

# “Ransomware payments in the Bitcoin ecosystem”

By M. Paquet-Clouston, B. Haslhofer, and B. Dupont

## Article Review

Jeremiah Price

CYSE 201S

Prof. Leigh Armistead

2/15/2021


## Introduction

Online ransomware attacks have been increasing at a rapid speed in recent years, evolving over time as well. They have been striking businesses, families, and individuals who will need to pay a large fee to ever see their files again. This article review will discuss the research, data, analysis and contributions of the “Ransomware payments in the Bitcoin ecosystem” journal as well as its relation to the principles of social science.

The purpose of this journal was for policy-makers and law enforcement to have adequate statistics to make decisions on how to deal with the cybersecurity threat.

## Research

Ransomware and Bitcoin is difficult to research due to its confidentiality and blockchain technology. Data collection is scarce and complicated. As stated “Most of the statistics available on cybercrime and ransomware are produced by private corporations.”



The authors used a “data-driven” method to gather Bitcoin transactions and patterns related to ransomware attacks. These data sets would be outside of those reported by government agencies.

It was found that ransomware was a bigger individual-issue than they thought.

- Many ransomware users relied on smaller attacks and smaller payout to avoid high risk business
- Money would still be made due to a high number of attacks

This was clearly related to certain social science principles. Attackers would send out mass emails, phishing methods, and more to prey on tech-knowledge lacking individuals. Even if the odds of success were 1 in 20, 1000 instances would show profitability.


To research and trace Bitcoin transactions, they took certain Bitcoin addresses that were flagged for possible ransomware activity and traced those addresses transactions. Conducted research concluded that over a two-year period, upwards of 16 million USD were paid for ransom in Bitcoin.

## Method

The researchers devised an intense and comprehensive method to target transactions involved with ransomware. They would take a single address and greatly expand on it, using many filters and equations to find patterns that indicated a flag. Over many instances, this method proved to be working and effective. It was quickly put to work to create multiple tables and models shown in the journal. This was one of the first and most effective methods of tracing bitcoin transactions.

## Data

This method allowed researchers to estimate ransomware market values, trends, and issues and put them into datasets.



In the span of 4 years, the ransomware market has had a minimum value of almost 13 million USD. A high percentage of this market is held by only a few shareholders. This number was fairly low in comparison to what they expected.

This data can be used by agencies and organizations to decide on security-based actions and policies.

## Contributions to Society

This journal had quite a few significant achievements and advances.

- First, the authors are some of the first to shed light on this issue. It is talked about commonly, but not much research is done on it due to the difficulty.
- Second, the method developed to research and target Bitcoin transactions related to ransomware proved to be effective. Corporations and agencies can use this method to help resolve issues and research.
- Third, the market value of the ransomware pandemic was estimated and light was shown on the scale of the problem.

## Relation to the Social Sciences


There are a few questions you might ask yourself while reading this.

- *Why would people do this?*
- *Why do people fall for these ransomware scams?*
- *Is this predictable?*

These questions can be answered if you look at the issue from the social science perspective. Let us begin.

### *Why would people do this?*

- There are criminal people everywhere one may look. Scamming has always been a pandemic.

- 
- In the recent decades, the world has become digitized. The internet is common and accessible to almost all. Tech-savvy scammers and criminals have discovered how to use technology to their advantage.
  - The internet can be anonymous and risk-free. Digital experts can easily manipulate and scam (risk free!) tech-ignorant people.
  - It has less of an impact on the criminals because it feels less personal and it is easier to do. It is anonymous and over the internet. *No one knows it was you!*
  - It grants access to an easy money-making method.

#### *Why do people fall for these ransomware scams?*

- Let's admit it, we all know somebody who is not the brightest when it comes to technology.
- Scammers are able to manipulate those who may not be able to differentiate between a scam email and a real email from the IRS.
- Technological-ignorant individuals are becoming less common, but with scammers being able to send possibly thousands of phishing lines in a minute, it is not hard to catch one bite.

#### *Is this predictable?*

- Many would say that the ransomware pandemic have predicted effectiveness based on the person.
- If you do know someone who is technologically ignorant, they may be subject to these scams.
- To battle this pandemic, digital and information literacy is key to the individuals. Teachers your peers, family members, and coworkers on how to spot these scams may save everyone a lot of money.

## **References**

Masarah Paquet-Clouston, Bernhard Haslhofer, Benoît Dupont, Ransomware payments in the Bitcoin ecosystem, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyz003

<https://doi.org/10.1093/cybsec/tyz003>

—