more anonymous cryptocurrency (e.g. Monero), such was the case with WannaCry. Bitcoin exchanges and services are also points of vulnerability. Furthermore, network discovery through transaction and address propagation reveals a list of IP addresses built up by the node so it can find peers to connect to and advertise its existence on the network for other nodes to find it (Antonopoulos, 2010). This is also a point of vulnerability, as nodes maintain a list of IP addresses of other peers in the network, and a timestamp, which can reveal the currency of the activity of the node (Biryukov et al., 2014). Attribution may be possible at these points, depending on the personally identifiable information (PII) stored on the user accounts of these exchanges and services.

Collection of key intelligence from the Bitcoin ecosystem is crucial to LEAs and the IC, though being able to break the Bitcoin system into two network graphs (addresses and transactions) for analysis is also important, as it makes it possible to cluster and map behaviours of users and transactions over time. For example, being able to

aggregate the balances belonging to public keys that are controlled by a particular user (Fleder et al., 2015) and visualising the resulting clusters on a map to determine any illicit activities being performed on the Bitcoin network. Having outlined what can be collected and analysed from the Bitcoin ecosystem, we now turn to the WannaCry – Bitcoin dynamic.

3.3.3 WannaCry – Bitcoin: Payment analysis

As per analysis from Bistarelli et al (2018), Conti et al (2017), Secureworks (2017), Kaspersky (2017), Neutrino (2017), the ransom seed Bitcoin (BTC) addresses identified in the WannaCry attack and the respective wallets owning these addresses are as follows:

Seed #1

- BTC Wallet ID: **d394a6a98a**
- BTC address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Seed #2

- BTC Wallet ID: **0f382fa542**
- BTC address: 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Seed #3

- BTC Wallet ID: **7fe1df02cb**
- BTC Address: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

WannaCry was meant to create a unique address for every victim infected, but failed to do so due to a software bug in the ransomware's execution (O'Brien, 2017). It therefore defaulted to the three hardcoded addresses identified above[14].

In a time series analysis, Conti et al (2018) examined the economic significance of the WannaCry ransomware over the course of four months (12th May 2017 to 2nd October 2017). Their data show a concentrated period of two weeks where WannaCry collected the majority of its ransoms (12th May 2017 to 26th May 2017). In fact, Bistarelli et al (2018), show that during this two-week period, 89% of the ransoms for WannaCry were collected in the first week of the campaign. Table 3.1 shows 238 ransom payments were identified using the ransom identification framework presented in Conti et al. (2018).

Ransom	**Time Period**	**Payments**	**BTC**	**USD value**
$300	May 12, 2017 – Oct. 2, 2017	192	32.3430	58,416.62
$600		46	14.8313	27,660.14
Total		**238**	**47.1743**	**86,076.76**

Table 3.1: WannaCry ransom payments (Source: Conti et al, 2018).

This is somewhat different to what Bistarelli et al (2018) reported in their analysis. Over the two-week period they found 248 ransomware payments totalling 50.14 BTC (Bistarelli et al, 2018) and cryptocurrency monitoring company, Neutrino (2017), reported a total of 333 incoming transactions collecting 51.93 BTC. Ransom payment identification methods can vary between analysts, researchers and software systems. This is due to differences in the observation of respective ransom identification frameworks, such as, ransom demand structure, BTC price and exchange rate at the

[14] It is programmatically possible to generate payment wallets and addresses automatically and communicate between victim and command and control (C2) server to manage the payment infrastructure at the time of exploitation.

time of the campaign, coverage of ransom seed addresses, transaction fees, timing of payments and transaction timestamps used for filtering (Ahn et al, 2016; Conti et al, 2018; Huang et al, 2018; Bistarelli et al, 2018).

Conti et al (2018) provide a general framework for identifying ransomware payments. Firstly, identify the Bitcoin seed addresses belonging to the ransomware. This could be many or it could be one depending on the execution of the ransomware. Next, collect the data associated with these seed addresses and understand what constitutes a ransom payment from the blockchain. This refers to the payment inflows from victims and the cash outflows by the attacker-controlled ransom addresses. In order to develop attribution of the attacker, it is also possible to augment the data collected on the blockchain with data from external sources. Examples could be data from Bitcoin exchanges and services relating to user accounts and open source data from social media or Internet forums.

The first reported infections of the WannaCry campaign began on the 12th May 2017. Initially, a victim's data would be encrypted and the WannaCry ransom would demand US$300 worth of Bitcoin. Subsequently, after three days, if payment is delayed the ransom would be raised to US$600. Then after 7 days the ransomware would report to the victim that their files would be impossible to decrypt (Bistarelli et al, 2018).

A twitter bot known as @actual_ransom on 3rd August 2017 identified the first outflows from the WannaCry attackers wallets. This bot was set up by journalist Keith Collins to monitor activity of the WannaCry ransom addresses (Woodward, 2017). Section 3.4

will highlight one path these outflows took and from an intelligence perspective why it is important to track the outflows to their ultimate destination.

3.3.4 WannaCry – Bitcoin: Sabotage or big business?

Return on Infections (ROI) and Ransom Payments per Infection (RPPI) are new concepts that we propose to use to evaluate the distinct financial effects and destructive impacts of particular ransomware campaigns.

1) ROI = $\frac{\Sigma\ Ransom\ collected\ in\ BTC}{\Sigma}$ $Ransomware\ infections$
2) RPPI = $\frac{\Sigma\ Ransom\ payments}{\Sigma}$ $Ransomware\ infections$

Firstly, by taking the number of reported WannaCry infections, 300,000, and the number of identified ransomware payments from 12th May to 2nd October 2017 as seen in table 2 and 3, it is possible to deduce the following for WannaCry:

- 238 ransom payments collected 47.1743 BTC; US$86,076.76; using the BTC to US$ exchange rate at the time of the WannaCry campaign.
- Ransom Payments per infection (RPPI) = 238/300,000 = 0.00079

By comparison, CryptoLocker, which had a more complex ransom payment structure and produced 250,000 infections (Kelion, 2013), collected 804 ransom payments over the time frame September 5th 2013 to January 30th 2014 (Conti et al, 2018). Therefore:

- 804 ransom payments collected 1403.7548 BTC; US$449,227.97; using the BTC:USD exchange rate at the time of the CryptoLocker campaign.
- RPPI = 804/250,000 = 0.003216

Address	**Payments**	**BTC**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	77	15.1129

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	92	18.5431
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	69	13.5183

Table 3.2: WannaCry ransom payments by ransom seed address (Source: Conti et al, 2018).

Ransomware	Overall			Ransom		
	Payments	**BTC**	**US$ value**	**Payments**	**BTC**	**US$ value**
CryptoLocker	**51,766**	**133,045.9961**	**42,292,191.17**	**804**	**1403.7548**	**449,274.97**
WannaCry	**341**	**53.2906**	**99,549.05**	**238**	**47.1743**	**86,076.76**

Table 3.3: Ransomware payments by ransomware attack (Source: Conti et al, 2018).

The effectiveness of WannaCry as a revenue generating ransomware campaign can be questioned with as little as 1 in 1,260 infected machines paying ransom. This compared with CryptoLocker, which yielded a ransom payment for every 310 infected machines. WannaCry's ROI stands at less than half Cryptolocker's.

(WannaCry = 47.1743 / 300,000 = 0.0023587 BTC per infected machine; and for CryptoLocker = 1403.7548 / 250,000 = 0.005615 BTC per infected machine.)

The relatively modest ROI was due to some design flaws in the software. For example, security researcher Marcus Hutchins discovered WannaCry was using an unregistered domain name (*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*) as a "kill switch" (Hutchins, 2017). If a request to the domain returned a response it would arrest the spread of WannaCry. If there were no response from the domain the malware would continue to propagate. By registering this domain name, Mr Hutchins was able to effectively sinkhole[15] the malware and stop any further infection (Bistarelli et al, 2018).

This comes in addition to the above-mentioned bug in the payment-management execution that limited the scope of ransom collection to 3 hard coded Bitcoin addresses

[15] A sinkhole acts as a tool for eradicating the spreading of malware infection vectors and also can be used to break the connection to the command and control server (Mazerick, 2018).

(O'Brien, 2017). This bug left the attackers unable to identify which victims have paid, making it impossible to restore a paying victim's files and prevent subsequent damages.

Either way, the effects of a ransomware attack are far reaching. Recalling that WannaCry rendered many important public service networks inoperable including the NHS at hospitals in the United Kingdom (Mayor, 2018).

The specific vulnerability it exploited allowed WannaCry to effectively propagate and achieve a high spread in a small time frame. The monetary return on these infections was quite low. With respect to the ROI and RPPI calculated above, this would indicate that WannaCry's malicious capacity outweighed the financial rewards ransomware can produce. This could suggest that the malware designers were more focused on infection and disruption than on revenue raising.

The matrix in Figure 3.1 will serve to classify ransomware with respect to its impact on victims and the complexity of its execution. It yields four classification quadrants. Starting from the bottom left, low complexity and low impact, typically trial runs for more sophisticated subsequent attacks. The bottom right, high complexity and low impact quadrant, refers to attacks that are advanced in their exploit and invasive in nature but are serve primarily to distract their targets and open the door for more devastating attacks to be executed. The top left quadrant refers to ransomware that disrupts a victim's computer or network, causing widespread confusion amongst victims and delaying effective response (Symantec, 2018). The top right quadrant refers to mature ransomware that is effectively designed to maximise profit. These attacks are typically highly complex due to their sophisticated payment management, infection

vectors and encryption strength. Furthermore, not only do these types of attacks render computer equipment and data un-useable, they also cripple the victim financially. WannaCry can be placed in the 'Tool of destruction' quadrant, halfway up the impact axis and towards a medium level of sophistication due to the nature of the exploit.

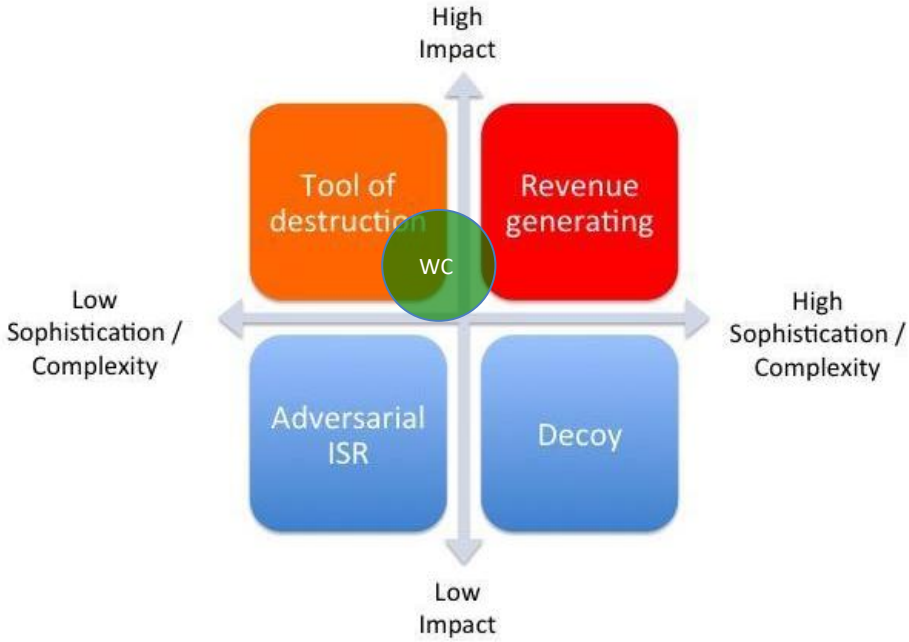


Figure 3.1: Ransomware classification matrix.

Reflecting on Figure 3.1, and to move forward on any criminal investigation, there is a need to understand what data can be collected to help reveal anonymity and attribution to a domain that seeks to conceal both.

3.3.5 WannaCry – Bitcoin: Tracing an Attack

Much has recently been made public regarding the attribution of the WannaCry ransomware attack. The U.S (U.S. District Court, 2018) has pointed the finger at North Korea (DPRK). Attributing ransomware attacks of this nature requires a high degree of computer forensic work. The US claims are based on the examination of cyber

infrastructure such as IP addresses, proxy servers, computers, mobile devices, Bitcoin addresses, email and social media accounts accessed by the cyber criminals using IP address ranges located in the DPRK that are used to control reusable Trojans and worms with signatures related to the Lazarus group to control victim's machines (U.S. District Court, 2018).

One of the intelligence gaps that stand out in this case is the lack of collection and analysis against the Bitcoin money flows. Questions could be asked as to whether these same email addresses or social media accounts have been used to also set up the Bitcoin address and exchange accounts and whether they have been accessed from the same computers or devices on the IP addresses linked to the DPRK. In a case where the primary charge is conspiracy to commit wire fraud a stronger focus could be put on the money laundering aspects of cryptocurrency. In order to provide that focus, it is important to break down the component parts of WannaCry against the cyber attack kill chain.

3.3.5.1 WannaCry Kill Chain

Ransomware typically follows the Advanced Persistent Threat (APT)[16] kill chain that is an archetypal system for describing the different phases a cyber attack moves through. Lockheed Martin defines seven steps in the "kill chain" that form the adversary functions, which contain the structures and processes of the ransomware system to be analysed (Hutchins et al, 2011). To this we have added an eighth step, "Mobilisation",

[16] An APT is aimed at nation states and large targets and is defined by Kaspersky Lab (2018) as: "[using] continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences."

to account for the infrastructure and resourcing activity that happens prior to executing a ransomware attack. This forms a “ransomware kill chain” and unfolds as follows:

1. Reconnaissance
2. Mobilisation
3. Weaponisation
4. Delivery
5. Exploitation
6. Installation
7. Command and Control (C2)
8. Actions on objectives

Figure 3.2 shows the system linking these processes for the WannaCry Ransomware.

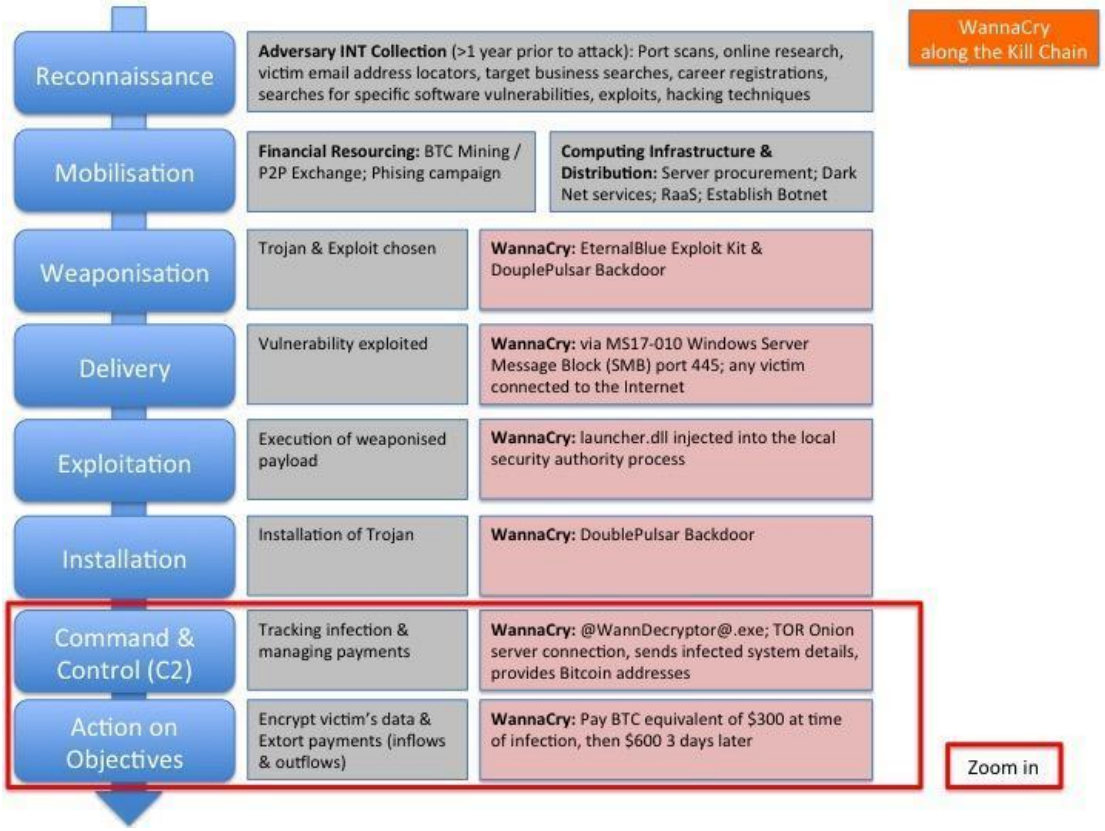


Figure 3.2: WannaCry “Ransomware Kill Chain.”

Focussing in on the Bitcoin component of WannaCry, evidence can be collected from victims who have paid the ransom to specified Bitcoin ransom addresses. The feedback from the Bitcoin payment actions to the Command & Control servers provide the means for the attackers to manage their payments and for LEAs and the IC to focus the target model around illicit payment flows. The data collected here should focus on BTC payment inflow from victims of the ransomware attack. In addition, when the attacker cashes-out the collected ransom, the BTC payment outflow from the ransom addresses should be monitored. Furthermore, there may be indicators of mobilisation, such as phishing campaigns, botnet set up and Bitcoin address creation at suspect exchanges. This could inform LEAs and the IC, allowing them to monitor known Bitcoin exchanges and services that facilitate money laundering activities. In order to build the required intelligence on ransomware it is important to understand these indicators and the observable data that these elements create.

3.3.5.2 WannaCry inflows

Analysis conducted by Huang et al (2018) reveals details about the exchanges used by victims to make payments to the WannaCry ransom seed addresses. This profile of victim payments shows that the Bitthumb.com and BTC-e.com exchanges make up approximately 10% of victim payments. The largest known inflows came from LocalBitcoins.com contributing about 15% of victim payments, whilst more than half were categorised as miscellaneous or unknown. The Bitthumb.com exchange is known to only accept Korean Won to purchase Bitcoins (Huang et al, 2018). Personal Identifiable Information (PII), such as Korean phone numbers is also collected on these accounts (Huang et al, 2018). A Russian national operated the BTC-e.com exchange

and this was taken down on allegations of running an international money-laundering scheme (U.S. DOJ, 2017). Localbitcoins.com is operated out of Finland and is a market place for peer-to-peer Bitcoin trades or to exchange BTC to cash or other payment types (Pineda, 2014). Whilst this exchange is still in operation, it has suffered a number of blocks from regulators in Germany, New York and Russia due to breaches of licensing requirements, and it was known to facilitate money-laundering operations in the past (Rizzo, 2014; Elliot, 2016; Young, 2015; Redman, 2016; Das, 2016).

3.3.5.3 WannaCry Cashing Out

The first known WannaCry cash-out occurred on August 3rd 2017. A high-level report conducted by the Neutrino Research Team in September 2017 identified an outgoing transaction moved 8.73 BTC on August 3rd 2017. It took just a few minutes and five more transactions to empty the wallet, where these cash-out transactions ultimately arrived at two known suspicious exchanges, Shapeshift and Changelly (Neutrino, 2017). As was noted in the U.S v. Park Jin Hyok criminal complaint (2018), WannaCry 1.0 and WannaCry 2.0 used a similar cash-out exchange and this appears to be Shapeshift where 13.53BTC were further exchanged into another more anonymous cryptocurrency, Monero.

The Changelly exchange received 33.83 BTC from the cash out of the WannaCry ransom wallets. Interestingly, the cash out behaviour of the WannaCry attackers changed as Shapeshift started blacklisting WannaCry addresses (Neutrino, 2017). The cash-out patterns of the WannaCry ransom addresses reveal exchange points where conversion of the BTC will occur and provide valuable Cyber Threat Intelligence (CTI), all registered and auditable on the blockchain.

3.3.5.4 WannaCry Target Model

Figure 3.3 forms the generic system model for a ransomware-cryptocurrency interaction between attacker and victim.

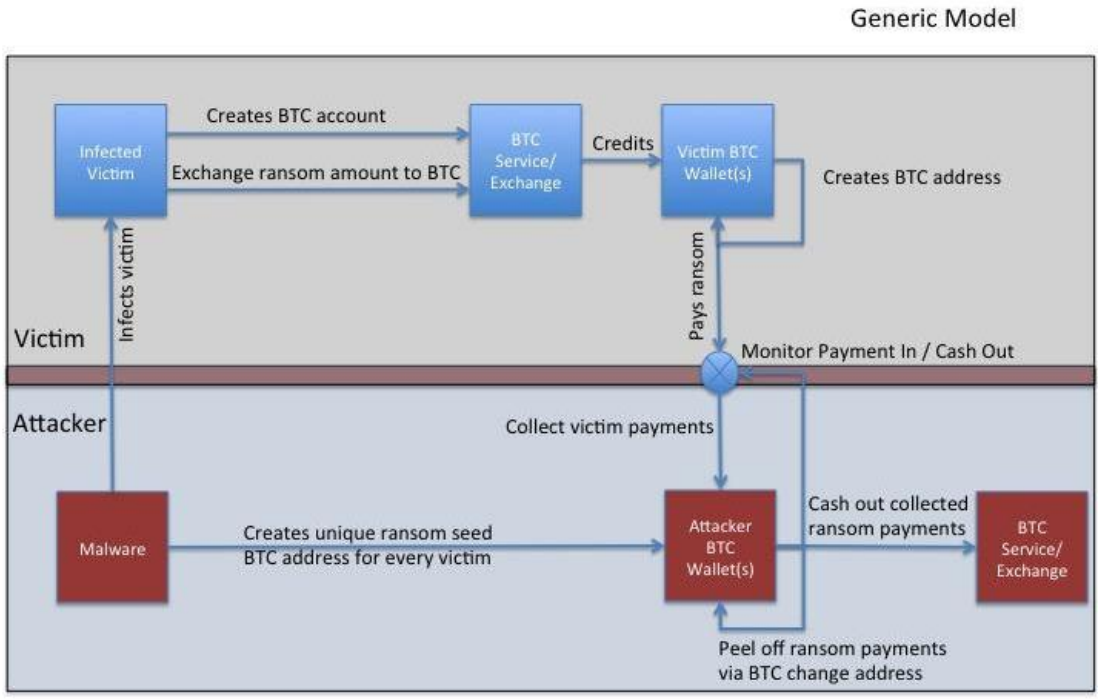


Figure 3.3: Ransomware – Bitcoin Generic System Model

The flow of Figure 3.3 is as follows:

1. Victim infected
2. Details sent to Command and Control server (C2)
3. Public encryption key sent to victim, ransom instructions on the lock screen sent to victim (i.e. ransom seed bitcoin wallet address)
4. Victim files encrypted
5. Machine keeps polling the C2 looking for updates (E.g. a decryption command)

6. Victim makes payment to the attackers wallet, via a hidden BTC service or exchange, using the ransom seed BTC address
7. C2 acknowledges payment, maps to a particular victim, and releases the private key needed for decryption and files are restored.

Figure 3.3 shows how an attacker infects a victim with malware (in this case the WannaCry ransomware), and triggers the interaction with the Bitcoin ecosystem setting in motion activity which requires the victim to generate Bitcoin by registering an account and crediting it through the exchange of fiat currency to Bitcoin by interacting with a Bitcoin exchange. The victim then proceeds to execute a Bitcoin transaction to pay the ransom to the attackers ransom address. The attacker also generates footprints on the Bitcoin ecosystem when the malware generates the ransom seed addresses. Furthermore, when an attacker cashes out at a virtual currency exchange, this generates pertinent intelligence on the blockchain and may interface with the fiat monetary system or other wallets and exchanges[17].

3.4 WannaCry – Bitcoin: Implications for Intelligence

This section will showcase target centric approach that we believe is the most effective way to leverage the cryptocurrency data and create an integrated, comprehensive and actionable intelligence picture in a timely manner.

[17] Custodial exchanges are those in possession and control of the user's wallet private keys. They require identity verification for accounts via user PII. Non-custodial exchanges are those exchanges that require no account registration and provide real time exchange from one cryptocurrency to another cryptocurrency (Woods, 2018).

3.4.1 Problem Definition Model (PDM): WannaCry Ransomware

Generating a problem definition model (PDM) could facilitate the creation of a common understanding of the WannaCry Ransomware operating environment using the Political, Military, Economic, Society, Infrastructure and Information (PMESII) approach to systems thinking (Clark and Mitchell, 2016). For example, in the WannaCry ransomware case, it could be of vital interest to understand how WannaCry managed its ransom proceeds and how these currency flows could be frozen or seized. The answer to questions like where does the WannaCry ransomware seed BTC addresses cash out their proceeds on the BTC network, become the specific focus. Figure 3.4 provides a top level PDM for a Ransomware cyber threat.

Figure 3.4: Ransomware Problem Definition Model (Adapted from Clark and Mitchell, 2016).

At a generic level, the PDM in Figure 3.4 will provide the basis to understand the structure, function and process of a ransomware cyber threat. This PDM shows that a ransomware cyber threat constitutes elements relating to the source of the cyber attack, the likely targets, the means of attack, other information warfare effects and the proceeds generated from the ransom attack. Populating the PDM allows analysts to "zoom-in" and target specific components, such as the Bitcoin flows from the WannaCry ransomware. Figure 3.5 shows the next level of detail relating to the specific ransomware attack, WannaCry.

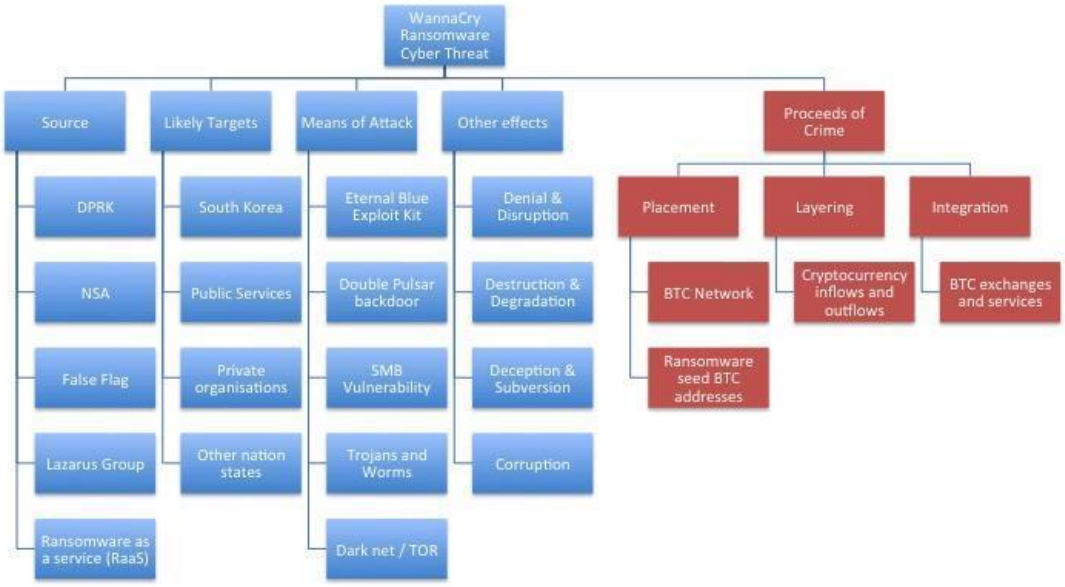


Figure 3.5: WannaCry Ransomware Problem Definition Model.

Describing Figure 3.5, it can be said that **the source** of the WannaCry attack has been attributed to the DPRK and shows similar signatures to other malware used by the Lazarus group. Hirsch (2018) mentions that the EternalBlue exploit was leaked from the U.S National Security Agency (NSA). Other working assumptions of interest to the IC could be the view that WannaCry is a false flag[18] operation and furthermore the attackers could be leveraging the Ransomware as a Service (RaaS) model across Darknet markets. The **targets of** the attack have a broad infection footprint covering public and private sector companies. With respect to targeted nations, it might be plausible to single out those that are adversarial to the DPRK. This includes South

[18] False flag operations in cyber warfare refer to: "tactics used in covert cyber attacks by a perpetrator to deceive or misguide attribution attempts including the attacker's origin, identity, movement, and/or code/exploitation." (Wikipedia, 2018).

Korea, the U.S and possibly disgruntled allies of the DPRK in the form of Russia and China (DoD, 2015). The **means of attack** are the malware kit targeting vulnerabilities in Windows Personal Computers using a worm to self-propagate to other machines. Command and Control was done behind TOR nodes on the Darknet that helped protect identity and location of the attackers and facilitate the ransom payment management. **Other effects** either intended or consequential of the ransomware attack include rendering victim's computers, networks and information unusable due to disruption to their operations, degradation of their services, subversion of their systems and corruption of critical data. The **proceeds of crime** breakdown allow the collection of intelligence and focussing of intervention efforts on the money laundering steps of placement, layering and integration with respect to Bitcoin. For example, in the case of WannaCry, placement can be seen when a victim's funds enter the BTC network and are collected using the three main Bitcoin ransom seed addresses. Layering is achieved by moving cryptocurrency in and out of the ransom seed addresses and referred to as Bitcoin inflows and outflows. Intelligence yielded here can provide victim profile details, i.e. where the BTC transfers are coming from (e.g. exchanges, locations, addresses).

3.4.2 WannaCry – Bitcoin: Extracting Cyber Threat Intelligence (CTI)

Clark and Mitchell (2016) note that well-defined PDMs are imperative to breaking the intelligence problem down into its component parts to ensure the transition to the desired target model is timely, feeds the intended purpose, can be shared and updated collaboratively and in a controlled manner. Here we outline the Cyber Threat Intelligence (CTI) that can be derived from the WannaCry – Bitcoin interaction.

Using the blockchain to monitor the transactions that involve a ransomware attacker's BTC wallet provides valuable intelligence. Recent policy and regulation on virtual currency exchanges, such as EU Directive 2018/843 (aka. the 5th AML Directive), requires virtual currency exchanges and custodian wallets (i.e. virtual currency wallet services where the service holds the user's private keys) to make data available to Financial Intelligence Units (FIUs).

Vital intelligence, in the form of Personal Identifiable Information (PII) can be collected on both the victim and perpetrator side of the WannaCry – Bitcoin target model. As a result, forensic investigation may be able to look at the details of the computing and network infrastructure (e.g. IP-address, geo-location, Bitcoin blockchain protocol details, BTC node activity, TOR connections, network traffic analysis, coding style and language and program compilers to provide intelligence to counter anonymity and reveal the identities of the bad actors controlling proceeds of crime from ransomware attacks).

Intelligence agencies can target the following:

At an operational level:

- Ransom Seed Address(es): The BTC addresses used by WannaCry to collect ransom payments.
- Transaction Inputs: The incoming transactions from a victim BTC address to the Ransom Seed Address(es) containing the ransom amount.
- Transaction Outputs: The outgoing transactions from the Ransom Seed Address(es) to another BTC address. This can go many levels deep in the network.

- Inflow: Those inputs aggregating into a particular transaction made up from previous transactions.
- Outflow: Those outputs from a particular transaction feeding the next transaction and providing the target out flow destination for ransom funds.
- Computer and network infrastructure components (E.g. IP addresses, proxy servers, email accounts, TOR connections, malware signatures).

At a tactical level:

- Popular victim exchanges: Bithumb, Localbitcoins.com and BTC-e
- Preferred attacker cash out exchanges: Shapeshift and Changelly (converting to the more anonymous cryptocurrency Monero).
- Virtual currency exchanges KYC and CDD processes.
- PII available from virtual currency exchanges.

At a strategic level:

- Policy and Regulation of Virtual Currency Exchanges, services and custodian wallets (E.g. EU Directive 2018/849, FATF AML/TF Recommendations and the Australian AML/CFT Act).
- Adversarial cyber capability and vulnerability of prospective attackers.
- High risk geographies (E.g. North Korea, Russia, Iran and China).
- Economic sanctions imposed by the United Nations (U.N), the U.S., the European Union (EU), South Korea and Japan (Albert, 2018).

3.4.3 WannaCry – Bitcoin: Populating the target model

Populating the CTI objects at an operational and tactical level with data collected from the blockchain with respect to the WannaCry ransomware attack yields a network graph as shown in Figure 3.6. The red circle identifies the ransom seed address, the blue circles represent the number of inputs into the green transaction circles. The pink circles represent the number of outputs from the green transaction circles and the grey circles identify the wallets owning the BTC addresses related to the inputs and outputs of a transaction.

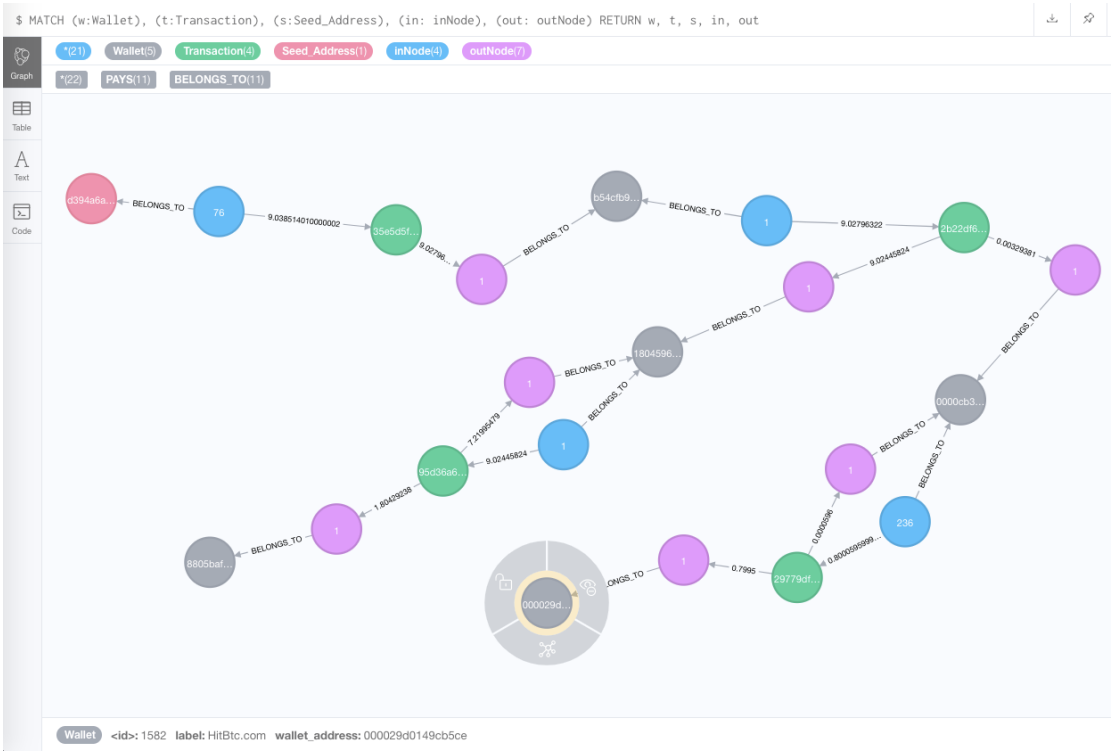


Figure 3.6: WannaCry ransom seed address cash out profile (transaction walk).

This graph shows a transaction walk of the cash out behaviour from one of the WannaCry ransom seed wallet addresses (d394a6a98aabeeae). The data was pulled from a blockchain API available from walletexplorer.com and read into the graph database neo4j where nodes and relationships were created to represent the operational

and tactical level CTI objects. The graph database can be queried to identify transaction walks N levels deep in the Bitcoin network to where it reaches a known cryptocurrency exchange and can activate intelligence collection or counter intelligence intervention. There is strong use of the "peeling" concept, mentioned in Section 3.2, using the change address to obfuscate the cash-out flow. In addition, the aggregation and disaggregation of transaction inputs and outputs is evident along this cash out path. Ultimately the graph reveals the wallets in control of the cash-out transactions, the amounts that are being moved, timestamps, transaction IDs and the destination of the funds. Tracing one of the cash-out branches from Figure 3.6 shows the final destination of 0.7995 BTC arriving at an exchange known as HitBTC.com under a wallet address 000029d0149cb5ce. This exchange requires user registration of email and password to perform trades (Hitbtc Review, 2018), however there are stringent Know Your Customer (KYC) processes in place if the user wishes to deposit or withdraw into fiat currency (Hitbtc Review, 2018). The exchange operates out of Hong Kong (Dale, 2018) and interfaces with the non-custodial exchange Changelly, which allows instant crypto-to-crypto exchanges with no account necessary (Munkachy, 2018). This provides the attacker further capability of obfuscating their illicit funds. Investigation into whether the wallet being used on HitBTC.com has PII associated to it or at least an email address would allow forensic examination and would help LEAs reveal the attribution of the attackers.

3.5 Future Research and Conclusion

Above we proposed an intelligence coordination method to target the Bitcoin blockchain for actionable intelligence on the WannaCry ransomware attack. This approach can support intelligence, cyber security and cyber crime investigation efforts. In addition, by using a common standard, such as STIX, a customised cyber observable

object could be created and shared containing threat information relating to the cryptocurrency components of ransomware.

Whether by intention or through the incompetence of its authors, WannaCry functioned more as a 'Tool of Destruction' than a 'Revenue Generating' attack. The proposed spectrum of ransomware classification extends the boundaries of the model. Tracing WannaCry along the "Kill Chain" focussing on the Bitcoin victim inflow and the attacker outflow allows analysts to formulate a target model to help drive CTI collection and collaboration efforts.

Our particular analysis only draws on the information available from the Bitcoin blockchain. Though these data are rich from a transaction audit trail and money flow perspective, the intelligence needed to defeat anonymity and facilitate attribution requires an augmentation of all-source intelligence to gain an in-depth understanding of what is really going on in terms of the structures and processes of a ransomware attack and be able to set up early warning detection in order to predict and defeat the next attack.

3.6 A problem half solved

The famous American inventor Charles Franklin Kettering is quoted as saying "a problem well stated is a problem half solved." This rings true for the work presented in Chapter 3. Here we present a working model, the Target Network Model (TNM) and the Problem Definition Model (PDM), for the interaction ransomware has with a cryptocurrency network. The case of WannaCry 2.0 is used to develop the model and what components need to be considered. Furthermore, the analysis undertaken in this

chapter breaks down the impact of the WannCry 2.0 ransomware attack in terms of ransom payments in Bitcoin (BTC). Metrics relating to Return on Infections (ROI), Ransom Payments per Infection (RPPI), and classifying an attack as sabotage versus revenue generating are created. Through the creation of a TNM and PDM for ransomware-Bitcoin interaction, a schematic is developed which provides a window into the cryptocurrency behaviour of ransomware-Bitcoin payments.

The other half of the ransomware-Bitcoin problem is using what has been defined in order to achieve the threat intelligence goals. These goals refer to requirements of scoping, collection, analysis, and dissemination where threat intelligence yields, as defined by Gartner (2013), "*evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.*" (McMillan, 2013). In order to satisfy this definition for the ransomware-Bitcoin problem space, this chapter recommends the further development of a common intelligence sharing standard, using the models outlined, for the collection and interpretation of threat intelligence. The next chapter demonstrates, using an industry accepted standard such as the Structured Threat Information eXpression (STIX), that it is possible to augment the available data on the blockchain to better understand the structures, processes, patterns, and payments relating to a ransomware attack and thus turning the data collected using the TNM and PDM to actionable insights.

Chapter 4: Ransomware-Bitcoin Threat Intelligence Sharing Using Structured Threat Information Expression (STIX)

"*The goal is to turn data into information and information into insight*." – Carly Fiorina, former chief executive officer, Hewlett Packard.

4.1 Abstract

To address the challenge of representing ransomware-cryptocurrency payments, this article outlines a novel approach to the extraction and sharing of threat intelligence data from the Bitcoin blockchain. This work results in the creation of two new cyber-observable objects, x-cryptocurrency-address, and x-cryptocurrency-transaction.

This article outlines a novel approach to the extraction and sharing of data from the Bitcoin blockchain to form the cash-in and cash-out networks of ransomware-Bitcoin money flows. These data can help fill a general gap in our understanding of ransomware attacks. Researchers and practitioners have tended to focus on the malware used and vectors of penetration while overlooking the no less significant information about the movement of ransom payments over cryptocurrency networks. This is evident in the WannaCry ransomware analysis performed by security researchers. For example, in research performed by Mackenzie (2019), the focus remains on the computer system vulnerabilities exploited: that is, Windows (CVE-2019-0708) using the EternalBlue exploit kit and installing the DoublePulsar backdoor. However, a comprehensive threat

intelligence approach and incident response must consider and exploit the cryptocurrency elements of ransomware attacks.

4.2 Background and Motivation

To address the challenge of representing ransomware-cryptocurrency payments, we use the Structured Threat Information Expression (STIX) format. STIX provides a means to consistently share threat intelligence relating to ransomware-Bitcoin payments among organizations, security researchers, investigators, and the intelligence community (Oasis, 2020). The STIX format provides the capabilities required to design custom objects and reuse existing objects to represent and understand and to share this intelligence among the stakeholders (Oasis, 2020). To adapt the usage of the STIX format to the utility of ransomware-Bitcoin payments, we establish a picture of what ransomware-Bitcoin threat intelligence could look like by modelling the target network, drawing on existing money laundering (ML) red flag indicators relating to cryptocurrency, and planning the required intelligence collection efforts.

The data collected from the WannaCry ransomware attack are then used to demonstrate our proposed use of the STIX format. We then develop the STIX-Ransomware-Bitcoin Framework (SRBF). By extending the STIX model to generate cyber threat intelligence (CTI) relating to a ransomware-Bitcoin attack, we define a common data model for sharing the cryptocurrency-related threat intelligence. This work results in the creation of two new cyber-observable objects, *x-cryptocurrency-address* and *x-cryptocurrency-transaction*. In addition, we leverage the "*external references*" parameter on the existing STIX Observed Data object to preserve the cash-in and cash-out Bitcoin network data generated by the WannaCry ransomware attack. Our proposed procedure

yields a standardized way threat data can be effectively constructed, shared, and exploited by both humans and machines. The gap this research aims to cover relates to an emerging threat prevalent in the use of Bitcoin during ransomware attacks and how STIX can capture this threat relating to the corresponding ransomware-Bitcoin payments.

4.3 CTI

This section describes the use of Cyber Threat Intelligence (CTI) applied to the ransomware-Bitcoin payments of the WannaCry ransomware attack. Understanding the target network structure and the information contained within the structure is the first step toward actionable CTI.

4.3.1 Target Network

CTI aims to synthesize intelligence to gain insight into a cyber adversary's strengths and weaknesses and foresight about the threat posed by the adversary and its implications. Successful threat intelligence within the cyber domain demands a knowledge base of threat information and an expressive way to represent this knowledge, typically by using shared taxonomies, standards, and ontologies (Mavroeidis and Bromander, 2017). All the data collected and presented as part of the intelligence collection process form patterns that are informed by a host of assumptions, both empirical and logical. The process must leverage the evolving information needs that create the complex patterns of illicit cryptocurrency money flows that are derived and developed from a ransomware campaign. The blockchain environment is readily accessible yet quite complex to analyse, making it easy for malicious agents to transact with victims and launder money behind a wall of anonymity.

In the case of a ransomware-Bitcoin network, the target could be the ransomware-Bitcoin seed address or the cash-out point of the attacker's ransom bounty. The data that are extracted from the blockchain are cognitively processed through various mental schemas by both humans and machines. A significant task in interpreting the data is to create schemas that are as specific as possible about the nature and processes that are involved in the execution of ransomware attacks, including the different motivations and modes of action adopted by attackers (Gottschalk, 2015). Having specific schemas of different modes of criminal behaviour allows analysts—be it human or virtual—to effectively characterize the intelligence target.

To reconstruct the Bitcoin-related events of the WannaCry ransomware attack, we need to look at the two sides of a ransomware-Bitcoin seed address. These two sides represent the cash-in and cash-out networks. The cash-in network models the victim's ransom payments. The cash-out network moves the collected ransom payments from the attacker-controlled ransomware-Bitcoin seed address into different financial destinations to launder the money. A subset of Bitcoin addresses and transactions resulting from the WannaCry ransomware attack is analysed throughout this article. The addresses and transactions are catalogued in Table 4.1 and will be referred to using the ID number in the subsequent diagrams and text.

Figure 4.1 represents a target network model for the ransomware-Bitcoin cash-in payment network for the WannaCry ransomware attack as analysed in the "Data Analysis" section and catalogued in Table 4.1. The cash-in network is formed by the victims at the start of a ransomware campaign when the victim pays ransomware into the attacker-controlled Bitcoin address, known as the *ransomware-Bitcoin seed address*

or *ransom seed address*. A similar network exists for the cash-out behaviour of the WannaCry ransomware-Bitcoin campaign. This is illustrated in Figure 4.2, analysed in the "Data Analysis" section, and catalogued in Table 4.1. It reveals the tactics that an attacker uses to move these ransomware proceeds into other areas of the cryptocurrency ecosystem to evade detection. This creates a cash-out trail and could lead investigators to key cryptocurrency exchanges and services or even into the traditional financial system.

Figures 4.1 and 4.2 form to create a target network model. This can be used to develop a common situational understanding (SU) and identify intelligence gaps.

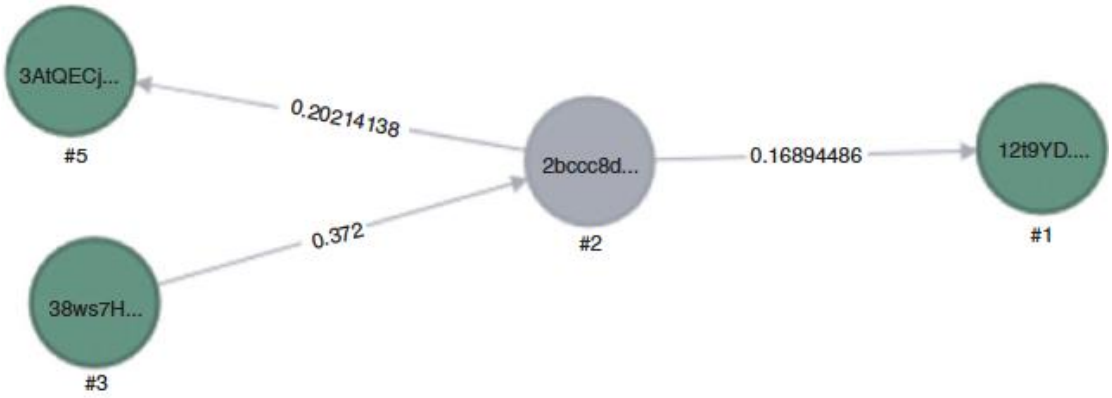


Figure 4.1: The Ransomware-Bitcoin Target Cash-in Payment Network Model.

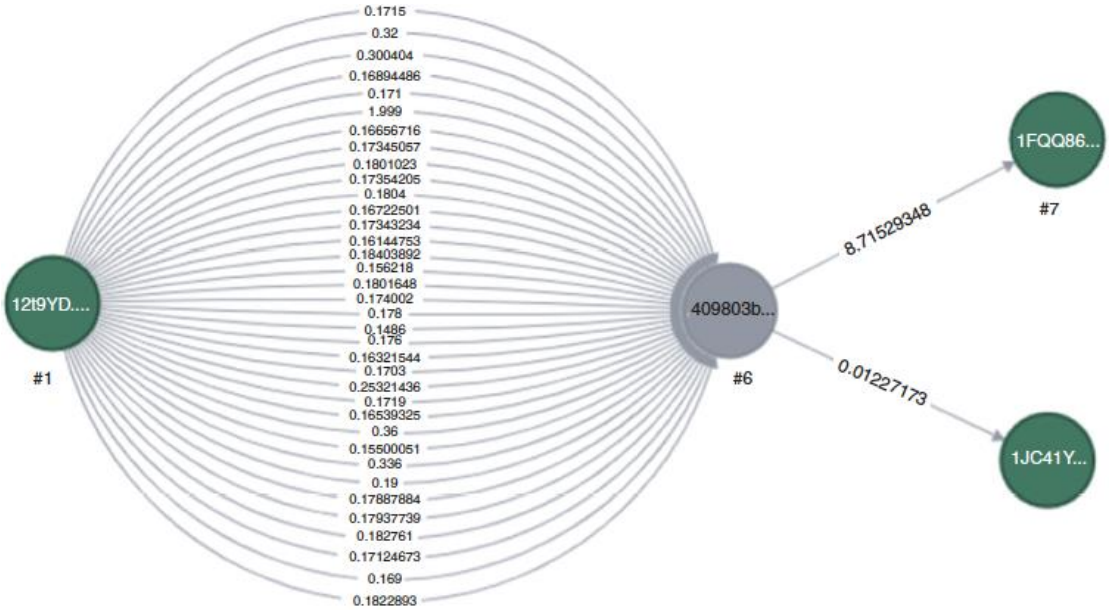


Figure 4.2: The ransomware-Bitcoin Target Cash-out Payment Network Model.

The figures are generated using the data collection framework in the "Data Collection" section.

ID	Address / Transaction (TX)	Purpose
#1	*12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*	Ransomware seed address
#2	*2bccc8d2b72da8c8733aef73a7bad85ae3bf834f86607540a68b4a8ef252e32c*	TX of victim ransom payment
#3	*38ws7HY9k2D8veJRfxgWCt5wxsAcFSUCDs*	Victim address (multisig)
#4	*1a4b96d4c4bf668f2fa98fc65617efbb93cf98b9089e229911f2ca9d5af5177a*	Linked TX of victim ransom payment
#5	*3AtQECjhyq7vv9o6AyTV5oytGnDvDGVnpq*	Change address from ransom payment
#6	*409803bb5e124fd028c0482027c7722e84ce55b78204b279d3a44aba5e7c1698*	TX of attacker cash-out
#7	*1FQQ86tMuvhQ4Ruyggbb8j7iaNfUZ69gpY*	Attacker owned address where bulk of ransom payments were moved to

Table 4.1: The addresses and transactions analysed as part of the cash-in and cash-out WannaCry ransomware payments.

This article proposes an SRBF that can help multiple stakeholders at different stages of the intelligence cycle collaborate on developing a common understanding of the situation and the gaps involved.

4.4 Intelligence Collection Planning

The Financial Action Task Force (FATF) recently released guidance on red flag indicators for ML and terrorism financing using virtual assets (VAs) (FATF, 2020). By referencing standards professionally developed from an international governing body, such as the FATF, we can build out intelligence collection plans (ICPs) for suspicious financial behaviour and use a prescribed collection of red flag indicators as common scenarios or patterns allowing investigators or analysts to periodically "review a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change." (CIA, 2009).

The ICP sets up targeted information collection with the aim of populating the SRBF with the required threat intelligence informed by analysts, intelligence officers, and investigators. In the case of the WannaCry ransomware-Bitcoin money flows, we developed an example ICP in Table 4.2.

Satisfying the requirements of the ICP will enable the provisioning of the SRBF. The ICP guides collection efforts. Once the indicators to analyse intelligence requirements are fulfilled, the extracted data can then form the basis of sharing threat intelligence in a standardized manner with the security community for the intention of countering the cryptocurrency movements of the ransomware attacker. This is where the SRBF will bring the targeted data together, populate a set of custom-defined cyber-observable

objects using the global standard STIX schema to understand the attacker behaviour, and possibly prevent the mobilization of funds and stop attackers receiving ransom payments.

Intelligence Requirement
1. Determine where victim inflows originate from with respect to ransomware.
Information Requirement
a. Where are the victims purchasing their Bitcoin from (exchanges)? b. Where do the victims make purchases (geographically)? c. Is there CDD/KYC information available? d. How much Bitcoin is being purchased? e. How many transactions take place from acquisition of Bitcoin to ransom payment?
Intelligence Requirement
2. Identify supply chains of Bitcoin for victim payments.
Information Requirement
a. How many levels deep do the payments take? b. Who has influence over these supply chains? c. Are there known fraud or other criminal linkages?
Intelligence Requirement
3. Identify key nodes (transactions/addresses) in the network that may be clustered under the same controlling entity.
Information Requirement
a. Where do these key nodes exist in the network? b. Are there any patterns with respect to the day of the week or month these key nodes activate? c. Do clusters or communities of nodes exhibit similar behaviour across ransomware campaigns?
Intelligence Requirement
4. Identify the cash-out behaviour of the attack
Information Requirement
a. What exchanges do the attackers cash-out at?

b. Is there Customer Due Diligence (CDD) / Know Your Customer (KYC) information available? c. What is the frequency and amount being cashed out? d. What are the cash-out transaction patterns?

Table 4.2: An ICP for Ransomware - Bitcoin campaign.

4.5 Data Collection

The data collection framework used to extract the data from the Bitcoin blockchain relating to specific ransomware campaigns, and according to the ICP defined in the "Intelligence Collection Planning" section, is identified in Figure 4.3. The data collected relate to a particular WannaCry ransomware-Bitcoin seed address, #1. In step 1 of Figure 4.3, the data for the SRBF are extracted from the walletexplorer.com application programming interface (API). In step 2, the extraction script effectively splits our intelligence collection into two networks. [The extraction script is available upon request from GitHub (https://github.com/AdamT23/bitcoin-seed-extract).] One represents the payments being received by the ransomware-Bitcoin seed address or cash-in network (the upper portion of Figure 4.3), and the other represents the movement of the collected ransom out of the ransomware-Bitcoin seed address, known as the cash-out network (the lower portion of Figure 4.3) (Turner et al, 2021). These extracted data are stored in files using the open standard file format JavaScript Object Notation (JSON). The files created from this research represent the Bitcoin payments made relating to the cash-in and cash-out network for the WannaCry ransomware attack. These files are available as part of the Supplementary Material (see supplementary materials that accompany this article on IEEE Xplore)[19].8 These JSON

[19] A. Turner, "Bitcoin blockchain data of address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*," IEEE Dataport, Dec. 22, 2021, doi: 10.21227/1amp-n662.

files are loaded into a graph database, in this case Neo4j, to perform further network analysis and to produce visualizations as seen in Figures 4.1 and 4.2.

Using the SRBF, developed as part of this research, will enable human and machine and government and industry experts to automate and securely share previously uncollected intelligence relating to the cryptocurrency components of a ransomware attack. In the case of WannaCry, we focus on the known ransomware-Bitcoin seed address, #1 (see Table 4.1), to demonstrate the practicality of following blockchain data and metadata that can be collected from the target network. The JSON files created in step 2 of Figure 4.3, *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw_txs_ins.json* and *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw_txs_outs.json*, have been added to the Supplementary Material as Supplementary File 1 and Supplementary File 2, respectively[20]. These files are analysed in the following sections and are catalogued in Table 4.1.

[20] Turner, "Bitcoin blockchain data".

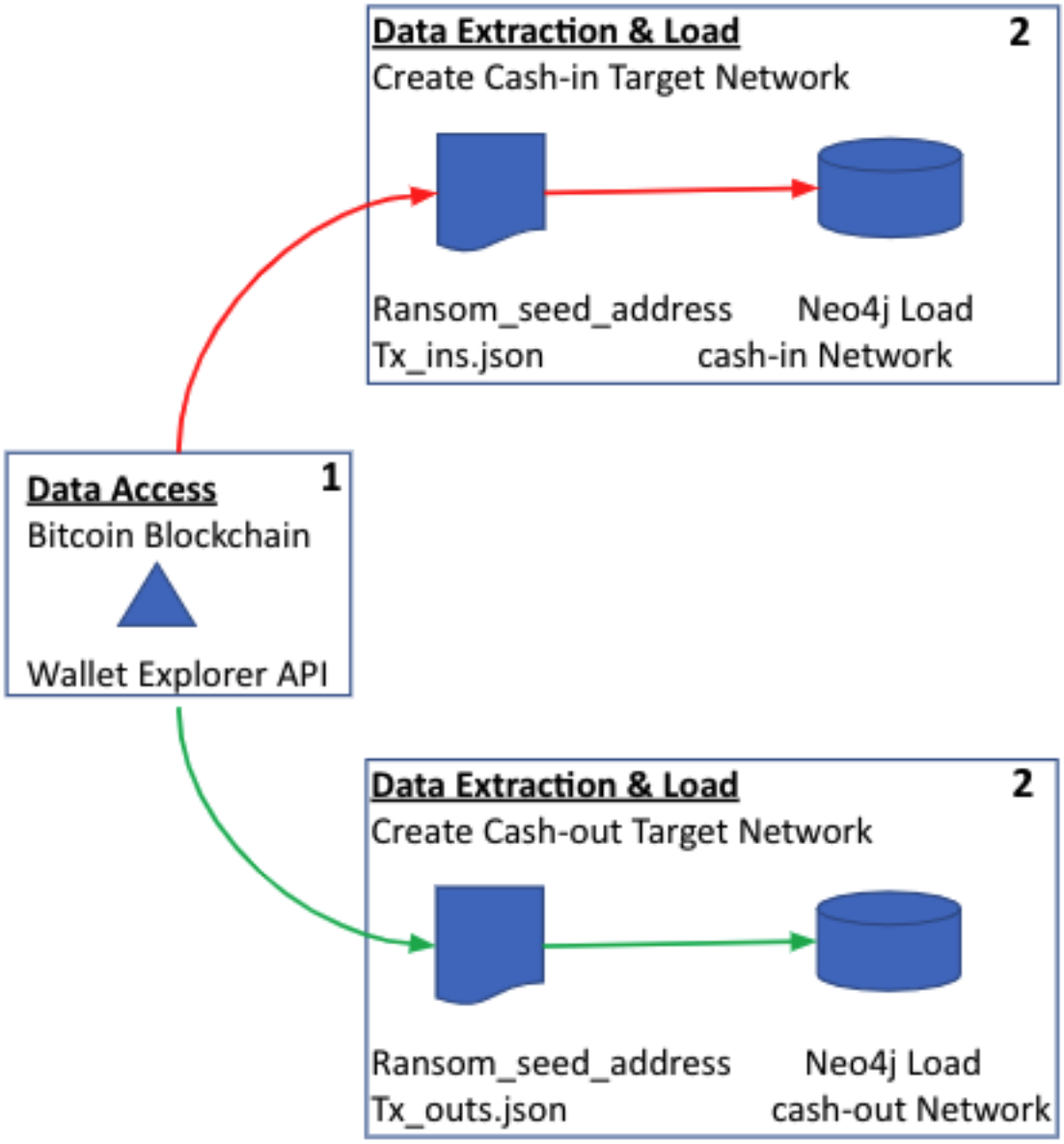


Figure 4.3: The ransomware-Bitcoin Data Collection Framework (Turner et al, 2021).

4.6 SRBF

The STIX-Ransomware-Bitcoin Framework (SRBF) utilises the Structured Threat Information eXpression (STIX) format for collecting and sharing CTI related to ransomware-Bitcoin payments. This section sets up an understanding of the STIX data model. In addition, analyses the data to collect and populate STIX Domain Objects (SDOs), Relationship Objects (SROs) and Cyber Observables (SCOs). As a result, a model of the WannaCry ransomware attack is proposed using STIX. Furthermore, this is evaluated with the data collected and extensions of the STIX format using customised SCOs.

4.6.1 An Introduction to STIX

The STIX format is a standardized schema used to exchange CTI. It is maintained and developed by the Mitre Corporation in the United States (Oasis, 2020). Notwithstanding the existence of similar standardized schemas, such as Open Threat Exchange (OTX) or Open Indicators of Compromise (OpenIOC), STIX remains the most universally accepted standard (Ussath et al, 2016). STIX provides a mechanism for entities to exchange CTI between them in a consistent manner that can be automatically processed and interpreted by humans and machines (Oasis, 2020). The latest version of the STIX specification is 2.1, and it defines 18 STIX Domain Objects (SDOs) and two STIX Relationship Objects (SROs).2 The SDOs and SROs categorize each piece of threat information and contain specific attributes within each SDO and SRO to be populated depending on the threat campaign and intelligence being shared. Thought of as a network, the SDOs represent entities, and SROs represent the links among them (Oasis, 2020).

STIX has been standardized over many different cyberattack types and contexts. However, the existing CTI standards do not support the complex patterns evident in cryptocurrency systems, and there is a need to close this gap by extending the capabilities of a common standard such as STIX.

Having a common format for capturing and disseminating CTI between entities provides a consistent way for threat intelligence platforms and security analysts to interpret, collaborate, process, automate, and report on CTI. This allows for the detection and prevention of cyberthreats, fostering the collaboration between security communities to better understand cyberattacks. This leads to enhanced readiness and response capabilities that allow entities to anticipate attacks more efficiently and effectively.

4.6.2 Data Analysis

Supplementary File 1 shows the cash-in network created from the collection method (Figure 4.3) for the WannaCry ransomware-Bitcoin seed address #1. The data are output in the JSON format to preserve the graph data structure generated as addresses and transactions that link together over the course of the ransomware campaign. Supplementary File 1 represents the cash-in payment network from the WannaCry ransomware attack. In total, this sample cash-in network contains 2,037 nodes (1,897 addresses and 140 transactions) and 2,099 edges connecting these addresses and transactions (4,136 total entities). The data collection framework can vary the number

of hops away from the seed address (#1) to expand and contract the scope of the analysis. In this analysis, a depth of four hops was used. The value of this parameter is based on knowledge of the ransomware campaign along with some trial and error using blockchain explorers to find the depth where payments start to hit Bitcoin exchanges.

Observing the transaction payload at *"block_height": 466181*, in Supplementary File 1, (lines 1,774–1,810), it is evident that the transaction number, #2, contains an amount of 0.372 BTC being paid from address #3, which participated in the previous transaction #4. This amount was chosen to be analysed as an example of a ransom payment being made by a victim to the ransomware-Bitcoin seed address #1. This transaction is visualized in Figure 4.1. Bitcoin addresses that begin with a "3" are referred to as "*multisig*" addresses. This means that multiple private keys are required to spend the amount on the address (Furneaux, 2018). The use of "*multisig*" addresses ensures a heightened level of security.

Typically, services like Bitcoin exchanges, susceptible to cyberattack on customer wallets, employ the use of "*multisig*" addresses (Bitfreeze, 2019). The working assumption here is that a victim has deposited funds using an exchange and created a "*multisig*" address for additional security, and the amount of 0.372 BTC is then split out into two output addresses, #1 receiving 0.16894486 BTC and #5 receiving 0.20214138 BTC. An additional observation can be made using a heuristic from Furneaux (2018). "Where a "*multisig*" address starting with a "3" is the input and the outputs are a "1" and a "3" address, the change address will likely be the "*multisig*" "3" address." (Furneaux, 2018).

We know from computers infected with the WannaCry ransomware that victims were required to pay US$300 after initially being infected (see Figure 4.4). The amount of 0.16894486 BTC being paid to the ransomware-Bitcoin seed address, #1, converts to US$300.47 at the time of that transaction, 2017-05-13 10:15 UTC. The WannaCry ransomware campaign was active from May 2017 to October 2017. Obviously, this transaction collected from the data extract represents a WannaCry ransomware victim payment.

Let's switch focus to Supplementary File 2. This file shows the cash-out network created from the collection efforts for the WannaCry ransomware attack that used the ransomware-Bitcoin seed address #1. In total, this sample cash-out network contains 299 nodes (280 addresses and 19 transactions) connected by 438 edges (737 total entities).

Observing the transaction payload at *"block_height": 478795*, lines 145–389 of Supplementary File 2 represent the transaction #6. This transaction is one of the two bulk money movements made by the ransom seed address #1 to cash out the ransom payments. To obfuscate the movement of funds out of the ransomware-Bitcoin seed address, the owners split the collected amount into 36 separate input payments. This begins at the key field *"ins":* within the *"block_height": 478795* payload (lines 150–365) of Supplementary File 2. This culminates into two output payments of interest as visualized in Figure 2. One of these payments moves the bulk of the ransom collected, 8.71529348 BTC ($US23,737.80) on 2017-08-03 04:28 UTC, to address #7.

In this case, peeling is the technique used to obfuscate illicit cryptocurrency payments (Meiklejohn et al, 2013). It is where a large number of small transactions are used to move funds in a convoluted manner from a particular address. Other obfuscation techniques may include observing a significant amount of "in-degree" and "out-degree" transaction activity at a particular Bitcoin address. Furthermore, the attacker may choose to keep the ransomware seed address "zeroed" after every day, avoiding any threshold detection for large sums of Bitcoin being transferred to other addresses or cryptocurrency services (Turner et al, 2020b).

Significantly, the data collected form a graph data structure. Nodes are represented by Bitcoin addresses linked by transactions that form the edges between the nodes. Representing the ransomware-Bitcoin network as two different graph structures enables the possibility of using graph algorithms for analysis of the networks formed by the victims paying their ransom to the attacker (cash-in) and the attacker moving their collected ransom payments for future use (cash-out). By sharing this information through a standard format like STIX, it is possible to share the full network of ransomware transactions with the security community, provide indicators of illicit cryptocurrency activity, and encourage deeper analysis and understanding of the payment patterns that ransomware victims and attackers undertake.

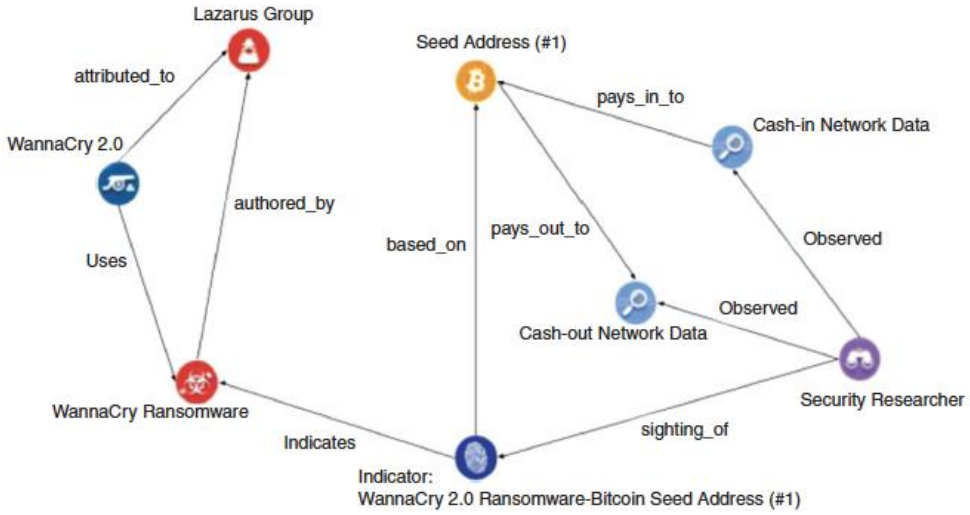


Figure 4.4: The STIX Model of information collected from the WannaCry ransomware attack.

Both Supplementary File 1 and Supplementary File 2 collectively contain 4,136 and 260 network nodes and edges, respectively. While these files contain all address and transaction nodes, along with their associated edges, of the cash-in and cash-out graphs formed over the course of the WannaCry ransomware campaign, it is important that a summary of the ransomware-Bitcoin address activity can also be provided. As a critical first step into the analysis, the summary provides an aggregate view of the entire history of the address or transaction. This summary can be retrieved from any blockchain explorer, such as walletexplorer.com or blockchair.com. When specified as well-formed STIX objects, both the collected summary and the detailed graph data provide a framework to guide the analyst into a contextual understanding and SU about the ransomware payment threat and what actions or decisions can be taken to circumvent such a threat via incident response protocols.

The following section will outline the proposed framework for capturing standardized CTI for ransomware-Bitcoin attacks in STIX format. The section introduces another structure available in STIX—the STIX Cyber Observable (SCO)—in addition to the

SDOs and SROs that have been discussed earlier. SCOs are used by SDOs to provide additional context to the data that are collected and characterized.

4.6.3 SCOs

To address the current gap in collecting cryptocurrency-related threat information from a ransomware attack, it will be necessary to define two new SCOs as there are currently no SCOs defined for cryptocurrency addresses or transactions. (We note that our proposed SCOs would need to be considered and approved by the STIX governing body if they are to be integrated into future releases of the STIX specification.) The two objects we propose are *x-cryptocurrency-address* and *x-cryptocurrency-transaction*. The specification of the custom cyber-observable types can be viewed in the Supplementary Material: see Supplementary Table A-1 *x-cryptocurrency-address* and Supplementary Table A-2 *x-cryptocurrency-transaction* (Appendix 4A).

The *x-cryptocurrency-address* cyber-observable object specifies the fundamental components of the blockchain data associated with, in the instance of WannaCry, a ransomware-Bitcoin seed address. Essentially, they will be the data returned from the blockchain explorer's API identified in the *x-explorer_url* parameter. The data returned from the blockchain explorer are arranged into the specifications outlined in Supplementary Tables A-1 and A-2 (Appendix 4A). Supplementary Table A-2 provides a specification for collecting the necessary CTI for cryptocurrency transactions. It uses the same principles as Supplementary Table A-1, utilizing the data returned from the *x-*

explorer_url parameter; however, the respective data will relate to the suspicious transaction involved in a ransomware money flow.

The custom cyber-observable objects (SCOs) can now be used to represent cyberthreats involving cryptocurrency in STIX. It is important to note that as a ransomware campaign progresses over time, the ransomware-Bitcoin seed address will see increased activity. Depending on when the *x-cryptocurrency-address* object samples the data, the parameters *x-last_seen_rx* and *x-last_seen_tx* can be used as timestamps to denote how active the ransomware-Bitcoin seed address is in receiving payments and cashing out collected ransom. Both the *x-cryptocurrency-address* and the *x-cryptocurrency-transaction* object are required to have the *created* and *modified* parameter to provide the timestamps of when the STIX object was created and subsequently modified.

Both the *x-cryptocurrency-address* and the *x-cryptocurrency-transaction* objects collect the respective metadata relating to a single address or transaction. Looking at addresses and transactions in isolation does not provide the full picture of money flows relating to a ransomware campaign. Therefore, we must capture the significance of the cash-in and cash-out networks generated. Considering that we are looking at networks of addresses and transactions involved in ransomware payments, we must reflect this data structure as a graph to link the money flows to and from any ransomware-Bitcoin seed address. As per Supplementary File 1 and Supplementary File 2[21], this means that the essential data components from the data source schema need to be represented as a list of dictionaries to capture the graph structure of the data (Rodriguez, 2020).

[21] Turner, "Bitcoin blockchain data".

We can then group the data elements from the list of dictionaries collected from the extracted data (see the "Intelligence Collection Planning" section), providing intelligence about the cash-in and cash-out network of payments. This can then be modelled using the existing "*Observed Data*" STIX objects. Using two of the STIX "*Observed Data*" objects, we leverage the STIX predefined parameters to create *external_references* that fit the required data structure, such as a list of dictionaries, for the cash-in and cash-out networks generated. For example, for the cash-in network, we would take Supplementary File 1 and add it to the STIX Observed Data *external_references* parameter, resulting in the object definition seen in Supplementary File 3 at key fields *"type": "observed-data," "id": "observed-data-a0d34360-66ad-4977-b255-d9e1080421c5," "name": "Cash-in Network Data,"* and *"external_references"* (lines 141–182).

In the next section, we will evaluate the usage of the different objects and how they can represent threat intelligence from the cryptocurrency ecosystem relating to a ransomware attack. We will use the WannaCry ransomware attack to demonstrate the scenario.

4.6.4 Evaluation

There are seven steps in the Cyber Kill Chain (CKC) model: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives (Hutchins et al, 2011). It is not uncommon to adapt this framework to model intelligence requirements. For example, when examining the

WannaCry ransomware attack along the kill chain, we focus on the "*Command and Control (C2)*" and the "*Actions on Objectives*" phases of the kill chain, which reveal the cryptocurrency components of the attack.

Homing in on these steps allows us to narrow down the attacker's intent on setting remote command of a victim's machine, exfiltration of data from the target, and also control access and management of the cryptocurrency network. In fact, Dargahi et al (2019), proposed a CKC taxonomy based on the features of ransomware, and the key activities identified in this taxonomy for C2 include "Hard-coded IP Addresses," "Domain Generation," and "Existing Botnet." In addition, the "Actions on Objectives" step focused on "Ransom Payment." Following a similar taxonomy, Figure 4.5 shows the details of these phases, "C2" and "Actions on Objectives," for the WannaCry ransomware attack that this research focuses on. The "Actions on Objectives" step is an aggregate representation of what the WannaCry ransomware attack collected in Bitcoin (BTC Cash-in) and what it moved out and where (BTC Cash-out).

Using Figure 4.5 as a reference for modelling the relevant cryptocurrency transactions in STIX, we would establish an indicator domain object that represents the presence of WannaCry ransomware, based on the ransomware-Bitcoin seed address (#1) used to collect ransom payments, modelled as an SCO. To understand what activity is triggered by the instantiation of this ransomware-Bitcoin seed address (#1), we set up two STIX Observed Data objects. One is created to observe the cash-in data on the cryptocurrency network (with a ransom equalling US$300 at the time of infection and an escalated amount of US$600 after three days of non-payment). Across the three ransomware-Bitcoin seed addresses deployed for WannaCry, Conti et al (2018), identified 238

ransom payments made, collecting 47.1743 BTC over a period from 12 May 2017 to 2 October 2017.

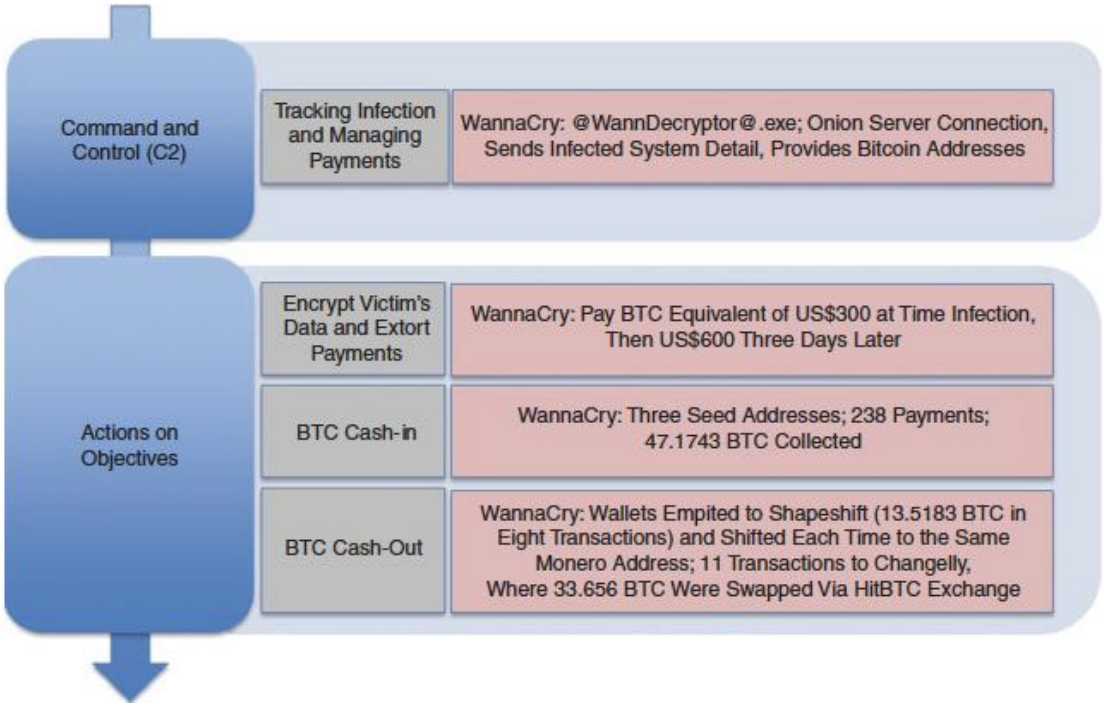


Figure 4.5: Kill chain components, C2 and Actions on Objectives for WannaCry Ransomware-Bitcoin attack.

Another observed data object is established to observe the cash-out data on the cryptocurrency network. This object will show the detailed cryptocurrency network data relating to the behaviour exhibited by the attackers as they begin to move the collected payments into other addresses, exchanges, or services attached to the Bitcoin network. In the case of the WannaCry attack, the cash-out STIX Observed Data object will collect the addresses and transactions used by the attacker to empty their ransomware-Bitcoin seed addresses. In September 2017, the Neutrino Research Team reported that the ultimate cash-out endpoints for WannaCry were two suspicious cryptocurrency exchanges. The Shapeshift/Poloniex exchange, which is known for converting between different cryptocurrencies, received 13.5183 BTC that was further converted into the more anonymous Monero cryptocurrency (Neutrino, 2017). The rest of the ransom proceeds, 33.656 BTC, was delivered to the Changelly/HitBTC.com

exchange (Neutrino, 2017). The STIX model representation of this scenario is shown in Figure 4.4.

Figure 4.4 shows a scenario for sharing threat intelligence between security researchers and an organization that has triggered an indicator of the ransomware-Bitcoin seed address #1. The figure depicts a STIX representation of the WannaCry ransomware-Bitcoin seed address, #1. At the start of a ransomware campaign, address #1 generates threat intelligence on the Bitcoin cryptocurrency network. That threat intelligence is a collection of Bitcoin addresses and transactions observed in a cash-out and cash-in network (represented by separate STIX observable objects).

The left side of Figure 4 represents the malware portion of the ransomware. WannaCry 2.0 uses the WannaCry malware, which has been attributed to the Lazarus group (U.S. District Court, Central District of California, 2018). In the middle of Figure 4.4, an indicator object has been created as a flag that WannaCry ransomware is present, and the ransomware-Bitcoin address has picked up the pattern data relating to the Bitcoin address #1. The indicator node is represented by the information in the Supplementary Material (Appendix 4B), Supplementary Table B-1 and specifically the field Pattern: *[x-cryptocurrency-address:x-address = "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"]*. This indicator object is based on the x-cryptocurrency-address object represented in Supplementary Table B-2. This contains the CTI on the address from a blockchain explorer, specifically triggered by the field *X-explorer url:* *https://blockchair.com/bitcoin/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*.

From here, an observer can witness the WannaCry ransomware-Bitcoin money flows unfold. The two STIX Observed Data objects can be used to collect the cash-in and cash-out network data, which pay in and pay out of the *x-cryptocurrency-address* object, respectively. Supplementary Table B-3 (Appendix 4B) represents the data collected for the cash-in network observed data object. These STIX cyber-observable objects are associated with the ransomware-Bitcoin seed address, #1, and contain the respective evolving transaction networks captured by the STIX predefined *external_references* field. The observed data represent the raw cash-in network information generated from victims paying their ransom payments into the ransomware-Bitcoin seed address #1. The JSON structure of the data provided to the *external_references* parameter provides a standardized way to integrate into security analysis and visualization systems.

4.7 Limitations and Challenges

To be truly effective, the proposed SRBF must be able to meet the demands of evolving ransomware attacks. It must also deal with various challenges in the representation of data that stem from the nature of the data and the analytic requirements. Such challenges include data quality, the breadth of collection, the timeliness of updated and modified intelligence, the context to the threat environment, the structure and relevance of the metadata proposed, durability and validity over time, and the cost in time and resources that it takes to curate such a list of intelligence requirements for effective CTI consumption.

Limitations are evident during the data wrangling, transfer, and mapping from the raw blockchain format into the STIX format that can be utilized for interpretation and

investigation downstream in the intelligence cycle. Significant modification of the extraction method would be required to provide the same functionality on different cryptocurrency platforms, such as Ethereum, or for different blockchain explorers. For this research, the scope of collection is limited to available Bitcoin blockchain data; however, there could be a need to combine this with other SCOs from WannaCry relating to the malware components of the ransomware attack (for example, file hashes, windows registry key, or other IOCs). For example, IOCs associated with WannaCry ransomware were identified by the U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center, and Federal Bureau of Investigation and released by the Cybersecurity and Infrastructure Security Agency[22] on 12 May 2017, listing IOCs in an initial STIX file[23] identifying malicious file hashes.

In addition, network analysis needs to be performed from the STIX observable object to effectively represent the material to humans to understand the cash-in and cash-out network behaviour. This means that the analysis will need to include integrations to relevant network analysis software.

Furthermore, it is not clear how the SRBF might operate under ransomware that generates cryptocurrency seed addresses in the scale of thousands and uses different types of cryptocurrency. WannaCry produced three ransomware-Bitcoin seed addresses, one of which (#1) was analysed and reported on as part of this research. Assessing all three ransomware-Bitcoin seed addresses would compound the amount of data by three times, resulting in six STIX cyber-observable objects, two objects for

[22] "Alert (TA17-132A): Indicators associated with WannaCry ransomware," Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/ncas/alerts/ TA17-132A (Accessed: Oct. 31, 2020).
[23] "WannaCry STIX file," Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/sites/default/files/publications/TA17-132A_WannaCry_stix.xml (Accessed: Oct. 31, 2020).

each ransomware-Bitcoin seed address containing the respective cash-in and cash-out networks. This will become substantially more complex with campaigns like CryptoWall, which generated 42 distinct addresses for its campaign (Conti et al, 2018).

Modern ransomware tactics can even produce a new ransomware-Bitcoin seed address for every infected machine. This would make sharing any sighting of the ransomware-cryptocurrency money flows hard to scale. In the case where there is a ransom seed address created for every victim, the threat map can become overcrowded, and filters or pattern matching may need to be applied to limit the amount of data being displayed. Future research will need to examine these scenarios for the effectiveness, scalability, and fit-for-purpose STIX provides for sharing cryptocurrency-related CTI.

4.8 Future Research and Conclusion

This article proposes new STIX specifications to facilitate the collection, analysis, and sharing of intelligence about cryptocurrency attacks, specifically Bitcoin addresses and transactions relating to ransomware. The focus was on extending the existing STIX framework to accommodate two new cyber-observable objects, *x-cryptocurrency-address* and *x-cryptocurrency-transaction*. The ransomware cash-in and cash-out network data were able to be captured using the STIX Observed Data object as victims pay into a specific ransomware-Bitcoin address and the attackers cash out their ransom proceeds. Collectively, this was identified as the SRBF. The model was evaluated using the WannaCry ransomware attack and its use of Bitcoin.

To correctly populate the SRBF with the necessary data, a target-centric approach to intelligence collection and analysis was described. This allowed us to identify the data feeds forming out of a ransomware-Bitcoin network and align them with context-enriching red flag indicators for VAs prescribed by subject matter experts from the FATF. Furthermore, the culmination of these efforts resulted in the design of an ICP that focuses intelligence requirements for targeted data collection and analysis of the STIX objects in the typology depicted in Figure 4.4.

The study draws on a collection approach based on a limited data set relating to the WannaCry ransomware attack. Though these data are rich in terms of reflecting the complexity of the ransomware money flows evident in a cryptocurrency network, the unilateral approach must be successfully applied to other ransomware attacks to ensure that the model is reliable, flexible and scalable and that it can be applied to other cryptocurrency types. The themes identified from the results will need to be further explored in future research. The SRBF will need to be tested against other ransomware campaigns to determine whether it is effective for practical CTI application.

A key observation from the data by undertaking this methodology is that intelligence collectors, analysts, and investigators can consume valuable threat information regarding a ransomware-Bitcoin attack using a well-trusted structured threat information standard such as STIX. The framework presented in this research closes the gap on bringing transparency and the ability to share valuable threat information across the security research community, bringing an in-depth understanding of what is going during the course of a ransomware-Bitcoin campaign as well as the payment patterns and processes ransomware attackers are using in cryptocurrency networks.

As a final thought, this research would provide the ability to open source multiple ransomware-Bitcoin CTI data sets for validation and analysis techniques to advance the development of future prevention mechanisms to be devised in the attempt to strangle the financial channels that ransomware attackers use to profit from their cybercrimes.

4.9 Data to insight

Limitations of the SRBF were evident whilst performing the validation process. The STIX format is traditionally used for capturing threat intelligence relating to computer and network security. This means it is designed for collecting information about malware viruses, Internet Protocol (IP) addresses, and other Indicators of Compromise (IOCs), such as changes in file hashes. When it comes to cryptocurrency threat intelligence there is no standard component in STIX available to share the contextual knowledge of ransomware-Bitcoin payments. Purpose built modules can circumvent these limitations; however, the networked nature of cryptocurrency payments means that threat intelligence representation becomes complex very quickly after identifying a ransomware seed address. Analysts need to trace the origin and destination of these payments to a sufficient depth in the network that will provide meaningful insight. As a result, a more dedicated intelligence information expression is needed for illicit cryptocurrency payment tracking. For example, Fröwis et al (2020) detail the importance of key legal requirements that ensures the evidence collected from cryptocurrency investigations will hold up in court and how this, along with a technical data sharing framework, can integrate into current analytical tools for successful investigation and prosecution in a court of law.

Furthermore, this chapter emphasised the importance of a data collection and sharing framework through the development of the SRBF. As a result, a data collection approach to capture the networked nature of cryptocurrency transactions was formed. The original code developed to extract the data from the blockchain is detailed in Appendix A. This code provides two views of the ransomware-Bitcoin network, cash-in and cash-out. As a result of running the code, in Appendix A, raw data extracts based on the walletexplorer.com Application Programming Interface (API) are created and are referenced in Appendix B. The code links together addresses and transactions for payments being made into and out of the ransomware seed address. A user-defined depth parameter instructs the code to collect transactions 'N' hops away from the ransomware seed address. The code outputs two raw extract files in JSON format which contain the cash-in and cash-out network data. Once the raw network data, relating to the ransomware seed address, has been collected from the blockchain in a consumable format, it is ready to be analysed for any discernible patterns. However, the insights analysts or investigators require could be concealed in the sparse or dense graph patterns formed by payments in a ransomware-Bitcoin network. From a data modelling perspective, this is what Liu et al (2021) examine, revealing emerging structural properties of Bitcoin transactions and the patterns they make. Analytical techniques are also discussed and how to interpret these patterns for deeper knowledge discovery.

These are significant limitations associated with the proposed approach in this chapter. The SRBF grapples with the manual batch collection of the blockchain data and does not provide the degree of automation, contextualisation or streaming data collection that would make cryptocurrency payment analysis more interpretable and real-time or near-real-time in nature. Such methods and systems are examined by Modi et al (2016),

through their Automated Threat Intelligence fuSion framework (ATIS) which fuses together isolated cyber threats including Bitcoin payments and their relation to the malware being used. In addition, another noticeable gap in the analysis presented here and henceforth, is the realm of markets Dark-Net and illicit cryptocurrency usage. Arnold et al (2019) develop a Cyber Threat Intelligence (CTI) Tool which collects Dark-Net market intelligence and provides the versatility of integrating multiple datasets, including cryptocurrency transactions, and represents the identified threats as a network or graph structure. Advancing on this, Su et al (2021) look at how to detect the criminal footprint of Ethereum[24] attacks in order to automatically detect the attack patterns and provide a tool for large scale investigation. The next chapter aims to advance upon the threat intelligence goals by examining the patterns relating to ransomware-Bitcoin transactions in the data collected by the SRBF, identifying what they reveal and what they disguise when it comes to ransomware-Bitcoin activity.

4.10 Appendix 4A – STIX custom specifications

Table A-1 - STIX custom specification for ***x-cryptocurrency-address***
Type name: *x-cryptocurrency-address*

Description: The cryptocurrency address object represents the Bitcoin address(es) used by the ransomware attackers to collect ransom payments from its victims.

Required Common Properties		
type, id, x-cryptocurrency, x-address, created, modified		
Property Name	**Type**	**Description**

[24] Ethereum is an open source technology for sending its own cryptocurrency, ETH, as well as a programmable blockchain technology that enables the development of applications, running 'smart contracts' that execute some computer code (see ethereum.org, 2021).

type (required)	string	The value of this property must be of type ***x-cryptocurrency-address***.
x-cryptocurrency (required)	string	Specifies which cryptocurrency the observable is dealing with. (E.g. Bitcoin, Monero, Etherum, etc).
x-address (required)	string	Cryptocurrency address.
name (optional)	string	Name label for the object.
x-explorer_url (optional)	string	Http URL of the cryptocurrency explorer used to derive further details of the address. (E.g. Walletexplorer, btc.com, blockchain.com, blockchair.com, bitcoinwhoswho.com, etc).
x-balance (optional)	float	The balance of the cryptocurrency address at the time of observation.
x-first_seen_rx (optional)	timestamp	Date and time of when the first amounts of cryptocurrency were received at this address.
x-last_seen_rx (optional)	timestamp	Date and time of the last known receipt of any cryptocurrency to this address.
x-first_seen_tx (optional)	timestamp	Date and time of when this address performed its first transaction.
x-last_seen_tx (optional)	timestamp	Date and time of when this address was last seen spending its cryptocurrency.
x-total_rx (optional)	float	Total amount of cryptocurrency received on this address at the time of observation.
x-total_tx (optional)	float	Total amount of cryptocurrency spent on this address at the time of observation.

x-transaction_count (optional)	integer	Specifies the number of transactions performed by the address.

Table A-2 - STIX custom specification for ***x-cryptocurrency-transaction***

Type name: ***x-cryptocurrency-transaction***

Description: The cryptocurrency transaction object represents the cryptocurrency transaction(s) conducted by the victims and/or ransomware attackers to send ransom payments to a seed address or move funds from the seed address.

Required Common Properties		
type, id, x-cryptocurrency, x-transaction, created, modified		
Property Name	**Type**	**Description**
type (required)	string	The value of this property must be of type ***x-cryptocurrency-transaction***.
x-cryptocurrency (required)	string	Specifies which cryptocurrency the observable is dealing with. (E.g. Bitcoin, Monero, Etherum, etc)
x-transaction (required)	string	Cryptocurrency transaction. Transaction id (Hash).
name (optional)	string	Name label for the object.
x-explorer_url (optional)	string	Http URL of the cryptocurrency explorer used to derive further details of the address. (E.g. Walletexplorer, btc.com, blockchain.com, blockchair.com, bitcoinwhoswho.com, etc)
x-tx_timestamp (optional)	timestamp	Time in UTC of the transaction.
x-block_id (optional)	integer	Block number of where the transaction occurred. (Blockchain based cryptocurrencies).
x-input_count (optional)	integer	Number of input addresses (senders) contributing to the transaction.

x-input_amount (optional)	float	Total input amount sent from the senders in the transaction in cryptocurrency.
x-output_count (optional)	integer	Number of output addresses (recipients) the total transaction amount is delivered to.
x-output_amount (optional)	float	Total output amount received from the senders in the transaction in cryptocurrency.
x-transaction_fee (optional)	float	Fee charged for the transaction. Seen as a difference between the total input amount and the total output amount.

4.11 Appendix 4B – STIX objects for the WannaCry Ransomware-Bitcoin seed address

Table B-1 – STIX Indicator object for WannaCry Ransomware-Bitcoin seed address (12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw)

Type: indicator
Spec version: 2.1
Id: indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f
Created by: identity--f431f809-377b-45e0-aa1c-6a4751cae5ff
Created: 2017-05-12T20:03:48.000Z
Modified: 2017-04-13T20:03:48.000Z
Indicator types: malicious-activity
Name: WannaCry 2.0 Ransomware-Bitcoin Seed Address (12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw)
Description: BTC Addresses: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Pattern: [x-cryptocurrency-address:x-address = '12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw']
Pattern type: stix
Valid from: 2017-05-012T00:00:00Z
Kill chain phase: Actions on Objectives

Table B-2 – Populated ***x-cryptocurrency-address*** object

Type:x-cryptocurrency-address
Id: x-cryptocurrency-address--4527e5de-8572-446a-a57a-706f15467461
Created: 2016-08-01T00:00:00.000Z
Modified: 2016-08-01T00:00:00.000Z
Name: Seed Address - 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
X-cryptocurrency: BTC
X-address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
X-explorer url: https://blockchair.com/bitcoin/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
X-balance: 1.88389022 BTC / 20,211.50 USD

X-first seen rx: 2017-05-12 12:43:33
X-last seen rx: 2020-09-27 04:49:48
X-first seen tx: 2017-08-03 04:28:20
X-last seen tx: 2017-08-03 04:41:34
X-total rx: 19.65502059 BTC / 41,518.14 USD
X-total tx: 17.77113037 BTC / 48,403.23 USD
X-transaction count: 213

Table B-3 – STIX Observed Data object for the WannaCry ransomware-Bitcoin seed address cash-in network (12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw)

Type: observed-data
Id: observed-data--a0d34360-66ad-4977-b255-d9e1080421c5
Created by: identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c
Created: 2017-02-28T19:37:11.213Z
Modified: 2017-02-28T19:37:11.213Z
First observed: 2017-02-27T21:37:11.213Z
Last observed: 2017-02-27T21:37:11.213Z
Number observed: 1
Name: Cash-in Network Data
External references: {"block_height":466038,"block_pos":496,"depth_":"4","found":true,"ins":[{"address":"1NTwLm63qF1rXG9JgC8xSzDSkBu3wyfEfM","amount":5.58103425,"is_standard":true,"next_tx":"e3eadb95ec082675f260c32fee2690833ae8bf7da312ad240169d278cdfa7be5"}],"is_coinbase":false,"label":"","out":[{"address":"1DwdNuntQmTDoYkC7Jv4HiwS2BLEJUhKJB","amount":0.21679223,"is_standard":true,"next_tx":"89e134e8354c127cb541c987ba1c03a517210f0c28495615eca8e508643b93d4","wallet_id":"446bc0544f1a9022"},{"address":"177cbF6GZHXiG6Pvbxkkm92iBEg2TzATwo","amount":5.36379002,"is_standard":true,"next_tx":"e91f99bdab7dd73543281522728bdaebc63dc94c6f234d2588d3153b1d2dfec3","wallet_id":"34bd99f652e18a34"}],"size":225,"time":1494589369,"txid":"bde10ffee36d3335912ad95f99b3b54216f111f8a2f03dd61009d1336da6c8e8","updated_to_block":589991,"wallet_id":"d8c2d9502250c9f4"}

Chapter 5: Discerning Payment Patterns in Bitcoin from Ransomware Attacks

"I was not caught

Though many tried

I live among you

Well disguised"

- Leonard Cohen (Nevermind[25])

5.1 Chapter Overview

In this chapter the large volume of data available from the Ransomware–Bitcoin Intelligence–Forensic Continuum is further leveraged to help frame relevant intelligence and forensic analysis. The continuum spans across the lifecycle of a ransomware campaign. The data is made available for analysis from the Bitcoin blockchain via an extract script written in the Python computer programming language. This script was developed as part of this body of research (see Appendix A). The data extracted populates a target network analysis model. From this data collection baseline, we introduce advanced machine learning and data science techniques such as community detection and graph reduction. These techniques examine the materiality and impact of ransomware via an attacker's usage of a cryptocurrency payment system. Analysis patterns discovered during this chapter include the day-of-the-week profile. The findings show discernible patterns in the network relating to the input and output side of the ransomware graphs. The day-of-the-week analysis shows two distinctly different behaviours: one where a ransomware seed address accumulates ransom

[25] Source: https://genius.com/Leonard-cohen-nevermind-lyrics

payments over time and holds on until it is the right time to cash out, and another where the ransom seed address is "zeroed" after every day. These two different strategies from ransomware attackers could be targeted, especially in the case where cash-out frequency is high. Adding machine learning to the data collected and producing models for deeper classification of ransomware payments is also explained in this and subsequent chapters. Distinctive patterns that are found in this chapter may also support attribution efforts. Using the day-of-the-week analysis and machine learning models can help enhance these efforts.

5.2 Abstract

Purpose: This paper seeks to investigate available forensic data on the Bitcoin blockchain to identify typical transaction patterns of ransomware attacks. Specifically, we explore how distinct these patterns are and their potential value for intelligence exploitation in support of countering ransomware attacks.

Design Methodology/Approach: We created an analytic framework – The Ransomware-Bitcoin Intelligence-Forensic Continuum, to search for transaction patterns in the blockchain records from actual ransomware attacks. Data of a number of different ransomware Bitcoin addresses was extracted to populate the framework, via the WalletExplorer.com programming interface. This data was then assembled in a representation of the target network for pattern analysis on the input (cash-in) and output (cash-out) side of the ransomware seed addresses. Different graph algorithms were applied to these networks. The results were compared to a "control" network derived from a Bitcoin charity.

Findings: The findings show discernible patterns in the network relating to the input and output side of the ransomware graphs. However, these patterns are not easily

distinguishable from those associated with the charity Bitcoin address on the input side. Nonetheless, the collection profile over time is more volatile than with the charity Bitcoin address. On the other hand, ransomware output patterns differ from those associated charity addresses, as the attacker cash-out tactics are quite different from the way charities mobilise their donations. We further argue that an application of graph machine learning provides a basis for future analysis and data refinement possibilities.

Research Limitations/Implications: Limitations are evident in the sample size of data taken on ransomware campaigns and the "control" subject. Further analysis of additional ransomware campaigns and "control" subjects over time would help refine and validate the preliminary observations in this paper. Future research will also benefit from the application of more powerful computing resources and analytics platforms that scale with the amount of data being collected.

Originality/Value: This research contributes to the maturity of the field by analysing ransomware-Bitcoin behaviour using the Ransomware-Bitcoin Intelligence-Forensic Continuum. By combining several different techniques to discerning patterns of ransomware activity on the Bitcoin network, it provides insight into whether a ransomware attack is occurring and could be used to trigger alerts to seek additional evidence of attack, or could corroborate other information in the system.

5.3 Introduction

Ransomware attacks continue to evolve as a significant threat to global cyber security. Although consumer ransomware detection rates declined in 2018, there has been an alarming 365% increase in enterprise detections from quarter two (Q2) 2018 to Q2 2019, and on average since Q4 2017 enterprise detections increased by 112%, according to an August 2019 Malwarebytes ransomware report (Kujawa et al, 2019).

Furthermore, ransomware security expert group Coveware (2019), shows the average ransom payment inflicted on enterprises in Q2 2019 increased by 184% to US$36,295, in comparison to Q1 2019 when the average payment was US$12,762 (Osborne, 2019). This suggests cybercriminals are increasingly targeting industry, rather than individuals, and enjoying greater Return on Infections (ROI – Turner et al, 2019), with the top three industries targeted in the first half of 2019 being Governments (27%), Manufacturing (20%) and Healthcare (14%) (TrendMicro, 2019; Clay, 2019).

With the threat of ransomware rapidly evolving and new families of malware emerging, it is ever more pertinent to understand the patterns and the footprint these attacks leave in the cryptocurrency ecosystem to understand and possibly circumvent ransomware attacks.

In what follows we rely on various analytic techniques to identify these patterns. We compare the emergent patterns to a "control" case of a charitable organisation receiving Bitcoin. Specifically, we will examine the time series and network patterns formed during the course of a ransomware campaign. These techniques are performed within the bounds of the Ransomware-Bitcoin Intelligence-Forensic Continuum framework and build on the findings of each other.

The day-of-the-week analysis shows how, over time, ransom is collected into and moved out of a ransom seed address. Specifically, the number of transactions that are used to move funds emerge as important in differentiating ransomware campaigns from the charity control subject. This is due to the unique ways the attackers control the

movement of ransomware yields and to the uniformity of demanded ransom amounts compared with the highly variable donation amounts that are collected by the charity.

We then turn to a visual graph representation that reveals both similarities between the collection or cash-in graphs, and the differences in the cash-out graphs between the ransomware campaigns and the charitable organisation.

Building on the graphs created from the data on the Bitcoin blockchain, community detection patterns reveal the dominance of the collection address in the network with a high in-degree common across the different ransomware and "control" subject. However, in the cash-out communities the patterns show no signs of commonality between them.

By performing graph embedding analysis and visualisation through reduced dimensionality we are able to cluster common nodes and separate out anomalies for further investigation of suspicious activity. We suggest ways to enhance the methodology in future research through an increase in sample size and data labelling. We further suggest that curating blockchain data and meta-data sets and making them openly available for researchers could enhance future practical research.

5.4 Ransomware – Bitcoin Intelligence – Forensic Continuum

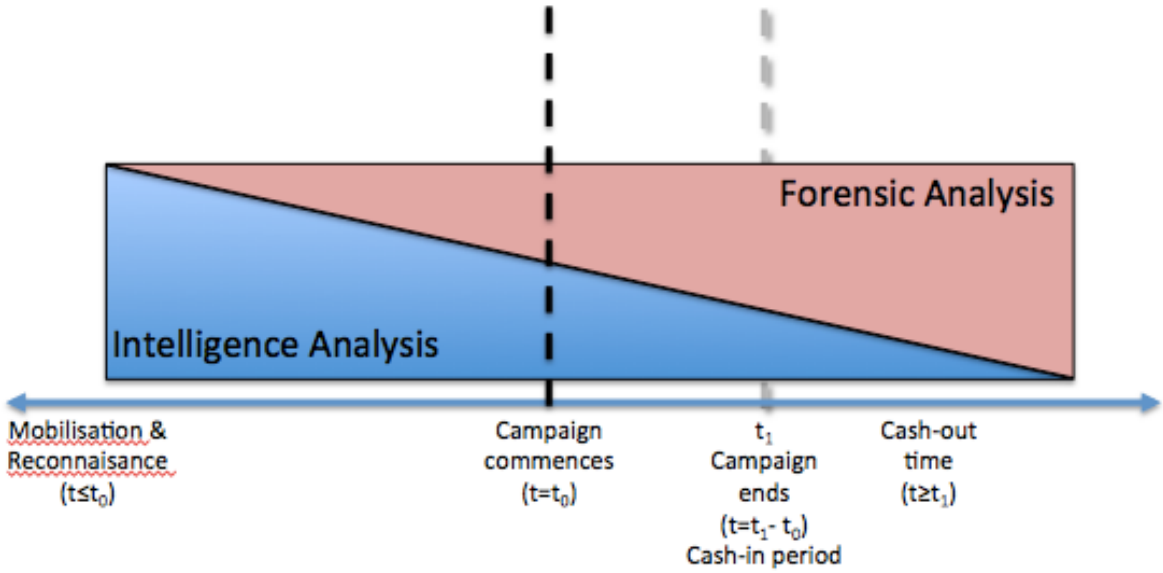


Figure 5.1: Ransomware – Bitcoin Intelligence – Forensic Continuum

Figure 5.1 shows the intelligence – forensic continuum with respect to a ransomware campaign. If we denote the ransomware campaign commencing at time $t=t_0$, we can then divide our analysis scope into three parts. Firstly, at time $t \leq t_0$, Intelligence, Surveillance and Reconnaissance (ISR) is the mode that is in operation referring to the 'reconnaissance and mobilization' phase, where behaviours leading to a ransomware campaign could be evident across different campaigns and provide an indicator for future campaigns using intelligence gathered from the Bitcoin blockchain. The time window between t_0 and t_1, (C2 phase), is seen as the period where ransom collection has hit a maximum and after a short period of time new payments to the ransomware seed address(es) taper off. Furthermore, at some time $t \geq t_1$, ('actions on objects' phase), the perpetrators of the ransomware attack will start to transfer funds collected from the ransom by placing, layering or integrating the collected bitcoin into other wallets in the Bitcoin ecosystem, other cryptocurrency systems or services and possibly even into the

traditional economy. Each of these three phases yields a typology of funds movement worth investigating for the purposes of discovering discernible patterns of ransomware activity.

5.5 Pattern Analysis & Findings

Finding patterns in large graph networks and looking at sub-graphs can reveal interesting patterns in the context of Ransomware – Bitcoin behaviour. Comparing the occurrence of such patterns across different ransomware graphs is a powerful way of identifying illicit activity on the Bitcoin network (Fokker and Beek, 2019). The campaigns analysed in this paper are: WannaCry, CryptoDefense and NotPetya. These campaigns were chosen due to the limited number of ransom seed addresses used, keeping a manageable limit on the amount of data to analyse. Nonetheless, these attacks still yielded a significant number of transactions collected from victims and also provided evidence of cash-out activity.

The dedicated Bitcoin charity collection address for "The Water Project"[26] was chosen as a control subject to test the analysis methodology against a Bitcoin address that is not used for ransomware purposes. This charity was chosen over others that accept Bitcoin because they are formally registered as a charity with the Internal Revenue Service (IRS) in the United States and provide fully auditable financials as a result. The charity has been ongoing for more than ten years and therefore provides a rich source of transactional data. Furthermore, this is in line with an established practice of using charities and similar fund raising activities as a comparative backdrop in research into

[26] The Water Project (https://thewaterproject.org/): "[a] 501(c)(3) non-profit organization unlocking human potential by providing reliable water projects to communities in sub-Saharan Africa"

money laundering (Evans and Schneider, 2019). The Bitcoin addresses and respective ransomware campaigns analysed are presented in Table 5.1 and Table 5.2 below.

Ransomware	Overall			Ransom			
	Payments	BTC	US$ value	Payments	BTC	US$ value	Time
WannaCry	**341**	**53.2906**	**99,549.05**	**238**	**47.1743**	**86,076.76**	**12 May 2017 - 2 Oct 2017**
CryptoDefense	**128**	**138.3223**	**70,113.41**	**108**	**126.6960**	**63,859.49**	**28 Feb 2014-11 Apr 2014**
NotPetya	**70**	**4.1787**	**10,284.42**	**33**	**4.0576**	**9,835.86**	**27 Jun 2017-3 Aug 2017**

Table 5.1: Ransomware payments by ransomware attack. Adapted from Conti et al (2018).

Significantly, the time period for the data collected against each of the addresses began prior to and stretched well beyond the identified time period for the ransomware campaign. This way it might be possible to discover what activity on the address may precede or follow the campaign.

Bitcoin research has profitably leveraged sub-graphs on the Bitcoin network. These sub-graphs include peeling activity where a single Bitcoin address starts with a large amount of Bitcoin and then bit by bit small amounts are transferred to another address and this pattern continues for multiple similar transactions through the constant use of change addresses and subsequently obfuscating the origin of the funds by layering them many levels deep throughout the Bitcoin network (Meiklejohn et al, 2013). In addition, the use of a common exchange or service, creation of many addresses or transactions from the same service or node, known as splitting, can occur for heightened anonymity

(Gaihre et al, 2018). Our challenge is to identify unique features of these sub-graphs that could speedily and conclusively identify ransomware activity.

Ransomware	Ransom Address	Data Collected
WannaCry 238 payments collected May 12, 2017 - Oct. 02, 2017	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	31 Dec 2016 – 8 Jul 2019
	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	31 Dec 2016 – 9 Jul 2019
	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	31 Dec 2016 – 9 Jul 2019
CryptoDefense 108 payments collected Feb. 28, 2014 - Apr. 11, 2014	19DyWHtgLgDKgEeoKjfpCJJ9WU8SQ3gr27	31 Dec 2016 – 9 Jul 2019
	1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1	31 Dec 2016 – 10 Jul 2019
NotPetya 33 payments collected Jun. 27, 2017 - Aug. 03, 2017	1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX	31 Dec 2016 – 10 Jul 2019
Control Subject	**Control Address**	
The Water Project	1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R	31 Dec 2013 – 17 Aug 2019

Table 5.2: Ransomware – Bitcoin Addresses. Adapted from Conti et al (2018).

5.6 Analysis Patterns

As a preliminary step we wish to establish a generic target network model (TNM) of ransomware transactions. Target network modelling helps coordinate and target

collection and analysis to reveal vulnerabilities, links, key nodes, weaknesses and relationships in the target network (cf. Clark, 2017).

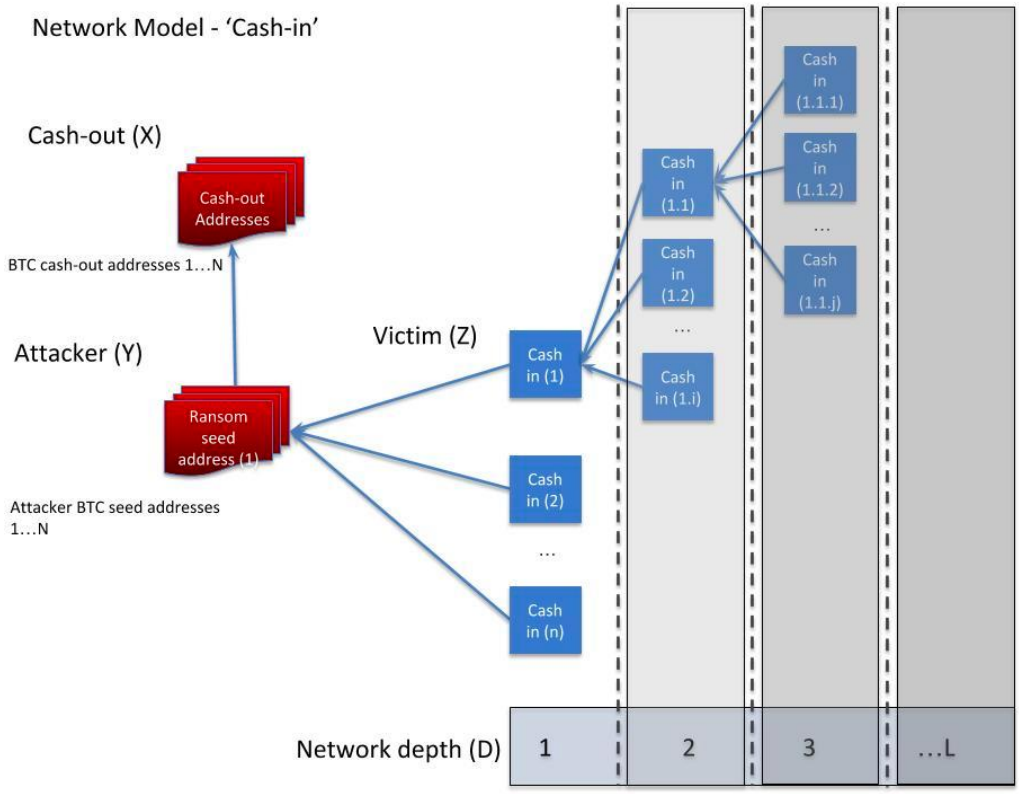


Figure 5.2: Ransomware – Bitcoin Target Network Model ('Cash-in').

While distinctive patterns of malware can be identified using the model above, a critical problem is finding diagnostic indicators, ones that can reliably identify ransomware activity and distinguish that activity from other activities (e.g. charity collection or crowd funding campaigns). The following sections will extract patterns that might have diagnostic value.

5.7 Which Day of the Week?

A temporal analysis of the ransomware seed addresses will provide a full picture of the transaction activity over the lifetime of the respective ransomware seed address being

analysed. There are numerous websites that facilitate the investigation of the transaction history of particular addresses. We chose btc.com because it provides statistics over a specific custom date range, allowing the analyst to look for activity across the intelligence-forensic continuum. In addition, the export feature provides all the transactions easily imported into a spreadsheet for the "year-month" vs "day of the week" analysis. It could be possible to provide a finer grain time window for analysis to reveal activity hour by hour, however this would restrict any bigger picture patterns going on in the network across the entire intelligence-forensic continuum. This type of analysis is relevant for seeking patterns in money laundering behaviour similar to that undertaken by Reardon et al (2012) which visualised ATM usage patterns to detect counterfeit card usage. Similar payment trend analysis specific to ransomware has also been conducted by Paquet-Clousten et al (2018), Conti et al (2018) and Huang et al (2018).

5.7.1 WannaCry

WannaCry collected ransom payments across three known ransomware seed addresses *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw;*
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94;
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn. The day-of-the-week profile of the WannaCry ransomware seed addresses exhibited very similar patterns of behaviour. With the campaign commencing on Friday, 12 May 2017, the largest amount of ransoms paid (Cash-in) into the seed addresses occurred on the following day, Saturday, 13 May 2017. Within the month of May, 2017, this addresses collected 104, 123 and 106 cash-in transactions respectively, meaning the reaction to this ransomware was immediate. According to Bistarelli et al (2018), the initial ransom amount WannaCry

demanded was US$300, between 0.15 and 0.18 BTC at the time of the attack. This then doubled after three days to US$600 (0.3 to 0.36 BTC). With such a reaction over a short period of time the attackers could have asked for a higher ransom. Interestingly, the attackers withdrew all the funds on 3rd August 2017, a Thursday, after an initial collection period of approximately 3 months.

There is no real discernible pattern from the cash-in activity to say victims acted on a certain day-of-the-week, except that the victims start paying the ransom soon after being infected by the ransomware. This data can be seen in Tables 5A-1 to 5A-3 in Appendix 5A. Furthermore, a graphical overlay of the three ransomware seed addresses is shown in Figure 5.3. This figure highlights the transaction count as the bar chart and the cumulative Bitcoin collected over the course of the campaign as the line chart. The account zeroing activity is represented in this chart with a large dip in the line where cash-out takes place. In addition, the cash-in profile shows how many small transactions fill the seed address in a short time frame after the campaign commenced. The large columns at the start highlight this.

There is no activity on the seed address prior to the campaign, which would mean the address is set-up in real time as the campaign or as an infection unfolds on a victim's computer. However, there is still activity on these addresses to date. Small transactions continue to cash into the ransomware seed address long after the campaign has concluded. This could be a sign the attackers are keeping it alive for future use and ideally law enforcement can continue Intelligence, Surveillance and Reconnaissance (ISR) on a known attacker addresses to monitor criminal behaviour.

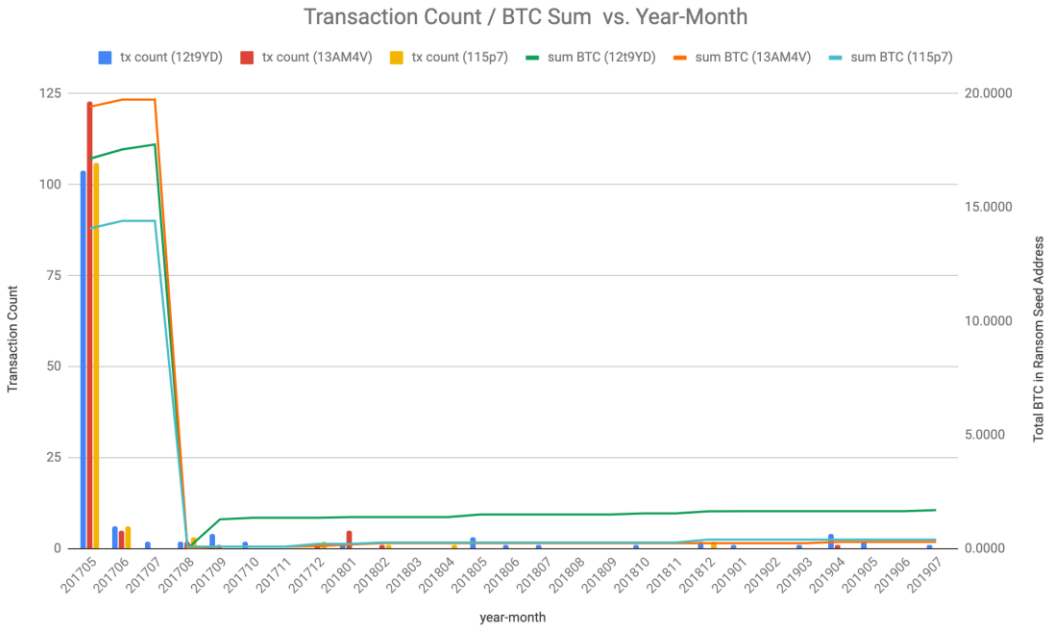


Figure 5.3: Account balance of the WannaCry ransomware seed addresses with respect to the number of transactions taking place over time.

5.7.2 CryptoDefense

The addresses used for CryptoDefense were *19DyWHtgLgDKgEeoKjfpCJJ9WU8SQ3gr27* and *1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1*. The ransom for the CryptoDefense attack was higher than WannaCry, starting at US$ 500 within the first four days of infection, then doubling to US$ 1000 (Conti et al, 2018). CryptoDefense exhibited a different profile to WannaCry, with ongoing withdrawals of funds throughout the campaign. The wallet was “zeroed” out each month. This can be seen in Figure 5.4, with the line graph in red for the *1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1* address. The data related to this can be seen in Tables 5A-4 and 5A-5.

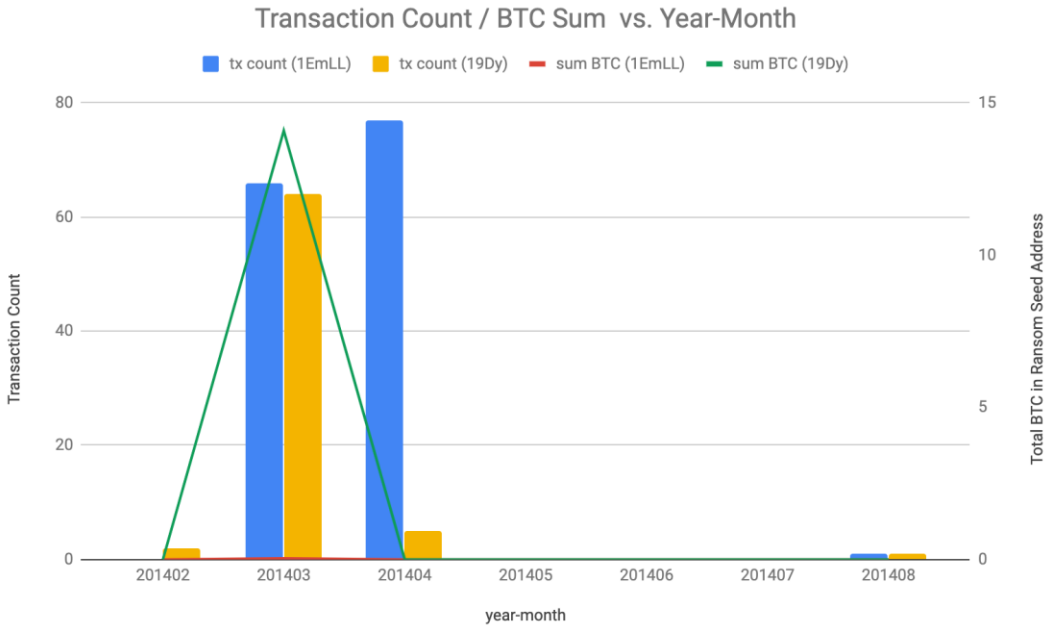


Figure 5.4: Account balance of the CryptoDefense ransomware seed addresses with respect to the number of transactions taking place over time.

This might be the result of the ransomware attackers seeking to prevent the wallet from rapidly accumulating large funds to avoid detection by authorities. They may also just want to access their profits immediately, without consideration of detection. However, moving the funds out as quickly as they come in help the attackers fly under the radar of any threshold detection alerts placed on Bitcoin addresses. In subsequent ransomware configurations, attackers have also addressed detection by dynamically setting up a new Bitcoin address for each victim once they are infected.

5.7.3 NotPetya

A single address was used for the NotPetya ransomware campaign, *1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX*, with a fixed ransom of US$300 (Conti et al, 2018). This address exhibited a similar pattern to the WannaCry campaign. NotPetya accumulated victim payments over the first month and then moved them next

month, which was longer than CryptoDefense held onto the ransom payments in the one address, but a shorter period of time than WannaCry did. NotPetya also collected the least amount of ransom from the other two campaigns, possibly reflecting NotPetya's intended use as a tool of destruction rather than a revenue generating attack (Conti et al, 2018). In fact, the department of homeland security and US Intelligence confirmed the malicious nature of the attack, rather than profit motivated, having emanating from the Russia military against the Ukraine (Greenberg, 2018). Table 5A-6 and the Figure 5.5 show that the address is still being used up until recently. Very small amounts are being transferred into the address to keep it alive on the network.

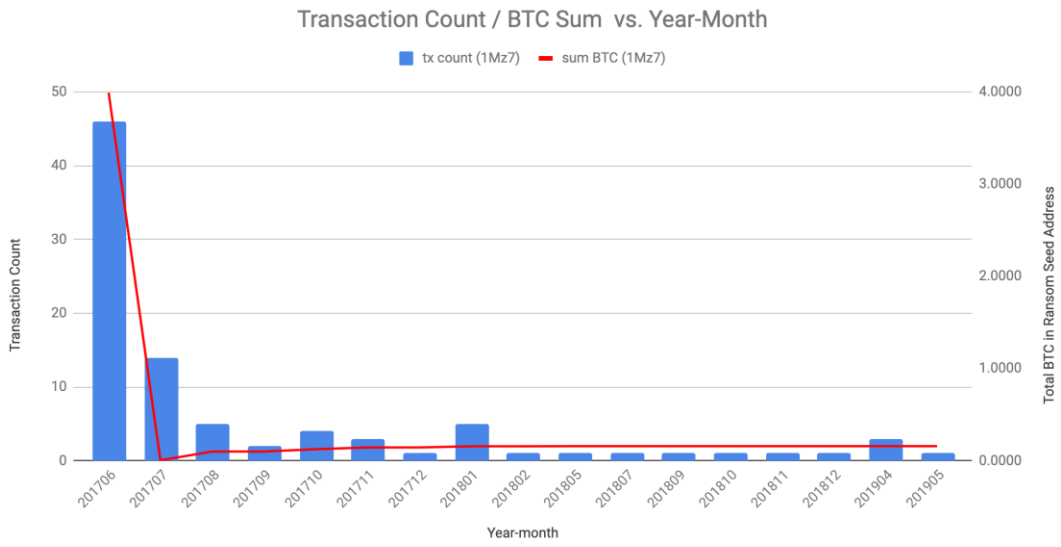


Figure 5.5: Account balance of the NotPetya ransomware seed addresses with respect to the number of transactions taking place over time.

The balance of the address is practically zero. This address could be reused for future criminal activity, though with it already being used in such a high-profile ransomware campaign, it is likely that this address is under surveillance by law enforcement. Therefore, the owners of this address would be able to leverage any future activity as a decoy and possibly feed misleading information to law enforcement.

5.7.4 Control Case: The Water Project Bitcoin Charity

The main address used for The Water Project charity is 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R. The patterns between transaction count, the amount of Bitcoin in the address over time and spread over the days of the week, for the control case bear little resemblance to that of the three ransomware campaigns analysed so far. Even though the balance is very small, Table 5A-7 and Figure 5.6 shows a more distributed profile over time.

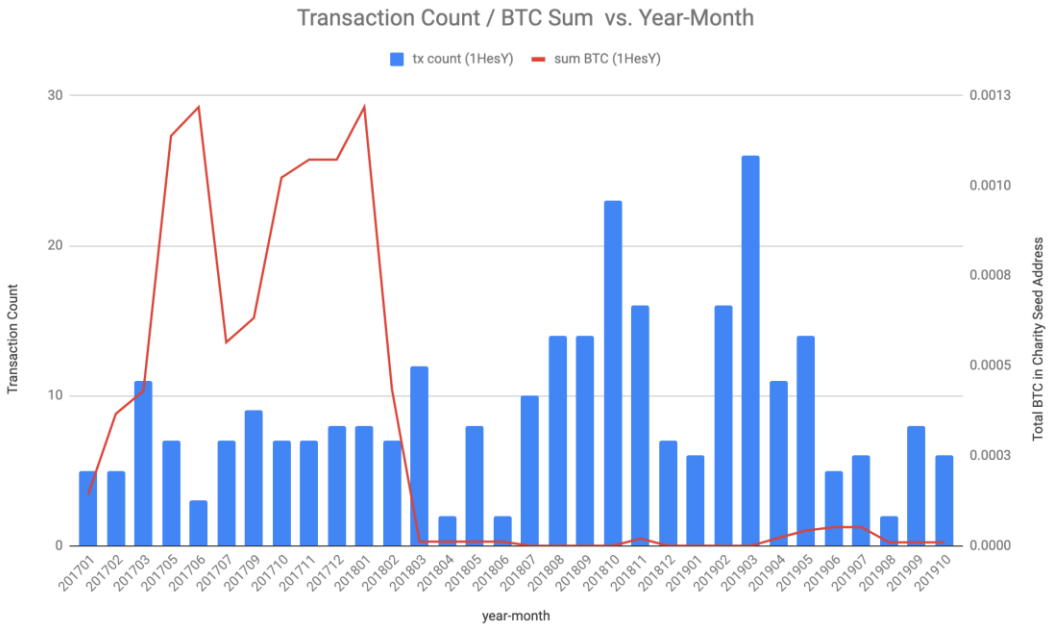


Figure 5.6: Account balance of the Charity seed addresses with respect to the number of transactions taking place over time.

For a charity, it is likely that people are donating in very small amounts when they donate. For example with the Water Project, the suggested amount ranges from US$20 to US$500 which ranges from 0.0025 BTC to 0.063 BTC (Coinmarketcap, 2020). In addition, the owner of the charity address would most likely keep this address balance as low as possible to use the funds or invest them, or does not want to lose their funds through a cyberattack on their charity address.

The day-of-the-week analysis reveals systematic differences between the Bitcoin transaction patterns of charity and ransomware campaigns. Ransomware has two distinct patterns after victims start making payments. First, where an accumulation of ransom payments happens over a longer period of time, a large balance of funds is allowed to accumulate in the ransomware address. This could make it a target for investigation if one address raises large amounts of Bitcoin, sits on this balance and waits to cash out, attracting surveillance from law enforcement to monitor the cash out-activity and where the illegal funds are being used. Another way ransomware attackers are controlling their ransom seed addresses is by keeping their balance close to zero. This overcomes any unnecessary attention from law enforcement and helps move the illegally acquired Bitcoin on quickly.

The analysis revealed that both WannaCry and CryptoDefense started collecting ransom on a Friday, 12 May 2015 for WannaCry and 28 February 2014 for CryptoDefense. This could indicate that the attackers are targeting a weekend to initiate their campaigns. Further indicating they may prefer to infect machines when computer activity is low in a corporate environment. Reinforcing this is the spike in collections on a Monday. Table 5A-1, 5A-2 and 5A-3 show 24, 40 and 27 collections in the first month. This is the highest number of ransom collection transactions for WannaCry for ransom seed addresses in Tables 5A-2 and 5A-3. However, to identify a statistically significant favoured day of the week for ransomware attacks a larger sample size of ransomware would need to be examined. One thing for certain is that most ransomware transactions take place immediately after the campaign starts, peaking in that first one

to two months, suggesting that these ransomware attacks are not sustained over a long period of time and responses to mitigate the attacks are mobilised quickly.

5.8 Graph Observations and Pattern Analysis

The following section evaluates the data collected from different ransomware attacks from the perspective of their ransomware seed address. It also includes an evaluation against a Bitcoin charity collection address which is the control subject. The observations start from the macro level – the overall transaction graph structure. The analysis then focuses in on communities forming within the graph structure. Furthermore, a finer level of granularity is provided through graph embeddings.

5.8.1 Bitcoin Transaction Graphs

Meiklejohn et al (2013), Reid and Harrigan (2013) and Ron and Shamir (2013) provided some of the pioneering analysis on Bitcoin transactions by visualising them as networks. This is the most intuitive way of observing the Bitcoin ecosystem. When looking for patterns of ransomware payments across the Intelligence - Forensic Continuum we can break the problem down by splitting the analysis into two. One side examines the victim ransom payments, the 'cash-in' patterns, and the other side examines the transfer of the attacker's proceeds of crime, or the 'cash-out' patterns. It is important to note that these patterns revolve around the ransom seed address for ransomware payment collection and the accurate identification of this address is a critical precursor for this analysis.

The ransomware cash-in patterns observed are very similar to those of the Bitcoin charity used as a control subject. Figure 5.7 compares three different cash-in graphs,

WannaCry address *13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94*, CryptoDefense address *1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1* and The Water Project address 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R.

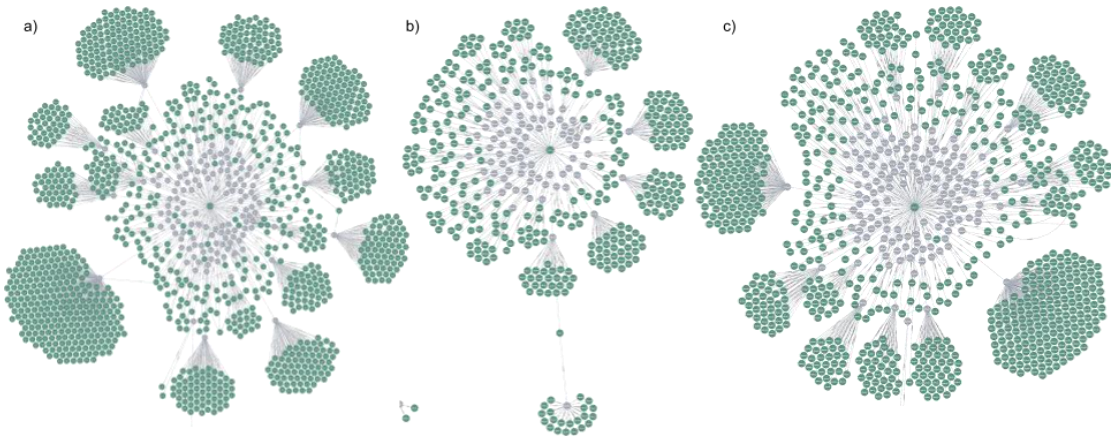


Figure 5.7: a) WannaCry, b) CryptoDefense and c) The Water Project 'cash-in' graphs.

The recurring pattern of the ransom seed address or collector address being at the centre of this graph and sprawling out towards the funds' origin is observable in Figure 5.7. The green dots represent Bitcoin addresses and the grey dots are the transactions connecting the addresses together. Although this pattern is quite distinctive, it does not distinguish between ransomware attacks and legitimate charity campaigns. That is there are similar clusters of green dots (Bitcoin addresses) formed in all three of the graphs in Figure 5.7. However, if the specific ransomware transactions were coloured and sized then compared to those of the charity graph a difference would be evident in the amount transacted.

The same three addresses on the cash-out side provide a different set of patterns completely. In Figure 5.8, we see that WannaCry takes the step of splitting one

transaction into many smaller amounts to the next address on its first move away from the ransomware seed address.

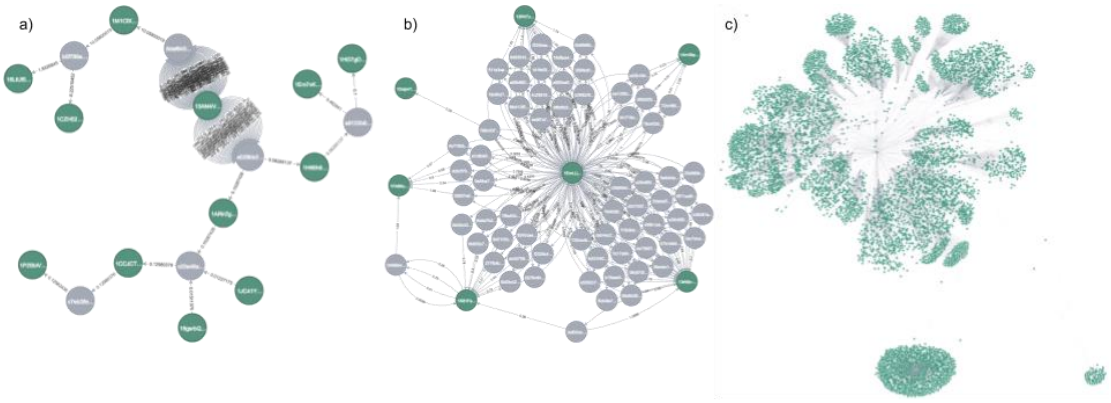


Figure 5.8: a) WannaCry, b) CryptoDefense and c) The Water Project 'cash-out' graphs.

CryptoDefense displays a different pattern by undertaking many transactions away from the ransomware seed address. This can be seen in Figure 5.8 b) by how the grey dots (transactions) outnumber the green dots (Bitcoin addresses). The Bitcoin charity address betrays yet another pattern where one transaction pays many different addresses. The cash-out graph analysis performed yields three distinct types of patterns. It appears that by visually examining the cash-out patterns of ransomware profiles nefarious behavior can be identified as a catalyst for further investigation. Providing more context to this behaviour is required to identify patterns for more deterministic ransomware detection.

5.8.2 Community Detection Patterns

Spagnuolo et al (2014), Fleder et al (2015) and Maesa et al (2018) provide the groundwork for developing an approach to Bitcoin community detection using a

machine learning technique based on the Louvain algorithm[27]. This involves focusing on the density of connections within particular clusters. The technique has been used to examine criminal networks based on hierarchy and structure (Needham and Hodler, 2019). In Figure 5.9, a Louvain community detection has been performed on each of the cash-in graphs from Figure 5.7 using the in and out degrees and PageRank score on each node.

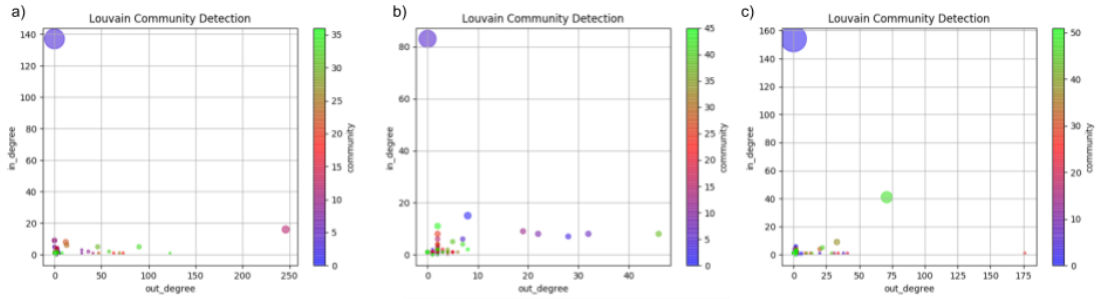


Figure 5.9: a) WannaCry, b) CryptoDefense and c) The Water Project 'cash-in' community detection patterns.

This provides a view of how influential the communities are based on the average PageRank for that community, in addition to how active the communities and particular nodes are in the network based on the number of connections (edges) coming in to (in-degree) and going out of (out-degree) the node. Judging by the high degrees of input connections on a ransomware seed address, it would be expected to see this node in a community with a high PageRank score. Running a PageRank algorithm over this graph will rank the nodes in the network with the most in-centrality.

[27] The Louvain Modularity algorithm finds clusters by examining the density of nodes connections within a cluster. This is used for determining how well a node belongs to a group. An example use of this is in fraud analysis to evaluate whether a single node or a collective (cluster) is misbehaving (Needham and Hodler, 2019).

PageRank belongs to the family of centrality algorithms, which measure the importance of a node with respect to other nodes in the network. It measures the number and quality of incoming relationships to a node to determine an estimation of how important that node is and can be used in the application of fighting financial fraud (Needham and Hodler, 2019). Nodes with more incoming relationships from other nodes are presumed to have more sway over a network (Needham and Hodler, 2019).

This is certainly the case for all three of the addresses tested. Observing the Tables 5B-1 through 5B-6 for the top 10 top PageRanked nodes on the cash-in and cash-out networks, the WannaCry *13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94* ransomware seed address, as seen in Table 5B-1, displays an in-degree of 137; out-degree of 0; PageRank of 16.66. Likewise, the ransomware seed address for CryptoDefense, *1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1*, as seen in Table 5B-2, has an in-degree of 83; out-degree 0; PageRank 12.39, the highest therefore the most central to the cash-in network. The Bitcoin charity address, *1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R*, also displays a similar dominant pattern compared to other nodes in the network. This can be seen in Table 5B-3, which shows an in-degree of 154; out-degree 0; PageRank 27.98.

Whilst community detection does not reveal the required uniqueness to determine a ransomware pattern for the cash-in networks, the cash-out network provides some distinguishing features between CryptoDefense and WannaCry. Figure 5.10 a) reveals a very low PageRank across the nodes of the cash-out network for WannaCry, meaning there is little influence of any node in the network.

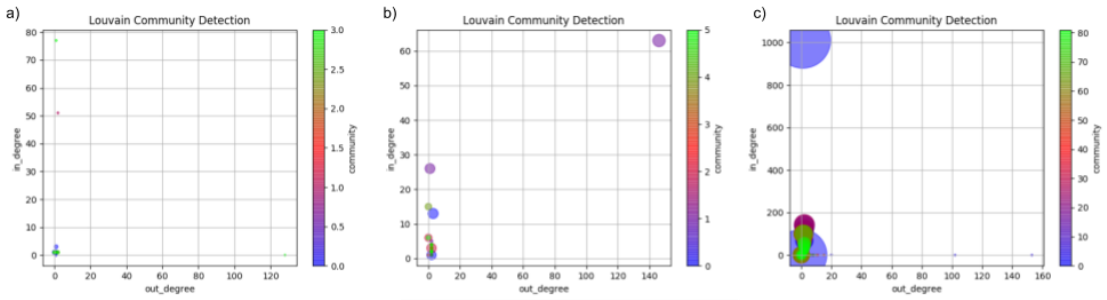


Figure 5.10: a) WannaCry and b) CryptoDefense 'cash-out' community detection patterns.

Perhaps this is a cash-out tactic of the attacks as instead of using multiple transactions or paying to multiple addresses they split the one transaction into micro amounts to avoid detection of dominant behaviour on the network. This is in contrast to CryptoDefense, which used many transactions to cash-out funds. The ransom seed address exhibited 146 transactions in the out-degree, yielding a PageRank of 6.52, creating a stand out marker in the community of nodes in this network.

Analysis so far shows community detection provides deeper insight into the Bitcoin behaviour patterns of ransomware compared to the day of the week analysis and standard graph visualisation. It applies statistical analysis to the graph networks formed by the cash-in, victim transactions, and the cash-out, attacker controlled transactions, providing a profile to help identify anomalies or unusual behaviour in financial systems with the use of a PageRank score as an indication of riskiness of a transaction or account in the payment network. However, there is limited knowledge revealed on these profiles when it comes to ransomware.

Advancing the analysis to consider the structure of such graphs and the metadata embedded on the graph structure may provide additional information for intelligence agencies to leverage when it comes to detecting ransomware payment networks.

5.8.3 Graph Embedding

After exhausting previous methods, we now explore a deeper analysis of the Ransomware-Bitcoin graph is to discover whether different campaigns exhibit similar clusters of connected Bitcoin addresses and transactions. Ahn et al (2016), Bistarelli et al (2018), Huang et al (2018) and Paquet-Clouston et al (2018) took applied graph analysis techniques to ransomware. Thus looking to reveal similar patterns of Bitcoin activity across the different campaigns on the input and output side of a targeted ransomware seed address. Tiao et al (2019), Li et al (2019), Perozzi et al (2014), Steenfatt et al (2018) and Yin and Vatrapu (2017) pushed the boundaries of graph analysis by applying machine learning to graphs. By analysing a graph's topology via the grouping of embedded features existing on a node, it is possible to learn the context of that node with respect to other nodes and features in the network.

The benefits of searching for patterns using graph embeddings is to help reduce the complexity of the network we are analysing and also provide input into machine learning techniques for the objective of node classification, predicting missing node attributes and predicting links between nodes in the network.

By inputting a graph, such as those revealed in Figure 5.7 and Figure 5.8, into a process that maps this complicated graph structure whilst capturing key features (embeddings), we are able to learn what is important and translate it into a simple representation for expert interpretation. Figure 5.11 shows the decomposition of the WannaCry 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94, CryptoDefense 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 and The Water Project

1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R cash-in graphs clustered with respect to common typological embeddings. The patterns revealed show how the clustered embeddings maintain the structure of the graph, for example, Figure 5.11 a) is the representation of the graph in Figure 5.7 a). Many transaction nodes surround the input graph with a large number of out degrees. The embedding analysis reveals patterns that differ from the majority of behaviour in the graph. The most extreme of these are sitting within cluster 3 and 5. These clusters represent anomalies in the graph. For example, the intense clustering of nodes at the centre of the figure is a representation of the low in-degree low out-degree nodes and those clusters external to that emphasise nodes that have relatively large in-degree (like the ransom seed address) or large out-degree, such as those transactions paying into many other addresses. As we move out from the centre we can see these secondary clusters of activity forming, this could be classified as exchange activity for the transfer of funds from an exchange where the victim creates a wallet to the ransomware address at the centre of all the clusters. The outlying clusters from the embedding analysis serve as a form of anomaly detection and can flag nodes for further investigation and risk classification.

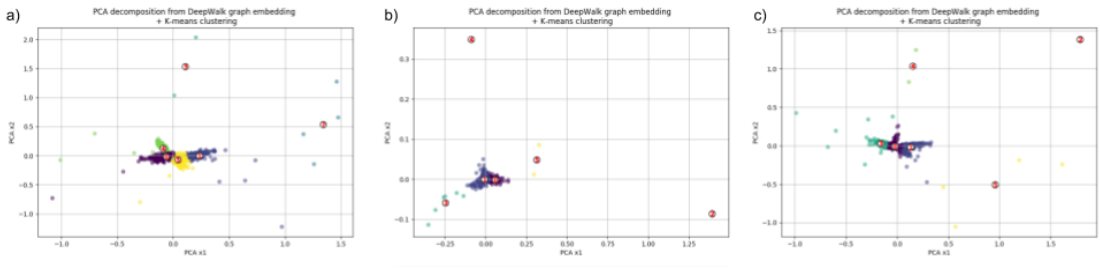


Figure 5.11: a) WannaCry, b) CryptoDefense and c) The Water Project ‘cash-in’ graph reduction patterns.

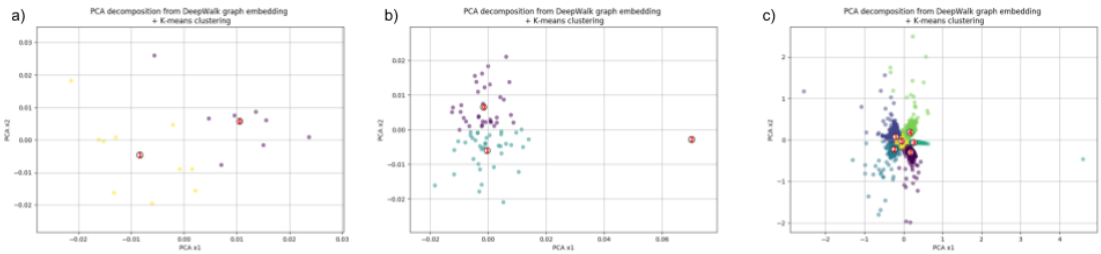


Figure 5.12: a) WannaCry, b) CryptoDefense and c) The Water Project 'cash-out' graph reduction patterns.

As we can see from both Figure 5.11 and Figure 5.12 the challenge is still with uniquely identifying a pattern of ransomware activity on the Bitcoin network when compared to other activities such as the control charity subject The Water Project. Observing the data from Figure 5.11 and Figure 5.12 cluster maps in Tables 5C-1 to 5C-6 reinforces the utility of anomaly detection. On the cash-in side we see clusters containing the maximum out-degree being of a very small population, which helps target potential service nodes that are helping facilitate victim payments, for example, Bitcoin exchanges. On the other hand, those clusters containing the maximum in-degree house a larger community of nodes with the highest in-centrality in the case of WannaCry and The Water Project, Table 5C-1 and 5C-3 respectively. This indicates the ransomware seed address exists in this cluster. On the cash-out side Tables 5C-4 to 5C-6 do not provide a definitive pattern for anomaly detection as the cash-in cluster data provides. The similarities in patterns between ransomware and the Bitcoin charity addresses requires an additional means to identify ransomware behaviour across the Intelligence - Forensic continuum. The subsequent sections will talk about some of these challenges and how they may be addressed in future research.

5.9 Future Research

One of the powerful results from the graph analysis is being able to embed features or meta-data into the graph for a deeper contextual understanding of what role nodes (addresses and transactions) play in their respective graphs. By providing open data this allows the community to flag certain behaviour or orientation of these nodes. A prime example of this is from the Wallet Explorer data where labels are provided with respect to which Bitcoin service (e.g. exchange, mixer or gambling site) these nodes emanate from or flow to. For example, intelligence gathered from the WannaCry ransomware seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw* cash-in graph shows 156 out 2000 addresses are labelled in the data with poloniex.com as the most prominent exchange used when crediting the ransom seed address. The cryptocurrency risk management company Elliptic has performed a similar labelling exercise that enriches our understanding of the blockchain graph information, categorising nodes as “licit”, “illicit” or “unknown” depending if a transaction has been created by an entity that belongs to a legitimate exchange, wallet, miner or service provider. On the contrary, a node can be flagged as illicit if it is deemed part of a ransomware scam, terrorist organization, or under nefarious control (Bellei, 2019). Labels such as those extracted from the Wallet Explorer API reveal dominate cryptocurrency exchanges and services in our target networks that produce payments into the ransom collector addresses. By disrupting these cryptocurrency services you could potentially disrupt the payment flows into ransom seed addresses. Though without sufficient categorisation of the content flowing in a Bitcoin network, similar to the way Internet traffic is managed via Content Delivery Networks (CDNs), runs a risk that disruption to legitimate services will occur. The subject matter expertise and analytics techniques required to identify and tag such datasets is intensive. Though if done correctly, can greatly enhance any

further machine learning analysis by intelligently clustering communities in a supervised way providing meaning and context to the data for law enforcement. By looking at these labelled properties on the incoming and outgoing sides of the ransomware graphs would allow authorities to target potential nefarious services to stifle their ability to play any part in illicit fund movement. This is an area that could be the subject of further research.

5.10 Conclusion

Comparing graphs created for ransomware versus charity collection using Bitcoin shows that ransom payment patterns into a ransom seed address are remarkably similar to those of the charity collection "control" case. This makes it difficult to distinguish between a charity Bitcoin address receiving legitimate payments from that of ransom payments from ransomware. However, the uniformity witnessed with the amounts being paid as ransom versus the volatility in the amounts being paid in charity is a distinct marker of a ransomware attack.

In addition, the day-of-the-week analysis shows up two distinctly different behaviours, one where a ransomware seed address accumulates ransom payments over time and holds on until it is the right time to cash out and another that likes to keep the ransom seed address 'zeroed' after everyday. These two different strategies from ransomware attackers could be targeted, especially in the case where cash-out frequency is high.

Furthermore, community detection techniques provide little distinction between the likes of Wannacry and the "control" case, although it does yield enough interest to warrant further investigation when such an influential node in a target network has high

levels of in-degree activity and large PageRank values. Moreover, using unsupervised machine learning techniques, in this case with the DeepWalk algorithm to preserve graph structure, produced graph embeddings and anomalous clusters that warrant further investigation.

A way to potentially improve the performance of the machine learning algorithms is to take the graph labelling another step further. This would require adding more meta-data to the graph that attributes the nodes and transactions to the categories of ransomware or other. As a result of this research datasets have been collected for which the aforementioned analysis tools and techniques have been applied to gain a deeper understanding of the Bitcoin payment structures related to ransomware in order to enhance the efforts of future research and law enforcement to combat illegal uses of cryptocurrency.

5.11 Well Disguised Patterns

Using these advanced machine learning techniques for graph analysis of ransomware-Bitcoin payments are very experimental and dependent on the quality and formation of data used as input into the algorithms. Significantly more focus should be placed on the data engineering side in order to test a broader range of features in ransomware-Bitcoin networks. Labelling data with richer detail regarding whether the address is illicit, whether it is coming from or going to a suspicious service, and whether it is controlled or reused by ransomware actors would provide more targeted analysis. This chapter uses the raw network data from Appendix B to load into the Neo4j graph database software. All source code and data resulting from this analysis is available from the

Harvard DataVerse repository created for this research project (see Appendices A, B, and C; https://dataverse.harvard.edu/dataverse/bitcoin-network-data). Appendix C references the analysis output from this chapter. By using a graph database and visualisation tool such as Neo4j, it is possible to interpret the graph structures created from the payment networks formed in Bitcoin. This then allows us to discern certain patterns of behaviour on the Bitcoin network that will support analysts profiling ransomware payments by targeting suspicious addresses, exchanges, and transactions that are complicit in a ransomware payment network. The distinction can only be emphasised through the unique identification of such features that reveal patterns of ransomware payments.

By examining a control subject that receives Bitcoin payments (The Water Project charity in this chapter) it is possible to reveal how illegitimate payment patterns can resemble legitimate ones. Encouragingly, it may be possible to unmask these patterns on the cash-out network with legitimate actors displaying different cash-out strategies to illegitimate actors. It would be prudent to dive deeper into the underlying data of these patterns. This chapter goes some way towards exploring the utility of the underlying data by applying graph algorithms such as PageRank, Louvain Community Detection, in-degree, and out-degree analysis. Further exploration of the underlying data will enable the possibility for data tagging, risk rating, and feature engineering that will expose the disguised patterns of ransomware-related Bitcoin payments.

Developments in the area of illicit Bitcoin transaction analysis techniques apply a range of sophisticated data science techniques. For example, Oliveira et al (2021) develop a method using random walks along a transaction graph called ‘GuiltyWalker’. This

method introduces new graph features not considered in this research. Using the structure of the graph and data labels they add the distance to an illicit transaction from the starting node, which enhances their illicit transaction classification model (Oliveira et al, 2021). This is similar to the ‘depth’ metric collected in this research; however, it is not implemented in our feature set. In addition, Alarab et al (2020) use an ensemble learning approach that utilises multiple machine learning algorithms to enhance the predictive nature of the classification system being used. It is noted that they are experimenting on the curated dataset from Elliptical, which is pre-labelled to help train their classifier more accurately. It is a step forward from this research as it takes one of the core recommendations of exploiting the underlying blockchain data to tag and curate a dataset that identifies illicit and legitimate transactions for machine learning algorithm development and training. This step forward takes the effort and complexity out of engineering the data and shifts the emphasis onto the analysis and investigation activities. Furthermore, Poursafaei et al (2021), Elbaghdadi et al (2020), and Nerurkar et al (2020) employ signature vectors, K-Nearest Neighbour, and Ensemble Decision Tree machine learning components for illicit bitcoin transaction analysis. Whilst these techniques do not explicitly focus on ransomware-Bitcoin activity, they provide a path for the application of their techniques to the ransomware-Bitcoin use case.

The next chapter explores the application of risk rating addresses and transactions evident on the cash-out network for a particular WannaCry ransomware seed address. By utilising the machine learning technique and graph embeddings, it is possible to follow the money and ascertain contextual information about the role a node plays in the cash-out network.

5.12 Appendix 5A – Day of the Week Analysis Tables

dayOfWeek	Values			12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	sum BTC
201705	13	2.4335	0.0000	24	3.6102	0	11	1.55E+00	0	11	1.9077	0	3	0.0182	0.0000	12	2.1556	0	30	5.4675	0	104	17.1448	0.0000	17.1448
201706							3	2.50E-01	0	1	0.0362	0				2	0.1235	0				6	0.4099	0.0000	17.5547
201707				1	0.2159	0													1	0.0005	0	2	0.2164	0.0000	17.7711
201708													2	0.0000	-17.7711							2	0.0000	-17.7711	0.0000
201709				1	1.1006	0							2	0.0900	0.0000	1	0.0960	0				4	1.2866	0.0000	1.2866
201710				1	0.0680	0	1	1.16E-03	0													2	0.0692	0.0000	1.3558
201801										1	0.0278	0										1	0.0278	0.0000	1.3835
201805										1	0.0573	0				2	0.0602	0				3	0.1175	0.0000	1.5010
201806				1	0.0000	0																1	0.0000	0.0000	1.5010
201807							1	1.44E-03	0													1	0.0014	0.0000	1.5024
201810																1	0.0459	0				1	0.0459	0.0000	1.5483
201812													1	0.0001	0.0000	1	0.0930	0				2	0.0931	0.0000	1.6415
201901										1	0.0029	0										1	0.0029	0.0000	1.6444
201903										1	0.0002	0										1	0.0002	0.0000	1.6445
201904	2	0.0001	0.0000	2	0.0002	0																4	0.0004	0.0000	1.6449
201905	1	0.0000	0.0000							1	0.0000	0										2	0.0000	0.0000	1.6449
201907				1	0.0480	0																1	0.0480	0.0000	1.6930
Grand Total	**16**	**2.4336**	**0.0000**	**31**	**5.0430**	**0**	**16**	**1.80E+00**	**0**	**17**	**2.0320**	**0**	**8**	**0.1083**	**-17.7711**	**19**	**2.5742**	**0**	**31**	**5.4680**	**0**	**138**	**19.4641**	**-17.7711**	

Table 5A-1: WannaCry Transaction Analysis by year-month and day of the week (Transaction History (2016-12-31 to 2019-07-08) Source from: https://btc.com/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw#stats)

dayOfWeek	Values			13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	sum BTC
201705	12	1.8797	0	40	6.4443	0	17	2.8188	0	10	1.6147	0	8	1.3861	0.0000	17	3.2241	0	19	2.0607	0	123	19.4285	0.0000	19.4285
201706	1	0.1958	0				2	0.0012	0							1	0.1195	0	1	0.0002	0	5	0.3167	0.0000	19.7451
201708													2	0.0000	-19.7451							2	0.0000	-19.7451	0.0000
201709				1	0.0900	0																1	0.0900	0.0000	0.0900
201712	1	0.0216																				1	0.0216		0.1116
201801	1	0.0001		1	0.0461		1	0.0201		2	0.0002											5	0.0665		0.1781
201802										1	0.0600											1	0.0600		0.2381
201904				1	0.0584																	1	0.0584		0.2965
Grand Total	**15**	**2.0973**		**43**	**6.6388**		**20**	**2.8401**		**13**	**1.6749**		**10**	**1.3861**	**-19.7451**	**18**	**3.3436**		**20**	**2.0609**		**139**	**20.0417**	**-19.7451**	

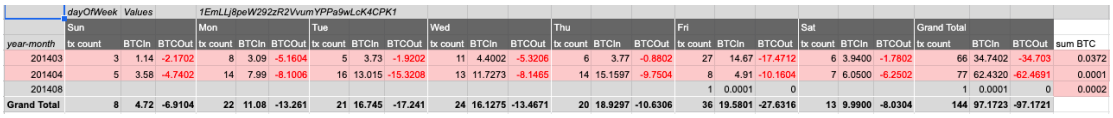
Table 5A-2: WannaCry Transaction Analysis by year-month and day of the week (Transaction History (2016-12-31 to 2019-07-08) Source from: https://btc.com/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94)

dayOfWeek	Values			115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	sum BTC
201705	12	1.8236	0	27	4.0867	0	10	1.6843	0	9	0.8796	0	14	0.9232	0.0000	10	1.7294	0	24	2.9541	0	106	14.0809	0.0000	14.0809
201706				1	0.0001	0	1	0.2078	0	1	0.0050	0	1	0.0769	0.0000	2	0.0400	0				6	0.3298	0.0000	14.4107
201708										1	0.0900	0	2	0.0000	-14.4107							3	0.0900	-14.4107	0.0900
201712				2	0.1195	0																2	0.1195	0.0000	0.2095
201802										1	0.0600	0										1	0.0600	0.0000	0.2695
201804				1	0.0004	0																1	0.0004	0.0000	0.2698
201812																			2	0.1296	0	2	0.1296	0.0000	0.3994
Grand Total	**12**	**1.8236**	**0**	**31**	**4.2066**	**0**	**11**	**1.8921**	**0**	**12**	**1.0346**	**0**	**17**	**1.0001**	**-14.4107**	**12**	**1.7694**	**0**	**26**	**3.0837**	**0**	**121**	**14.8101**	**-14.4107**	

Table 5A-3: WannaCry Transaction Analysis by year-month and day of the week (Transaction History (2016-12-31 to 2019-07-08) Source from: https://btc.com/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn)

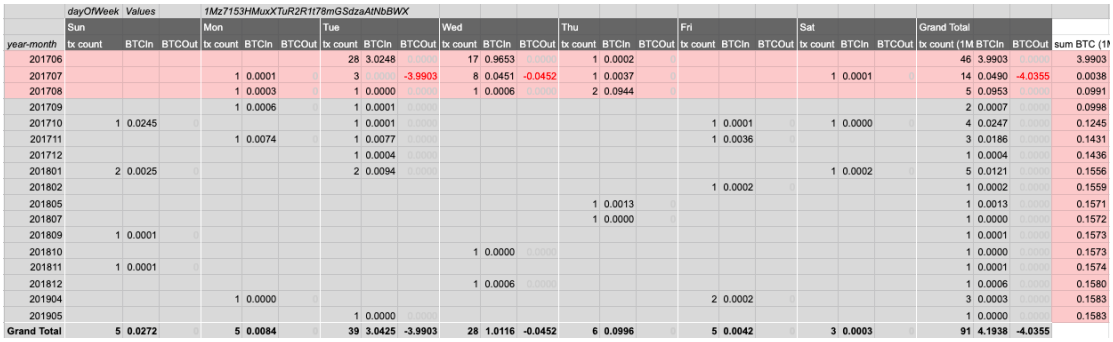
dayOfWeek	Values			19DyWHtgLgDKgEeoKjfpCJJ9WU8SQ3gr27																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	sum BTC
201402																2	0.4500	-0.4491				2	0.4500	-0.4491	0.0009
201403	6	3.7898	-1.7292	13	7.5730	-1.8293	9	5.4402	-2.6403	10	5.9080	-12.4775	8	6.0201	-1.6602	6	5.3500	-1.6602	12	5.4590	-3.4604	64	39.5401	-25.4571	14.0839
201404							1	1.1600	0	4	0.0000	-15.2435										5	1.1600	-15.2435	0.0004
201408																1	0.0001	0.0000				1	0.0001	0	0.0005
Grand Total	**6**	**3.7898**	**-1.7292**	**13**	**7.5730**	**-1.8293**	**10**	**6.6002**	**-2.6403**	**14**	**5.9080**	**-27.721**	**8**	**6.0201**	**-1.6602**	**9**	**5.8001**	**-2.1093**	**12**	**5.4590**	**-3.4604**	**72**	**41.1502**	**-41.1497**	

Table 5A-4: CryptoDefense Transaction Analysis by year-month and day of the week (Transaction History (2012-12-31 to 2019-07-09) Source from: https://btc.com/19DyWHtgLgDKgEeoKjfpCJJ9WU8SQ3gr27)



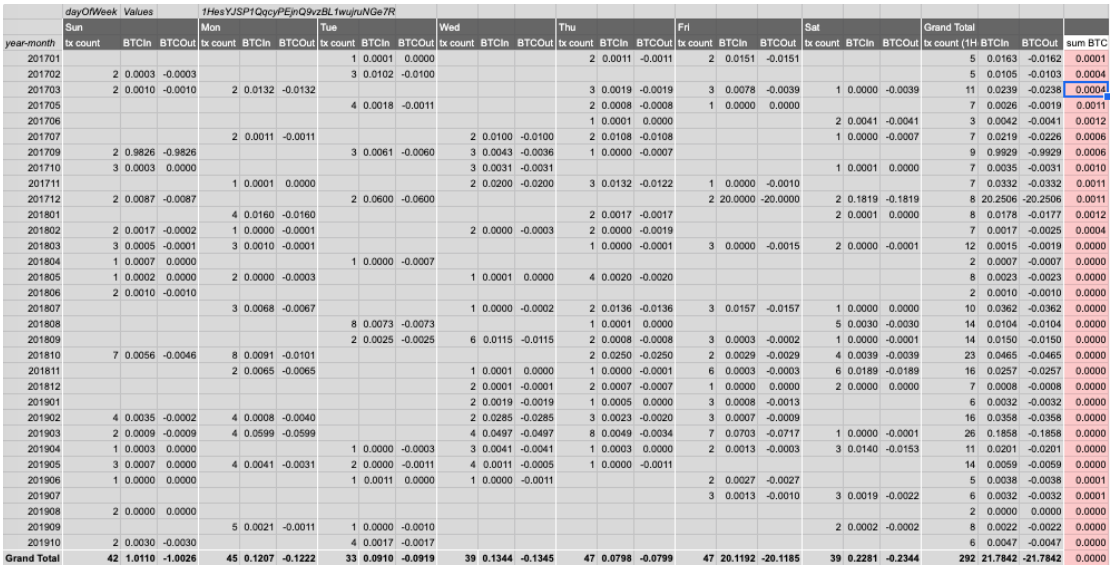
	dayOfWeek	Values		1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	sum BTC
201403	3	1.14	-2.1702	8	3.09	-5.1604	5	3.73	-1.9202	11	4.4002	-5.3206	6	3.77	-0.8802	27	14.67	-17.4712	6	3.9400	-1.7802	66	34.7402	-34.703	0.0372
201404	5	3.58	-4.7402	14	7.99	-8.1006	16	13.015	-15.3208	13	11.7273	-8.1465	14	15.1597	-9.7504	8	4.91	-10.1604	7	6.0500	-6.2502	77	62.4320	-62.4691	0.0001
201408																1	0.0001	0				1	0.0001	0	0.0002
Grand Total	**8**	**4.72**	**-6.9104**	**22**	**11.08**	**-13.261**	**21**	**16.745**	**-17.241**	**24**	**16.1275**	**-13.4671**	**20**	**18.9297**	**-10.6306**	**36**	**19.5801**	**-27.6316**	**13**	**9.9900**	**-8.0304**	**144**	**97.1723**	**-97.1721**	

Table 5A-5: CryptoDefense Transaction Analysis by year-month and day of the week (Transaction History (2012-12-31 to 2019-07-10) Source from: https://btc.com/1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1)



	dayOfWeek	Values		1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count (1M	BTCIn	BTCOut	sum BTC (1
201706							28	3.0248	0.0000	17	0.9653	0.0000	1	0.0002	0							46	3.9903	0.0000	3.9903
201707				1	0.0001	0	3	0.0000	-3.9903	8	0.0451	-0.0452	1	0.0037	0				1	0.0001	0	14	0.0490	-4.0355	0.0038
201708				1	0.0003	0	1	0.0000	0.0000	1	0.0006	0.0000	2	0.0944	0							5	0.0953	0.0000	0.0991
201709				1	0.0006	0	1	0.0001	0.0000													2	0.0007	0.0000	0.0998
201710	1	0.0245	0				1	0.0001	0.0000							1	0.0001	0	1	0.0000	0	4	0.0247	0.0000	0.1245
201711				1	0.0074	0	1	0.0077	0.0000							1	0.0036	0				3	0.0186	0.0000	0.1431
201712							1	0.0004	0.0000													1	0.0004	0.0000	0.1436
201801	2	0.0025	0				2	0.0094	0.0000										1	0.0002	0	5	0.0121	0.0000	0.1556
201802																1	0.0002	0				1	0.0002	0.0000	0.1559
201805													1	0.0013	0							1	0.0013	0.0000	0.1571
201807													1	0.0000	0							1	0.0000	0.0000	0.1572
201809	1	0.0001	0																			1	0.0001	0.0000	0.1573
201810										1	0.0000	0.0000										1	0.0000	0.0000	0.1573
201811	1	0.0001	0																			1	0.0001	0.0000	0.1574
201812										1	0.0006	0.0000										1	0.0006	0.0000	0.1580
201904				1	0.0000	0										2	0.0002	0				3	0.0003	0.0000	0.1583
201905							1	0.0000	0.0000													1	0.0000	0.0000	0.1583
Grand Total	**5**	**0.0272**	**0**	**5**	**0.0084**	**0**	**39**	**3.0425**	**-3.9903**	**28**	**1.0116**	**-0.0452**	**6**	**0.0996**	**0**	**5**	**0.0042**	**0**	**3**	**0.0003**	**0**	**91**	**4.1938**	**-4.0355**	

Table 5A-6: NotPetya Transaction Analysis by year-month and day of the week (Transaction History (2015-12-31 to 2019-07-10) Source from: https://btc.com/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX)



	dayOfWeek	Values		1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R																				
	Sun			Mon			Tue			Wed			Thu			Fri			Sat			Grand Total			
year-month	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count	BTCIn	BTCOut	tx count (1H	BTCIn	BTCOut	sum BTC
201701							1	0.0001	0.0000				2	0.0011	-0.0011	2	0.0151	-0.0151				5	0.0163	-0.0162	0.0001
201702	2	0.0003	-0.0003				3	0.0102	-0.0100													5	0.0105	-0.0103	0.0004
201703	2	0.0010	-0.0010	2	0.0132	-0.0132							3	0.0019	-0.0019	3	0.0078	-0.0039	1	0.0000	-0.0039	11	0.0239	-0.0238	0.0004
201705							4	0.0018	-0.0011				2	0.0008	-0.0008	1	0.0000	0.0000				7	0.0026	-0.0019	0.0011
201706													1	0.0001	0.0000				2	0.0041	-0.0041	3	0.0042	-0.0041	0.0012
201707				2	0.0011	-0.0011				2	0.0100	-0.0100	2	0.0108	-0.0108				1	0.0000	-0.0007	7	0.0219	-0.0226	0.0006
201709	2	0.9826	-0.9826				3	0.0061	-0.0060	3	0.0043	-0.0036	1	0.0000	-0.0007							9	0.9929	-0.9929	0.0006
201710	3	0.0003	0.0000							3	0.0031	-0.0031							1	0.0001	0.0000	7	0.0035	-0.0031	0.0010
201711				1	0.0001	0.0000				2	0.0200	-0.0200	3	0.0132	-0.0122	1	0.0000	-0.0010				7	0.0332	-0.0332	0.0011
201712	2	0.0087	-0.0087				2	0.0600	-0.0600							2	20.0000	-20.0000	2	0.1819	-0.1819	8	20.2506	-20.2506	0.0011
201801				4	0.0160	-0.0160							2	0.0017	-0.0017				2	0.0001	0.0000	8	0.0178	-0.0177	0.0012
201802	2	0.0017	-0.0002	1	0.0000	-0.0001				2	0.0000	-0.0003	2	0.0000	-0.0019							7	0.0017	-0.0025	0.0004
201803	3	0.0005	-0.0001	3	0.0010	-0.0001							1	0.0000	-0.0001	3	0.0000	-0.0015	2	0.0000	-0.0001	12	0.0015	-0.0019	0.0000
201804	1	0.0007	0.0000				1	0.0000	-0.0007													2	0.0007	-0.0007	0.0000
201805	1	0.0002	0.0000	2	0.0000	-0.0003				1	0.0001	0.0000	4	0.0020	-0.0020							8	0.0023	-0.0023	0.0000
201806	2	0.0010	-0.0010																			2	0.0010	-0.0010	0.0000
201807				3	0.0068	-0.0067				1	0.0000	-0.0002	2	0.0136	-0.0136	3	0.0157	-0.0157	1	0.0000	0.0000	10	0.0362	-0.0362	0.0000
201808							8	0.0073	-0.0073				1	0.0001	0.0000							5	0.0030	-0.0030	14	0.0104	-0.0104	0.0000
201809							2	0.0025	-0.0025	6	0.0115	-0.0115	2	0.0008	-0.0008	3	0.0003	-0.0002	1	0.0000	-0.0001	14	0.0150	-0.0150	0.0000
201810	7	0.0056	-0.0046	8	0.0091	-0.0101							2	0.0250	-0.0250	2	0.0029	-0.0029	4	0.0039	-0.0039	23	0.0465	-0.0465	0.0000
201811				2	0.0065	-0.0065				1	0.0001	0.0000	1	0.0000	-0.0001	6	0.0003	-0.0003	6	0.0189	-0.0189	16	0.0257	-0.0257	0.0000
201812										2	0.0001	-0.0001	2	0.0007	-0.0007	1	0.0000	0.0000	2	0.0000	0.0000	7	0.0008	-0.0008	0.0000
201901										2	0.0019	-0.0019	1	0.0005	0.0000	3	0.0008	-0.0013				6	0.0032	-0.0032	0.0000
201902	4	0.0035	-0.0002	4	0.0008	-0.0040				2	0.0285	-0.0285	3	0.0023	-0.0020	3	0.0007	-0.0009				16	0.0358	-0.0358	0.0000
201903	2	0.0009	-0.0009	4	0.0599	-0.0599				4	0.0497	-0.0497	8	0.0049	-0.0034	7	0.0703	-0.0717	1	0.0000	-0.0001	26	0.1858	-0.1858	0.0000
201904	1	0.0003	0.0000				1	0.0000	-0.0003	3	0.0041	-0.0041	1	0.0003	0.0000	2	0.0013	-0.0003	3	0.0140	-0.0153	11	0.0201	-0.0201	0.0000
201905	3	0.0007	0.0000	4	0.0041	-0.0031	2	0.0000	-0.0011	4	0.0011	-0.0005	1	0.0000	-0.0011							14	0.0059	-0.0059	0.0000
201906	1	0.0000	0.0000				1	0.0011	0.0000	1	0.0000	-0.0011				2	0.0027	-0.0027				5	0.0038	-0.0038	0.0001
201907																3	0.0013	-0.0010	3	0.0019	-0.0022	6	0.0032	-0.0032	0.0001
201908	2	0.0000	0.0000																			2	0.0000	0.0000	0.0000
201909				5	0.0021	-0.0011	1	0.0000	-0.0010										2	0.0002	-0.0002	8	0.0022	-0.0022	0.0000
201910	2	0.0030	-0.0030				4	0.0017	-0.0017													6	0.0047	-0.0047	0.0000
Grand Total	**42**	**1.0110**	**-1.0026**	**45**	**0.1207**	**-0.1222**	**33**	**0.0910**	**-0.0919**	**39**	**0.1344**	**-0.1345**	**47**	**0.0798**	**-0.0799**	**47**	**20.1192**	**-20.1185**	**39**	**0.2281**	**-0.2344**	**292**	**21.7842**	**-21.7842**	**0.0000**

Table 5A-7: Control: WaterProject Transaction Analysis by year-month and day of the week (Transaction History (2016-12-31 to 2019-10-18) Source from:

https://btc.com/1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R

5.13 Appendix 5B – Community Detection and Clustering Tables

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	2	0	137	16.6649		[0]	
a69ae40e77691ae0121205068751b890c61c22e0b56ee8f4f444d17c21913f30	11	246	16	2.1900		0	14/05/2017 03:14:03 UTC
98e0ba2897a32823faebedf92a7dd3fad1ae6dfa349bc817e8a28aa13f137e89	23	12	8	1.1700		0	15/05/2017 20:37:58 UTC
65764ca84aa6acfecbac5f6d48cb56c434de0a7371e4cc7acb45fe256ce65de2	26	13	6	0.9150		0	16/05/2017 10:33:47 UTC
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	9	0	9	0.8613		[0]	
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	9	0	9	0.8613		[0]	
64eca1c32095b777bb9ef3c5a0e81b9c40ef1b328d022619e05e3ed6e03861c4	32	90	5	0.7875		0	19/05/2017 13:06:42 UTC
d38b15ef5fac7c843ca000cbe18d4478c84ffcc472653b2691bfe6076aed61b2	29	46	5	0.7875		0	18/05/2017 05:51:28 UTC
96015c757e440554005965b97349234dcae8d4c0f8cc3410a0743cbcc9bacd6c	9	3	4	0.6600		0	15/05/2017 15:40:34 UTC
df03af3a2b1d0ce2a43771b55f0258a94262ceeda0b0fc92f02c49a9f2229851	2	2	4	0.6600		0	15/05/2017 07:03:17 UTC

Table 5B-1: WannaCry - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 - Top 10 top PageRanked nodes for cash-in

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1	4	0	83	12.3961		[0]	
26dc7b3bd0a761399e63832d9e7d575d8abf0131230e822a52c3ac7f0707d809	1	8	15	1.8712		2	18/03/2014 09:25:05 UTC
ede9f8e9386eb987f67a2820d9939ad4906112d74038956cce21c368d786c04a	43	2	11	1.2975		0	10/04/2014 23:51:18 UTC
3acaa7d2504df7b52bbc007d69244e4ad6b9da7d8c27cd54d67501603eb01194	37	46	8	1.1700		0	09/04/2014 10:52:54 UTC
e345169084494a0682e956178c11cd9ef05ce17eaa5a58ce1fee61db4f22332d	7	32	8	1.1700		0	19/03/2014 22:14:50 UTC
5ab14f0ff07bb895ca8f493c09226ce7e3ea5c1e1a518dbde31ba76edd553a55	8	22	8	1.1700		0	21/03/2014 03:03:09 UTC
6c692a7cc58c50fe99efa52188b1c476203b958996e602a937baada44231e423	24	2	8	1.1700		0	03/04/2014 18:41:28 UTC
d2230af6d0ef4b48c416e8f5df3c8e0f2c0f1631c95ea5ec0c21d3b0bd8329c9	12	19	9	1.1062		0	22/03/2014 12:59:43 UTC
afdec6d9670d9a70fa1428f7a7e9ff270eb9cff744663449f9b7d6c1bbf20764	3	28	7	1.0425		0	18/03/2014 19:43:02 UTC
da769728a1706395e1a9ae2d41996607cdffb80a0732cc69faea2d1d1f136b66	15	2	6	0.8336		0	27/03/2014 13:16:57 UTC

Table 5B-2: CryptoDefense - 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 - Top 10 top PageRanked nodes for cash-in

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R	2	0	154	27.9822		[0]	04/09/2016 10:20:45 UTC
33dbcca823c4c500441ad90894dfe723c00c414f04d6057315170b08dcf1c21c	48	71	41	5.2500		0	
15db7db1387b080181bf34c9df54d8ca57008624b2f865e6c1b17866f40c854e	38	33	9	1.2975		0	17/09/2017 15:05:03 UTC
19ed01550d1c7087f5a657d310cfddc1841cb4218b13391192e44e1dbf7a2926	2	1	4	0.6600		0	13/12/2018 20:23:16 UTC
1a21e86355230005c5d4174b20842ed2de31680aa70f1837d10abc5a1ee173ee	13	1	4	0.6600		0	18/02/2019 11:55:05 UTC
3a4c04e51839f01881b5895864b6f873320e33cf478be9227a6c905014a71bed	32	2	4	0.6600		0	11/02/2018 19:32:21 UTC
7d168c9f9ed3ebf5ede286c7127d285d6d95e871fa38b874528bb2fd7585e297	33	20	4	0.6600		0	29/01/2018 17:59:37 UTC
ba840bc3d5cad98bc88475789b5ed34977f28563e50639bf4e1e9b4b4ca30611	46	22	5	0.6600		0	27/01/2017 16:54:24 UTC
147e71ef619368ed5691b377ba9c5d2448acefdb3dcd5d762222dd35dbaa5733	42	2	1	0.5914		0	03/03/2017 20:07:54 UTC
5dd5113339b4787774f1dae3df79140681070601059547 1b55e262d1daf31c1d	47	2	3	0.5325		0	22/11/2016 14:55:28 UTC

Table 5B-3: Control: The Water Project - 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R - Top 10 top PageRanked nodes for cash-in

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	0	0	1	0.76032		[4]	
c7eb28c30d8b23e0612b1678a2ca1cd879655eda3e9f190ea3f6f67a176e475d	0	1	1	0.71802		4	03/08/2017 08:28:51 UTC
1CCJCTiotg75x826rmWJzSFKtrnBaqjQWu	0	1	1	0.66826		[4,3]	
c03e48ad9fc778170c86542c0414a89052b21679a3576121ca6b1c2d340f1e22	0	1	3	0.60972		3	03/08/2017 06:45:42 UTC
b0f788ea6f24dbf7d77b38f894311b12ec3f4ac2ec2e6ebf05ffac34145a5247	3	2	1	0.43193		3	03/08/2017 08:05:33 UTC
a9132b6161dfbbeea46fe627c2a3f0ce98e7d3e53c80493b351648a6390a6d0e	2	2	1	0.35472		3	03/08/2017 07:13:58 UTC
16LtUf54vnwvQkcdDTFYtGAeYC5G31yQMG	3	0	1	0.33357		[3]	
1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR	3	0	1	0.33357		[3]	
1M1CfXLynR6vqbjwTqSiiLRVDQZEXHHJbb	3	1	1	0.33169		[3,0]	
1HG7gDBAYnPCJBC7eiwhX9dNRVi1c5naou	2	0	1	0.30075		[3]	

Table 5B-4: WannaCry - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 - Top 10 top PageRanked nodes for cash-out

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1	1	146	63	6.5223		[0,4]	
1K81FeS3TH7DkqrMECtVDwXruRiXPXa6dZ	0	3	13	4.3918		[0,4]	
13H5hrYgTnohrcWKni6v9V7jJp7kVDt5G3	1	1	26	4.1624		[0,4]	
2465fa41bfcc597edf4479717b5b62f551d308d320257f5f67f6b683ec8b4602	2	2	3	3.8829		4	19/03/2014 15:20:22 UTC
2ef03cec91e3c05d928b116f10bcd98a200f2b14895d4eff984046520296a954	0	2	1	3.6880		4	19/03/2014 12:17:23 UTC
1FAB6uvKD9q5MnGm3ta1ERvmeVpYgyNQwj	2	0	6	2.2612	BTC-e.com-old	[4,0]	
13RhTuFDfAw874nfCHJqg1uPWbHugCRVX3	4	0	15	1.8674		[0]	
1Arn3kpLoFLwtzXHBKwVJVWZG6aLBpV4rU	5	0	6	0.7681		[0]	
7204a4bfabd7e6e663d1b881221164b6cb419a445a0a68b96f203d9fbe52f2c3	1	2	5	0.3632		0	28/03/2014 13:12:26 UTC
1d1fe930c41723cbf7a9611493ae3b8eb443c699058db8db0587e671205443e9	4	2	4	0.3206		0	07/04/2014 09:35:23 UTC

Table 5B-5: CryptoDefense - 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 - Top 10 top PageRanked nodes for cash-out

n.index	community	out_degree	in_degree	pagerank	n.label	n.depth	n.time_stamp
9267c6ae3a98dffc4096d07345777adfbadf02648d9e1c406425167899679f84	0	2	68	12.7536		4	04/08/2019 18:14:04 UTC
bc1qv4lh6qccjppzl6lgmujcgq2y242x9n2krjcp0q	0	1	0	0.1500		[4]	
bc1q4ln4y3xcq475j5p7935zphlspc08q2h02cy0qj	0	1	0	0.1500		[4]	
bc1q0nxeejrdstsul7gmnr5r3jjnygetff2pqndly6	0	1	1	4.7778		[4,0]	
bc1q5qezakfetlhg8pp480jatzderxgjjzq63d8dje	0	1	0	0.1500		[4]	
bc1qtactjnwz593sw8rxj506yhap2xdkj4hz86l7a8	0	1	0	0.1500		[4]	
bc1q48aryt2mk5hu8uwe79hdye8trjaxz34ryp8hn4	0	1	0	0.1500		[4]	
bc1qtuxl9d6c4rfj5u7nj4x6xh4haemul304npk5q2	0	1	0	0.1500		[4]	
bc1q47s6xqtxuqvkq55c43wk78jxap0f7dwl5cnn3a	0	1	0	0.1500		[4]	
bc1qtj5563nhang7tfw8wemfpnyawpugu58y7vkjyn	0	1	0	0.1500		[4]	

Table 5B-6: Control: The Water Project - 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R - Top 10 top PageRanked nodes for cash-out

5.14 Appendix 5C – Cluster Profile Tables

	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 Cash-in								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	73	0.5788	9	0.8738	539	43	0.9150	-0.0669	-0.0084
1	69	0.4962	2	0.9470	264	4	0.4050	-0.0770	0.1344
2	41	0.8095	8	1.0476	147	4	1.1700	0.2332	-0.0146
3	123	68.5000	5	2.2500	4	4	0.7875	1.4434	0.5344
4	246	154.5000	16	8.5000	2	2	2.1900	0.3262	1.5758
5	90	0.7174	137	1.2561	453	84	16.6649	0.0347	-0.0753
Grand Total	**246**	**1.0433**	**137**	**1.0433**	**1409**	**141**	**16.6649**	**0.0000**	**0.0000**

Table 5C-1: WannaCry - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 - Cluster profile for cash-in nodes

	1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 Cash-in								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	6	0.4844	11	0.9844	64	5	1.2975	0.0578	-0.0006
1	8	0.8161	15	0.8207	435	74	1.8712	-0.0095	0.0001
2	46	46.0000	8	8.0000	1	1	1.1700	1.3918	-0.0858
3	32	9.8333	83	18.0000	6	4	12.3961	-0.2466	-0.0589
4	28	28.0000	7	7.0000	1	1	1.0425	-0.0893	0.3490
5	22	20.5000	9	8.5000	2	2	1.1700	0.3124	0.0489
Grand Total	**46**	**1.1002**	**83**	**1.1002**	**509**	**87**	**12.3961**	**0.0000**	**0.0000**

Table 5C-2: CryptoDefense - 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 - Cluster profile for cash-in nodes

	1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R Cash-in								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	20	0.6737	6	0.7982	659	136	0.6600	-0.0242	-0.0021
1	10	0.1145	1	0.9736	227	2	0.3017	0.1277	-0.0161
2	176	176.0000	1	1.0000	1	1	0.2775	1.7884	1.3858
3	71	1.7931	154	2.4224	116	12	27.9822	-0.1636	0.0309
4	29	21.5000	1	1.0000	2	2	0.2775	0.1497	1.0381
5	41	36.5000	9	3.0000	4	4	1.2975	0.9578	-0.5057
Grand Total	**176**	**1.0337**	**154**	**1.0337**	**1009**	**157**	**27.9822**	**0.0000**	**0.0000**

Table 5C-3: Control: The Water Project - 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R - Cluster profile for cash-in nodes

	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 Cash-out								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	128	16.8750	77	16.7500	8	3	0.6097	0.0105	0.0058
1	2	0.8000	1	0.9000	10	3	0.7603	-0.0084	-0.0046
Grand Total	**128**	**7.9444**	**77**	**7.9444**	**18**	**6**	**0.7603**	**0.0000**	**0.0000**

Table 5C-4: WannaCry - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 - Cluster profile for cash-out nodes

	1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 Cash-out								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	3	1.8824	26	3.6765	34	30	4.3918	-0.0017	0.0066
1	2	1.8919	6	2.4865	37	35	3.8829	-0.0004	-0.0060
2	146	146.0000	63	63.0000	1	0	6.5223	0.0703	-0.0028
Grand Total	**146**	**3.8889**	**63**	**3.8889**	**72**	**65**	**6.5223**	**0.0000**	**0.0000**

Table 5C-5: CryptoDefense - 1EmLLj8peW292zR2VvumYPPa9wLcK4CPK1 - Cluster profile for cash-out nodes

	1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R Cash-out								
cluster_label	MAX of out_degree	AVERAGE of out_degree	MAX of in_degree	AVERAGE of in_degree	COUNTA of n.index	COUNTA of n.time_stamp	MAX of pagerank	AVERAGE of X_red_X	AVERAGE of X_red_Y
0	8	1.0636	140	1.7426	645	18	16.7197	0.1727	-0.2989
1	10	1.0030	143	0.8999	1648	60	17.5121	-0.2101	0.0850
2	153	1.6725	144	3.3391	516	39	16.4162	-0.2474	-0.2164
3	2	1.0278	1009	1.0801	936	1	129.9262	0.2516	-0.0564
4	6	1.0076	103	1.2740	1456	25	13.0283	0.1606	0.1845
5	3	0.9627	100	0.1285	1876	12	12.3953	-0.0569	-0.0274
Grand Total	**153**	**1.0509**	**1009**	**1.0509**	**7077**	**155**	**129.9262**	**0.0000**	**0.0000**

Table 5C-6: Control: The Water Project - 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R - Cluster profile for cash-out nodes

Chapter 6: Follow the Money: Revealing Risky Nodes in a Ransomware-Bitcoin Network

"*Go where the money is…and go there often*." – attributed to Willie Sutton.

6.1 Chapter Overview

This chapter continues the theme of discovering networked payment patterns that reveal a certain type of typology that is consistent across different ransomware-Bitcoin payments. However, it goes a step further by applying a risk-based approach to the nodes contained within these typologies. It does so by leveraging the techniques within this research using unsupervised machine learning to understand the context and influence certain nodes have. In particular, this chapter examines the cash-out network of the WannaCry ransomware attack, as attackers place a high level of importance on being able to move their collected ransom payments to other areas of a financial network to then effectively utilise these proceeds of crime for their benefit.

When applied to the ransomware "cash out" graph, the method derived "riskiness" scores for specific nodes. Analysing the derived "riskiness" at a community level (groups of nodes in the network) provides an enhanced aggregation for identifying and targeting influential nodes. In order to ascertain the community structure of the payment networks formed, along with a value of risk that a node assumes in a ransomware-Bitcoin network, the technical approach uses the notion of mathematical similarity applied to nodes embedded with values calculated in Chapter 5 to represent latent features in the ransomware-Bitcoin network. By deriving and associating a risk metric

at an individual node and at a community level of a cash-out network we are able to flag key nodes (Bitcoin addresses or transactions) that may be targets for disrupting or corrupting the utility of an attacker's proceeds of crime. Such insight could potentially support both intelligence and forensics investigations. The findings of this approach show that in isolation targeting identified "risky" nodes can be hit-or-miss. The attacker can easily adapt or even learn to deceive the analysis system by creating convoluted paths in their cash-out network, rendering the tagging of individual nodes as "risky" a futile effort. However, when a "risk community" was identified, a group of interconnected nodes can be targeted at once, proving more difficult for the attacker to avoid. Despite this, the complexity of the calculation and its implementation at any meaningful scale (for example millions of addresses and transactions) would prove difficult without a high performance computing capability, an adaptable analysis system to automatically recognise the community threat based on risk indicators, and a speedy response to validate and act in order to disrupt such risks.

6.2 Abstract

This paper demonstrates the use of network analysis to identify core nodes associated with ransomware attacks in cryptocurrency transaction networks. The method helps trace the cyber entities involved in cryptocurrency attacks and supports intelligence efforts to identify and disrupt cryptocurrency networks.

A data corpus is built by the unsupervised machine learning graph algorithm 'DeepWalk' (Perozzi et al, 2014). DeepWalk evaluates the position of nodes within networks. It compares the relative position of different nodes (similarity) and identifies those whose removal would most affect the network (riskiness). This method helps

identify on the blockchain the key nodes that are involved in the execution of a ransomware attack.

When applied to the ransomware "cash out" graph, the method derived "riskiness" scores for specific nodes. Analysing the derived "riskiness" at a community level (groups of nodes in the network) provides an enhanced granularity for identifying and targeting influential nodes. Such insight could potentially support both intelligence and forensics investigations.

6.3 Introduction

In 2019 over US$6.6 million was paid globally to cryptocurrency addresses related to ransomware, according to the 2020 Crypto Crime Report from blockchain analysis company Chainalysis (Chainalysis, 2020). This is emphasised by the fact that the United States Securities and Exchange Commission (US SEC) has seen over 1,000 documents submitted by companies between April 2019 and May 2020 that list ransomware as a critical risk factor to their businesses (Cimpanu, 2020). Companies face multi-million dollar outages such as those faced by the city of New Orleans in 2019. The city's Chief Administrative Officer, Gilbert Montaño, indicated that the ransomware attack will cost the city at least US$7 million (Sussman, 2020). There are plenty of opportunities for cyber criminals to cash out their booty. One of the most popular ways for ransomware attackers to do so between 2013 and 2016 was through the Russian based BTC-e exchange (Chainalysis, 2020).

Identifying the magnitude and location of illicit funds throughout the blockchain is no easy endeavour, the cryptocurrency investigation companies Elliptic and Chainalysis provide their own powerful proprietary software platforms to do this. However, there are some open-source tools and techniques that allow us to analyse this evolving threat to confront ransomware attacks.

Throughout this paper, network and graph will be used interchangeably as we explore the utility of graph analysis for cyber financial crime prevention. Out of the hundreds of thousands of Bitcoin transactions on a blockchain, the first challenge is to isolate the relevant Bitcoin nodes used in a ransomware attack. We will further show how graph analysis reveals patterns and provides the capability to expose nefarious relationships between the Bitcoin transactions and addresses in the ransomware-Bitcoin network. In addition, DeepWalk (Perozzi et al, 2014) embeddings provide a machine-learning technique for graphs that sets up feature extraction from the ransomware-Bitcoin cash-out network. These features can be used in a similarity analysis that is based on Cosine Similarity to identify the risk posed by the removal of a node from the Bitcoin-ransomware cash-out network. We will apply the Cosine Similarity calculation comparing nodes with the ransomware seed address to isolate individuals and communities of risky nodes. Furthermore, our target network dataset can be enriched with contextual labels derived from other open source blockchain analysis tools setting up future research with more advanced machine learning prediction techniques.

6.4 Fighting financial crime with graph analysis

Tracing illicit flows of money through a network requires techniques that reveal patterns and provide the capability to expose nefarious relationships across vast amounts of data. The trails left behind by these financial flows provide a web of transactions interconnected by accounts and services to obfuscate identity on purpose by blending seamlessly into the economic system. In traditional banking, the transactions, accounts and services form a network and can be modelled as a graph. For example, De Marzi (2019) uses credit card fraud as a case study, modelling where credit card holders make legitimate transactions at different services and in another graph showing where fraud actors with stolen credit card data test the stolen credit card numbers. By modelling this fraud scenario as a graph, it helps identify patterns where the credit card data may have been stolen or where stolen credit card data is being tested at certain services.

Voutila (2020) uses the PaySim mobile money network financial dataset originally posited by Lopez-Rojas et al (2016). The graph model created contains transactions, merchants, clients and client identifiers in order to filter a large set of activity and perform graph analysis, such as weakly connected components, to identify fraud rings within the larger graph. Components, nodes, in a graph are said to be weakly connected if they are all connected or reachable from any other node in the same graph. Galler and Fischer (1964), first revealed this algorithm and it has been used to understand how well connected networks are, how clusters of activity form and how well the network remains connected when nodes of certain authority are eliminated.

Furthermore, the case for revealing money laundering has an even stronger emphasis today. Anti-Money Laundering laws, regulation and compliance such as, The Anti-money Laundering and Counter-terrorism Financing Act 2006 (Cth) in Australia (Reeves and Wilcock, 2019) and the 5th Anti-Money Laundering Directive of the European Union (European Union, 2018b) provide a legislative framework for the prevention and detection of money laundering and terrorism financing. However, detecting money laundering networks still proves extremely difficult as seen in the 2017 royal commission into the Australian banking, superannuation, and financial services industry, where over 200 money laundering compliance failures were revealed with one bank alone (Hayne, 2019; Frost, 2018). Data and Analytics firm Dun and Bradstreet put this difficulty down to the scale and complexity of the data that needs to be analysed to find the nefarious relationships within the financial transactions. As a firm they are using graph technology to meet the Anti-Money Laundering standards previously mentioned (Flood, 2020).

Whilst graph analysis has become an established tool for identifying and fighting financial fraud in the traditional economy, a question remains as to the utility of the method in the emerging space of cryptocurrencies, especially Bitcoin, which is the cryptocurrency of choice for most ransomware attacks today. Bitcoin uses Bitcoin addresses as a banking client would use their bank account number. Bitcoin value is sent and received between addresses via transactions. There are many Bitcoin addresses that make up a Bitcoin wallet. It is not uncommon for wallet users to create a new Bitcoin address for every new transaction to help preserve their anonymity (Miles, 2020). The full balance of a Bitcoin address needs to be spent during a transaction and as such change addresses are often found, where the balance of the transaction is paid

back to the originating Bitcoin address. Spotting irregular Bitcoin activity and unusual connections occurring in the blockchain at scale proves extremely difficult without the aid of graph visualization tools (Miles, 2020). These reveal patterns and anomalies in intuitive and interactive ways. Therefore, the graphs derived for ransomware-Bitcoin behaviour provide a powerful analysis capability which leverages the Bitcoin ecosystem to build the scope of the ransomware-Bitcoin target network.

6.5 The Ransomware-Bitcoin target network

In line with Clark and Mitchell's target centric approach, we begin the intelligence process by defining a generic target model to guide intelligence collection and analysis (Clark and Mitchell, 2016). The generic Target Network Model (TNM) for our ransomware-Bitcoin target network is represented by Figure 6.1.

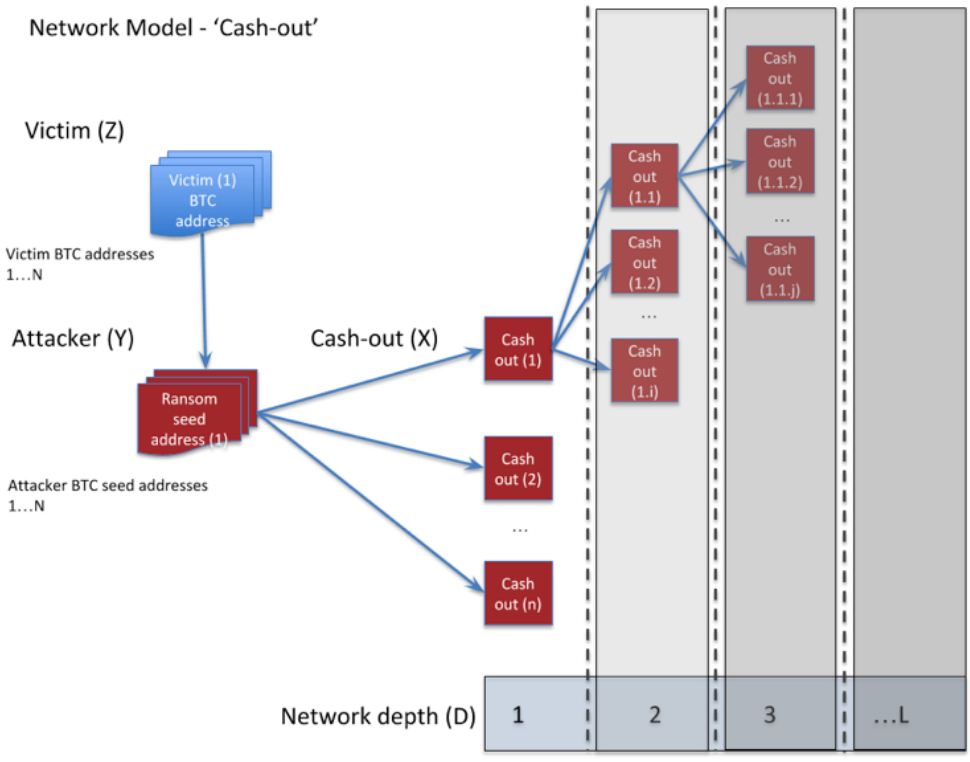


Figure 6.1: Ransomware - Bitcoin Target Network Model ('Cash-out').

Figure 6.1 shows the representation of Bitcoin addresses and transactions at different levels of a target network in a model of a ransomware campaign. Due to the size and complexity of the overall ransomware campaign network the TNM is split between cash-in and cash-out models. Figure 6.1 only shows the cash-out side of the network. The cash-out network models the proceeds of crime as they flow from the ransomware seed address that victims of the ransomware attack have paid into to other addresses in the Bitcoin universe. These ransom payments ultimately exit the network where they are exchanged for other cryptocurrencies or even fiat currency.

In order to demonstrate the method, we will collect data related to the cash-out network of the ransomware campaign, WannaCry 2.0 and populate the generic target model. This campaign was chosen because the findings from our network investigation can be validated against other sources. The next section will identify the data collection requirements and methods used and introduce the analysis system being applied to the populated TNM.

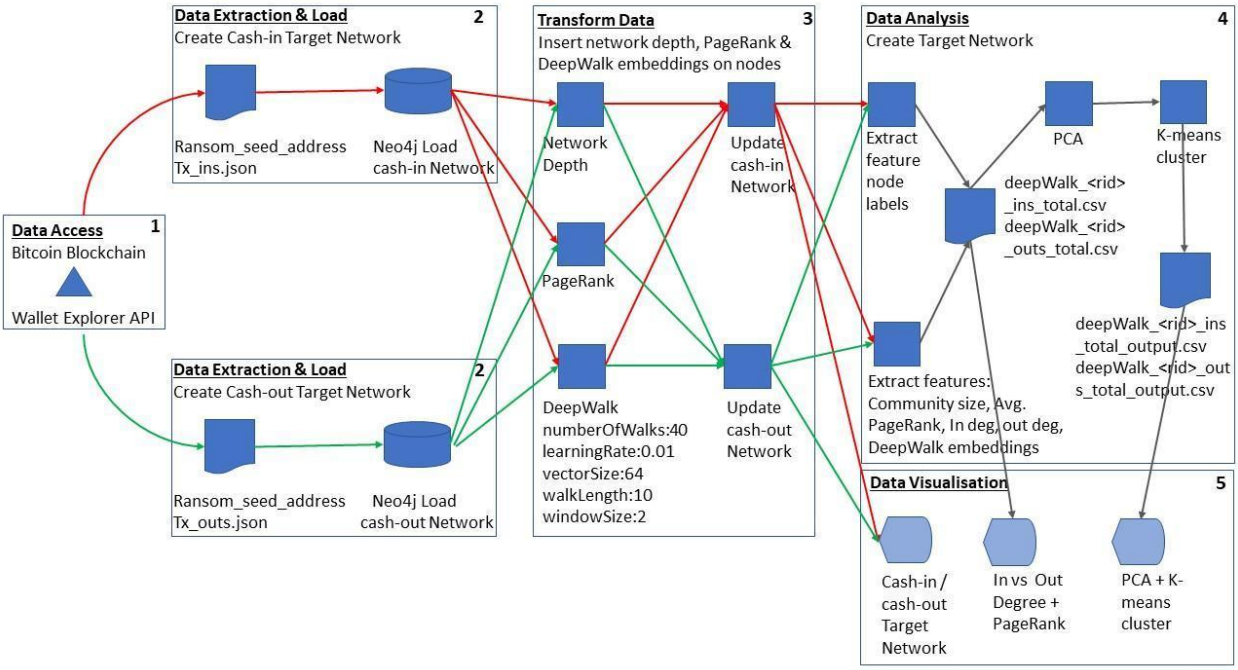


Figure 6.2: Ransomware-Bitcoin Graph Analysis System.

6.6 Data Collection

The Bitcoin blockchain contains the record of addresses and transactions involved in Bitcoin transactions. This ‘on-chain’ data along with the respective meta-data can be exploited.

Figure 6.2 shows a data pipeline with associated analysis techniques that are used to exploit Bitcoin blockchain data.

Step one – Extract data from the Bitcoin blockchain

- Extract transaction history relating to the ransom seed address from the walletexplorer.com Application Programming Interface (API).
- For each incoming and outgoing transaction from the seed address, build the input and output graphs respectively at ‘D’ levels deep away from the seed address (see Figure 6.1).

Step two – Load data into graph database (Neo4j)

- Load extracted input and output graph files setting input/output addresses as nodes; transactions as nodes; and Payments as a relationship between them.
- Post process address nodes to include corresponding depth ‘D’ of transaction nodes.

Step three – Transform data

- Run the PageRank algorithm and add this as a property on the nodes in the network.
- Run the DeepWalk algorithm on nodes and embed the results onto the nodes in the network

Step four – Data analysis preparation

- Run Louvain community detection algorithm using average in/out degree and PageRank. Aggregate results of communities.
- Run community detection and return non-aggregated results, returning all nodes in the network with the respective in/out degree, PageRank, DeepWalk embeddings, labels, depth, timestamp. Export to Comma Separated Values (CSV).
- These network analysis algorithms were run from within the Neo4j graph database

Step five – Data visualisation

- Import the CSV into python script to:
- Visualise community detection profile
- Python was used to perform Principal Components Analysis (PCA) + K-means clustering on DeepWalk embeddings
- Output results to CSV for deep dive analysis into comparing communities and clusters across different ransomware by using Cosine Similarity.

The key transformation of the data we will focus on in this publication relates to the graph embeddings derived in steps three and four. The graph embeddings will become features for future graph machine learning applications. The PCA undertaken in step five is essential for managing the dimensionality of the embedding computations. It is key to the analysis to examine specific nodes and determine how influential they are within the Bitcoin-ransomware network. This would serve as an indicator of their relative importance in the transfer and circulation of ransom payments. For this reason, the PageRank algorithm was chosen as an appropriate centrality measure for this purpose. The subsequent sections elaborate on the proposed methodology.

6.7 Risky node analysis

The blockchain data should yield a network of wallets and transactions involved in the WannaCry ransomware attack, but the network data on its own does not provide sufficient context to identify the key nodes that are involved in the process. We propose to approximate the significance of each node in the network by measuring the effect the

node's removal would have on the viability and function of the network. We conceptualise this effect as risk to the network, and the measurement involved as a measure of riskiness. Using the DeepWalk graph embeddings that encode the structure of a graph at each node relative to its position in the target network (see Figure 6.1), we can leverage these embeddings as features into a Cosine Similarity calculation which provides an index of how 'risky' the nodes are relative to the ransomware Bitcoin seed address. Furthermore, analysing the risky nodes collectively forms target communities which could prove more effective as opposed to targeting these nodes individually.

6.7.1 Graph embeddings and features

Once the TNM has been created and populated with the extracted data, the graph itself becomes very large and dense making it difficult to detect any unusual behaviour at face value. There needs to be a simplified way of preserving the graph properties like the structure and the features on the nodes and edges (Tong, 2019). This is achieved by the graph embedding algorithm that transforms all the information learned from a graph into a lower dimensional vector space representation. The graph embedding algorithm chosen for this analysis is DeepWalk by Perozzi et al (2014).

DeepWalk learns structural representations of a graph's nodes by capturing its similarity in a neighbourhood of other nodes and allocating individual nodes to cliques we call communities (Perozzi et al, 2014). By taking a graph as an input to the algorithm, latent representations are produced as an output. These representations become the input to a neural network. Operating a neural network on a graph structure allows for deep feature learning of nodes and edges for a graph (Rossi et al, 2017).

DeepWalk uses deep learning for unsupervised feature learning, which means, the system learns the node's embeddings without any prior knowledge of the graph topology. Depending on what nodes are encountered and how often they are traversed during a random walk, the neural network makes a prediction about a node feature or classification and embeds that into the node as metadata. By sampling the graph via random walks, we build the data corpus for that graph. The data corpus is then used as the reference library for a node's purpose within the graph. For example, in the ransomware-Bitcoin TNM the ransomware seed address can be taken and its "context" predicted within the scope of the entire graph. This means embedding an understanding of a node's features, such as, transaction amount, connectivity to other nodes (how many input and output transactions there are from a node) and structural role (e.g. the root node of the network or a leaf of a weakly connected branch). Having these embeddings encoded into a node provides a basis for subsequent generalisation through various possible means. In this case, we chose the PCA and K-means clustering analysis (see Figure 6.2) to reduce the dimensionality of the embeddings. PCA as a method of reducing large datasets whilst preserving as much information, or statistical variability, from the original data (Jolliffe and Cadima, 2016). In this case we were able to reduce the relevant dimensionality from 128 down to a two-dimensional vector space. This two-dimensional representation of the graph embeddings will now be used in the next section as input into a similarity analysis to ascertain which nodes in the TNM are riskier than others.

6.7.2 Concept of Similarity

Cosine Similarity is a measure used to identify how similar entities, or in this case nodes in a network, are irrespective of their magnitude (Han et al, 2012). In this case, the graph analysed by the DeepWalk algorithm is reduced to a series of variables which incorporate latent features of a node's community structure as an output for use in calculating the similarity between the vector representations of these features.

Seeing as the theory of this process has its roots in natural language processing, we use the analogy of finding meaning and context (similarity) in a text. The process allows us to analyse the similarity in words' meanings, while ignoring the words' location in the text.

The procedure we are proposing would be equivalent to having a graph (the document), containing many random walks (sentences) from each of the nodes (words) in the graph. Ultimately arriving at a meaningful similarity of a node's context with respect to the other nodes in the graph. An illustration of this can be seen in Figure 6.3.

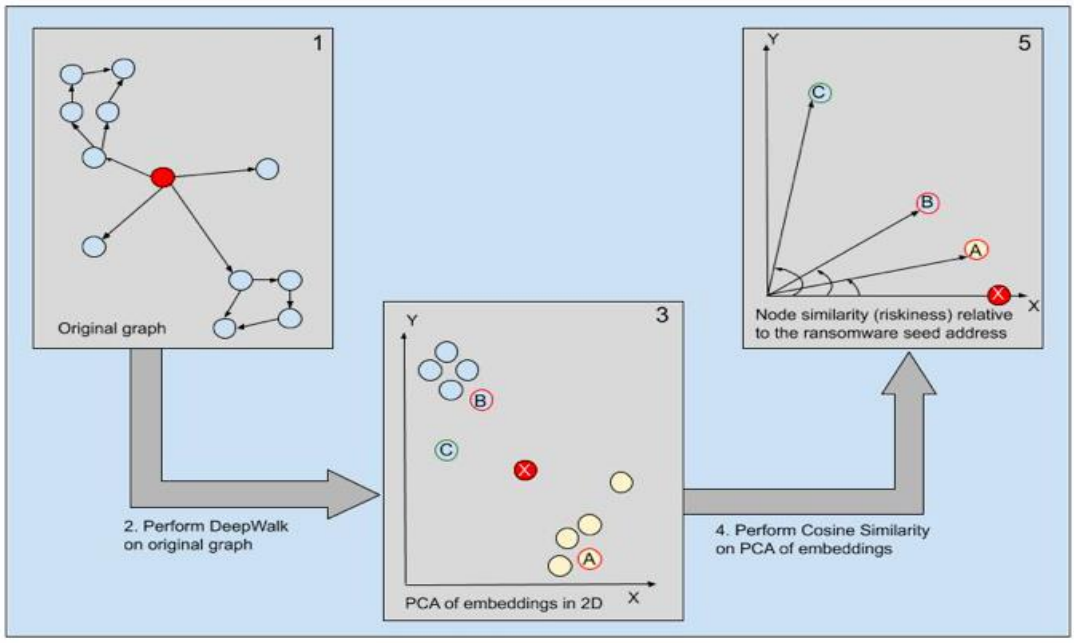


Figure 6.3: Conceptual view of arriving at a measure of riskiness in the ransomware-Bitcoin graph.

6.7.3 Application

Instead of measuring the distance between two nodes, Cosine Similarity measures the cosine of the angle between them. Cosine similarity is superior to a simple measure of distance in identifying the common features of disparate nodes. Plotting the distribution of the cosine similarity, box labelled 5 in Figure 6.3, assert that there are close similarities between nodes not purely related to the latent features derived from the DeepWalk embeddings. By taking the cosine similarity of these features we are not only considering the proximity of a node to the ransomware seed address, rather the context of the node in the whole graph being analysed. This can be seen Figure 6.3, box labelled 3, where node C is in close proximity to the ransomware seed address X, however in Figure 6.3, box labelled 5, the angle between C and X is larger than the angle between A and X, where A is more distant from the ransomware seed address in box labelled 3.

There could be several reasons for this. The number of nodes directly connected to nodes C and A, or closely connected in the neighbourhood (two or three hops away). Additionally, how many times the particular node occurs in context to other nodes in the generated corpus of the entire graph relative to the ransomware bitcoin seed address in the network. For example, in the cash-out graph for WannaCry ransomware Bitcoin seed address, 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, in Figure 6.4 a node, 1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM, with a high similarity relative to the ransom seed address resides at a Bitcoin exchange Poloniex.com. This was identified as one of the cash-out exchanges used by the attackers in WannaCry (Bistarelli et al 2018).

Therefore, it follows that similarity scores relative to the ransom seed address might usefully serve as a proxy measure for riskiness. The higher the similarity calculated for a node with respect to the ransom seed address, the higher the risk score for that node. For example, if a high-risk scoring node was removed from the network the attackers would be unable to cash out their proceeds of crime. Therefore, risk used in this context refers to the risk imposed on the attacker fulfilling the objectives of the network.

6.7.4 Similarity as a measure of risk

Similarity can therefore be used as a proxy for riskiness. Using the mathematical calculation of Cosine Similarity, a proxy measure for riskiness is established relative to the ransomware seed address. Taking the ransomware seed address as the most significant node on a ransomware-Bitcoin cash-out network (because if there was no seed address created, there would be no ransom collected), then using the graph

embeddings to computationally calculate the similarity of every other node relative to this node we are able to derive a risk score.

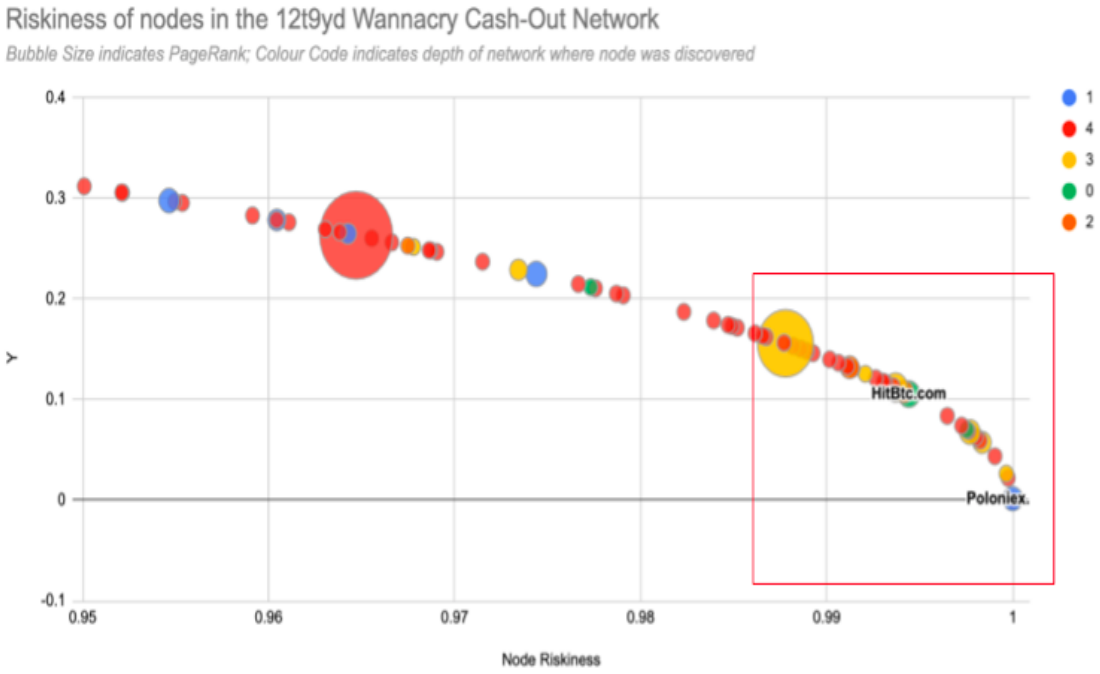


Figure 6.4: Distribution of node similarity for WannaCry Ransomware seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw* cash-out network. Top 20% of nodes by risk score.

As a result of this analysis a similarity matrix is produced that can be used as a heatmap to target the risky nodes in the network. If another node in the ransomware cash-out network scores a high ‘similarity’ relative to the ransomware seed address, and if that highly scored node is removed from the network this node is the next critical to the network fulfilling its objective of cashing out the ransom collected. This would allow for the targeting of nodes with the high similarity scores and hence if we target or neutralise this node, it puts the network’s objectives “at risk”. For example, using a

classification range the heatmap could be represented as follows: ‘Very High’ for risk scores ranging from 0.95 to 1, shaded in red; ‘High’ from 0.75 to 0.95, shaded in Orange-Red; ‘Medium’ from 0.5 to 0.75, Yellow-Orange; ‘Low’ from 0 to 0.5, Green-Yellow. Applying this concept to the Wannacry cash-out network produces the following results in Table 6.1.

ID	Node (Address / Transaction)	Community	Risk Score
1	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	1	1
2	1LZ9WozeiHEQWE3JQbikGHLXa6qiKLXJjN	4	0.9999999066
3	1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM	1	0.9999987018
4	1EqmnkqcN9MQzPLH8zVMGeJwicENe9PQhz	4	0.999752307
5	19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6	3	0.999649391
6	1D3U69XBgqpvHwU5q6U2237AWWnGyFUVz7	4	0.9990430646
7	340b44c7a7857e36f81b2e8ba713911ea93e82afde6ea5590df1a35688845d16	3	0.9983512281
8	1BmnfremSpD7GBySqi4mqvz3Pc1JiVQvoG	4	0.9982444506
9	178NdniKXphgQifBKcuxbTQyU1ro42k3LP	4	0.9980235722
10	1FN5JaTm1EdMjou9Rydu4htvRHXDHK8Hzr	4	0.9977387825
11	1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR	3	0.9977009081
12	1P9MofjYUCquw5AzhdHT4uQsf2hrNuqojL	4	0.9976210255
13	1697wz4hwVXNqNa7WaAVyLQ8UAdLP3JyNA	0	0.9975391621
14	1Ph8BFiuxPWS22V24qBcdDMkLu5oq8vCqE	4	0.9972508058
15	1HY8jUGFg6DwE3fHEwVFViHjZLQwLwV4Tj	4	0.9964831496
16	1Dha5e1jbTtu4YGALQ3DnfTAk5yxzm4XSR	0	0.9944175344
17	1b2a3333f583ae54dba78ccc71f4fe24a22acd0991d364e75bcf099ce3a84759	2	0.9941592119
18	131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3	3	0.9937028227
19	193C6ArL53dZ5k3wSSe8a4FjVx56Drir74	4	0.9935641946
20	1ANeJQbuuDxBATkWRaHL378EczzbA1zUyu	4	0.9931619272

Table 6.1: Top 20 by risk score for nodes in the WannaCry Ransomware seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw cash-out network.

Figure 6.4 shows the distribution of the risk scores and the respective node index (address or transaction) for the WannaCry cash-out graph. In this figure we concentrate on those nodes with riskiness ranging from 0.95 to 1, representing the top 20% of nodes by risk score. On the x-axis, node riskiness is represented by a score from 0 to 1 across the entire network dataset. Where a score closer to ‘0’ shows little similarity relative to the ransomware seed address and can be interpreted as a node in the network that

exhibits little risk when it comes to facilitating the cash-out of ransom collected. On the other hand, those scores closer to '1', show a similarity or closeness to the ransomware seed address. The actual riskiness should be viewed from both the X & Y measures as it is the cosine of the coordinate point of one node relative to the ransomware seed address which is always at position (1,0). Because the analysis is normalised the radius (or arc in this case) will not exceed a radius of 1 as it moves from (1,0) to (0,1). This calculation removes the emphasis on magnitude of the vectors and measures the angle between two nodes showing a relative importance to the network no matter how many levels deep in the network we move away from the ransomware seed address.

The ransomware seed address, 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, sits at position Y=0 and X=1 on the chart and the next closest node 1LZ9WozeiHEQWE3JQbikGHLXa6qiKLXJjN represents an address that has a node riskiness of 0.9999 (see table 1) and is therefore deemed critical to the movement of funds out of the ransomware seed address. The second most risky node with risk score = 0.9999987018 is another Bitcoin address 1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM. This is an address directly linked to the Poloniex.com exchange where the WannaCry attackers cashed out their proceeds of crime (Bistarelli et al, 2018).

Looking into why these nodes are deemed risky in the context of this research, we could determine the Bitcoin address, 1LZ9WozeiHEQWE3JQbikGHLXa6qiKLXJjN, to be a false positive in our detection system as it seems to be part of a bigger cluster of nodes, centred around the transaction (ID:

29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27) contributing a small amount of Bitcoin (0.0034398 BTC) taking place on 31st August 2017 at 16:32:00 UTC. Considering the WannaCry campaign cashed out on the 3rd August 2017 from the ransomware seed address (Neutrino, 2017), this has greatly exceeded the campaign time window and targeting this particular node might provide little impact on the risk of the network fulfilling the objectives. However, some forensic analysis might be warranted. This address is one out of 236 other addresses taking part in peeling activity which ultimately outputs to an address (1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe) linked to another exchange, HitBTC.com which could be targeted for investigation for playing a part in soliciting illegal ransomware money flows (Neutrino, 2017). As previously mentioned for the next risky node, 1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM, it has a direct link to the exchange Poloniex.com. This can be interpreted as a true positive result from the analysis system shown in Figure 6.2. Looking at the detail behind this address, it directly receives 17 BTC, the full amount of ransom collected from the WannaCry campaign on the 3rd August 2017 at 10:04:51 UTC. The same time a twitter bot known as @actual_ransom identified the first outflows from the WannaCry attackers' wallets. This bot was set up by journalist Keith Collins to monitor activity of the WannaCry ransom addresses (Turner et al, 2019).

6.7.5 Risk in communities

To complement the derivation of the risk score is the identification of additional data that has been extracted from the walletexplorer API and collected as part of the analysis system depicted in Figure 6.2. This takes the form of 'labels', 'PageRank' and

‘community’. The labels nominate what service the node belongs to and provide a strong indicator for the attribution of real world identification into the Bitcoin ecosystem. In Figure 6.4 we can see HitBTC and Polinex on two of the highly ranked nodes (1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM and 1Dha5e1jbTtu4YGALQ3DnfTAk5yxzm4XSR) indicating these could be cash-out exchanges used by the attackers. In addition, PageRank is represented by the size of the bubble in Figure 6.4 and defines node influence in a network based on the frequency of its connections to other nodes (Needham and Hodler, 2019). That is the larger the bubble in Figure 6.4, the larger the PageRank and the larger the influence of the node in the network.

It is interesting to observe the node position relative to PageRank and the risk score. The second largest page ranked nodes, 1ArG3JwEbF4WrCiEnXQXUAgQumAVzqnQHD [PageRank=20.493] is used as a change address during the WannaCry campaign on 4th August 2017 and subsequently linked to the largest page ranked node which is a transaction, 29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27 [PageRank=40.4775] occurring on 31st August 2017 having over 230 inputs with an output connected to an address (1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe) controlled by exchange HitBTC.com. Despite these intricate connections these nodes only yield a risk score of 0.987784659211026 and 0.964703062973474 respectively and are positioned well outside the top 20 risky nodes identified in Table 6.1. Therefore, in this instance, little correlation can be derived between the risk score and page rank. However, using the combination of risk score on individual nodes and community

detection it is possible to augment decision intelligence on what areas of the graph to monitor and investigate. This is illustrated in Figure 6.5.

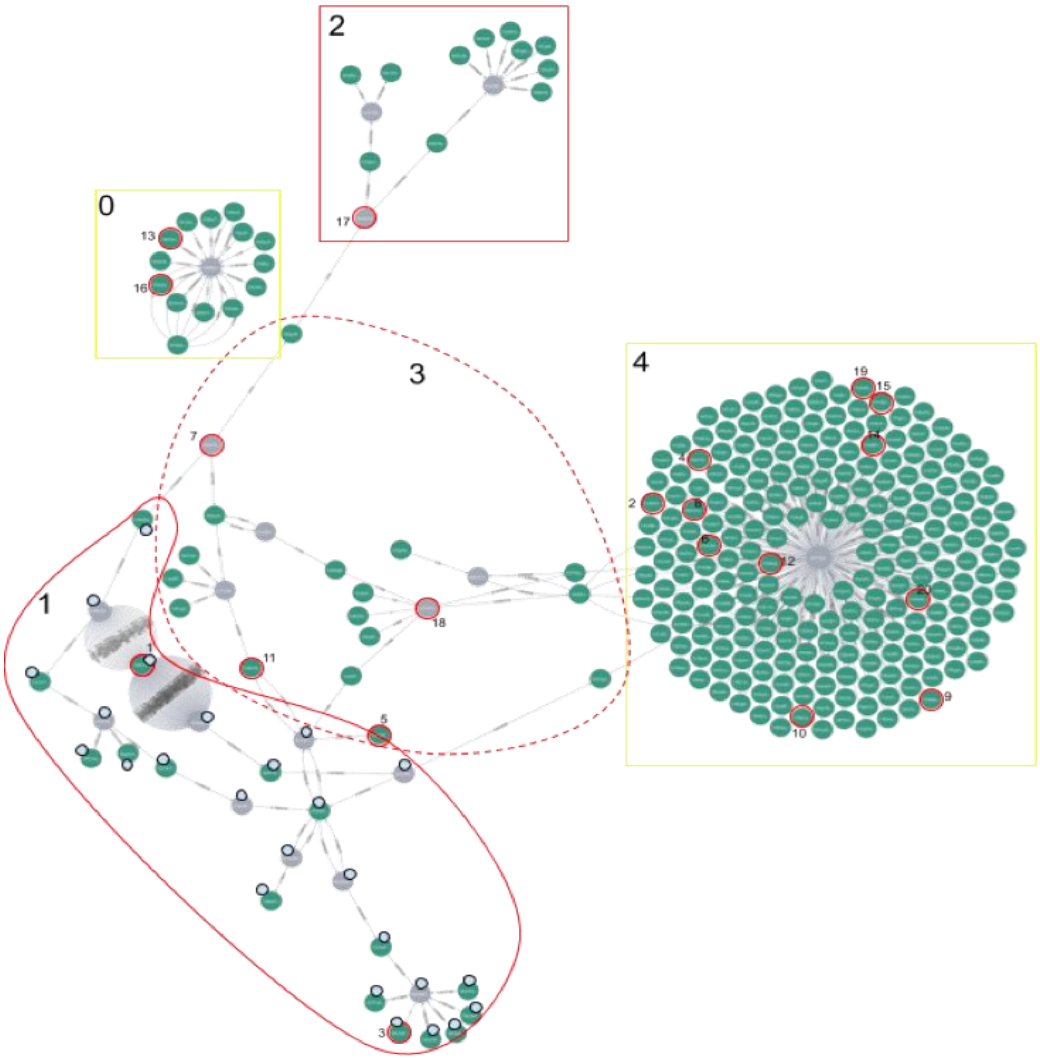


Figure 6.5: Graph representation of the WannaCry Ransomware seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw* cash-out network

Community detection is another common fraud detection technique used on networks to identify communities of nodes exhibiting anomalous behaviour that can be targeted for investigation (Hodler, 2020). Attributing a risk score to these communities on the aggregate we can determine which communities pose the greatest risk to the successful fulfilment of the network objectives. Table 6.2 demonstrates this.

Community	Node Count	Avg. Riskiness	Median Riskiness	Avg. PageRank
0	15	0.568214791	0.5539839493	0.3471999825
1	25	0.7281286781	0.7821614957	0.3968711842
2	14	0.7220384599	0.866469264	0.384656545
3	21	0.7797696805	0.8503920419	2.629416667
4	224	0.623651481	0.6648694238	0.3300336552
Grand Total	**299**	**0.6451774993**	**0.7116752424**	**0.5005359857**

Table 6.2: Median risk score grouped by community for nodes in the WannaCry Ransomware seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw cash-out network.

By using the median riskiness for the communities, it is possible to see how high the middle score is in the ordered set of risk scores for that community. The higher that middle score the higher the concentration of risky nodes to go after. This can be further validated via the graph visualisation in Figure 6.5. The nodes highlighted by the red circles indicate the top 20 risky nodes from Table 6.1 and the groups of nodes encircled by the shapes highlight the communities of nodes from Table 6.2.

It can be seen from Table 6.2 and Figure 6.5 that communities two and three share the highest community risk scores. Community three contains four of the top 20 risky nodes and visually plays a very central role in the facilitation of cashing out the proceeds of the WannaCry ransom. Node number 7 is a transaction within community three, 340b44c7a7857e36f81b2e8ba713911ea93e82afde6ea5590df1a35688845d16, that handles 8.715 BTC of the collected ransom and routes 6.877 BTC through community three on 3rd August 2017 and a further 1.8376 BTC splits off into community two. Community three acts as a mixing community to obfuscate this portion of the ransom with the transaction at node 18

(131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3) combining the ransom cash-out with four other inputs to produce an output of 32 BTC on the 4th August 2018 to HitBTC.com owned address 1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe. A considerable sized transaction heading to an exchange that would certainly raise suspicion. An interesting observation on community two is that even though it has a high community risk score it only contains one of the top 20 risky nodes, a transaction 1b2a3333f583ae54dba78ccc71f4fe24a22acd0991d364e75bcf099ce3a84759, ranked 17th in Table 6.1, occurring on 3rd August 2017 which facilitates 1.8376 BTC of the cash-out for the WannaCry ransom via one input address and two output addresses. This is where the combination of the risk score and community detection provides further targeted analysis. If we were only to go on the list of risky nodes in Table 6.1 the investigator could spend their time looking at community four where 11 of the nodes reside. However, examining the collective reveals the median riskiness of that community is only 0.66 (see Table 6.2). Community four is also the largest community by membership and the relevance of the risk score dispels the myth that a more populated community would produce a higher concentration of risky nodes.

6.7.6 Targeted disruption

Now that there is a way of identifying risky nodes in the ransomware-Bitcoin network, intervention can be considered to target these nodes and disrupt or eliminate them. Looking at Figure 6.6 which is a replication of Figure 6.5. with one of the risky nodes, transaction

131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3, node 18, removed.

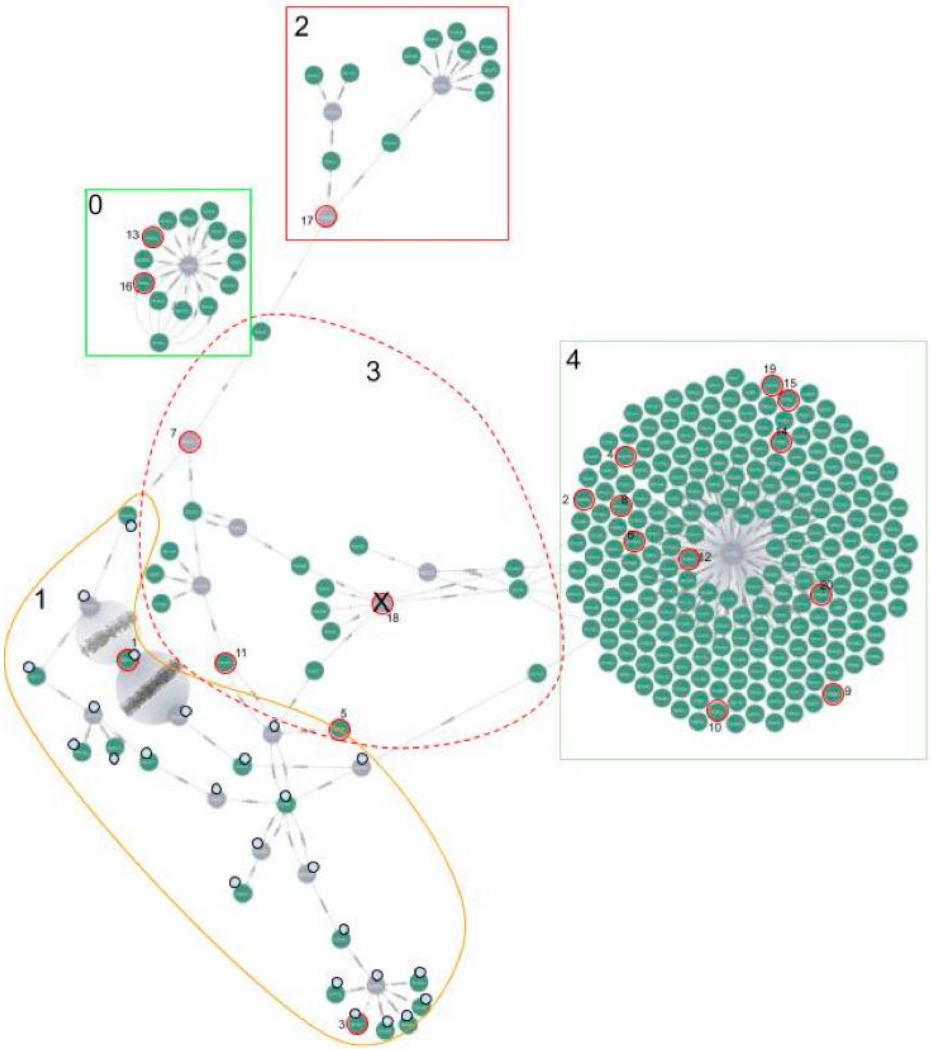


Figure 6.6: Graph representation of the WannaCry Ransomware seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw cash-out network, disrupting node 18.

At first glance this looks like a good tactic, severing the transaction at node 18 will inhibit the ability of the attackers to continue cashing out their proceeds of crime. However, the practical implications of doing this are not so simple. Node 18 represents a transaction with ID 131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3, the

details of this transaction can be seen in Figure 6.7. If it were possible to disrupt this transaction, there would be significant impact to the attackers fulfilling their objectives. Tracing the amount from the ransomware seed address, this transaction receives 5.1309 BTC of the ransom from address 1HQiNjBRrHZpuyaWYXnCMhwcvJPqF5e97M. This amount is combined with inputs from four other addresses to send a total of 32.02476446 BTC to address 1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe which belongs to exchange HitBtc.com.

Figure 6.7: Transaction details for transaction ID: *131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3* (screenshot courtesy of walletexplorer.com)

It would take significant effort, knowledge and real time action to be able to disrupt this transaction. This would have to be done in near real time by corrupting the transaction script by hacking at the Bitcoin software as was the case when Mt Gox destroyed 2,609 BTC (Sedgewick, 2019). Alternatively, fictitious addresses can be simultaneously generated with their public and private keys, at the time of the transaction, to receive payments and sign the Bitcoin over to the next owner in the chain and divert the ransom funds away from being exchanged at HitBtc.com (Ducklin, 2018).

6.8 Limitations

The concept of the similarity analysis and the application to a ransomware-Bitcoin cash out network was only applied to one of the WannaCry 2.0 ransomware seed addresses (12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw). The analysis system is highly dependent on the quality of graph embeddings produced by the DeepWalk algorithm. Whilst preserving the structure of the nodes of the graph in relation to each other, the embedding algorithm used in this analysis was still only in development and not released in the Neo4j (graph database) production library for graph data science. Therefore, at this stage, validating the quality of the embeddings is difficult. In addition, using the output of the DeepWalk algorithm as input features to the cosine similarity score, the risk rating or recommendation on which nodes to attack in the network for intervention in illicit money flows has a dependency on knowing the ransomware seed address. Nevertheless, the system can still be used to initiate responses based on the 'riskiness' score obtained from the cosine similarity calculation and auto classify existing and new nodes coming into the network. To be effective in this manner the operation would need to be done in near or real-time. For example, we see the cash-out activity for the 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw ransomware seed address during the WannaCry campaign all happen within the space of six hours. The initial transactions out from the ransomware seed address, (409803bb5e124fd028c0482027c7722e84ce55b78204b279d3a44aba5e7c1698 and 35e5d5fe8c8128cfa6884f56be5817e4138c58c91b79d78d3e78a8d365b9d8a7), began at 03/08/2017 04:28:20 UTC. The transaction (36ef488e59d719fb906254aed61bfe46e8f64778bc6cac97e56a68c241004c28) that facilitated a cash out at the exchange Poloniex.com occurred at 03/08/2017 10:04:51 UTC.

6.9 Future Research

Considering the most targeted pieces of information revealed from the similarity analysis are the identity of the address node and its risk score. There remain gaps in the available identity information from the raw data. Nonetheless, several features could be used in further machine learning techniques to predict the nature of nodes. A prediction algorithm could be built that would identify, for example, probable exchange services or other types of categories such as whether a node is involved in ransomware or not. This would allow analysts and investigators to estimate the location and ultimate owner of the address in the Bitcoin network removing significant barriers to the anonymity afforded to nefarious actors using cryptocurrencies. This would be an enormous improvement given the magnitude of the gap in the raw data. For example, in the data on the cash-out graph for WannaCry ransom seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw only 3 out of the 280 addresses are labelled with exchange services (approx. 1%). Table 6.3 highlights Poloniex.com and HitBtc.com as the most prominent exchanges used when cashing out the ransomware proceeds.

n.label	n.index
"HitBtc.com"	"1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe"
"HitBtc.com"	"1Dha5e1jbTtu4YGALQ3DnfTAk5yxzm4XSR"
"Poloniex.com"	"1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM"

Table 6.3: Available labels on the 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw WannaCry ransom seed address.

Building a prediction engine at scale to assist attribution of anomalous nodes in the network is outside the scope of this research paper. However, the data collected from the analysis system paves the way for future research in this area. As an example, cryptocurrency forensic analysis firm Elliptic and researchers at IBM and Massachusetts Institute of Technology (MIT) have released a public data set of around 200,000 transactions partially labelled with illicit or non-illicit flags to identify suspicious transactions on the blockchain within the context of Anti-money Laundering (AML) (Weber et al, 2019).

Understanding a graph in the past helps create a baseline for what to look for in the future. In order to understand how a current scenario relates to that baseline it is important to know what has changed and what hasn't. This helps detect any anomalies, or unusual patterns, within the dynamic nature of a Bitcoin blockchain graph. More sophisticated algorithms such as, Microcluster-Based Detector of Anomalies in Edge Streams (MIDAS), are able to detect dynamic behaviours in graphs (Mishra, 2018). This lends itself well to the Bitcoin - blockchain environment as the graphs formed here are constantly being updated with new addresses and transactions. In addition, when it comes to discovering ransomware graphs in such an environment micro cluster detection helps detect sudden bursts of activity on nodes or edges, which are common to the behaviours of both the cash in and cash out graphs in ransomware / Bitcoin activity (Bhatia et al, 2019).

6.10 Conclusion

This research paper concludes that to target nodes of a ransomware-Bitcoin payment network for disruption it is imperative to understand their risk in the sampled network. This paper derives a mechanism to measure this risk. It draws insights into using machine learning techniques combined with human interpretation to identify nefarious nodes in the WannaCry ransomware-Bitcoin cash-out network. The focus of this paper has been on using the Cosine Similarity calculation on DeepWalk embeddings to define a risk index that identifies what nodes, if eliminated from the network, carry the greatest risk to the attacker achieving their objectives, i.e. cashing out collected ransom payments. Using the Cosine Similarity as a risk index on an individual basis may not yield a targeted disruption of the network objectives. However, when the risk index was taken in combination with community detection a more powerful analysis emerged to isolate risky sections of the network. In particular, the practices of graph embedding and principal component analysis provide a truly reusable set of features for future machine learning applications. Furthermore, finding mechanisms to estimate the identities of nodes on the network will help attribute nodes with a particular Bitcoin service. However, limitations are evident with these techniques having only used a data set relating to the WannaCry ransomware-Bitcoin cash-out network. One broader benefit to the research community would be to open source multiple ransomware-Bitcoin network data sets for validation of analysis techniques.

Significantly, the entire approach remains predicated on identifying the ransomware seed address to build the target network.

6.11 Signal and Noise

This chapter detailed the utility of the graph embedding technique applied to a ransomware-Bitcoin cash-out graph. Graph embeddings using the DeepWalk algorithm provide a set of downstream features to be utilised by other machine learning techniques; in the case of this research, a Cosine similarity measure was calculated for each node on the WannaCry cash-out network. This measure was then used as a proxy for a node's risk score relative to the ransomware seed address and the node's influence in the cash-out network.

Whilst the method aimed to target individual influential nodes in a network for investigation, analysis, and possible disruption, it was the collective communities of nodes and their aggregate risk scores that proved to be the most compelling for analysis. By targeting high risk communities, it could be possible to immobilise complete sections of the network.

As statistician Nate Silver notes, "distinguishing the signal from the noise requires both scientific knowledge and self-knowledge" (Silver, 2012, p. 453). Ultimately, it is possible to ascertain some analytical signal out of the existing data from the ransomware-Bitcoin network; however, it is important to reflect on the need to augment expert knowledge in order to interpret the significance of what the data is telling us. As such, this research has developed an analysis system for future research and development. Significant data analysis has been an output due to this process. Silver (2012) provides conviction for establishing such a process and stipulates that "*sometimes the only solution when the data is very noisy* [as is the case with cryptocurrency data]—*is to focus more on process than on results*" (Silver, p. 327,

2012). Appendix C represents the yield of the data analysis conducted as part of Chapters 5 and 6. Furthermore, this has been made available on the bitcoin-network-data Harvard Dataverse repository[28] for researchers to openly access and reference for any future research and analysis into the domain of ransomware-Bitcoin payments.

This chapter has revealed a technical system for ransomware-Bitcoin payment analysis. Multiple data analyses are an output of this system with a particular focus on revealing risk inherent in the WannaCry ransomware-Bitcoin cash-out network. The next chapter builds on graph embedding techniques, taking the concepts derived from this chapter another step further by deriving a reusable data engineering pipeline to feed a prediction model with features that characterise ransomware-Bitcoin transactions.

[28] https://dataverse.harvard.edu/dataverse/bitcoin-network-data

Chapter 7: Classifying Ransomware-Bitcoin Nodes Using Graph Embeddings

"*It's just enough glitter amongst the chicken-feed*." - George Smiley (Le Carré, 2002).

7.1 Abstract

With the recent proliferation of ransomware attacks law enforcement agencies have been trying to find methods to systematically identify ransomware transactions within cryptocurrency payment networks (Paquet-Clouston, et al, 2019). This research seeks to develop a methodology to identify such transactions through data-driven tracking and analysis of Bitcoin payment networks. We demonstrate the methodology by applying the GraphSAGE embedding algorithm to the WannaCry ransomware-Bitcoin cash-out network for the ransomware-Bitcoin seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*. The paper takes a data-driven approach to building a machine learning system that allows analysts to define features relevant to ransomware-Bitcoin payment networks. In addition, we define an auxiliary feature, *exposure*, to describe the amount of exposure nodes on this network have to the facilitation of ransomware payments. We use the exposure feature in combination with other Bitcoin payment network features, including graph algorithms such as pageRank, to determine a set of graph embeddings that can be used to predict the classification of ransomware network nodes. We perform tests on a dataset of 299 Bitcoin nodes and derive three distinct clusters. We also evaluate the performance of the clustering method on a dataset of 59 nodes. Our proposed method achieves 80% of true-positive predictions. Further, examining the False Positives (FPs) and False Negatives (FNs)

created greater analytical insight for investigators due to their anomalous nature. We also explore how our proposed method can be leveraged by law enforcement authorities to investigate and curb suspicious activities such as money-laundering and ransomware payments via Bitcoin.

7.2 Introduction

The union of a computer intrusion via malware and cryptocurrency has enabled ransomware as we know it today. With this harmonious partnership, a cybercrime is undertaken that can be considered a tool of destruction through computer exploitation and also a financial crime through the illicit monetization by means of cryptocurrency (Turner et al, 2019). Across the main cryptocurrencies -- Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH) and Tether (USDT) -- approximately US$20 million of ransom was paid by victims in 2016, and in 2020 this almost reached US$350 million, a 311% increase from 2019 (Chainalysis, 2021a). In 2019 and 2020 the dominant ransomware strain was Ryuk, which yielded around US$200 million in ransom payments (Chainalysisa, 2021).

Cryptocurrency network data has often been overlooked by law enforcement agencies who address the threat of ransomware, yet as we show below, analysis of cryptocurrency logs can support law enforcement and security agencies by revealing critical information about the relevant criminal behaviour.

Turner et al (2020b), proposed an experimental graph machine learning system using the DeepWalk algorithm (Perozzi et al, 2018). It used a sample of the WannaCry ransomware-Bitcoin cash-out network. Data related to the ransomware-Bitcoin seed

address[29] was curated from the Bitcoin blockchain and then engineered into a Neo4j graph database. The DeepWalk algorithm belongs to a family of graph algorithms that yield embeddings based on latent features inherent in a particular graph. Further developing the concepts from Turner et al (2020b), we look at another graph embedding algorithm known as GraphSAGE (Hamilton et al, 2017). GraphSAGE takes a different approach to learning the structure of a network. Whereas the DeepWalk algorithm uses a transductive approach, GraphSAGE uses an inductive approach to better understand unseen data being revealed in the network. Hamilton et al, (2017), posit this in their paper which defines the GraphSAGE algorithm. "*By using an inductive framework that leverages node feature information (e.g., text attributes) to efficiently generate node embeddings for previously unseen data. Instead of training individual embeddings for each node, we learn a function that generates embeddings by sampling and aggregating features from a node's local neighborhood*." (Hamilton et al, 2017).

This research uses a number of software tools. The walletexplorer.com Application Programming Interface (API) serves to extract the Bitcoin network data in JavaScript Object Notation (JSON) format to build the target network. The Neo4j graph database community edition with the Graph Data Science (GDS) application library runs the respective graph algorithms. Cypher code, the Neo4j standard programming language, is developed to build the ransomware-Bitcoin graph and enrich it with the graph algorithms set forth in this paper. Finally, the Python programming language runs further machine learning procedures on the graph embeddings coming from the Neo4j

[29] Ransomware-Bitcoin address: *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*

GraphSage implementation. The code and data files are available on GitHub for further development.[30]

The analysis that follows seeks to demonstrate what can be inferred from cryptocurrency payment networks created by a ransomware attack. Specifically, we examine the ransomware WannaCry by using big data and machine learning techniques to define different clusters, and predict what cluster a Bitcoin node belongs to. As an example, this cluster could be representative of certain Bitcoin addresses or transactions belonging to certain exchanges or services that are frequented by illicit users of Bitcoin. This paper outlines the fundamental Bitcoin data model and how the ransomware-Bitcoin problem can be broken down into a target network. In addition, it details changes to the system first defined in Turner et al, (Turner et al, 2021) by enriching the network with features used by the GraphSage embedding algorithm. Furthermore, by leveraging the vast amounts of data present on the Bitcoin blockchain, this paper demonstrates the utility of the graph embeddings in a downstream machine learning prediction algorithm along with the introduction of an exposure metric for each node's exposure to the activity on the network. Following this, a brief recourse is made as to why graph machine learning is becoming a pivotal capability when analysing cryptocurrency networks and why embeddings provide the analyst with the greatest insight. In Sections 7.5, 7.6 and 7.7, the paper critically evaluates and validates the results produced with this method from the perspective of law enforcement and suggests directions for future research. We conclude this paper in Section 7.8.

[30] https://github.com/AdamT23/bitcoin-seed-extract

7.3 Background

7.3.1 Ransomware-Bitcoin data modelling

Cryptocurrency is built on blockchain technology. This technology, as the name suggests, works by providing blocks of transactions (packets of data), linked to other transactions that are propagated through a peer-to-peer network in order to move a store of value from a source to destination address (Reyna et al, 2018). In doing so a network[31] of transactions is formed which represents a Directed Acyclic Graph (DAG)[32]. The ransomware-Bitcoin payment activity can be represented as a graph. Splitting the network into a cash-in (ransom payments received) network, and a cash-out (payments moved by the attacker) network, creates two distinct graphs. These graphs connect at a collector address identified as the ransomware-Bitcoin seed address shown in Figure 7.1. The figure represents a generic scheme that forms an intelligence Target Network Model (TNM). This scheme can be used to structure the analysis of concrete instances of blockchain to identify and characterise ransomware transactions.

This research focuses on collecting data for the cash-out network in WannaCry for ransomware-Bitcoin seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*[33].

[31] Throughout this paper, graph and network will be used interchangeably.

[32] Directed Acyclic Graph (DAG) - For a DAG there exists at least one node with zero in-degree and at least one node with zero out-degree (Thulasiraman and Swamy, 2011).

[33] https://www.blockchain.com/cs/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

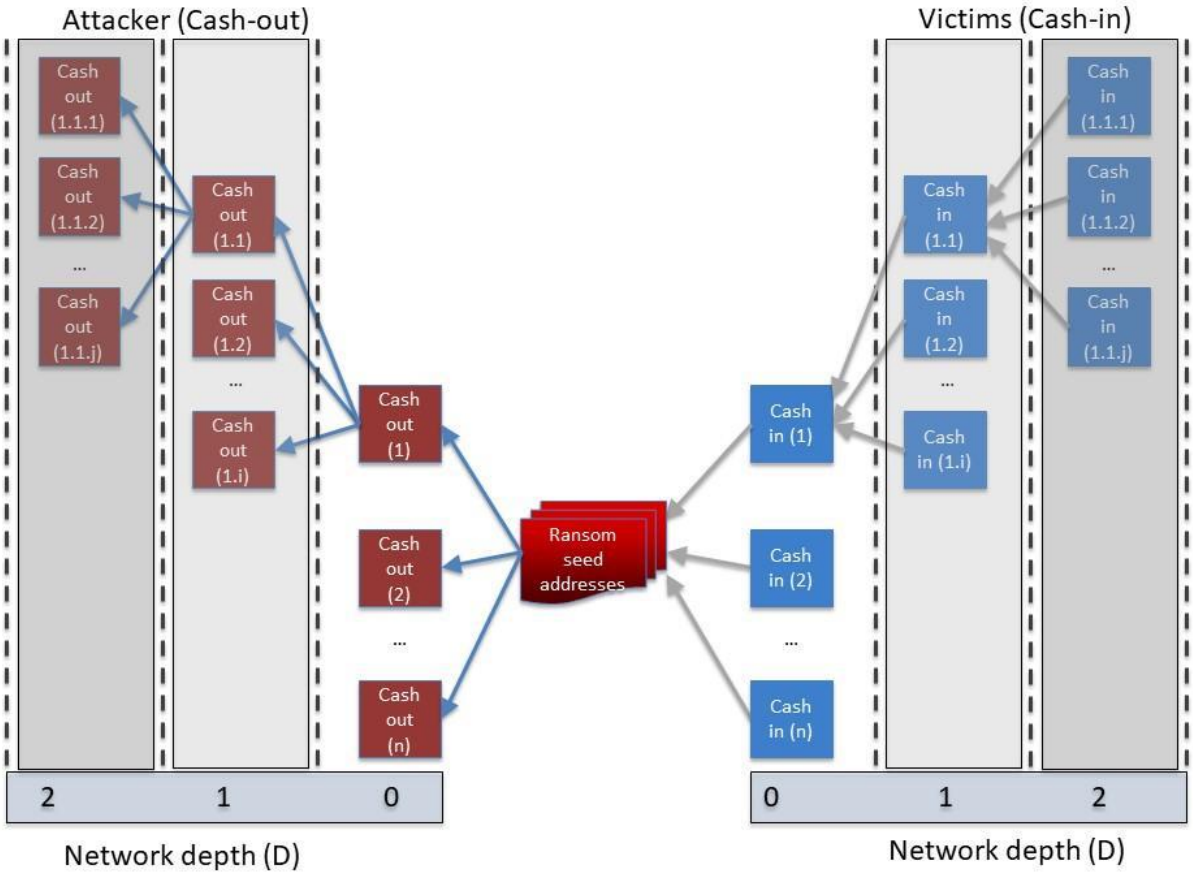


Figure 7.1: Ransomware-Bitcoin Target Network Model (TNM).

Figure 7.1 shows the representation of Bitcoin addresses and transactions at different levels of a specific target network in the WannaCry ransomware campaign. The cash-out network, in red, models the attacker's movement of their ransomware revenue from the ransomware seed address out to other areas of the Bitcoin ecosystem. It is possible that these ransom payments ultimately exit the network where they are exchanged for other cryptocurrencies or fiat currency. Using techniques that allow the graph to be enriched with the analytical properties of the network provides further context to the patterns of behaviour that are represented in the graph. Furthermore, these properties can formulate feature sets for machine learning models to enable future prediction based on the topological structure and their distribution in the network neighbourhood.

7.3.2 A brief look at the Bitcoin blockchain structure

The block is the main structure for transactions in Bitcoin as seen in Figure 7.2.

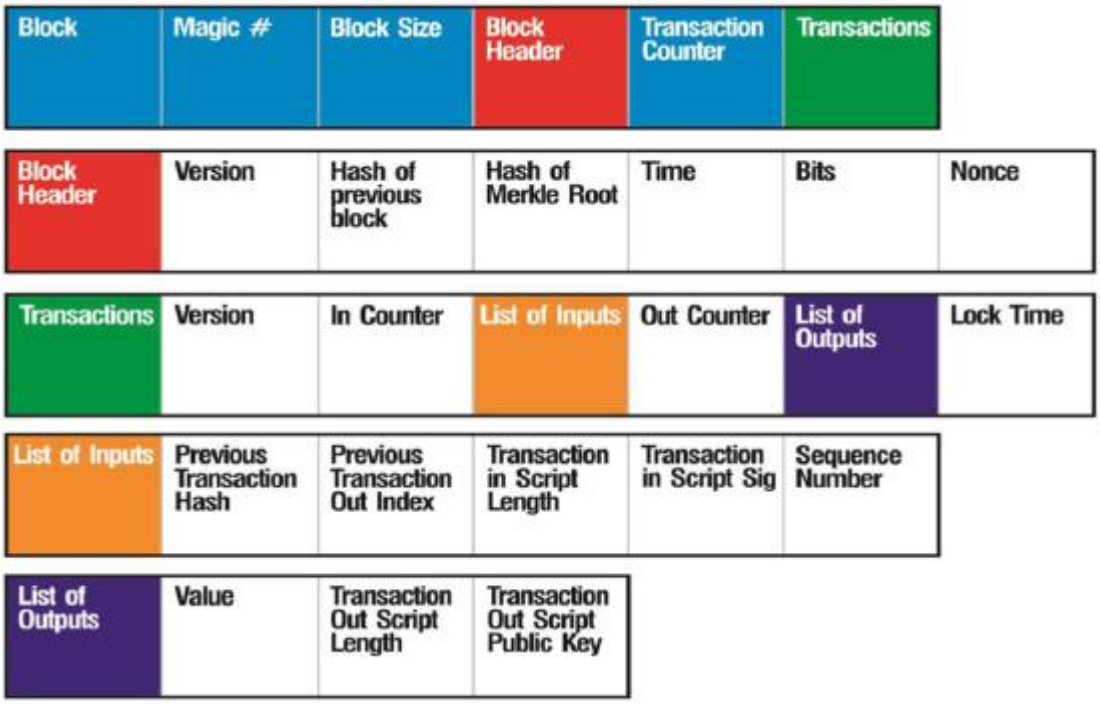


Figure 7.2: The Bitcoin blockchain structure (Source: Turner and Irwin (2018)).

The blockchain structure includes a public record of all transactions. A Bitcoin transaction maintains a list of inputs, with an index to unspent transactions and the associated signature (Transaction in script sig, in Figure 7.2), and outputs, which contains the receiving address and value to transfer along with other key data in the block header such as transaction timestamp. We will use data extracted from the blockchain structure to construct the graph data model. The next section will show how these data are collected and used to classify and predict nodes on a ransomware-Bitcoin cash-out network.

7.4 Proposed System

The following subsections outline a proposed system for collecting, engineering, modelling, and training data collected from a ransomware-Bitcoin cash-out payment network. This model can then be used for evaluating unseen data to predict the classification of a transaction to belong to certain nefarious clusters in the network. Ultimately, the system is designed to maintain a feature catalogue with the goal of testing different ransomware payment networks with different feature sets from the catalogue.

7.4.1 Data collection and machine learning pipeline

Working with the TNM in Figure 7.1, it is now possible to set up the data extraction and pipeline to derive the data model, features and embeddings needed to predict the classification of nodes on a ransomware-Bitcoin cash-out network. Figure 7.3 outlines the steps taken in this research to arrive at a predicted cluster label.

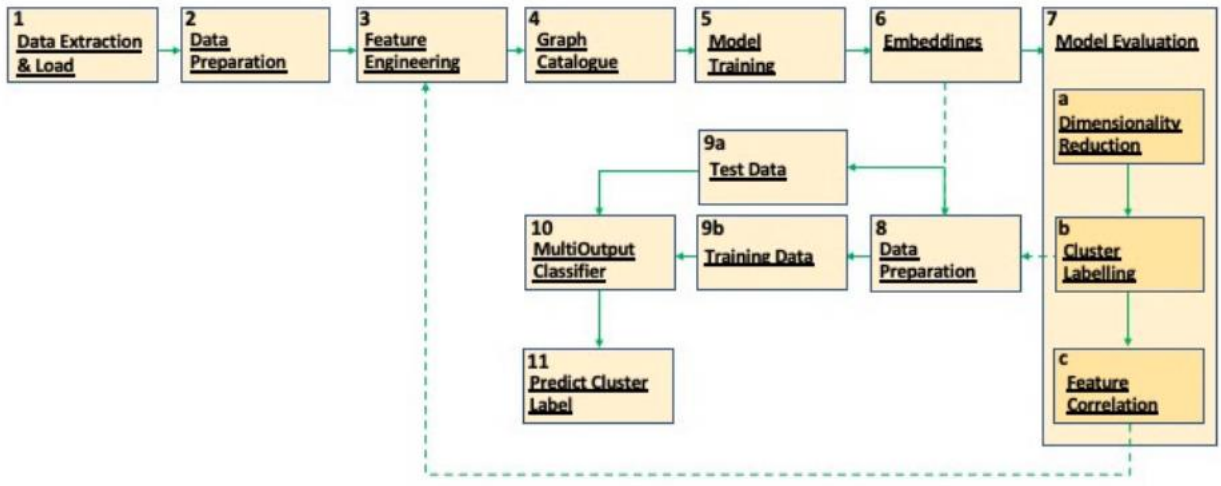


Figure 7.3: System representation of the graph machine learning pipeline for cluster label prediction.

Step one in Figure 7.3, forms the lifeblood of the system by defining the data extract and load procedure. By loading the raw blockchain data into the Neo4j graph database we preserve the graph structure. Bitcoin addresses and transactions are represented as

nodes while the relationship between addresses and transactions are represented as edges in the graph. This model is visualised in Figure 7.4, identifying the basic properties required to form the standard ransomware-Bitcoin graph data model.

We used the Application Programming Interface (API) offered by walletexplorer.com to extract the data. This research is focused on the cash-out network, formed by the ransomware-Bitcoin seed addresses -- *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*. This address is used as the data collection focal point. The extraction script produces a JavaScript Object Notation (JSON) file so as the network structure and hierarchy are preserved. Below we describe the components of the system in Figure 7.3, starting with the standard ransomware-Bitcoin graph data model, which further details the data preparation step and flows into step three – feature engineering.

7.4.2 The standard ransomware-Bitcoin data model

The extracted data are modelled to reflect the blockchain structure depicted in Figure 7.4. The graph data model is created using Neo4j and consists of a green node labelled '*output*' which represents a Bitcoin address, a grey node labelled '*tx*' which represents a Bitcoin transaction and the '*PAYS*' relationship which refers to payments being sent and received between addresses. This model links the list of transaction inputs to the list of transaction outputs which move the amounts paid to certain addresses throughout the Bitcoin network. The semantics between the '*output*' and '*tx*' nodes is many to many. That is, there can be many '*PAYS*' relationships forming inputs to a transaction and many '*PAYS*' relationships forming outputs from a transaction.

Figure 7.4: Standard graph data model of a Bitcoin transaction in Neo4j.

The model in Figure 7.5 demonstrates that these transactions can be linked to the same or a different Bitcoin address in the network.

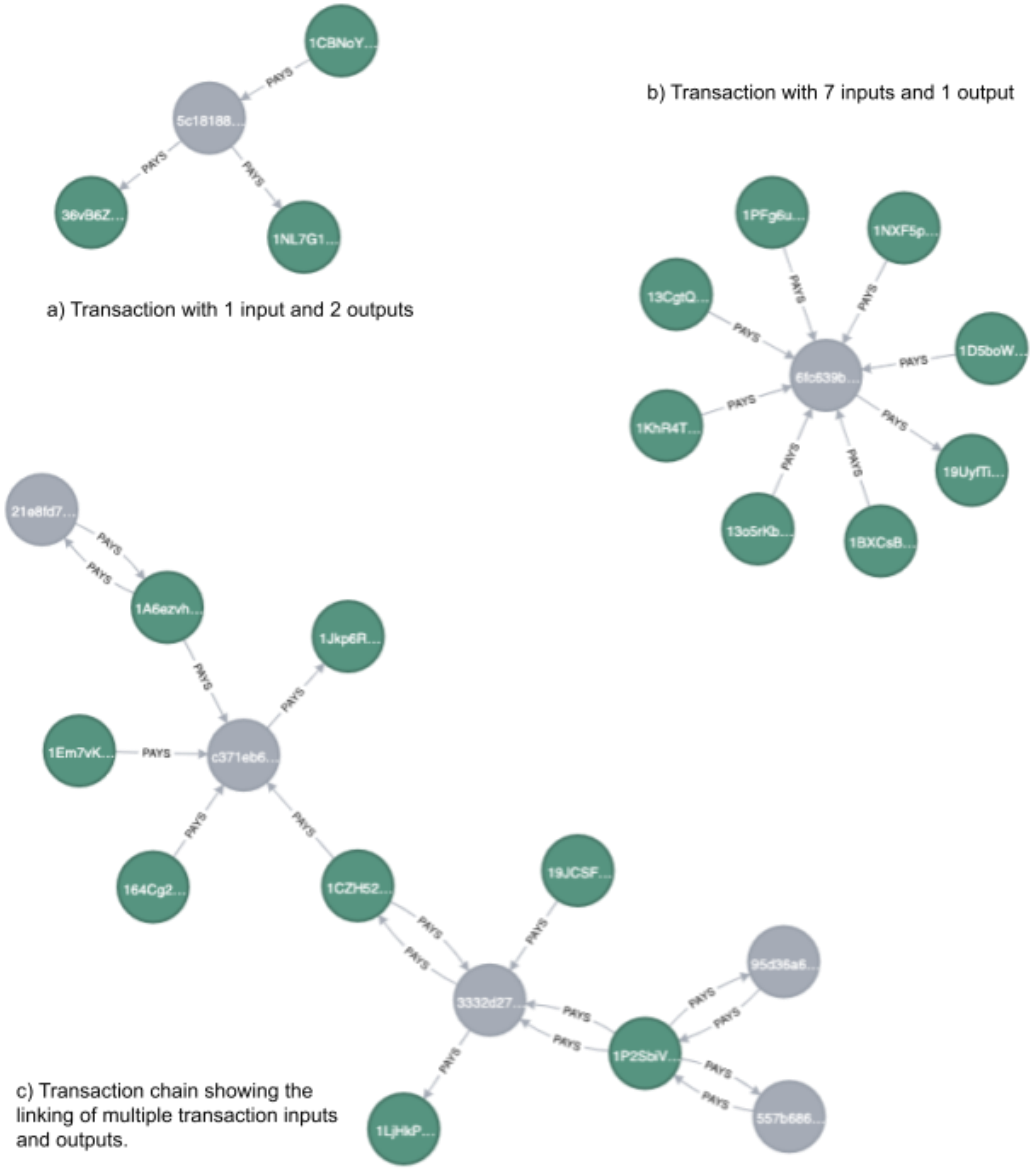


Figure 7.5: Data model in practice for WannaCry ransomware-Bitcoin cash-out network properties of the standard graph data model. 5a) Transaction with 1 input and 2 outputs; 5b) Transaction with 7 inputs and 1 output; 5c) Transaction chain showing the linking of multiple transaction inputs and outputs.

As part of the standard graph data model the following properties in Table 7.1 are inherited from the blockchain data extraction.

Node / Relationship	Graph Metric	Definition
PAYS	next_tx	This property refers to a transaction id that is part of the list of input and output transactions that constitute a transaction. There is one PAYS relationship for each input and output transaction.
PAYS	amount	The amount spent by the individual input or output transaction (next_tx).
PAYS	time_stamp	The timestamp of the transaction.
TX	index	Transaction ID linking the inputs and outputs to the address of the recipient of any money paid.
OUTPUT	index	Bitcoin address that receives payments from transactions.

Table 7.1: Properties evident on the standard graph data model.

These are the raw properties from the Bitcoin blockchain loaded into the standard graph data model. Already at this preliminary stage we can identify structures that conform to one of three suspicious structures that have been identified by Jobse (2017). Specifically, these structures are: Long Chains, similar to Figure 7.5 c); Fork-Merger Patterns, also evident in Figure 7.5 c); and Self Loops and Binary Tree-Like distributions, similar to Figure 7.5 a) (Jobse, 2017).

These properties alone are sufficient to generate preliminary insight into how ransomware money flows through the Bitcoin ecosystem. However, in what follows we seek to reveal additional features of a ransomware-Bitcoin network and leverage these features for graph machine learning classification and prediction tasks.

7.4.3 Graph Machine Learning

Data science applied to graphs is a combination of graph statistics, graph analytical methods and graph-enhanced Machine Learning (ML) (Needham and Hodler, 2021). Having enhanced the standard ransomware-Bitcoin graph data model and derived the standard properties of this particular graph from steps one and two (see Figure 7.3), we now turn to triggering the graph machine learning components of the system. This will guide the data pipeline into the analysis system and produce graph embeddings as an output in order to be used as the basis of the cluster classification. Feature engineering is a process in the machine learning system which creates features representative of the input data that will feed the embedding algorithm (Lakshmanan et al, 2020). Selecting features that will provide the most salient information and more accurately inform the prediction model is a balance between selecting via experience, through subject matter expertise, and scientific process. The feedback loop from step 7c, '*Feature Correlation*' to step three, '*Feature Engineering*', aims to integrate that experience and allows for the adjustment of the feature set in order to refine what is deemed to impact the understanding of the graph being analysed. The next sections will walk through steps three to seven from Figure 7.3 (Feature Engineering, Graph Catalogue, Model Training, Embeddings and Model Evaluation), and explain why these steps are important for analysing the ransomware-Bitcoin cash-out graph.

7.4.4 Feature engineering - Enriching the network

Enriching the standard graph data model, from Figure 7.4, requires significant post-processing of the graph. The techniques use the Graph Data Science (GDS) library[34]

[34] https://neo4j.com/docs/graph-data-science

for Neo4j and rely on the centrality algorithms PageRank and Degree Centrality, along with GraphSage embeddings and a node exposure metric defined as part of this research. The centrality measures and node exposure metric provide an enhanced set of feature properties for the GraphSage algorithm to calculate meaningful embeddings from the ransomware-Bitcoin graph. This is in line with the approach presented by Gaihre, et al (2019) at the 2019 IEEE Conference on Communications and Network Security (CNS), whose paper outlines traditional graph features and how they are exploited for machine learning purposes such as classification.

For this research, PageRank is chosen to evaluate the importance of nodes within a network (Page and Brin, 1999). PageRank is particularly appropriate because of the variety of graph structures formed through the transfer and circulation of ransom payments in a ransomware-Bitcoin network. By measuring the number of incoming and outgoing relationships a node has it is possible to estimate how important that node is relative to other nodes in the network. That is, nodes exhibiting higher connectivity, those having more incoming and outgoing connections, are deemed a higher quality (higher PageRanked) node to target for investigation. (Page and Brin, 1999; cf Needhamd and Hodler, 2019 on the use of this measure in financial fraud investigations).

In addition, in-degree and out-degree, at each node are used to calculate exposure. The exposure calculation borrows the concept of risk exposure from insurance pricing techniques (Bertsimas and Orfanoudaki, 2021). It is a function of the frequency and magnitude of payments being made through a node. We use the term exposure as this measure reveals a given node's behaviour on the network. That is the proportion of the

sum of the in-degree and out-degree at that node, with respect to the total degrees across the entire sampled network multiplied by the severity of these payments, or total amount of Bitcoin moving through that node. In essence, those nodes with a greater exposure on the network are the most active and could be targeted for deeper investigation by law enforcement. This can be represented by using the degree sum formula in graph theory. In equation (A), we find the total sum of the degrees at each node (also known as a vertex) in the ransomware-Bitcoin graph vertex set V. This is also equivalent to twice the number of edges, E, or 'PAYS' relationships, in the ransomware-Bitcoin graph.

$$\textbf{A)}\ \sum_{v \epsilon V} \deg v = 2|E|$$

In addition, the sum of the number of in-degrees and out-degrees at each node is represented by:

$$\textbf{B)}\ \deg v = \deg^{-} v + \deg^{+} v$$

Then the total amount of Bitcoin moving through each node can be represented by:

C) total_amount v

Thus, forming the exposure equation for each node in the ransomware-Bitcoin network as:

Exposure at a node = (B ÷ A) × C

The ransomware-Bitcoin cash-out graph has now been enriched with selected features based on graph analytics algorithms and derived properties that reveal relevant context of the network. This then leads to the enhanced list of properties in the next section, detailed in Table 7.2.

Thus, data for WannaCry cash-out graph using ransomware-Bitcoin seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*, yields a total sum of the degrees of 876, which means there are 438 'PAYS' relationships, across the sampled network.

7.4.5 Enhanced data model

Enrichment of the graph is established with the properties in Table 2. From this it is possible to identify the top 10 nodes of interest in descending order, for the WannaCry ransomware-Bitcoin cash-out graph, depicted in Appendix 7A by the Tables 7A-1 to 7A-4. These tables describe what nodes are significant in the WannaCry ransomware-Bitcoin cash-out graph, given the features of the newly enriched ransomware-Bitcoin graph.

Node	**Graph Metric**	**Definition**
TX/OUTPUT	index	Transaction ID linking the inputs and outputs to the address of the recipient of any money paid. Bitcoin address (output) that receives payments from transactions.
TX/OUTPUT	total_amount	The total amount of Bitcoin (BTC) passing through a node.
TX/OUTPUT	exposure (programmed as risk_rating)	The proportion of the sum of in and out 'PAYS' relationships (degrees) at a node to the total number of 'PAYS' relationships in the network. Multiplied by the total amount passing through the node.
TX/OUTPUT	out_degree	The number of outgoing 'PAYS' relationships from a node.
TX/OUTPUT	in_degree	The number of incoming 'PAYS' relationships from a node.
TX/OUTPUT	depth	The number of hops away from the ransomware-Bitcoin seed address.
TX/OUTPUT	pageRank	A Centrality algorithm used to measure the importance of a node in the graph. It considers the incoming relationships and the pageRank measures of directly connected nodes.
TX	time_stamp	Transaction ID linking the inputs and outputs to the address of the recipient of any money paid.
OUTPUT	label	Text identifier from the walletexplorer.com API indicating if a node has any affiliation with a Bitcoin service such as an exchange.

Table 7.2: Additional properties on the enriched graph data model.

The results recorded on the properties shown in Tables 7A-1 to 7A-4 provide insight when analysed independently of each graph metric. For example, observing transaction

id, *29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27*, across the different metrics, we confirm that this node is important to the ransomware-Bitcoin cash-out network for WannaCry ransomware seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*. The analysis shows it has the top pageRank in the network, 41.9379236, the most number of combined in-degrees and out-degrees on the network, 238, and the sixth highest exposure rating, 0.434599737. However, the total amount of BTC passing through this node only ranks 42nd highest in the network at 1.5996192 BTC. The exposure calculation is effective in reweighting the importance of the node in the network with respect to the total amount of BTC moving through it. The rebalancing of the node's position in the top 10 highlights the interconnectedness of the enriched properties on the ransomware-Bitcoin graph. Whereas one node in isolation may provide a rich set of properties for law enforcement and the intelligence community to use for investigation and disruption, it is often the collective communities of nodes and what salient information can be extracted from the community and conveyed in the most concise way. As shown in Figure 7.6, once the *29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27* transaction node, the grey node at the centre of Figure 7.6, is expanded a cluster of addresses appear and the analysis quickly becomes complex.

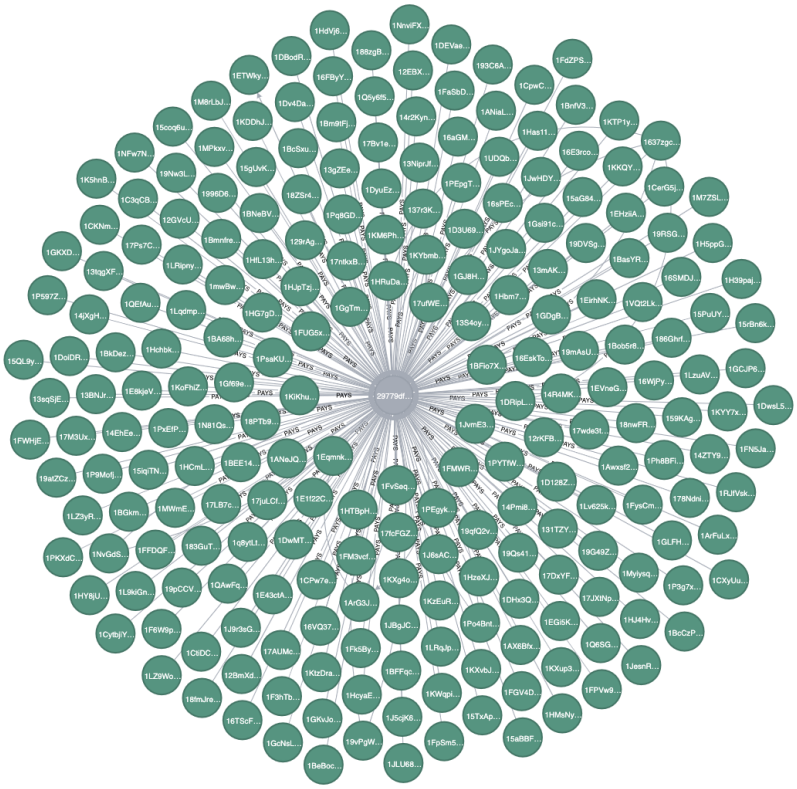


Figure 7.6: WannaCry ransomware-Bitcoin cash-out network, transaction id, 29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27[35] and the 238 connected addresses.

Collectively using the input data associated with the enriched properties listed in Table 7.2 creates a feature extraction process for preserving the relevant information required for a model to learn essential patterns in the data (Lakshmanan et al, 2020). For example, predicting communities or clusters to which transactions and addresses belong is a machine learning problem. Using a graph embedding algorithm will capture the properties of the ransomware-Bitcoin graph. Through this process we provide the learnable data representation needed to handle the disparate property data chosen as input features in order to predict the output cluster of a new node in the graph.

[35] https://www.blockchain.com/btc/tx/29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27

The next section will look at turning the graph properties into a feature set and how the GraphSage machine learning algorithm takes this feature set to create embeddings that compress the dense properties of the graph and express them as features that can be used for downstream machine learning operations, such as predicting the corresponding cluster of an unseen Bitcoin transaction or address.

7.4.6 Graph catalogue

The graph catalogue is a specific component of the Neo4j Graph Data Science (GDS) library. This component allows graph algorithms in the GDS package to run on a graph data model. Here we use the data model defined in Figure 7.4 along with the enhanced graph properties outlined in Table 7.2. This formulates a projection of the Neo4j property graph data model. A graph projection can be seen as a materialised view over the actual graph. It only contains the analytically relevant, topological and property information. Graph projections can be aggregated. This provides optimisation for topology and property lookup operations. In practice, the data scientists and analysts can better handle multiple graph projections (Neo4j Docs - Graph Catalogue, 2021). When there is a need to engineer different models with different features, it becomes possible to use one created graph many times in the analytical workflow. This means steps one to three in Figure 7.3 do not need to be re-run every time the model changes. In step four of Figure 7.3, it is possible to end up with a catalogue of multiple models to apply to different ransomware payment networks. Appendix 7B shows the graph catalogue used during this research. The graph catalogue is a prerequisite for training the GraphSage embedding algorithm in the Neo4j environment. The next section explores the use of the graph catalogue for training (step five, Figure 7.3) the GraphSage embedding model (step six, Figure 7.3).

7.4.7 Graph embeddings

The graph catalogue established in step four of Figure 7.3 can now be used to train a GraphSAGE model in Neo4j. By applying the properties defined in the graph catalogue as '*featureProperties*' into the training routine, we use the existing graph and the feature set, *featureProperties:['pageRank', 'risk_rating', 'in_degree', 'out_degree', 'total_amount'],* to produce contextualized embeddings. These can then be used to classify new nodes introduced to the graph without having to retrain the model created with the graph catalogue and '*featureProperties*'. GraphSAGE is an inductive algorithm for computing node embeddings (Hamilton et al, 2017). GraphSAGE uses node feature information and the neighbourhood proximity of a node to generate node embeddings. Based on this information, the embeddings are then induced on unseen nodes or graphs. This algorithm removes the need of training individual embeddings for each node. This provides greater efficiency compared with DeepWalk algorithm (Perrozzi et al, 2018) which needs to sample new random walks and run new classifications to embed unseen nodes (Hamilton et al, 2017; Neo4j Docs - GraphSage, 2021). The output of the GraphSage routine are the embeddings that get fed into step seven, Model Evaluation. This will help determine the utility of the embeddings derived from the GraphSAGE algorithm and how accurate the classification is on any unseen data.

7.5 Model evaluation

Step seven, Model Evaluation, takes the derived graph embeddings and analyses the output in a two-dimensional space (Step 7a). This provides a human readable interpretation highlighting the significance of the ransomware-Bitcoin cash-out graph

embeddings for the analyst. The GraphSAGE model that is trained, in step five, has an embeddingDimension:256. By using a high embedding dimensionality relative to the number of nodes in the graph, 299, it is possible to preserve more information about the graph (Goyal and Ferrara, 2018). Running Principal Components Analysis (PCA) over the 256 embedding dimensions allows the analyst to work in a reduced dimensionality (2-Dimensions) to visualise trends in the distribution of the embedding output associated to the nodes in the graph (step 7a).

Clustering of nodes in the network (step 7b) is one of the observable patterns that results from this analysis. It helps the analyst compare behaviour in a ransomware-Bitcoin payment network. The PCA / K-means cluster plot in Figure 7.7, reveals three distinct clusters from the embeddings derived from the WannaCry cash-out graph with ransomware-Bitcoin seed address *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*.

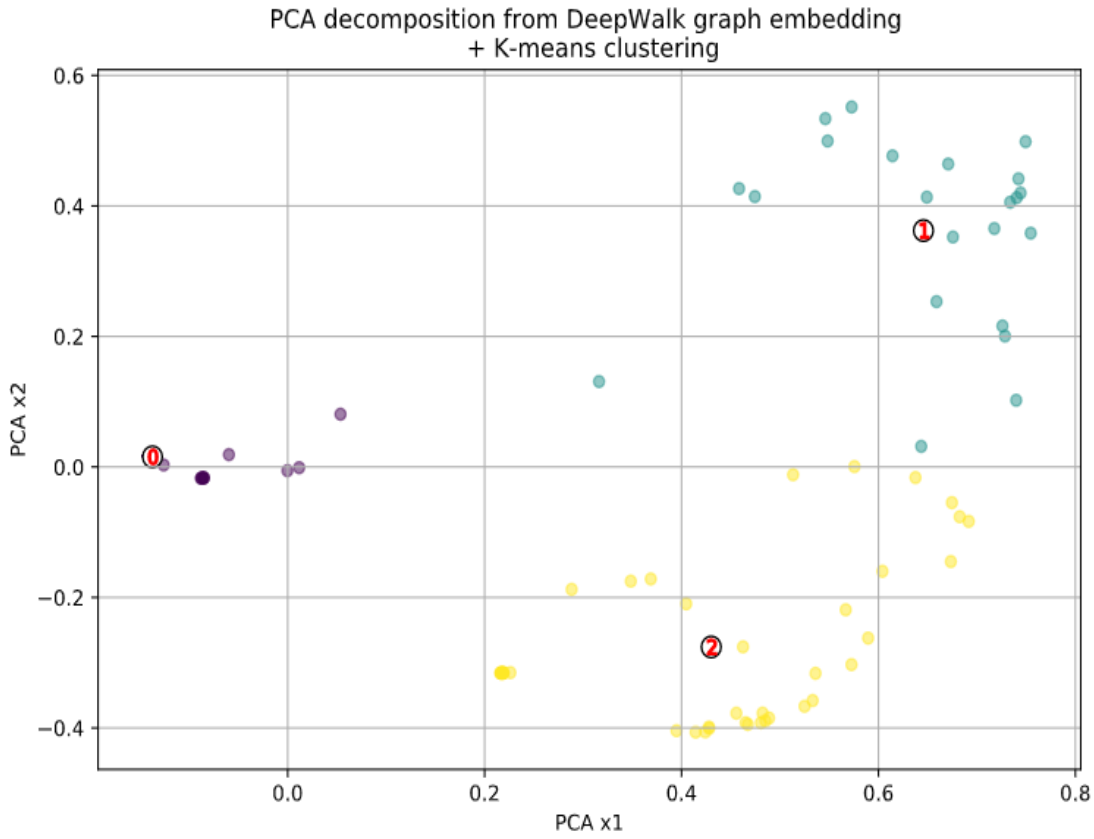


Figure 7.7: PCA / K-means cluster plot of the GraphSAGE embeddings from WannaCry cash-out graph with ransomware-Bitcoin seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw.

Table 7.3 shows the results from querying the feature properties, aggregated against the clusters formed.

Cluster Label	# Nodes	AVG PageRank	AVG Exposure	SUM of outdeg	SUM of indeg	SUM total_amount (BTC)
0	235	0.2384683224	0.0000215551	247	6	1.77125989
1	22	3.463109622	0.2956276672	131	404	254.0277611
2	42	0.4149004362	0.03180070117	60	28	322.795742
Grand Total	299	0.5005160059	0.02623579788	438	438	578.594763

Table 7.3: Cluster label and associated feature properties of the WannaCry cash-out graph with ransomware-Bitcoin seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

This is an important evaluation point in the system as the '*Cluster label*' serves as the target prediction parameter of the overall system. Therefore, if it is possible to derive a classification that is meaningful to law enforcement investigators or intelligence

analysts. For example, we might like to replace the numeric '*Cluster Label*' index (0, 1, 2), with something like '*Cluster Label*' at index 0 = '*Small Transaction Cluster*', due to the large amount of small transactions taking place within this cluster. There could be evidence of peeling within this type of cluster and further investigation might be required. Peeling is a technique used to obfuscate illicit cryptocurrency payments (Meiklejohn, et al, 2013). However, out of the three clusters, this one would most probably be deprioritised for investigation due to the low average exposure over the cluster (0.00002). The next '*Cluster Label*' at index 1 could represent '*Seed Target Cluster*'. This is a high profile target cluster based on our feature set. The ransomware-Bitcoin seed address is located in this cluster. There is also a significant amount of '*In degree*' and '*Out degree*' activity, 404 and 131 respectively. Furthermore, a large average PageRank ('*AVG PageRank*') (3.463) and average exposure ('*AVG Exposure*') (0.2956) exist across the cluster within a small number of nodes (22). This indicates most of the influential nodes in this network sit within this cluster and can be targeted by investigators for maximum disruption to the ransomware attacker's cash-out behaviour. The nodes in this cluster would be a high priority for investigators. The last cluster in this set of data is '*Cluster Label*' at index 2. An appropriate label for this cluster would be '*Large Transaction Cluster*'. The intuition behind this label refers to a small number of nodes (42) yielding the highest total amount of BTC ('*SUM total_amount (BTC)*') (322.795742) moving in and out of these nodes under a low '*In degree*' (28) and '*Out degree*' (60) conditions. Therefore, there appears to be a number of large transactions taking place within this cluster worth investigating. The most significant is, transaction *131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3*, moving approximately 65 BTC through it. In addition, transactions

2b22df65026d8384e01e0deb9b115ba9725bbe9d95c4f61d18dee6e40fa47b74, *3332d270983f3183af866714b8eb4ad226f4f4bea2ce42efcfd2de2dfdaf0f12*, *340b44c7a7857e36f81b2e8ba713911ea93e82afde6ea5590df1a35688845d16*, *557b6869ba2c6293d76e11f495afc7f30e6c7a53fb6355cefa8354eaab53b020*, and, *95d36a6926639ba50d02f190d3ca2f9322ce721502d47b32a1e8d8be1b13cb40* move an approximate total of 85 BTC through them and are all worth investigation due to the large size of the transactions. This cluster would be ranked as a medium priority for investigation.

The next section will examine the correlation between the selected features and the target label to determine what confidence the embeddings bring to the prediction of any cluster classification.

7.5.1 Feature correlation

Feature engineering requires input from a mixture of subject matter experts, for example, financial crime experts and data scientists, in order to arrive at the right feature selection. Examining the correlation matrix between the features earmarked for use in the system, helps visualise the importance each feature has relative to the other. Features with high correlation, for example those displaying correlation scores between 0.75 to 1 in Figure 7.8, are more linearly dependent and hence have almost the same effect on the dependent variable. When two features have high correlation, it is possible to drop one of the two features. For example, '*outdeg*' (out degree) and '*exp*' (exposure) metrics produce a correlation score of 0.8. The results produced from this research did not exclude features on this basis. Step 7c seeks to evaluate the features being used as

part of the graph machine learning pipeline used in this research. Figure 7.8 illustrates the dependency between features used in this system via the correlation matrix.

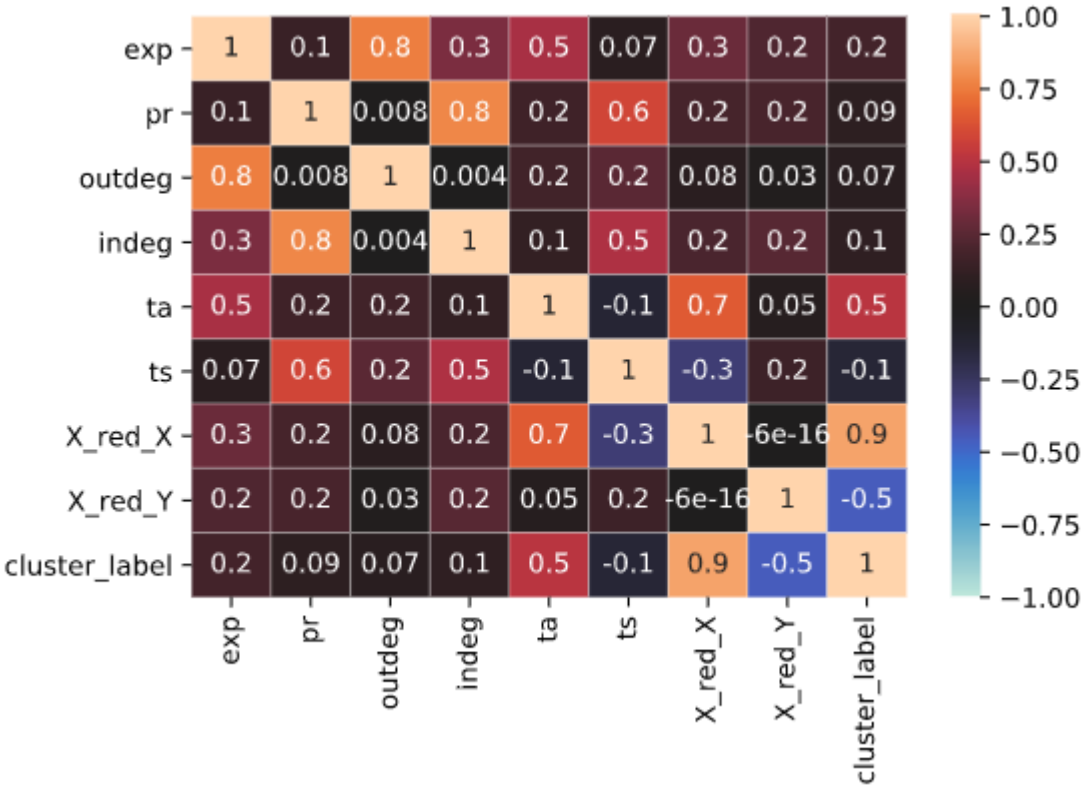


Figure 7.8: Feature correlation of the properties deployed to the enhanced data model. (exp=Exposure; pr=PageRank; outdeg=Out Degree; indeg=In Degree; ta=Total Amount; ts=Timestamp; X_red_X=PCA dimensionality reduced embeddings, X-axis; X_red_Y=PCA dimensionality reduced embeddings, Z-axis; cluster_label=Prediction target, Cluster Label)

Here our target (dependent variable) is '*Cluster Label*' and from Figure 7.8 we find a strong and weak correlation with the independent variables that form the basis for the GraphSAGE embeddings. An indication of a strong correlation is a value close to 1 (perfect positive correlation) or -1 (perfect negative correlation). The observation of '*X_red_X*' having 0.9 relative to the '*cluster_label*' shows a strong correlation. This is significant, as '*X_red_X*' is the PCA reduced parameter of the GraphSAGE embeddings. This means that the combination of features used in the GraphSAGE algorithm provides strong conviction to the prediction of the '*Cluster Label*'.

The next section runs through steps eight through eleven in order to show how the classification and prediction mechanisms work with the derived graph embeddings.

7.5.2 Classification and Prediction

Performing the classification and prediction tasks, steps 10 and 11, requires the features from the graph embeddings derived in step six and the cluster labels applied from step 9b. Assuming we are satisfied with the evaluation of the model features for predicting the '*cluster_label*' parameter, we now split the data into a testing and training dataset. This will validate the predictive power of the classification algorithm chosen. The algorithm used in this instance is the MultiOutputClassifier because the '*Cluster Label*' may take the form of 0, 1 or 2. The Stochastic Gradient Descent (SGD) optimization algorithm is also used. This boosts the convergence of the model parameters that correspond to the best fit between the actual and predicted outputs. In this case, SGD was chosen as it is a widely applied and stable algorithm for prediction (Bottou, 2004). Therefore, users of the system are assured some trust and confidence in the results obtained. This is important because the users may not always be data scientists or machine learning engineers and an explainable Artificial Intelligence (AI) system allows for transparency, trust and traceability of the algorithms being deployed (Gunning, et al, 2019).

7.5.3 Testing and Validation

Based on training and test data derived from the WannaCry cash-out network (ransomware Bitcoin seed address: *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*) we derive a cluster prediction confidence of 80% using the GraphSAGE embeddings. This result converged quickly after four training runs of the prediction algorithm. In step

eight of Figure 7.3 the data preparation randomly samples an 80/20 split. This ensures each training and test run utilises different data.

A primitive validation was done for the prediction methodology used in this paper. Appendix 7C shows four tables that represent the correct and incorrect predictions. Table 7C-4 in Appendix 7C, shows the results of the fourth training run. In this table, the *Actual Cluster Label* is in the first column and shows that within the data the *Cluster Label* takes the form of a 0, 1 or 2. However, the *predicted_cluster_label* only reveals a value of 0. This is due to the speed of convergence of the SGD algorithm. It quickly learns that 0 is the dominant cluster grouping in the dataset and ultimately overfits the test data by labelling all the *Predicted Cluster Labels* as 0. Nonetheless, this procedure actually increases the accuracy of the prediction to 80.33% (Table 7C-4). Table 7C-1 demonstrates that the first training run only yields an accuracy of 53% in total. Predicting 30 out of 49 *Cluster Label* '0' correctly and 5 out of 5 *Cluster Label* '1' correctly.

Determining the accuracy of fraud detection systems is complex. Accuracy when determining if a transaction is 'fraudulent' or 'not fraudulent' is not binary. It is necessary to balance what the model predicts as suspect against the quality of those predictions. As seen in Appendix 7C, True Positives (TP) and False Positives (FP), along with True Negatives (TN) and False Negatives (FN) will emerge from the model and we must maximise the True Positives (TP) across a broad set of test data. This may also require a rebalancing of the model. Putting this into context and recalling the labels we posited for our clusters of Bitcoin addresses and transactions in the ransomware-Bitcoin cash-out network. These are: *small_tx_cluster, seed_target_cluster* and

large_tx_cluster. Our criteria for a suspected address or transaction facilitating a ransomware payment is not simply a '*fraud*' flag. Rather, it takes a multi classification approach. This along with the aggregated community statistics to target investigation gives analysts a more informed decision making basis. Having three clusters within the data, the 3x3 confusion matrix in Table 7.4 reveals the True Positive Rate (TPR) and True Negative Rate (TNR) for the actual and predicted clusters.

Actual Cluster Label	*Small Transaction Cluster (0)*	**49 83.05%**	**0 0.00%**	**0 0.00%**
	Seed Target Cluster (1)	**4 6.78%**	**0 0.00%**	**0 0.00%**
	Large Transaction Cluster (2)	**6 10.17%**	**0 0.00%**	**0 0.00%**
		Small Transaction Cluster (0)	*Seed Target Cluster (1)*	*Large Transaction Cluster (2)*
		Predicted Cluster Label		

Table 7.4: Confusion matrix for multi classification of ransomware-Bitcoin payment clusters.

The TPs can be seen in the diagonal from the top left to bottom right. Examining one particular execution of the model, the analysis shows that of the 59 samples in our test data, all 59 are predicted to fall into a *Small Transaction Cluster* (0). Of the 59 samples, 49 (83.05%) are correctly classified as a *Small Transaction Cluster* (0). There are 10 (16.95%) FPs in total where the model incorrectly predicts a classification that it should be. In addition, the model flags 4 (6.78%) and 6 (10.17%) Bitcoin addresses or

transactions respectively as FNs. By contrast, 55 and 53 Bitcoin addresses or transactions are identified as TNs.

The classification and prediction model proposed in this research can serve as a tool for anomaly detection. FPs and FNs hold greater investigative insight especially when they are falsely flagged as *Small Transaction Cluster* when in fact the actual clusters contain high-value addresses and transactions relating to the ransomware-Bitcoin seed address and large transactions. For example, transaction *35e5d5fe8c8128cfa6884f56be5817e4138c58c91b79d78d3e78a8d365b9d8a7* that was predicted to be in the *Small Transaction Cluster* but actually belongs to the *Seed Target Cluster*. This transaction appears in Appendix 7A, Top Ten Nodes of Interest Tables 7A-2 with In + Out degree of 77 (third highest in the network), 7A-3 with Exposure of 1.59 (second highest in the network) and 7A-4 with Total Amount of 18.1 BTC (sixth highest in the network).

It must be said that the test data set used is very limited and only included 57 cases in total. Regardless, it still demonstrates the utility of the research. In order to train the classification and prediction model more diversely to handle different sets of data and consequently different types of ransomware payments, it is important to pass more sampled cash-out graphs through the system. For the system presented in this research, this is not a trivial undertaking. It would require repeating the process from step one of Figure 7.3 and running a new extract through the feature engineering process, arriving at a new set of embeddings that a representative of the new ransomware-Bitcoin cash-out graph of the new ransomware variant being tested for. This is a clear limitation of the system. An improvement to this is to store the different models that

produce the embeddings, and using an embeddings catalogue to train the classification and prediction algorithm. This facilitates a selection of the respective set of embeddings for the graph that classification and prediction is being performed on.

Alternatively, a test could be made using a derived set of embeddings from one ransomware-Bitcoin cash-out graph that is universally representative of all ransomware-Bitcoin cash-out graphs, to use as the basis for all cluster predictions and anomalies. Both cases would require further extensive testing to provide any validity to enhancing the current method. Furthermore, data not specifically relating to a ransomware-Bitcoin cash-out network would also need to be tested for behaviour of the model under control and edge cases.

Looking beyond the data science technicalities, the next section explorers the implications this method could have on the law enforcement and investigation communities.

7.6 Implications for law enforcement

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly playing a role in policing. Macnish, Wright and Jiya (2020), Asaro (2019), Oswald and Babuta (2021) and Joh (2017) identify the use of big data and machine learning techniques in predictive policing. In addition, they raise concerns around bias and fairness in the data (e.g., unfairly targeting race or demographics), and the impacts on justice, legislation, ethics and culture.

The analysis system designed in this research makes it possible to target ransomware-Bitcoin payments by predicting the cluster group of an unseen node in the network. This provides a utility for policing and law enforcement to further understand the payment dynamics of a ransomware attack. However, for such a system to take effect, and beyond the strategic considerations previously identified, the analysis must be integrated into cyber operations and investigation processes. Hunton (2011; 2012) provides a method to trigger cybercrime execution and augment intelligence gathering and investigation processes to provide a continuous and evolving input of cyber threat intelligence into the investigation process (Figure 7.9).

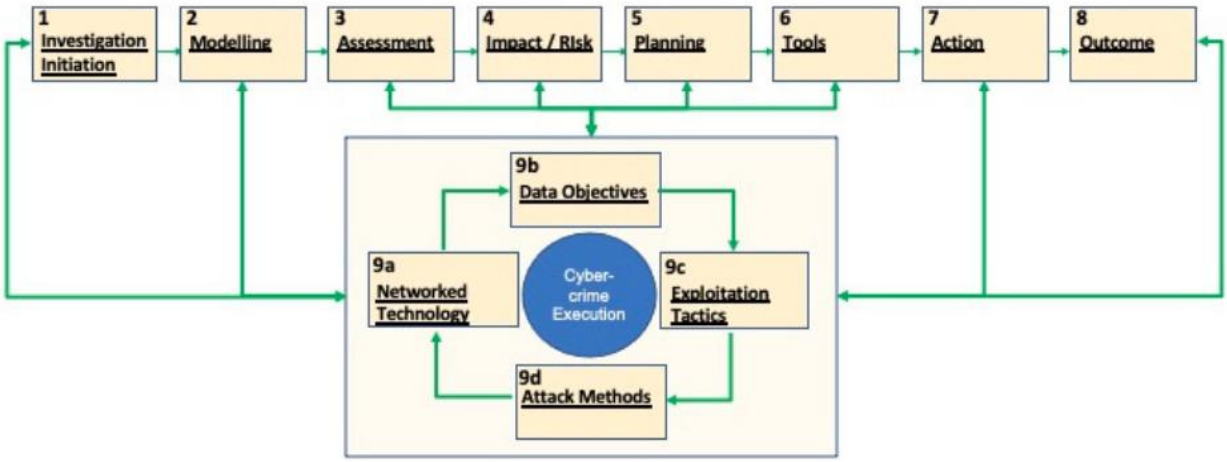


Figure 7.9: Cybercrime investigation stages (adapted from Hunton (2012)).

Based on the Investigation Doctrine of the Association of Police Officers (ACPO) in the United Kingdom, Hunton (2012) outlines how each investigation phase underpins the execution of a cybercrime and how it then guides the distinct policing activities in response to a cybercrime taking place (Hunton, 2012). The challenges Hunton (2012) raises regarding this model are the trade-offs between the spheres of influence and control law enforcement have over cybercrime investigations. Most notably, establishing '*Criminal or Illicit Intent*', detection and operations across borders in a

'*Globalised Environment*' and the tactics, techniques and procedures the cybercriminal uses for '*Evasion and Concealment*'. This is particularly relevant to the cryptocurrency environment ransomware attackers operate in. Using cryptocurrencies such as Bitcoin as a means of moving proceeds of cybercrime provides the perfect evasion from authorities by using an unregulated global financial network that conceals the identity of the source and destination of illicit funds.

Furthermore, Chang (2010), raises the implication of knowledge management in cybercrime investigations. Sharing investigative knowledge across intelligence and law enforcement agencies relating to cybercrime is critically important in the conviction of cybercriminals and the prevention of future crime. Applied at a conceptual level, knowledge management enables organisations to collect, detect, arrange, disseminate and communicate essential information and case history to enhance problem solving and decision making, root cause analysis, education and learning along with strategic planning, standards and policy development (Gupta et al, 2000). In the absence of any knowledge management system for ransomware-Bitcoin investigations, a system such as the one proposed in this research could be a catalyst for future research combining the knowledge management components identified by Gupta et al, (2000). The next section goes into more detail about how a knowledge graph for ransomware-Bitcoin investigations could shape future research.

7.7 Discussion and future work

Cryptocurrency systems are inherently anonymous or pseudonymous by design. Generally speaking, they operate on a peer-to-peer networking basis without the

controls or regulations of a central authority that provides governance and compliance to the law and financial standards.

Participants on cryptocurrency networks are not always required to provide Personal Identifiable Information (PII) or customer identification which would allow for attribution of transactions between cryptocurrency addresses (accounts). Even though cryptocurrency networks typically contain a publicly available ledger, the blockchain, of all transactions between sender and receiver, it remains a challenge, without the right data, to know who is actually behind any transaction. The graph machine learning system presented in this paper is based on the GraphSage algorithm.

Applied to the WannaCry cash-out payment network generated from the ransomware Bitcoin seed address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, the system leverages graph embeddings to produce a methodology for classification and prediction in ransomware-Bitcoin networks. This can be used for targeted intelligence collection, investigation and analysis into the behaviour of ransomware-Bitcoin networks. In fact, if law enforcement had a similar system in place during the course of the WannaCry attack, the investigation into the payment networks created from the associated seed addresses may have started sooner and investigators might have begun monitoring, clustering and predicting the path of payments being made by victims and attackers. One hypothetical course of action that would have been made possible with our proposed method might have been the early shut down of Bitcoin exchanges with a visible influx of addresses making payments to the seed address. Such action might have further limited the yield of ransom payments collected by the WannaCry attackers.

Furthermore, the data collected from the attack, once analysed and catalogued using our proposed system, may serve as a basis for future models of ransomware payment networks. Thus, by defining an enhanced data model for ransomware-Bitcoin payments, policing and law enforcement actors can work from a common basis when investigating the Bitcoin components of a ransomware attack. Using a system similar to that described in this paper we could ultimately produce a Bitcoin knowledge graph that would reveal the real origin and destination of any Bitcoin transaction.

A critical challenge facing law enforcers is determining whether a criminal transaction has taken place. Our model does this from a ransomware payment perspective, though more diverse data would be needed to mitigate bias as much as possible. In addition, one must identify the ultimate beneficiaries and the source of these criminal proceeds (transactions). Addressing these two things is highly dependent on the available data that the cryptocurrency system can reveal. Suspecting a certain address on the network of having criminal intention is simply not enough. Having targeted intelligence to inform our analysis will provide steps in the right direction as addresses under surveillance may be traced to their ultimate points of presence (e.g., exchanges, services, different currency networks) which could help in their attribution.

In this paper, only one source of data has been examined, namely the available blockchain data, known as ‘on-blockchain’ data. By examining the inherent features existing in the structures of the networks formed by ransomware attackers cashing out their ransomware payments, this research showed the utility of the graph embedding techniques combined with existing graph features to predict cluster membership. However, future research could broaden the scope to include historical criminal data

collected on aggregate by examining generalised patterns of suspicious behaviour that correlate with criminal activity.

Another potential line of investigation may seek to develop an indexation of a cryptocurrency network to allow law enforcement to develop a knowledge graph schema defined by meta-data points relating to addresses and their activity, interlinking objects, context, events, situations or abstract concepts. This would be an interoperable knowledge graph that will make threat intelligence available to law enforcement agencies and financial intelligence units. For example, by being able to look up addresses and have information revealed about which exchanges the addresses belong to, what purchases might have been made, what exchanges or services have they sent to, do they have illicit transactions flagged, what IP addresses are being used and what their geolocation is. The reverse is also possible, by searching IP address ranges, geolocations, exchanges and services to reveal addresses and transactions that are flagged as illicit.

Nonetheless, this would involve a costly effort of data integration, modelling and additional data engineering. This raises many subsequent questions for future research to address. As an example, how and who populates the meta-data so investigations can become more targeted? Can data be integrated from other law enforcement systems? What data governance, privacy and quality controls are in place? The exploration of these questions are needed to make sure the knowledge graph is trustworthy ensuring downstream machine learning systems can use even more reliable features for prediction and detection.

7.8 Conclusion

This research develops a machine learning system that applies advanced techniques to the challenge of identifying, classifying, and predicting active nodes in a ransomware-Bitcoin payment network. Indeed, if a system like the one we discuss in this paper were to be implement on a large scale across different cryptocurrencies, the capacity of law enforcement and security agencies to identify unfolding ransomware attacks in real time may be dramatically enhanced, as would their capacity to launch immediate countermeasures to disrupt such campaigns.

From a technical perspective, the GraphSAGE algorithm was used to induce embeddings representative of the network structure. These provide crucial information that facilitates the classification and prediction steps of the method. An analysis of sample data yielded three clusters as follows: a *Small Transaction Cluster*, a cluster of addresses and transactions centred around the ransomware seed address *(Seed Target Cluster)*, and a cluster that represents large transaction amounts *(Large Transaction Cluster)*. Ultimately, training enabled our system to predict the cluster of hitherto unseen data with above 80% accuracy. Furthermore, mis-classified nodes emerge as significant objects of further investigation. These anomalies revealed high-valued addresses and transactions that appeared in the Top Ten Nodes of Interest in Appendix 7A.

Importantly, this research draws on one set of data only. This could result in the model overfitting the test and validation data sets. However, these data are rich in terms of representing a particular ransomware campaign, WannaCry. The system and features should be validated more broadly across other ransomware and non-ransomware

payment networks. This would also include an extensive data labelling exercise to enhance node clustering.

7.9 Appendix 7A – Top Ten Nodes of Interest

Transaction id / Bitcoin Address	PageRank
29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27	41.9379236
1ArG3JwEbF4WrCiEnXQXUAgQumAVzqnQHD	20.49719017
1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe	20.49719017
d66b4c334c21e7d250b05477c013af1430f3c2680a06a173dc9bfff25e374be9	4.632821567
1589f5d03ee14227c84a4e02abd9c0956ff3636f2e53491d5a2004e59ba65e5c	1.679999858
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	1.309936988
131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3	1.30523067
6fc639ba056de897d32c26cc2f5a917dfb38256eef5e92244edf06284cd82ab0	1.187964619
19UyfTi6hv8CGTVP62DcLu4EmyBuihQiNy	1.159769952
3332d270983f3183af866714b8eb4ad226f4f4bea2ce42efcfd2de2dfdaf0f12	1.095922448

Table 7A-1: Top 10 highest PageRanked nodes in the WannaCry-Bitcoin cash out network

Transaction id / Bitcoin Address	In + Out degree
29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27	238
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	112
35e5d5fe8c8128cfa6884f56be5817e4138c58c91b79d78d3e78a8d365b9d8a7	77
409803bb5e124fd028c0482027c7722e84ce55b78204b279d3a44aba5e7c1698	38
1589f5d03ee14227c84a4e02abd9c0956ff3636f2e53491d5a2004e59ba65e5c	21
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	8
6fc639ba056de897d32c26cc2f5a917dfb38256eef5e92244edf06284cd82ab0	8
131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3	7
1ArG3JwEbF4WrCiEnXQXUAgQumAVzqnQHD	7
1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe	7

Table 7A-2: Top 10 nodes with the highest ‘in-degree’ + ‘out-degree’

Transaction id / Bitcoin Address	Exposure
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	2.272107993
35e5d5fe8c8128cfa6884f56be5817e4138c58c91b79d78d3e78a8d365b9d8a7	1.588035099
409803bb5e124fd028c0482027c7722e84ce55b78204b279d3a44aba5e7c1698	0.7574051366
1589f5d03ee14227c84a4e02abd9c0956ff3636f2e53491d5a2004e59ba65e5c	0.5441211254
131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3	0.5183707623
29779df2e2a5a1f823b22e7e974a0082bdfd389edc1c11d1d4f6b290d8118d27	0.434599737
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	0.3361561715
36ef488e59d719fb906254aed61bfe46e8f64778bc6cac97e56a68c241004c28	0.271876212
1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe	0.1259019088
3332d270983f3183af866714b8eb4ad226f4f4bea2ce42efcfd2de2dfdaf0f12	0.1085622182

Table 7A-3: Top 10 nodes with the highest exposure metric

Transaction id / Bitcoin Address	Total Amount (BTC)
131551e35e7a644b76ea5366f744313bff3f959207c416f7b7b7f9b1cc90b0a3	64.87039825
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	36.80910078
1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe	36.76335736
36ef488e59d719fb906254aed61bfe46e8f64778bc6cac97e56a68c241004c28	34.02336596
1589f5d03ee14227c84a4e02abd9c0956ff3636f2e53491d5a2004e59ba65e5c	22.69762409
35e5d5fe8c8128cfa6884f56be5817e4138c58c91b79d78d3e78a8d365b9d8a7	18.06647723
16dfTuSx4f78eQ81PzTgBtBDyZ7QhNZ8Vy	18.05592644
2b22df65026d8384e01e0deb9b115ba9725bbe9d95c4f61d18dee6e40fa47b74	18.05571527
95d36a6926639ba50d02f190d3ca2f9322ce721502d47b32a1e8d8be1b13cb40	18.04870541
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	17.77113037

Table 7A-4: Top 10 nodes with the largest transaction amount

7.10 Appendix 7B – Graph Catalogue

```
//--3.c. Graph Embeddings
//--GRAPH SAGE - http://snap.stanford.edu/graphsage/
//--Ref: Inductive Representation Learning on Large Graphs - https://arxiv.org/pdf/1706.02216.pdf
//--Representation Learning on Graphs: Methods and Applications - https://arxiv.org/pdf/1709.05584.pdf
//--Git - https://github.com/williamleif/GraphSAGE
//--Default parameters taken from: https://neo4j.com/docs/graph-data-science/1.3-preview/algorithms/alpha/graph-sage/
//--BETA release : https://neo4j.com/docs/graph-data-science/current/algorithms/graph-sage/
//--https://neo4j.com/developer/graph-data-science/graph-embeddings/


//--3.c.i CREATE ANOTHER GRAPH CATALOG - TO TRAIN THE GRAPH SAGE MODEL
//--Addresses with transactions
//--make sure the data types are the same be mindful of the fact that not all properties exist on each node label and maybe projected as 0
values
//--the same properties are required on each node label for the model to train
//--Node properties MUST BE present for each label in the graph: Example: [exposure, time_stamp, total_in_amount
//--total_out_amount]. Properties that exist for each label are [in_degree, pageRank, out_degree]
CALL gds.graph.create(
  'addresses_with_transactions_1', {
     output: {
           label: 'output',
           properties: {
              risk_rating: {
                 property: 'risk_rating',
                 defaultValue: 0.0
              },
              pageRank: {
                 property: 'pageRank',
                 defaultValue: 0
              },
              in_degree: {
                 property: 'in_degree',
                 defaultValue: 0
              },
              out_degree: {
                 property: 'out_degree',
                 defaultValue: 0
```

```
            },
            time_stamp: {
                property: 'time_stamp',
                defaultValue: 0
            },
            total_amount: {
                property: 'total_amount',
                defaultValue: 0.0
            }
        }
    },
tx: {
        label: 'tx',
        properties: {
            risk_rating: {
                property: 'risk_rating',
                defaultValue: 0.0
            },
            pageRank: {
                property: 'pageRank',
                defaultValue: 0
            },
            in_degree: {
                property: 'in_degree',
                defaultValue: 0
            },
            out_degree: {
                property: 'out_degree',
                defaultValue: 0
            },
            time_stamp: {
                property: 'time_stamp',
                defaultValue: 0
            },
            total_amount: {
                property: 'total_amount',
                defaultValue: 0.0
            }
        }
    }
```

```
  }, {
  PAYS: {
     type: 'PAYS',
     orientation: 'NATURAL',
     properties: {
        amount: {
           property: 'amount',
           defaultValue: 0.0
        },
        time_stamp: {
           property: 'time_stamp',
           defaultValue: 0
     }
    }
  }
 }
)
YIELD graphName, nodeCount, relationshipCount;
```

7.11 Appendix 7C – Predicted Cluster Label

	0		1		Total	
Cluster Label	*# Predicted Cluster Label*	%	*# Predicted Cluster Label*	%	*# Predicted Cluster Label*	%
0	**30 (45.45%)**	**45.45%**	**19 (28.79%)**	**28.79%**	49 (74.24%)	74.24%
1	-		**5 (7.58%)**	**7.58%**	5 (7.58%)	7.58%
2	**5 (7.58%)**	**7.58%**	**7 (10.61%)**	**10.61%**	12 (18.18%)	18.18%
Grand Total	**35 (53.03%)**	**53.03%**	**31 (46.97%)**	**46.97%**	**66 (100.00%)**	**100.00%**

Table 7C-1: *Training run 1 for test data on WannaCry ransomware-Bitcoin cash-out graph 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*

	0	Total
Cluster Label	# Predicted Cluster Label	Predicted Cluster Label
0	**46 (71.88%)**	**71.88%**
1	**6 (9.38%)**	**9.38%**
2	**12 (18.75%)**	**18.75%**
Grand Total	**64 (100.00%)**	**100.00%**

Table 7C-2: *Training run 2 for test data on WannaCry ransomware-Bitcoin cash-out graph 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*

	0	Total
Cluster Label	# Predicted Cluster Label	% Predicted Cluster Label
0	**56 (80.00%)**	**80.00%**
1	**6 (8.57%)**	**8.57%**
2	**8 (11.43%)**	**11.43%**
Grand Total	**70 (100.00%)**	**100.00%**

Table 7C-3: *Training run 3 for test data on WannaCry ransomware-Bitcoin cash-out graph 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*

	0	Total
Cluster Label	# Predicted Cluster Label	% Predicted Cluster Label
0	**49 (80.33%)**	**80.33%**
1	**3 (4.92%)**	**4.92%**
2	**9 (14.75%)**	**14.75%**
Grand Total	**61 (100.00%)**	**100.00%**

Table 7C-4: *Training run 4 for test data on WannaCry ransomware-Bitcoin cash-out graph 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw*

Chapter 8: Conclusion

8.1 Chapter Overview

Due to the inherent complexities of monitoring cryptocurrency transactions associated with ransomware activity, failure to associate context and reveal clear patterns of behaviour that can lead to attribution or seizure of funds is a common occurrence. Typically, these issues are related to the scale and convolutedness of cryptocurrency data residing on the blockchain. In order to obtain sustainable ransomware-Bitcoin analysis approaches it is imperative that we exploit the data rich cryptocurrency platforms using reusable and open source techniques. Enhancing this data by harvesting meta-data for knowledge graph analysis enables us to learn the complexities of attributing context to cryptocurrency data and move from raw data collection to knowledge (graph) based contextualisation. As such, this thesis is a culmination of work addressing the intelligence applications of Bitcoin payments related to ransomware. This research has contributed to the development of models and frameworks for researchers, investigators, and law enforcement to use for the collection, analysis, and dissemination of insights into the nature of ransomware-Bitcoin payments. This chapter provides a summary of results, detailing the key findings and contributions (Section 8.2) and discussing directions for future research (Section 8.3).

8.2 Summary of Results

Chapters 1 to 3 provide the initial grounding for this research, outlining the importance of this work and its place within the general field of illicit Bitcoin transaction analysis.

These chapters also provide the focus needed to develop the collection and analysis models for target centric intelligence and forensic analysis purposes. The collection and analysis models are designed to be agnostic in nature. This provides a certain standardisation to the approach of analysing this problem space. For example, in Chapter 3, ROI and RPPI are generic metrics developed as part of this research, and applicable to multiple ransomware campaigns. In addition, figure 3.1 shows a newly developed classification matrix, which gives analysts a tool to assess the strategic intention of any ransomware campaign. Furthermore, figure 3.3 is, by definition, a generic system model for ransomware payment movement, and can be used to map the attack/victim workflow. Chapters 4 and 5 apply this modelling through the development of a system that enables collection and analysis using a commonly used Cyber Threat Intelligence (CTI) standard, STIX. Although we focus on WannaCry, Chapter 4 yields a reusable ICP for ransomware-Bitcoin campaigns. Table 4.2 uses generic information requirements to form a picture of ransomware payment networks. In addition, the SRBF is utilising an open standard framework for CTI. The newly developed objects relate specifically to ransomware-Bitcoin payments. Therefore, the objects can be reused for those campaigns using the Bitcoin cryptocurrency. Other objects would need to be developed for other types of cryptocurrencies. Chapter 5 conceives the Ransomware – Bitcoin Intelligence – Forensic Continuum in figure 5.1. This can be applied to all types of ransomware campaigns as different campaigns share similar phases along the kill chain at different points in time. Furthermore, pattern analysis and a machine learning system were developed to reveal deeper insights into the data collected from various ransomware-Bitcoin cash-in and cash-out campaigns in Chapters 6 and 7. The Ransomware-Bitcoin Graph Analysis System is proposed in Chapter 6, figure 6.2 as a reusable machine learning pipeline. It can be applied to any

ransomware campaign that is using a Bitcoin address as the seed address or ransom collector. Chapter 6 goes on to provide a novel approach to determining a risk rating of nodes in a ransom payment network. Similar approaches have been applied to fraudulent credit card payments. Chapter 7 enhances figure 6.2 by providing a classification and prediction step to the pipeline of figure 7.3. This is important as we look to build up feature sets of different ransomware payment networks which give experts a knowledge bank to help predict and simulate with higher precision how ransomware payment networks unfold. A standard graph data model (table 7.1) and an enriched graph data model (table 7.2) are defined. Exposure is a unique feature in the enriched data model derived in this research. This is a risk rating feature that could be used in any type of fraudulent payment network scenario. The prediction model used in figure 7.3 is not trained on diverse datasets. This is where further testing and validation is required. This can result in more time spent on feature engineering than desired.

Each chapter of this thesis addresses an objective (O1 – O5). How these objectives are addressed is summarised in the following subsections.

8.2.1 Analysis Techniques for Illicit Bitcoin Transactions

Chapter 2 addresses O1, namely to identify the incumbent techniques used for analysis of illicit Bitcoin transactions and use these techniques to explore the technical (blockchain) and non-technical (regulatory) mechanisms for identifying and preventing ransomware-Bitcoin payments. The literature review in Chapter 2 examines the current literature relating to analysis techniques for illicit Bitcoin transactions. The chapter reveals a need to address the absence of techniques available to security researchers, the intelligence community, and investigators when it comes to specifically discovering

illicit ransomware payments using cryptocurrencies such as Bitcoin. A regulatory environment scan is undertaken to elucidate the numerous policy and compliance efforts being conducted around the world when it comes to regulating cryptocurrency payment networks. The chapter highlights the various instruments in play; however, there is a lack of implementation and jurisdictional consequences if cryptocurrency services do not follow the policy guidance. The chapter also takes a more technical approach to analysis by leveraging the vast swathes of data cryptocurrency networks contain. It examines the original analysis heuristics on clustering and how this can be used to provide greater attribution to the illicit users of Bitcoin. In addition, graph analysis dives into the structures of payment networks and what they reveal by modelling cryptocurrency addresses and transactions as a graph problem. Furthermore, advanced machine learning techniques are discussed and how deep learning can be applied to the graph problems for greater understanding of transaction behaviour patterns. Finally, a subset of these techniques is examined through the lens of a ransomware attack.

8.2.2 A Ransomware-Bitcoin Target Network Model

Chapter 3 addresses O2, namely to develop a framework based on the characteristics of a ransomware-Bitcoin network to classify a ransomware attack as destructive or revenue generating. In this chapter, a Target Network Model (TNM) of the underlying financial infrastructure of the WannaCry ransomware is established. This includes understanding the payment networks formed to conduct ransomware attacks. By breaking down the WannaCry system and cyber kill chain, a timeline is formed to understand the key elements from attack mobilisation to cash-out of the ransom payment collected in Bitcoin. Identification of the potential involvement of nation states

also forms part of this system breakdown. Ransomware-Bitcoin addresses (seed addresses), inflows (cash-in network), outflows (cash-out network), and the payment mechanics were examined to create a generic target model of the adversary.

A number of observations on ransomware-Bitcoin transactions reveal certain payment patterns and what happens to the transactions at certain nodes, Bitcoin exchanges, and anonymising services. A Problem Definition Model (PDM) is created for WannaCry 2.0 and is used as a template for understanding the driving components of a ransomware attack. By examining the component parts of a ransomware attack the proceeds of crime are revealed. The ransomware seed address patterns uncover the what, when, and where of ransom payments. The subsequent analysis of inflows, outflows, and formation of key communities as clusters of nodes can be indexed and categorised over the course of a ransomware campaign. Furthermore, the analysis of outflows is undertaken to discover who is attributed to an attack and to recommend intervention strategies. The ransomware kill chain is examined for command and control of the ransomware accounting and Bitcoin address creation. The chapter develops a blueprint that provides a visual guideline for analysis of the ransomware-Bitcoin problem space.

8.2.3 A Threat Intelligence Collection and Dissemination Framework

Chapter 4 addresses O3, namely to develop a ransomware-Bitcoin cyber threat intelligence sharing framework using the Structured Threat Intelligence eXpression (STIX) standard. This chapter develops an innovative methodology for modelling, analysing, collecting, and sharing intelligence on a ransomware adversary using Bitcoin blockchain data. Vast amounts of data were collected relating to the WannaCry ransomware attack so that the cash-in and cash-out ransom payment networks could be

modelled and analysed for threat intelligence relating to the Bitcoin payments made in a ransomware attack. By developing the STIX-Ransomware-Bitcoin Framework (SRBF) we are able to represent the threat intelligence of ransom payments moving through the Bitcoin ecosystem as a result of a ransomware attack. By using an internationally accepted standard for threat intelligence sharing such as STIX, the information can be shared, consumed, and analysed across the security community for an effective understanding of the threat these nefarious payments pose. The aim is to drive consumption of such intelligence sharing models in order to counter any future attacks and follow the money that leads investigators to the attackers and their bounty of Bitcoin that can be seized and returned to victims of ransomware.

8.2.4 Ransomware-Bitcoin Transaction Pattern Identification and Characterisation

Chapter 5 addresses O4, namely to examine patterns of ransomware-Bitcoin transactions that determine common profiles and attacker behaviour on the Bitcoin payment network for deeper graph analysis. Data were collected over the duration of the campaigns analysed (WannaCry, CryptoDefense, NotPetya and The Water Project charity, a non-ransomware control case), revealing the cash-in and cash-out strategies of these attacks. Systematic differences between the Bitcoin transaction patterns of charity and ransomware campaigns do exist. The ransomware attacks analysed reveal two distinct patterns after victims start making payments: either attackers accumulate ransom payments over a longer duration and then decide to move the funds on, or attackers keep their balance close to zero. The limitations are evident in the small sample of ransomware attacks analysed. However, by taking this approach a catalogue of strategies could be developed for law enforcement officials to leverage in their

investigations. Other analysis techniques were also applied to discern specific patterns of ransomware payment behaviour. Graph observations were built to visualise patterns of the standard transaction graph to look for any similarities between the structure of the cash-in and cash-out graphs. Community detection analysis and graph embeddings were utilises to produce definitive insights for risk analysis using the PageRank algorithm and unsupervised machine learning techniques that embedded latent features into the graphs for a deeper contextual understanding of what role specific Bitcoin addresses and transactions perform in the ransomware payment network.

8.2.5 A Machine Learning System using Graph Embeddings with Derived Risk and Exposure

Chapters 6 and 7 address O5, namely the development of a measure of risk in a ransomware-Bitcoin payment network that reveals nodes and communities that can be targeted for investigation and disruption. It was evident from the investigation into various ransomware campaigns and the results of the applied methods developed throughout this thesis that pattern analysis techniques can reveal unique payment strategies of ransomware attackers during their cash-out networks. Moreover, graph machine learning techniques, such as graph embeddings, are able to reveal context within a cash-out network. The lesser impact of these techniques was experienced on the cash-in networks as these networks are indistinguishable to other services receiving payments on the Bitcoin network. Further research should be focused on the cash-in network, as this will provide an earlier point of intervention into the payments of ransom during a ransomware campaign.

In particular, the practice of graph embedding was experimented with using the DeepWalk algorithm developed by Perozzi et al (2014). The application of graph embedding techniques is an important emerging practice in the area of graph machine learning. When embeddings are derived from a given graph, latent features are used to reduce a collection of properties from the graph that can be further utilised in downstream machine learning operations. For example, in this research the embeddings were used as input into the Cosine Similarity function in order to determine a node's proxy for risk relative to a ransomware-Bitcoin seed address. This is a powerful concept in the case of ransomware-Bitcoin payment analysis. The study draws on one set of data only. These data are rich in blockchain properties relevant to a ransomware-Bitcoin payment network. This research mainly focuses on the cash-out graph for WannaCry 2.0 using graph embeddings. However, future research may consider a general collection of properties on the network, such as payment amount, pageRank, node riskiness, and the in and out degree of a node, which can be deemed influential for identifying ransomware-Bitcoin payments. This creates the potential to develop a reusable feature store which implants domain knowledge into the raw network data for other analysts, data scientists or researchers to use and reference for future machine learning model development (Lakshmanan et al, 2020). Multiple feature sets can be created and documented with essential meta-data that can serve a searchable knowledge base to discover what feature sets of a ransomware-Bitcoin network may provide the best predictive powers for a classification or anomaly detection algorithm.

8.3 Directions for Future Research

The concepts developed and application of these developed concepts throughout the course of this research have demonstrated enhanced ransomware-Bitcoin intelligence

collection and analysis methods. However, the rapidly evolving discourse on the subject of ransomware calls for similarly evolving action against this threat and the associated ransomware payments. Recent developments in the field of ransomware-cryptocurrency analysis reveal three key areas of potential focus, detailed in the following subsections. Along the with the research presented in this thesis, these three future research areas are inextricably linked and as the threat of ransomware perpetuates, research must push into these areas to influence the use of data, technology, policy, and governance to enable intelligence agencies and law enforcement to protect individuals, organisations, and critical infrastructure. Further research in these areas is likely to help increase the effectiveness of intelligence collection and analysis capabilities to detect, disrupt, prevent or to subrogate money flows relating to ransomware.

8.3.1 Focus on Data

Firstly, a future focus needs to be placed on data. As we continue to collect data on ransomware attacks, it is imperative that the volume, variety, and velocity of this data render our capabilities for advanced threat detection more intelligent. Underreporting and continued ransomware identification challenges were highlighted in the 2022 Crypto-crime report from Chainalysis (Chainalysis, 2022). It is understandable that private enterprises look to monetise cryptocurrency data assets. However, research needs to direct efforts towards open standards and data models that allow for open threat intelligence sharing on illicit cryptocurrency activity. This will lead to actionable intelligence and allow law enforcement in addition to public and private enterprises to enact more collaboratively on the emergence of legislation like the Ransomware Payments Bill 2021 (No. 2) (Parliament of Australia, 2021). For example, Part 2 of the

Ransomware Payments Bill 2021 (No. 2) outlines the need for entities to conduct timely mandatory reporting on ransomware payments made:

> "*(2) The notice must set out:*
>
> *(a) the **name and contact details of the entity**; and*
>
> *(b) the **identity of the attacker**, or what information the entity knows about the identity of the attacker (including information about the purported identity of the attacker); and*
>
> *(c) a **description of the ransomware attack**, including:*
>
> *(i) the **cryptocurrency wallet** etc. to which the attacker demanded the ransomware payment be made; and*
>
> *(ii) the **amount of the ransomware payment**; and*
>
> *(iii) any **indicators of compromise** known to the entity.*
>
> *(3) An indicator of compromise is **technical evidence** left by the attacker that indicates the attacker's identity or methods.*" (Parliament of Australia, 2021).

When it comes to the topic of data, there are further steps that can be taken. With the mass collection of illicit cryptocurrency activity there would be low barriers to developing a large scale distributed database with today's computing power and capability. The formation of an entire knowledge graph that is searchable on metadata criteria retrieving illicit patterns and money flows could be learned from illicit activity and indexed like current web and map search capabilities. Pushing the collection boundaries further, real time contextual knowledge could also be provided along with integrated messaging for intelligence and investigation knowledge sharing along with cross-border collaboration. This would vastly improve the metrics and features used to prevent and track illicit money flows.

8.3.2 Evolution of Ransomware Business Models

Ransomware business models, such as Ransomware-as-a-Service (RaaS), are rapidly evolving, with a large uptick in ransomware strain development and deployment. Identified as the top risk in the 2021 Gartner Emerging Risks Monitor Report, “new ransomware models” are enabling organised cyber crime gangs to use ready made ransomware infrastructure making the business of ransomware more specialised, highly efficient, and more rewarding (Gartner, 2021). Developers are able to put their ransomware code on darknet marketplaces and collect a fee for every usage of their released strain (Chainalysis, 2022). This is also reflected in the increase of active ransomware strains. The number of these strains increased from 79 (2019) to 119 (2020) to 140 (2021) (Chainalysis, 2022). This shows a Compound Annual Growth Rate (CAGR) of 20%. A perpetual self-funding model could be emerging. This creates a dichotomy between the dark markets that facilitate proceeds of crime and funding for malicious Software-as-a-Service (SaaS) that must be investigated further to arrest the further propagation of ransomware variants.

8.3.3 Geopolitical Implications and Impacts of Critical Infrastructure

As outlined in this research, the ransomware classification matrix demonstrates that a ransomware attack can be seen primarily as a tool of destruction and/or a revenue generating campaign (Turner et al, 2019). However, recently observed ransomware attacks reveal a shift in motivation towards a tool of destruction. As such, it is vital to investigate the increasing geopolitical implications and impacts on critical infrastructure. For example, the current Ukrainian-Russian tensions have led to several

targeted ransomware attacks: a malicious program known as BootPatch held government systems ransom demanding “$10k via bitcoin wallet” (CERT-UA, 2022) and WhisperGate (a NotPetya look-alike) targeted Ukrainian organisations (Trend Micro, 2022). In addition, a NotPetya attack on Ukrainian organisations in 2017 that disrupted critical financial, energy, and government systems was attributed to the Russian Military (National Cyber Security Centre, 2018). The largest revenue generating ransomware strain of 2021, Conti, is purportedly operated by a government controlled cybercrime gang based in Russia (Chainalysis, 2022). In 2021 the Colonial Pipeline attack associated with an Eastern European cybercrime group (Trend Micro, 2021) disabled systems responsible for “45 percent of the fuel used on the East Coast of the United States” (U.S Department of State, 2021). The recovery of 63.7 bitcoins paid in ransom from this attack has also highlighted the importance of cryptocurrency traceability capability (U.S. DOJ, 2021b; Wolf, 2021).

Appendices

The following appendices provide links to the Harvard Dataverse: *Bitcoin Network Data Dataverse*. Published on 9 October 2022. Available from: https://dataverse.harvard.edu/dataverse/bitcoin-network-data/.

Appendix A – Source Code

Turner, A. (2021). Source Code. Available from: https://doi.org/10.7910/DVN/BYV3FW, Harvard Dataverse, Published (Oct, 2022).

Turner, A. (2021). Bitcoin-seed-extract. Available from: https://github.com/AdamT23/bitcoin-seed-extract (GitHub public repository).

Appendix B – Raw Network Data

Turner, A. (2021). Transaction History. Available from: https://doi.org/10.7910/DVN/3SH9O6, Harvard Dataverse, Published (Oct, 2022).

Turner, A. (2021). Raw Network Data. Available from: https://doi.org/10.7910/DVN/WGXC9G, Harvard Dataverse, Published (Oct, 2022).

Appendix C – Data Analysis

Turner, A. (2021). Analysis. Available from: https://doi.org/10.7910/DVN/PRJ8Y2, Harvard Dataverse, Published (Oct, 2022).

References

Ahn, G. J., Doupe, A., Zhao, Z., and Liao, K. (2016). Ransomware and cryptocurrency: partners in crime. In *Cybercrime Through an Interdisciplinary Lens* (pp. 119-140). Routledge.

Alarab, I., Prakoonwit, S., and Nacer, M. I. (2020). Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In *Proceedings of the 2020 5th International Conference on Machine Learning Technologies* (pp. 11-17).

Albert, E. (2018). What to know about the sanctions on North Korea: Council on Foreign Relations. Available from: https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea [Accessed 15 November 2018].

Alpaydın, E. (2020). *Introduction to Machine Learning, 4th edition.* Massachusetts Institute of Technology (MIT) Press.

Anti-Money Laundering and Counter-Terrorism Financing Act (2006). No. 169. Available from: https://www.legislation.gov.au/Details/C2019C00011/Html/Text [Accessed 22 July 2020].

Arnold, N., Ebrahimi, M., Zhang, N., Lazarine, B., Patton, M., Chen, H., and Samtani, S. (2019). Dark-net ecosystem cyber-threat intelligence (CTI) tool. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 92-97).

Asaro, P. M. (2019). AI ethics in predictive policing: From models of threat to an ethics of care. *IEEE Technology and Society Magazine,* 38(2): 40-53.

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013). Evaluating user privacy in bitcoin. In Sadeghi, A.R. (Ed.), Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, Springer, Berlin, Vol. 7859.

Antonopoulos, A. (2010). *Mastering Bitcoin*. O'Reilly Media.

AUSTRAC. (2019). A guide to preparing and implementing an AML/CTF program for your digital currency exchange business. Available from: https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/guide-preparing-and-implementing-amlctf-program-your-digital-currency-exchange-business. [Accessed 25 July 2020].

Barnum, S. (2012). Standardizing cyber threat intelligence information with the structured threat information expression (stixTM). MITRE Corp. 11, 1–22 (2012).

Bartoletti, M., Carta, S., Cimoli, T., and Saia, R. (2020). Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 102: 259-277.

Bechtel, K. (2014). *Malware's Journey from Hobby to Profit-Driven Attacks.* Available from: http://www.tenable.com/blog/malware-s-journeyfrom-hobby-to-profit-driven-attacks [Accessed 8 October 2015].

Bellei, C. (2019). *The Elliptic Data Set: opening up machine learning on the blockchain.* Available from: https://medium.com/elliptic/the-elliptic-data-set-opening-up-machine-learning-on-the-blockchain-e0a343d99a14 [Accessed 11 November 2019].

Bertsimas, D., and Orfanoudaki, A. (2021). Pricing Algorithmic Insurance. arXiv preprint arXiv:2106.00839.

Bhatia, S., Hooi, B., Yoon, M., Shin, K., and Faloutsos, C. (2019). MIDAS: Microcluster-Based Detector of Anomalies in Edge Streams. In *Proceedings of the AAAI Conference on Artificial Intelligence*, 34(4): 3242-3249.

Biryukov, A., Khovratovich, D., and Pustogarov, I. (2014). Deanonymisation of Clients in Bitcoin P2P Network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15-29).

Bistarelli, S., Parroccini, M., and Santini, F. (2018). Visualizing Bitcoin flows of ransomware: WannaCry one week later. ITASEC, *CEUR Workshop Proceedings, no. 2058.* Available from: http://ceur-w s.org/Vol-2058/#paper-13 [Accessed 6 November 2018].

Bitfreeze (2019). *Threshold Signatures: MultiSig is Not Enough.* Available from: https://medium.com/@bitfreeze/threshold-signatures-multisig-is-not-enough-e1ba468f6102 [Accessed 21 October 2020].

Blockchain.info (2018). *Mining Pools.* Available from: https://blockchain.info/pools [Accessed 13 November 2018].

Bottou, L. (2004). Stochastic Learning. In *Advanced Lectures on Machine Learning* (pp. 146–168). Springer.

Carbon Black (2017). *The Ransomware Economy.* Available from: https://www.carbonblack.com/resource/the-ransomware-economy/ [Accessed 19 October 2018].

Carbon Black (2018). *What is Ransomware?* Available from: https://www.carbonblack.com/resources/definitions/what-is-ransomware/ [Accessed 18 October 2018].

CERT-UA (2022). Fragment of the study of cyberattacks 14.01.2022. Computer Emergency Response Team of Ukraine (CERT-UA). Available from: https://cert.gov.ua/article/18101 [Accessed 30 April 2022].

Chainalysis (2018). *The Changing Nature of Cryptocrime, January 2018*. Available from: https://www.chainalysis.com/static/Cryptocrime_Report_V2.pdf [Accessed 18 October 2018].

Chainalysis (2020). *The 2020 State of Crypto Crime, January 2020.* Available from: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf [Accessed 18 May 2020].

Chainalysis (2021a). *The Chainalysis 2021 Crypto Crime Report.* Available from: https://go.chainalysis.com/2021-Crypto-Crime-Report.html [Accessed 23 October 2021].

Chainalysis (2021b). *Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware.* Available from: https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest [Accessed 23 October 2021].

Chainalysis (2022). *The 2022 Crypto Crime Report - Original data and research into cryptocurrency-based crime.* Available from: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf [Accessed 20 February 2022].

Chang, W. (2010). Fighting Cybercrime: A KM Perspective. In *Pacific-Asia Workshop on Intelligence and Security Informatics* (pp. 28-30).

Choi, N., Chen, P.P., Hu, X., Lee, K.J., Maguire, J.D., & Song, I. (2006). Designing a Data Warehouse for Cyber Crimes. JDFSL, 1, 5-22.

CIA. (2009) *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis.* Available from: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf [Accessed 3 January 2021].

Cimpanu, C. (2020). *Ransomware mentioned in 1,000+ SEC filings over the past year.* Available from: https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/? [Accessed 18 May 2020].

CipherTrace. (2020). *Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report.* Available from: https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/ [Accessed 9 August 2020].

Clark, R., M., and Mitchell, W., L. (2016). *Target-Centric Network Modeling: Case Studies in Analyzing Complex Intelligence Issues*. CQ Press, Washington DC.

Clark, R. M. (2017). *Intelligence analysis: a target-centric approach, 5th edition.* CQ Press, Washington DC.

Clay, J, (2019). *Where will Ransomware go in the second half of 2019?* Available from: https://blog.trendmicro.com/where-will-ransomware-go-in-the-second-half-of-2019/ [Accessed 9 November 2019].

Cloherty, J. (2013). *Black Market Bank Accused of Laundering $6B in Criminal Proceeds. ABC News.* Available from: https://abcnews.go.com/US/black-market-bankaccusedlaundering6bcriminalproceeds/story?id=19275887#:~:text=May%2028%2C%202013%E2%80%94%20%2D%2D%20Internet,child%20pornography%20and%20narcotics%20trafficking [Accessed 17 February 2021].

CoinMarketCap (2018). *Top 100 Cryptocurrencies by Market Capitalization.* Available from: https://coinmarketcap.com/ [Accessed 18 October 2018].

CoinMarketCap (2020). *Convert BTC to USD.* Available from: https://coinmarketcap.com/converter/btc/usd/ [Accessed 9 January 2020].

Computer Emergency Response Team of Ukraine (2022). [English Translation] *Fragment of the study of cyberattacks 14.01.2022. 01/26/2022.* Available from: https://cert.gov.ua/article/18101 [Accessed 20 February 2022].

Condon, C. (2012). *How do cybercriminals profit from infecting websites with malware?* Available from: http://www.stopthehacker.com/2012/05/29/howdocybercriminals profit from infecting websites with malware/ [Accessed 8 October 2015].

Conti, M., Gangwal, A., and Ruj, S. (2018). On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. *Computers & Security*, 79: 162-189.

Coverware (2019). *Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread.* Available from: https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread [Accessed 29 November 2019].

Crowdstrike (2021a). *History of Ransomware.* Available from: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ [Accessed 12 December 2021].

Crowdstrike (2021b). *What is a Botnet? Botnet Attack Types Defined.* Available from: https://www.crowdstrike.com/cybersecurity-101/botnets/ [Accessed 12 December 2021].

Dale, O. (2018). *Beginner's Guide to HitBTC: Complete Review.* Available from: https://blockonomi.com/hitbtc-review/ [Accessed 15 November 2018].

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., and Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, 15(4): 277-305.

Darknetmarkets. (2017). *European union launches 'Titanium' project investigating criminal use of bitcoin and dark web*. Available from: https://darknetmarkets.co/european-union-launchestitanium-project-investigating-criminal-use-of-bitcoin-and-dark-web/ [Accessed 15 July 2017].

Das, S. (2016). *Russia Blocks Access to Bitcoin P2P Exchange LocalBitcoins. CryptoCoinsNews.* Available from: https://web.archive.org/web/20160914181612/https://www.cryptocoinsnews.com/russia-blocks-access-bitcoin-p2p-exchange-localbitcoins/ [Accessed 8 November 2018].

Decree of the President of the Republic of Belarus No. 8. (2017). National Legal Internet Portal of The Republic of Belarus, No. 1/17415. Available from: http://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0 (in Russian), archived at https://perma.cc/7PJ7-YEKA, available in English at http://law.by/document/?guid=3871&p0=Pd1700008e, archived at https://perma.cc/V7UZ-TYM8. [Accessed 26 August 2020].

De Marzi, M. (2019). *Finding Fraud.* Available from: https://maxdemarzi.com/2019/08/19/finding-fraud/ [Accessed 18 May 2020].

Department of Defense (DoD) (2015). Military and Security Developments Involving the Democratic People's Republic of Korea 2015. Office of the Secretary of Defense 2015. Available from: https://dod.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF [Accessed 26 August 2020].

Dingledine R., Mathewson N., and Syverson P. (2004). *Tor: The Second-Generation Onion Router*. The Freehaven Project, Navy Research Lab. Available from: https://www.usenix.org/legacy/event/sec04/tech/full_papers/dingledine/dingledine_html/ [Accessed 7 November 2018].

Drainville, D. (2012). *An analysis of the bitcoin electronic cash system*. University of Waterloo.

Ducklin, P. (2018). *Serious Security: How to cut-and-paste your way to Bitcoin riches*. SophosLabs. Available from: https://nakedsecurity.sophos.com/2018/07/05/serious-security-how-to-cut-and-paste-your-way-to-bitcoin-riches/ [Accessed 18 May 2020].

E-gold Legal Update (2008). Plea as to 18 U.S.C. §§ 1956(h) and 371 by e-gold, Ltd. (2008-07-21) and Plea as to 18 U.S.C. §§ 1956(h) and 1960(b)(1)(A), (B), and (C) by Douglas L. Jackson (2008-07-21) and Plea as to 26 D.C. Code § 1002 by Barry K. Downey (2008-07-21). U.S Department of Justice, U.S Attorney District of Columbia. Available from: https://legalupdate.e-gold.com/2008/07/plea-agreement-as-to-egold-ltd-20080721.html; https://legalupdate.e-gold.com/2008/07/plea-agreement-as-to-douglas-l-jackson-20080721.html; https://legalupdate.e-gold.com/2008/07/plea-agreement-as-to-barry-k-downey-20080721.html [Accessed 17 February 2021].

Elbaghdadi, A., Mezroui, S. and El Oualkadi, A. (2021). K-Nearest Neighbors Algorithm (KNN): An Approach to Detect Illicit Transaction in the Bitcoin Network. In *Integration Challenges for Analytics, Business Intelligence, and Data Mining* (pp. 161-178). IGI Global.

Elliot, M. (2016). *Arrests and Prosecutions Reveal Big Vagaries in Bitcoin Selling Regulations, CryptoCoinsNews* [Accessed 23 May 2016].

Emsisoft. (2020). *Report: The cost of ransomware in 2020. A country-by-country analysis.* Emsisoft Malware Lab. Available from: https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/ [Accessed 12 August 2020].

Ethereum.org (2021). What is Ethereum? Available from: https://ethereum.org/en/what-is-ethereum/ [Accessed 14 December 2021].

European Union (EU). (2018a). *2018/843.* Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018L0843 [Accessed 26 August 2020].

European Union (EU). (2018b). *The 5th Anti-Money Laundering Directive*. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en [Accessed 18 May 2020].

Europol (2018). *Internet Organised Crime Threat Assessment (IOTA) 2018.* Technical Report, Europol.

Europol (2017). *Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation.* Press Release, 20 July 2017. Available from: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation [Accessed 7 November 2018].

Evans, C. A., and Schneider, A. B. (2019). Nonprofit Reputation and Bitcoin Use. *Journal of Ideology*, 40(1): 1.

Farghaly, M. (2014). *Bitcoin Programming, 1st edition.* CreateSpace Independent Publishing Platform.

FATF. (2012). *The FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.* Available from: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html. [Accessed 25 July 2020].

FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* Available from: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. [Accessed on: 25 July, 2020].

FATF (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.* Available from: www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html [Accessed 30 October 2020].

Federal Bureau of Investigation (FBI). (2012). *Bitcoin Virtual Currency Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Report from the Intelligence Assessment, Cyber Intelligence and Criminal Intelligence Section. Available from: cryptome.org/2012/05/fbibitcoin.pdf [Accessed 1 March 2016].

FBI National Press Office (2021). *FBI Deputy Director Paul M. Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline*. Available from: https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline

FIN-2019-G001. (2019). *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies.* May 9, 2019. Available from: https://www.fincen.gov/sites/default/files/201905/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. [Accessed 25 July 2020].

FinCEN. (2019). *New FinCEN Guidance Affirms Its Longstanding Regulatory Framework for Virtual Currencies and a New FinCEN Advisory Warns of Threats Posed by Virtual Currency Misuse.* Available from: https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual. [Accessed 25 July 2020].

Fleder, M., Kester, M. S., and Pillai, S. (2015). Bitcoin transaction graph analysis. arXiv:1502.01657.

Flood, G. (2020). *Graph proves an ideal way to answer the 'Who Owns Me?' anti-money laundering question.* Available from: https://diginomica.com/graph-proves-ideal-way-answer-who-owns-me-anti-money-laundering-question [Accessed 18 May 2020].

Frost, J. (2018). *Banking royal commission: CBA finds 45 new money-laundering flaws*. Available from: https://www.afr.com/companies/financial-services/banking-royal-commission-cba-finds-45-new-money-laundering-flaws-20181120-h184fs [Accessed 18 May 2020].

F-Secure (2017). *Wannacry, the biggest ransomware outbreak ever.* Available from: https://safeandsavvy.f-secure.com/2017/05/12/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/ [accessed 28 June 2017].

Fokker J., and Beek C. (2019). *McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – Follow The Money*. Episode 3: Follow the Money, McAfee Labs. Available from: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-follow-the-money/ [Accessed 11 November 2019].

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., & Pesch, P. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, 33: 200902.

Furneaux, N. (2018). *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence.* John Wiley & Sons.

Gaihre, A., Luo, Y., and Liu, H. (2018). Do bitcoin users really care about anonymity? an analysis of the bitcoin transaction graph. In *2018 IEEE International Conference on Big Data* (pp. 1198-1207).

Gaihre, A., Pandey, S., and Liu, H. (2019). Deanonymizing cryptocurrency with graph learning: the promises and challenges. In *2019 IEEE Conference on Communications and Network Security* (pp. 1-3).

Galler, B. A., and Fisher, M. J. (1964). An improved equivalence algorithm. *Communications of the ACM*, 7(5): 301-303.

Gartner (2021). *Gartner Says Threat of New Ransomware Models is the Top Emerging Risk Facing Organizations.* Available from: https://www.gartner.com/en/newsroom/press-releases/2021-10-21-gartner-says-threat-of-new-ransomware-models-is-the-top-emerging-risk-facing-organizations [Accessed 20 February 2022].

Gottschalk, P. (2015). *Internal investigations of economic crime: Corporate case studies and regulatory policy.* Universal-Publishers.

Goyal, P., and Ferrara, E. (2018). Graph embedding techniques, applications, and performance: A survey. *Knowledge-Based Systems*, 151: 78-94.

Graves, A. and Clancy, K. (2019). *Unsupervised learning: The curious pupil.* Available from: https://deepmind.com/blog/article/unsupervised-learning [Accessed 12 August 2020].

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Wired Magazine. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 19 January 2020].

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social net- works. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, 7-10 November 2005, pp. 71-80.

Guerrero-Saade J., A., and Moriuchi P. (2018). *North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign*. Recorded Future Report, CTA-2018-0116. Available from: https://www.recordedfuture.com/north-korea-internet-usage/ [Accessed 7 November 2018].

Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S., and Yang, G. Z. (2019). XAI—Explainable artificial intelligence. Science Robotics, 4(37): p.eaay7120.

Gupta, B., Iyer, L. S., and Aronson, J. E. (2000). Knowledge management: practices and challenges. *Industrial Management & Data Systems*, 100(1): 17-21.

Hamilton, W. L., Ying, R., and Leskovec, J. (2017). Inductive representation learning on large graphs. In *Proceedings of the 31st International Conference on Neural Information Processing Systems* (pp. 1025-1035).

Hampton, N., and Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. In *13th Australian Information Security Management Conference* (pp. 47-56).

Han, J., Kamber, M., and Pei, J. (2012). Getting to Know Your Data. In *The Morgan Kaufmann Series in Data Management Systems, Data Mining (Third Edition)* (pp. 39-82). Morgan Kaufmann.

Harlev, M. A., Sun Yin, H., Langenheldt, K. C., Mukkamala, R., and Vatrapu, R. (2018). Breaking bad: De-anonymising entity types on the bitcoin blockchain using

supervised machine learning. In *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Hayne, K. M. (2019). *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*. Australian Government. Available from: https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf [Accessed 18 May 2020].

Heuer, R. J. (1999). *Psychology of intelligence analysis.* Center for the Study of Intelligence.

Hitbtc Review (2018). *Trading Blog: HitBTC Exchange: The Registration Steps.* Available from: https://hitbtc-review.net/hitbtc-exchange-registration-steps.html [Accessed 15 November 2018].

Hirsch, C. (2018). *C*ollateral Damage Outcomes are Prominent in Cyber Warfare, Despite Targeting. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (pp. 281-6).

Hodler, A. E. (2020). *Financial Fraud Detection with Graph Data Science.* Available from: https://neo4j.com/blog/financial-fraud-detection-graph-data-science-identifying-fraud-rings/ [Accessed 18 May 2020].

Holley, M. (2018). *Ransomware - Identifying Patient Zero.* Available from: https://www.contextis.com/en/blog/ransomware-identifying-patient-zero [Accessed 22 October 2018].

Huang, D. Y., McCoy, D., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., and Snoeren, A., C. (2018). Tracking

Ransomware End-to-end. In *2018 IEEE Symposium on Security and Privacy* (pp. 20-24).

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, 28(2): 201-207.

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, 7(3-4): 105-113.

Hutchins, M. (2017). *How to Accidentally Stop a Global Cyber Attack.* Available from: https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html [Accessed 22 October 2018].

Hutchins E., M., Cloppert M. J., and Amin R., M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*, 1(1): 80.

Intel 471 (2020). *Ransomware as a service.* Available from: https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/)

Irwin, A. S., and Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control*, 21(3): 297-313.

Jobse, F. (2017). *Detecting suspicious behavior in the Bitcoin network.* PhD thesis, Tilburg University. Available from: http://arno.uvt.nl/show.cgi?fid=145288 [Accessed 23 October 2021].

Joh, E. E. (2017). Artificial intelligence and policing: First questions. *Seattle University Law Review*, 41: 1139.

Jolliffe, I. T., and Cadima, J. (2016). Principal component analysis: a review and recent developments. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2065): 20150202.

Jones, T., Chapman, G., Cleese, J., Gilliam, T., Idle, E. and Palin, M. (1999). *Monty Python's life of Brian*. Python pictures.

Jung, K. (2019). *Bitcoin Ransomware Detection with scalable Graph Machine Learning.* CSIRO, Data61. Available from: https://yowconference.com.au/slides/yowdata2019/KevinJung_BitcoinRansomwareDetection.pptx [Accessed 18 August 2019].

Kamath, V. (2011). *Introduction to Machine Learning using Python.* Available from: https://in.pycon.org/2011/static/files/talks/11/Introduction_To_ML_Partial_2.pdf [Accessed 12 March 2016].

Kaminsky, D. (2011). *Some thoughts on Bitcoin.* Available from: http://dankaminsky.com/2011/08/05/bo2k11 [Accessed 15 July 2015].

Kaspersky Lab. (2017). *WannaCry: Are you safe?* Available from: https://www.kaspersky.com/blog/wannacry-ransomware/16518/ [Accessed 19 October 2018].

Kaspersky Lab. (2018). *What is an Advanced Persistent Threat (APT)?* Available from: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats [Accessed 24 October 2018].

Karame, G. O., Androulaki, E., and Capkun, S. (2012). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 906-917).

Kelion, L. (2013). *Cryptolocker ransomware has 'infected about 250,000 PCs'*. Available from: https://www.bbc.com/news/technology-25506020 [Accessed 23 October 2018].

Kujawa, A., Zamora, W., Umawing, J., Segura, J., Tsing, W., Rivero, M., Hasherezade, Boyd, C., Arntz, P., and Ruiz, D. (2019). *Cybercrime tactics and techniques: ransomware retrospective.* Available from: https://blog.malwarebytes.com/reports/2019/08/labs-quarterly-report-finds-ransomwares-gone-rampant-against-businesses/ [Accessed 30 November 2019].

Kumar, D. K., and Sanicola, S. (2021). *Pipeline outage causes U.S. gasoline supply crunch, panic buying.* Available from: https://www.reuters.com/business/energy/us-fuel-supplies-tighten-energy-pipeline-outage-enters-fifth-day-2021-05-11/

Laffan, K. (2020). *A Brief History of Ransomware.* Varonis. Available from: https://www.varonis.com/blog/abriefhistoryofransomware/#:~:text=The%20first%20documented%20and%20purported,known%20as%20PS%20Cyborg1.&text=But%20after%2090%20reboots%2C%20the,%24189%20to%20PC%20Cyborg%20Corp [Accessed 16 February 2021].

Lakshmanan, V., Robinson, S., and Munn, M. (2020). *Machine learning design patterns.* O'Reilly Media.

Law Library of Congress. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions.* Available from: https://www.loc.gov/law/help/legal-reports.php; https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf [Accessed 25 July 2020].

Le Carré, J. (2002). *Tinker, tailor, soldier, spy*. Simon and Schuster.

Li, V. (2020) *Intro to Malware Detection using YARA*. Available from: https://medium.com/bugbountywriteup/intro-to-malware-detection-using-yara-eacab8373cf4 [Accessed 26 August 2020].

Li, Y., Gu, C., Dullien, T., Vinyals, O., and Kohli, P. (2019). Graph Matching Networks for Learning the Similarity of Graph Structured Objects. In *Proceedings of the 36th International Conference on Machine Learning* (pp. 3835-3845).

Lim, J.W., 2015. A Facilitative Model for Cryptocurrency Regulation in Singapore. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, p.361.

Logical Clocks. (2019). *AI & Deep Learning for Fraud & AML*. Available from: https://www.logicalclocks.com/blog/ai-deep-learning-for-anti-money-laundering [Accessed 11 August 2020].

Lopez-Rojas, E. A., Elmir, A., and Axelsson, S. (2016). PaySim: A financial mobile money simulator for fraud detection. In *The 28th European Modeling and Simulation Symposium, EMSS* (pp. 249-255).

Macnish, K., Wright, D., and Jiya, T. (2020). Predictive policing in 2025: A scenario. In *Policing in the Era of AI and Smart Societies* (pp. 199-215).

Mackenzie, P. (2019). *WannaCry Aftershock.* Sophos. Available at: https://www. sophos. com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf [Accessed 27 January 2021].

Maesa, D. D. F., Marino, A., and Ricci, L. (2018). Data-driven analysis of Bitcoin properties: exploiting the users graph. *International Journal of Data Science and Analytics*, 6(1): 63-80.

Malwarebytes (2020). *Threat spotlight: the curious case of Ryuk ransomware*. Available from: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware)

Mann, J., Lawal, T., Czajka, D., and Kelley, J. (2011). The ethical implication of computing and how public policy can shape the future of technology. Subsection - E-gold. Academic research project for CS181: Computers, Ethics, and Public Policy. Taught by Eric Roberts. Stanford University. Available from: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Bitcoins/e-gold.html [Accessed 17 February 2021].

Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World Neurosurgery*, 104: 972-974.

Mavroeidis, V., and Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98).

Mayor, S. (2018). Sixty seconds on . . . the WannaCry cyberattack. *British Medical Journal*, 361: k1750. Available from: https://doi.org/10.1136/bmj.k1750 [Accessed 7 November 2018].

Mazerick, R. (2018). *Understanding DNS Sinkholes – A weapon against malware.* Available from: https://resources.infosecinstitute.com/dns-sinkhole/#gref [Accessed 19 November 2018].

McMillan, R., (2013) *Definition: Threat Intelligence*. Gartner Research ID: G00249251, May 16, 2013. Available from: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence [Accessed 06 May 2021].

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement* (pp. 127-140).

Michalski, R., Macek, P., Dziubałtowska, D. (2020). *Bitcoin addresses and their categories.* Available from: https://doi.org/10.7910/DVN/KEWU0N

Miles, C. (2020). *Detecting Cryptocurrency Fraud with Neo4j*. Available from: https://neo4j.com/blog/detecting-cryptocurrency-fraud-with-neo4j/ [Accessed 18 May 2020].

Mishra N. (2018). *Anomaly detection in dynamic graphs using MIDAS: An interesting approach to modelling network security.* Available from:

https://towardsdatascience.com/anomaly-detection-in-dynamic-graphs-using-midas-e4f8d0b1db45 [Accessed 18 May 2020].

Modi, A., Sun, Z., Panwar, A., Khairnar, T., Zhao, Z., Doupé, A., Ahn, G. J., and Black, P. (2016). Towards automated threat intelligence fusion. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)* (pp. 408-416).

Monamo, P., Marivate, V., and Twala, B. (2016, August). Unsupervised learning for robust Bitcoin fraud detection. In *Information Security for South Africa (ISSA)* (pp. 129-134).

Munkachy, A. (2018). *HitBTC Exchange Review – A High Volume Exchange with Anonymous Leaders.* Available from: https://coiniq.com/hitbtc-exchange-review/#Verification [Accessed 15 November 2018].

Nair, P. (2020). *FBI Warns of DoppelPaymer Ransomware Attack Surge*. Available from: https://www.bankinfosecurity.com/fbi-warns-doppelpaymer-ransomware-attack-surge-a-15630)

Nakamoto, S. (2008). *A peer-to-peer electronic cash system.* Available from: https://bitcoin.org/bitcoin.pdf [Accessed 13 August 2020].

National Cyber Security Centre (2018). *Russian military 'almost certainly' responsible for destructive 2017 cyber attack.* Available from: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack [Accessed 20 February 2022].

Needham, M., and Hodler, A. E. (2019). *Graph Algorithms: Practical Examples in Apache Spark and Neo4j*. O'Reilly Media.

Needham, M., and Hodler, A. E. (2021). *Graph Data Science For Dummies. Neo4j Special Edition.* John Wiley & Sons, Inc.

Neo4j Docs - GraphSage (2021). *GraphSage Beta.* Available from: https://neo4j.com/docs/graph-data-science/current/algorithms/graph-sage/#algorithms-embeddings-graph-sage [Accessed 10 October 2021].

Neo4j Docs - Graph Catalogue (2021). *Graph Catalogue.* Available from: https://neo4j.com/docs/graph-data-science/current/management-ops/graph-catalog-ops/ [Accessed 10 October 2021].

Nerurkar, P., Busnel, Y., Ludinard, R., Shah, K., Bhirud, S., and Patel, D. (2020). Detecting Illicit Entities in Bitcoin using Supervised Learning of Ensemble Decision Trees. In *Proceedings of the 2020 10th International Conference on Information Communication and Management* (pp. 25-30).

Neutrino. (2017). WannaShift to Monero. Neutrino Research Team - 2017-09-01. Available from: https://www.neutrino.nu/Research_WannaShift_to_Monero.html [Accessed 7 November 2018].

Oasis (2020). Introduction to STIX. Cyber Threat Intelligence Technical Committee. Available from: https://oasis-open.github.io/cti-documentation/stix/intro.html [Accessed 31 October 2020].

O'Brien, D. (2017). *Internet Security Threat Report (ISTR) Ransomware.* Symantec. Available from: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf [Accessed 19 October 2018].

Oliveira, C., Torres, J., Silva, M. I., Aparício, D., Ascensão, J. T., and Bizarro, P. (2021). *GuiltyWalker: Distance to illicit nodes in the Bitcoin network*. arXiv preprint arXiv:2102.05373.

Osborne, C. (2019). *Ransomware still dominates the cyber threat landscape in 2019*. Europol report. Available from: https://portswigger.net/daily-swig/ransomware-still-dominates-the-cyber-threat-landscape-in-2019-europol-report [Accessed 29 November 2019].

Osinski, S. (2003). *An algorithm for clustering of web search results*. Master Thesis, Poznan University of Technology, Poznan.

Oswald, M., and Babuta, A. (2021). Machine learning predictive algorithms and the policing of future crimes: governance and oversight. In J. L. M. McDaniel and K. G. Pease (eds.) *Policing and Artificial Intelligence*. Routledge.

Oxford Dictionary (2018). Script Kiddie. Oxford Leaner's Dictionary, Oxford University Press. Available from: https://www.oxfordlearnersdictionaries.com/definition/english/script-kiddie [Accessed 19 October 2018].

Page, L., Brin, S., Motwani, R., and Winograd, T. (1999). *The PageRank citation ranking: Bringing order to the web*. Stanford InfoLab.

Paquet-Clouston, M., Haslhofer, B., and Dupont, B. (2018). Ransomware payments in the bitcoin ecosystem, in *The 17th Annual Workshop on the Economics of Information Security (WEIS)* (Innsbruck). doi: 10.1093/cybsec/tyz003.

Paquet-Clouston M., Haslhofer B., and Dupont B. (2019). Ransomware Payments in the Bitcoin Ecosystem. *Journal of Cybersecurity*, 5(1): 1-11.

Park, J. (2021). *The Lazarus group: The Cybercrime Syndicate Financing the North Korea State*. Harvard International Review, 42(2), 34-39.

Parliament of Australia (2021). *Ransomware Payments Bill 2021 (No. 2).* Available from: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fs1313%22 [Accessed 20 February 2022].

Perozzi, B., Al-Rfou, R., and Skiena, S. (2014). Deepwalk: Online learning of social representations. In *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 701-710).

Pilarowski, G. and Yue, L. (2017). *PBOC, CAC, MIIT, SAIC, CBRC, CSRC, and CIRC, Announcement on Preventing Financial Risks from Initial Coin Offerings.* Available from: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html (in Chinese), archived at https://perma.cc/N88N-5CV5. See also China Bans Initial Coin Offerings and Cryptocurrency Trading Platforms, China Regulation Watch. Available from: http://www.pillarlegalpc.com/en/news/2017/09/21/china-bans-initial-coin-offerings-and-cryptocurrency-tradingplatforms/, archived at https://perma.cc/VQ2W-T4HY. [Accessed 28 August 2020].

Pineda, M. (2014) *Exclusive interview with founder of LOCALBITCOINS.COM: Jeremias Kangas.* Available from: https://bitcoinist.com/exclusive-interview-with-founder-of-localbitcoins-com-jeremias-kangas/ [Accessed 23 October 2018].

Poursafaei, F., Rabbany, R. and Zilic, Z. (2021). SigTran: Signature Vectors for Detecting Illicit Activities in Blockchain Transaction Networks. In *Pacific-Asia Conference on Knowledge Discovery and Data Mining* (pp. 27-39).

Purplesec. (2020). The Growing Threat of Ransomware. Available from: https://purplesec.us/resources/cyber-security-statistics/ransomware/ [Accessed 12 August 2020].

Poisel, R. A. (2013). *Information warfare and electronic warfare systems*. Artech House.

Reardon, B., Nance, K., and McCombie, S. (2012). Visualization of ATM usage patterns to detect counterfeit cards usage. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3081-3088).

Redman, J. (2016). *Russian Authorities Ban LocalBitcoins, Contradicting Previous Statements.* Available from: https://news.bitcoin.com/russian-blacklist-localbitcoins/. [Accessed 8 November 2018].

Reeves, P., and Wilcock, G. (2019). *Anti-Money Laundering.* Available from: https://gettingthedealthrough.com/area/50/jurisdiction/5/anti-money-laundering-australia/ [Accessed 18 May 2020].

Reid, F., and Harrigan, M. (2011). An analysis of anonymity in the bitcoin system, in 2011 *International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing* (Boston, MA). doi: 10.1109/PASSAT/SocialCom.2011.79

Reid, F., and Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, and A. Pentland (eds.)

Security and Privacy in Social Networks (pp. 197 – 223). Springer.

Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems*, 88: 173-190.

Richardson, R., and North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1): 10.

Richert, W., and Coelho, L. P. (2015). *Building machine learning systems with Python, 2nd edition.* Packt Publishing.

RiskSense (2021) Ransomware – Through the Lens of Threat and Vulnerability Management. Available from: https://risksense.com/ransomware-report-2021/ [Accessed 22 April 2021].

Rizzo, P. (2014). *LocalBitcoins 'Exploring Options' After Service Halt in Germany*, *CoinDesk*. Available from: https://web.archive.org/web/20160410172937/http:/www.coindesk.com/localbitcoins-exploring-options-service-halt-germany/ [Accessed 1 March 2017].

Rodriguez, L., J. (2020). Defining ATT&CK Data Sources, Part I: Enhancing the Current State. Available from: https://medium.com/mitre-attack/defining-attack-data-sources-part-i-4c39e581454f [Accessed 31 October 2020].

Ron, D., and Shamir, A. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph. *The International Association for Cryptologic Research (IACR) Cryptology ePrint Archive*, 584.

Ron, D., and Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. In *International Conference on Financial Cryptography and Data Security*, (pp. 6-24).

Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980.

Rossi, R. A., Zhou, R., and Ahmed, N. K. (2017). Deep feature learning for graphs. arXiv preprint arXiv:1704.08829.

Sanger D. E., and Perlroth, N. (2021). *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity.* New York Times. Available from: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Seagle, A.N. (2015). Intelligence sharing practices within NATO: an English school perspective. International Journal of Intelligence and CounterIntelligence, Vol. 28 No. 3, pp. 557-577.

Schwartz, M. J. (2020). *More Ransomware-as-a-Service Operations Seek Affiliates*. Available from: https://www.databreachtoday.com/more-ransomware-as-a-service-operations-seek-affiliates-a-15378)

Secureworks (2017). *WCry Ransomware Analysis.* Available from: https://www.secureworks.com/research/wcry-ransomware-analysis [Accessed 7 November 2018].

Sedgewick, K. (2019). *Bitcoin History Part 17: That Time Mt. Gox Destroyed 2,609 BTC*. Available from: https://news.bitcoin.com/bitcoin-history-part-17-that-time-mt-gox-destroyed-2609-btc/ [Accessed 18 May 2019].

Silver, N. (2012). *The Signal and the Noise – Why so many predictions fail – but some don't.* Penguin Press.

Skiena, S. (2008). *The Algorithm Design Manual.* Springer.

Spagnuolo, M., Maggi, F., and Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security* (pp. 457-468).

Statista (2018). *Bitcoin market capitalization quarterly 2012-2018.* Available from: https://www.statista.com/statistics/377382/bitcoin-market-capitalization/ [Accessed 18 October 2018].

Steenfatt, N., Nikolentzos, G., Vazirgiannis, M., and Zhao, Q. (2018). Learning Structural Node Representations on Directed Graphs. In *International Conference on Complex Networks and their Applications* (pp. 132-144).

Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. *Information & Communications Technology Law*, 21(3): 221-236.

Su, L., Shen, X., Du, X., Liao, X., Wang, X., Xing, L., and Liu, B. (2021). Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications. In *30th USENIX Security Symposium (USENIX Security 21) (pp. 1307-1324).*

Sussman, B. (2020). *New Orleans Ransomware Attack Costs Climb to $7 Million*. Available from: https://www.secureworldexpo.com/industry-news/new-orleans-ransomware-attack-update-cost [Accessed 18 May 2020].

Symantec (2018). *Internet Security Threat Report (ISTR) Volume 23.* Available from: https://www.symantec.com/security-center/threat-report [Accessed 19 October 2018].

Thulasiraman, K., and Swamy, M. N. (2011). *Graphs: theory and algorithms.* John Wiley & Sons.

Tiao, L., Elinas, P., Nguyen, H., and Bonilla, E.V. (2019). Variational Spectral Graph Convolutional Networks. arXiv:1906.01852.

Trend Micro (2019). *Report: Huge Increase in Ransomware Attacks on Businesses.* Available from: https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/report-huge-increase-in-ransomware-attacks-on-businesses [Accessed 29 November 2019].

Trend Micro (2021). What We Know About the DarkSide Ransomware and the US Pipeline Attack. Available from: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html [Accessed 20 February 2022].

Trend Micro (2022). Ukraine Cyberattack 2022: Geopolitical Cybersecurity. Available from: https://www.trendmicro.com/en_ae/research/22/b/ukraine-cyberattack-2022.html [Accessed 20 February 2022].

Tong, F. (2019). *Graph Embedding for Deep Learning Graph Learning and Geometric Deep Learning - Part 1.* Available from: https://towardsdatascience.com/overview-of-deep-learning-on-graph-embeddings-4305c10ad4a4 [Accessed 18 May 2020].

Tromer, E. (2008). *Cryptanalysis of the Gpcode.Ak ransomware virus.* Available from: rump2008.cy.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf

Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. *Berkeley Technology Law Journal*, 30(4): 1127-1170.

Tu, K. V., and Meredith, M. W. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Washington Law Review*, 90: 271.

Turner, A. (2021). Bitcoin blockchain data of address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw. IEEE Dataport. Available from: doi: https://dx.doi.org/10.21227/1amp-n662.

Turner, A., and Irwin, A. S. M. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. *Journal of Financial Crime*, 25(1): 109-130.

Turner, A., McCombie, S., and Uhlmann, A. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control*, 22(4): 646-665.

Turner A. B., McCombie, S., and Uhlmann, A. J. (2020a). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science*, 2: 600596.

Turner, A. B., McCombie, S., and Uhlmann, A. J. (2020b). Discerning payment patterns in Bitcoin from ransomware attacks. *Journal of Money Laundering Control*, 23(3): 545-589.

Turner, A., McCombie, S., and Uhlmann, A. (2021). Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 1560).

Turner, A.B., McCombie, S. and Uhlmann, A. J. (2022). Ransomware-Bitcoin threat intelligence sharing using Structured Threat Information Expression (STIX), *IEEE Security & Privacy*. DOI: 10.1109/MSEC.2022.3166282 Manuscript Number: SP-2021-07-0157.

Twitter (2017). Actual ransom. Available from: https://twitter.com/actual_ransom?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fqz.com%2F982993%2Fwatch-as-these-bitcoin-wallets-receiveransomware-payments-from-the-ongoing-cyberattack%2F [Accessed 21 June 2017].

UNODC (2021). *US v Liberty Reserve et al.* Case Law Database. Available from: https://sherloc.unodc.org/cld/caselawdoc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html [Accessed 17 February 2021].

Ussath, M., Jaeger, D., Cheng, F., and Meinel, C. (2016). Pushing the limits of cyber threat intelligence: extending STIX to support complex patterns. In *Information Technology: New Generations* (pp. 213-225).

U.S. District Court, Central District of California (2018). *United States of America v. Park Jin Hyok.* Available from: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and [Accessed 20 September 2018].

U.S. DOJ (2014). *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator.* Available from: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware [Accessed 12 December 2021].

U.S. DOJ (2017). *Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit, Boston, MA.* Available from: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit [Accessed 18 October, 2018].

U.S. DOJ (2021a). *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe.* United States Department of Justice. Available from: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and)

U.S. DOJ (2021b). *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside.* United States Department of Justice. Available from: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

U.S. DOJ (2021c). *Department of Justice Launches Global Action Against NetWalker Ransomware.* United States Department of Justice. Available from: https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware)

United States (U.S) Department of State (2021). DarkSide Ransomware as a Service (RaaS). Available from: https://www.state.gov/darkside-ransomware-as-a-service-raas/ [Accessed 20 February 2022].

Voutila, D. (2020). *Analyzing First Party Fraud with Neo4j*. Available from: https://www.sisu.io/posts/paysim-part3/ [Accessed 18 May 2020].

Wagstaff, J., and Karpeles, M. (2014). *Mt. Gox bitcoin debacle: Huge heist or sloppy glitch.* Reuters. Available from: https://www.reuters.com/assets/print?aid=USBREA1R0Y720140228 [Accessed 22 July 2020].

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., and Leiserson, C., E. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. Tutorial in the Anomaly Detection in Finance Workshop at the 25th SIGKDD Conference on Knowledge Discovery and Data Mining.

Wikipedia. (2018). *False flag*. Available from: https://en.wikipedia.org/wiki/False_flag [Accessed 15 November 2018].

Wolf, B. (2021). *Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say*. Thomas Reuters. Available from: https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipelineransomfunds/#:~:text=When%20announcing%20the%20DOJ's%20recovery,at%20U.S.%20East%20Coast%20gas [Accessed 20 February 2022].

Woods, J. (2018). *Crypto Exchanges: Custodial vs. Non-Custodial vs. Decentralized.* Available from: https://medium.com/@jacobrobertwoods/crypto-exchanges-custodial-vs-non-custodial-vs-decentralized-3d1d04cf205 [Accessed 15 November 2018].

Woodward, A. (2017). *WannaCry ransomware bitcoins move from online wallets. Analysis by Andrew Woodward.* Available from: https://www.bbc.com/news/technology-40811972 [Accessed 23 October 2018].

Yin, H. S., and Vatrapu, R. (2017). A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In *2017 IEEE International Conference on Big Data* (pp. 3690-3699).

Young, J. (2015). BitQuick and Local Bitcoins Terminate Service in NY due to BitLicense Compliance Costs. *Bitcoin Magazine.* Available from: https://bitcoinmagazine.com/articles/bitquick-local-bitcoins-terminate-service-ny-due-bitlicense-compliance-costs-1439414074/. [Accessed 8 November 2018].

Zetter, K. (2015, September 17). Hacker Lexicon: A guide to Ransomware, the scary hack that's on the rise. Available from: http://www.gocs.de/lektionen/handbuch/original/H-L-RAMSON_origin.pdf. [Accessed 30 April 2022].

Zhang, S. J., Hagenbuchner, M., Scarselli, F., and Tsoi, A. C. (2009). Supervised encoding of graph-of-graphs for classification and regression problems. In *International Workshop of the Initiative for the Evaluation of XML Retrieval* (pp. 449-461).