Ransomware, Bitcoin, and Social Science

Richard W. Young

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Matthew Umphlet

March 28th, 2024

Ransomware, Bitcoin, and Social Science

Ransomware is a popular form of cyber extortion that encrypts a victim's data until a payment is made. One of the most common forms of payment for ransomware is Bitcoin, a form of cryptocurrency. Researchers can use different social sciences, common research strategies, and public cryptocurrency blockchains to investigate why internet crime like ransomware happens so often and how to help thwart it.

Paquet–Clouston et al (2019) explained that "ransomware is a class of malicious software that, when installed on a computer, prevents a user from accessing the device - usually through unbreakable encryption - until the ransom is paid to the attacker." While it may not be easy to research internet crime like ransomware because of international law and the amount of unreported crime, researchers can utilize social sciences (like psychology, sociology, and criminology) and the public peer-to-peer blockchain to hypothesize solutions. One solution to help slow down ransomware could be creating software that organizes public Bitcoin transactions and wallets that would help researchers and law enforcement pinpoint malicious malware families.

Internet crimes like ransomware can be studied through the social sciences. Criminology is the study of crime and the motivations behind it. Sociology is the study of human behavior within a society and the consequences of those behaviors. Psychology is the study of the mind and behavior. These three social sciences tie directly into internet crime because to fix something, one must first know how it works inside and out. The principles of social science also tie to internet crime because an attacker needs a victim for the attack to be successful. Attackers use fear, urgency, computer negligence, and social engineering to execute ransomware attacks. In *The Social Order* by Robert Bierstedt, he argues that the social sciences adhere to the natural

sciences like relativism, objectivity, parsimony, skepticism, determinism, and ethical neutrality. One can relate relativism to internet crime and ransomware by realizing that modern societies promote ransomware through the evolution of technology and the internet. One question that arises when tying natural and social sciences to internet crime could be: What if we wanted to explain why people commit cybercrime?

Common strategies used to study the social dynamics of crime and human behavior are surveys, experiments, case studies, field research, and archival research. Three research methods used in this article to pinpoint malware families and attackers are Bitcoin traceability research, payment inspection, and seed dataset collection. Paquet–Clouston et al (2019) showed that through archival and field research, they were able to separate other Bitcoin users like gambling sites (another inflated Bitcoin user) from malware groups by investigating the clusters of addressed transactions by using publicly available websites that post Bitcoin transactions like Walletexplorer.com, Blockchain.info, and GraphSense.

While tying together how researchers use social and natural sciences with different research methods, one must ask: Who are the biggest targets of a malware team? Small to medium-sized businesses are valuable targets because they commonly lack the cybersecurity resources needed to protect critical information and are highly susceptible to social engineering. Small to medium-sized businesses are key targets because, in the eyes of an attacker, they seem to be the easiest. Another highly valued marginalized group would be critical infrastructure organizations like government, healthcare, and financial institutions. Even though these groups may be harder targets because of higher cybersecurity training, the monetary gain is much higher because these organizations are known for collecting personally identifiable information of employees and have the funds to make the ransom.

The overall contribution to society that this article has made would be how accessible they made their research. This research is important because it provides society with knowledge of how to pinpoint ransomware attackers in the Blockchain and how organizations can protect their critical data. Analyzing Bitcoin blockchain data and applying research through the social sciences can help educate a society which would lessen the amount of ransomware being spread.

References

Paquet–Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity (5)*1. https://doi.org/10.1093/cybsec/tyz003