Exposed: The path of ransomware payments

March 23 2018

Credit: CC0 Public Domain

The murky ecosystem of ransomware payments comes into focus in new research led by Damon McCoy, an assistant professor of computer science and engineering at the NYU Tandon School of Engineering. Ransomware attacks, which encrypt and hold a computer user's files hostage in exchange for payment, extort millions of dollars from

individuals each month, and comprise one of the fastest-growing forms of cyber attack.

In a paper slated for presentation at the IEEE Symposium on Security and Privacy in May, McCoy and a team including researchers from the University of California, San Diego; Princeton University; Google; and the blockchain analytics firm Chainalysis provide the first detailed account of the ransomware payment ecosystem, from initial attack to cash-out.

Key findings include the discovery that South Koreans are disproportionately impacted by ransomware campaigns, with analysis revealing that $2.5 million of the $16 million in ransomware payments tracked by the researchers was paid in South Korea. The paper's authors call for additional research to determine the reason that so many South Koreans are victimized and how they can be protected.

The team also found that most ransomware operators used a Russian bitcoin exchange, BTC-E, to convert bitcoin to fiat currencies. (BTC-E has since been seized by the FBI.) The researchers estimate that at least 20,000 individuals made ransomware payments over the past two years, at a confirmed cost of $16 million, although the actual payment total is likely far higher.

McCoy and his collaborators took advantage of the public nature of the bitcoin blockchain technology to trace ransom payments over a two-year period¬. Bitcoins are the most common currency of ransomware payments, and because most victims do not own them, the initial bitcoin purchase provides a starting point for tracking payments. Each ransomware victim is often given a unique payment address that directs to a bitcoin wallet where the ransom is collected. The research team tapped public reports of ransomware attacks to identify these addresses and correlate them with blockchain transactions.

To boost the number of transactions available for analysis, the team also executed real ransomware binaries in a controlled experimental environment, essentially becoming victims themselves and making micropayments to real ransom wallets in order to follow the bitcoin trail. "Ransomware operators ultimately direct bitcoin to a central account that they cash out periodically, and by injecting a little bit of our own money into the larger flow we could identify those central accounts, see the other payments flowing in, and begin to understand the number of victims and the amount of money being collected," McCoy said.

The research team acknowledged that ethical issues prevent exploration of certain aspects of the ransomware ecosystem, including determining the percentage of victims who actually pay to recover their files. McCoy explained that despite having the ability to check for activity connected to a specific payment address, doing so would effectively "start the clock" and potentially cause victims to either pay a double ransom or lose the opportunity to recover their files altogether.

Criminal use of cryptocurrencies is one of McCoy's research focuses. He and fellow researchers previously tracked human traffickers through their use of Bitcoin advertising.

Provided by NYU Tandon School of Engineering