Review

This article by ECN Magazine details the results and accomplishments of a study led by assistant professor Damon McCoy. This study essentially demystifies ransomware and its ecosystem, inevitably highlighting several challenges that we need to face in order to solve this issue. It first details the key findings of the study — affected demographics and the network's key innerworkings. The study found that South Koreans were disproportionately affected by ransomware attacks, accounting for $2.5 million out of the $16 million in total ransom money extorted. Along with some other details about demographics, the study also found that BTC-E, the Russian Bitcoin exchange platform, was a popular means of converting ransomware payments, typically received in Bitcoin, into US Dollars. BTC-E has since been seized by the US law enforcement, and whether this was due in part by the results of this study was not made clear by the article.

The article, along with the research paper in subject, makes it clear that tackling the problem of ransomware is not exactly a clear task. Bringing arguably the most significant issue into light, both sources acknowledge the existence of ethical issues when facing this problem: researchers are left with the dilemma of prioritizing either the problem or those affected by it. In purely choosing one option, the researchers would have to ignore the other. In other words, according to the article, although it was made clear that a solution was present, executing it "would effectively start the clock," causing the victims to potentially be required to pay an increased amount for their files (1). Although the research paper went into full detail on the challenges they faced, the article did not fully cover them, which in a way undermined the gravity of the issues and how difficult eliminating ransomware was.

Although the public may be becoming more and more aware ransomware, that is not to say that ransomware itself is not evolving. With the rise of cryptocurrencies, ransomware collectors no longer need to rely on archaic online cash payment systems and instead turned to Bitcoin for its unregulated, anonymous nature (2). Thus, it becomes more and more important to address this issue as time goes on. Fortunately, the study yielded impressive results that can potentially enable further study in this field. It takes us one step closer to directly addressing the issue of ransomware and its effects on unsuspecting victims. However, due to the nature of the problem, the study is severely restricted in what it can do to solve the issue directly. Between coverage limitations and ethical boundaries, the study's estimations provide a good starting point in illustrating the impact of ransomware, but it is definitely an underestimation. It is nearly impossible to estimate the total effect of every ransomware family. In addition, by nature, we cannot determine the total number of people affected by ransomware: only the number of people who have completed transactions for these ransoms. The actual figures could be much larger because of unconfirmed and untraceable ransomware interactions.

Overall, there is no clear solution outside of better ransomware detection and backing up files. Finding a clear solution is and will still be a difficult goal that I feel is brought closer by the results of this study.

(1) "Exposed: The Path Of Ransomware Payments." *Electronic Component News*, NYU Tandon School of Engineering, 23 Mar. 2018, www.ecnmag.com/news/2018/03/exposed-path-ransomware-payments.

(2) Huang, Danny YuXing, et al. *Tracking Ransomware End-to-End,* San Francisco, CA, May 2018.