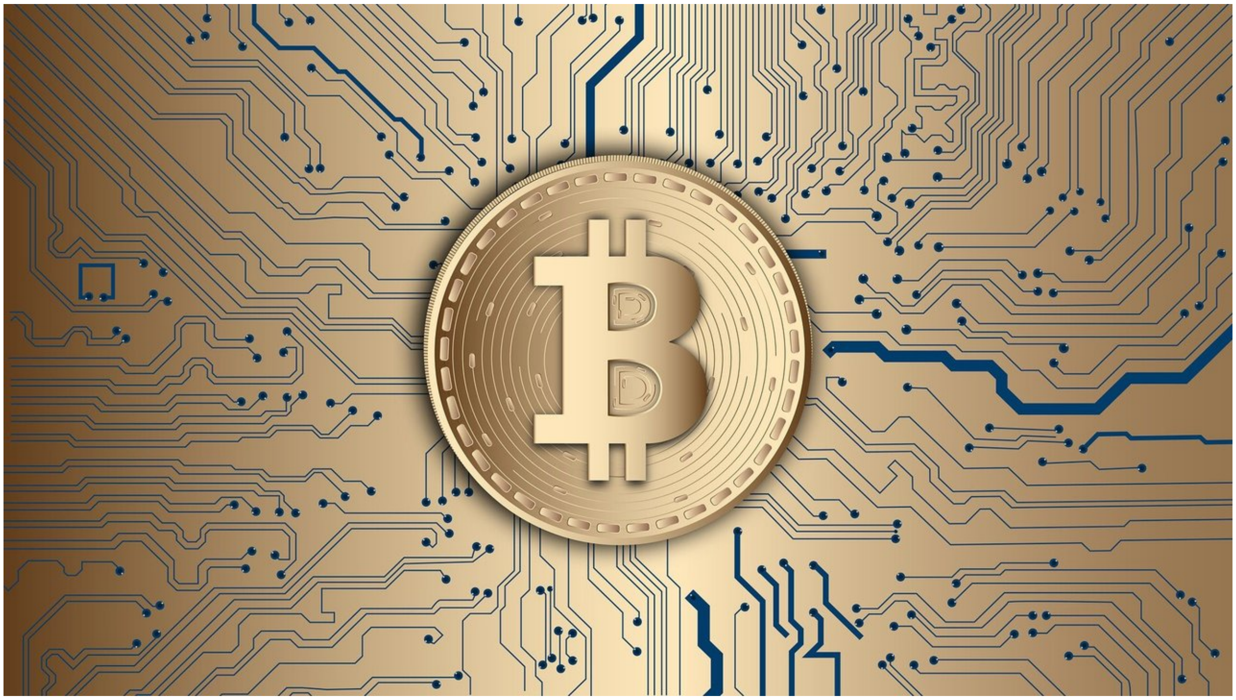
TechXplore

Researchers reveal hidden fortunes and surprising underestimations in cybercrime revenue

December 16 2023



Credit: CC0 Public Domain

To what extent methodological limitations and incomplete data impact the revenue estimations of cybercriminal groups using the Bitcoin blockchain was largely unknown. A new study, conducted by IMDEA Software Institute researchers Gibran Gomez, Kevin van Liebergen, and

Juan Caballero challenges existing figures regarding cybercriminals' Bitcoin earnings to date.

The study, titled "Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage," published as part of the *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, reveals the full scale of the financial impact of cybercriminal activity.

In general, it's largely accepted that cybercriminal revenue is underestimated due to the lack of coverage on cybercriminal campaigns, like the complete set of Bitcoin addresses they use to receive payments from their victims.

This latest research, for the first time, is able to quantify how large that underestimation may be. Additionally, the research shows that some estimation methodologies may hugely overestimate the revenues, and they implement an estimation tool that avoids such methodological errors.

The study's findings come from a meticulous analysis of more than 30,000 payment addresses used by various cybercriminal groups, engaged in activities such as ransomware, clippers, sextortion, Ponzi schemes, giveaway scams, and cryptocurrency exchange scams.

A key contribution of this research is that the authors are able to quantify for the first time, how large the underestimation may be. For this, they analyze the DeadBolt ransomware, which encrypts the data hosted in Internet-connected storage servers.

The researchers are able to identify the complete set of payment addresses belonging to DeadBolt, estimating its revenue at $2.47 million, a figure 39 times higher than previous estimates. These results not only shed new light on the magnitude of cybercrime, but also highlight the importance of innovative approaches to collecting accurate data in the fight against online criminal activity.

Cryptocurrency payments are widely used by cybercriminals. For example, according to the U.S. Federal Trade Commission in 2022, cryptocurrencies were the most reported payment method by fraud victims, above other payment methods such as credit cards, wire transfers and bank transfers. Among cryptocurrencies, Bitcoin rules, followed by Ethereum, and much further behind by other cryptocurrencies such as Monero and Cardano.

This research could have a profound impact on cybersecurity and law enforcement communities and will spark a fresh look at how to combat cybercrime and dismantle its financial networks. The study is a testament to the importance of constantly evolving methodologies and tools in the fight against digital criminal enterprises.

More information: Gibran Gomez et al, Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage, *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (2023). DOI: 10.1145/3576915.3623094

Provided by IMDEA Software Institute

Citation: Researchers reveal hidden fortunes and surprising underestimations in cybercrime revenue (2023, December 16) retrieved 2 May 2024 from https://techxplore.com/news/2023-12-reveal-hidden-fortunes-underestimations-cybercrime.html