POLICING BITCOIN: INVESTIGATING, EVIDENCING AND PROSECUTING CRIMES INVOLVING CRYPTOCURRENCY

Cryptocurrencies have increasingly become a common method of value exchange in a number of types of criminal activity; notably in May 2017 the NHS was crippled by a global cyber-attack whereby Ransomware was utilized to demand payment for the decryption of encrypted files in bitcoin. This collaborative project has brought together a variety of experts from different disciplines and practices to explore the challenges posed by criminal use of cryptocurrency with regard to the investigation, production of conclusive evidence of wrongdoing, and prosecution of offenders.

KEY FINDINGS

- Cryptocurrencies (mainly Bitcoin) have become a popular choice for criminals.
- They are facilitating criminal transactions and crimes such as money laundering, extortion (ransomware), blackmail, and fraud.
- There is currently a lack of experience in law enforcement agencies in conducting effectively investigations and prosecutions of crimes involving cryptocurrencies.
- UK law enforcement needs to coordinate a more strategic approach to counter the threat posed by cryptocurrencies.
- Bitcoin transactions are not completely anonymous so by improving training and access to industry tools, UK law enforcement would improve its capability to investigate and prosecute these types of crimes.
- In this research scenarios were developed based upon dark-web purchases and sextortion using crypto-currencies bitcoin and monero.
    - Mock warrants were executed and devices seized.
    - The purchase of Bitcoin using ATMs, exchanges was also explored.
    - Both open-source and private industry track and trace tools were used to identify potential lines of enquiry on the blockchain.
- A review of different types of cryptocurrency was compiled.
- Training and Guidance has been produced for police officers and agencies.
- Academic publications will be produced from this research.

INTRODUCTION

- Cryptocurrencies (mainly Bitcoin) have become a popular choice of criminals. They are facilitating criminal transactions and also crimes such as money laundering, extortion (following data breaches), blackmail (the threat of DDOS attacks) and fraud. Whilst loopholes currently exist to encourage criminality, such as the pseudo-anonymous nature of bitcoin and the lack of experience by law enforcement agencies, the technology underlying cryptocurrencies, especially the Blockchain principle, possesses some potentially interesting opportunities for investigators. It is therefore essential to adopt a strategic approach to training UK law enforcement to effectively investigate and prosecute crimes involving cryptocurrencies.
- This collaborative project between law enforcement and academia has brought together a variety of experts from different disciplines and practices to explore these challenges, particularly with regard to the investigation, production of conclusive evidence of wrongdoing, and prosecution of offenders.
- The research was conducted in two parts. The first was a practical exploration involving the development of crime scenarios involving Bitcoin, part-based upon an actual forensic examination of criminal activity and also some sample purchases of criminal goods from the dark web. The second was an open sourced review that explored all contemporary crypto-currencies, at how they operate and how they are developing in order to ascertain their potential for criminal use.
- The outcome of this research, therefore, provides increased general knowledge about crypto-currencies, their variations and developments and also their relative strengths and weaknesses.
- The research also provides specific guidance for police officers to use in relation to bitcoin investigations.

SCENARIO 1 – DARK WEB PURCHASES

As part of this research dark web marketplaces were accessed and a number of goods were purchased using crypto-currencies bitcoin and monero. A mock warrant was executed and devices seized; Dr Syed Naqvi of Birmingham City University then conducted digital forensic examinations to identify bitcoin activity.

SCENARIO 2 – SEXTORTION

A likely scenario was recreated and officers analysed transaction data on the blockchain – the publicly accessible ledger which records all bitcoin transactions. A mock warrant was executed and bitcoin was seized, this generated debate amongst the group regarding the current legal powers available to the police.

BITCOIN ATMS

In order to purchase goods from the criminal marketplace Alphabay, bitcoin was bought from an ATM at a local high street store in Manchester City Centre. There is currently no regulation of Bitcoin ATMs in the UK; subsequently they provide an ideal opportunity for criminals to launder and transfer the proceeds of crime.

BITCOIN EXCHANGES

Bitcoin exchanges have made various attempts to comply with international money laundering standards; many conduct "Know Your Customer" checks, requiring passports or driving licence scans to set up accounts. It is however possible for criminals to bypass these and further industry collaboration is needed.

TRACK AND TRACE TOOLS

There are a number of open source tools available that can be used by law enforcement to try and attribute and trace bitcoin activity on the blockchain. These do however require a certain amount of knowledge and expertise. Private companies such as Chainalysis and Elliptic provide user-friendly alternatives however current access across UK law enforcement is limited.

LITERATURE REVIEW AND SEARCH OFFICER GUIDE

There is a significant knowledge gap across UK law enforcement with regards to cryptocurrency and experience in identifying bitcoin activity, both physically and digitally. As part of the project a literature review was commissioned by Professor David Wall; this comprehensive document will provide a foundation for further research in to crypto-currencies and associated criminal activity such as ransomware.

BOOKLET DESIGNED TO HELP OFFICERS TO IDENTIFY BITCOIN ACTIVITY

Officers regularly seize cash from criminals utilising POCA and PACE legislation however the seizure of bitcoin remains a rarity and this is anecdotally, due to officers not knowing A. what bitcoin is, and B. what to look for. Subsequently Phil Larratt and Paul Taylor from GMP have produced a four page booklet designed to help officers to identify bitcoin activity.

NATIONAL LAW ENFORCEMENT CRYPTOCURRENCY WORKING GROUP

As part of the N8 research, the first UK law enforcement community of interest group meeting was held in February 2017, bringing together officers from across the UK who all have experience of bitcoin investigations. Key issues have since been identified and the network of expertise is being utilised to provide advice to live crimes, financial investigations and front line officers.

STRATEGIC TRAINING RECOMENDATION

As a result of the research, it has been determined that there are significant knowledge gaps amongst UK law enforcement, from frontline staff to national agencies. A recent estimate by Europol states that 3% of all money laundering globally is now committed using cryptocurrencies and subsequently a more coordinated approach to training and development is needed. A four tier training programme has been recommended to upskill officers across UK law enforcement;

- Tier 1 – Bitcoin experts – The skills, knowledge and experience of the BTC working group should be formalised and staff trained as expert witnesses. Evidence from investigators indicates that police forces are paying private companies to provide expert witness statement and evidence in relation to bitcoin investigations. By developing an in-house capability, substantial savings could be made.

- Tier 2 - National Cyber-Crime Units / Regional Cyber Crime Units – Officers at both national and regional cyber-crime units should have access to private industry track and trace tools, this would improve their capability to investigate bitcoin transactions and associated activity.
- Tier 3 – Digital Media Investigator (DMI) network – DMIs should be upskilled through CPD sessions and bespoke training events. This would enable investigators to utilise open source tools to identify and track bitcoin activity.
- Tier 4 – Frontline officers and investigators – All UK police staff should be required to complete a mandatory Bitcoin e-learning package (NCLAT), on how to identify bitcoin activity and who to contact for further advice.

UK LEGISLATIVE FRAMEWORK

As part of the project research was conducted and advice sought regarding the legislative framework available for officers to lawfully seize bitcoin. Subsequently guidance has been produced in relation to detailing bitcoin on search warrants and utilising powers afforded under PACE and POCA to seize and restrain bitcoin. A recommendation has also been made to the Home Office regarding a potential legislative amendment to categorise bitcoin as cash for the purpose of cash seizure legislation.

OTHER ACTIVITY

As part of the research, training inputs have been produced. These are all focused on the evidence base generated from scenario 1 and 2. The talks, “Bitcoin for Investigators” and “Bitcoin for DMIs” have been delivered at local and regional conferences.

FURTHER RESEARCH

The project has identified number of practical and intellectual issues for further research, namely how bitcoin relates to the Proceeds of Crime Act, but also how it is used in ransomware attacks. The research is informing the EPSRC funded EMPHASIS project on Ransomware (EP/P011721/1) that David Wall & Alena Connolly at Leeds are working upon.

The bitcoin working group are also drafting a detailed Bitcoin seizure guide that will provide step-by-step information on how to seize bitcoin. The document is based on the evidence based research conducted as part of the project and also through collaboration with international law enforcement partners.

Philip Larratt (NCA), Paul Taylor (GM Police), David S. Wall (Univ. Leeds), Syed Naqvi (Birmingham City Univ.) Matthew Shillito, Rob Stokes (Liverpool University)

July 2017