

Bitcoin scams steal at least \$11 million in virtual deposits from unsuspecting customers

January 28 2015

Fraudulent schemes have scammed at least \$11 million in Bitcoin deposits from unsuspecting cyber customers over the past four years, according to new cyber security research from Southern Methodist University, Dallas.

Bitcoin is the digital world's most popular virtual currency, with millions in circulation.

In the first empirical study of its kind, SMU researchers found that hucksters used four different types of schemes through authentic-looking web-based investment and banking outlets to lure customers and heist deposits, said computer security expert Marie Vasek, lead researcher on the study.

"Our calculation of \$11 million is almost certainly at the low-end," said Vasek. "The amount of Bitcoin that depositors have lost to these scams is probably many millions more."

Typically the scams succeed by exploiting not only people's greed, but also the urge to "get rich quick," coupled with the inability to judge the legitimacy of web services to decide which financial sites are good or bad, said Bitcoin and [cyber security](#) expert Tyler W. Moore, co-researcher on the study.

"Because the complete history of Bitcoin transactions are made public, we have been able to inspect, for the first time, the money flowing in

and out of fraudulent schemes in great detail. It's like having access to all of Bernie Madoff's books for many of these scams," said Moore, director of the Economics and Social Sciences program of the Darwin Deason Institute for Cyber Security in SMU's Bobby B. Lyle School of Engineering.

13,000 victims and counting in four different kinds of scams

The researchers identified 41 scams occurring between 2011 and 2014, in which fraudulent sites stole Bitcoin from at least 13,000 victims, and most certainly more.

"We found that the most successful scams draw the vast majority of their revenue from a few victims," Vasek said.

The researchers were only able to track revenues for about 21 percent of the scams, which would indicate that the amount of Bitcoin actually stolen most likely far exceeds \$11 million.

The findings emerged when the researchers ran a Structured Query Language database dump of all relevant Bitcoin transactions, then analyzed Bitcoin addresses (the account numbers) of both victims and the siphoning transactions of scammers.

The researchers presented their findings, "[There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams](#)," at the 2015 19th International Financial Cryptography and Data Security Conference, Jan. 26-30, in San Juan, Puerto Rico. Vasek is a graduate student and Moore is assistant professor, both in the Lyle School's Computer Science and Engineering Department.

"The amount of fraud being attracted by Bitcoin is a testament to the fact the [virtual currency](#) is gaining in legitimacy," said Moore. "But scams that successfully hijack funds from depositors may end up scaring away consumers who will fear using Bitcoin for their legitimate digital transactions."

The research was partially funded by the U.S. Department of Homeland Security's Science and Technology Directorate, Cyber Security Division, and the Government of Australia and SPAWAR Systems Center Pacific.

There are 13.7 million Bitcoin in circulation, according to [blockchain.info](#). The number of Bitcoin transactions exceeds 100,000 per day.

Four scams, each with varying lifespans, strategies and success

Vasek and Moore identified four common scams by tracking forum discussions, where scams are often initially advertised and later exposed, and by tracking web sites.

—High-yield investment programs, otherwise known as online Ponzi schemes, which promise investors outlandish interest rates on deposits. The scammers lure both unsuspecting victims as well as those fully aware it's a Ponzi scheme who hope to cash out in time. Of all the scams, this type has taken in the lion's share of money from victims. The biggest of these scammers was Bitcoin Savings & Trust, formerly First Pirate Savings & Trust. When such schemes collapse, as they eventually do, and often within about 37 days, they're replaced with a new program, often run by the same criminals, say the researchers. These scammers consistently pay out to their investors far less than they take in.

—Mining investment scams are classic advanced-fee fraud, taking orders and money from customers but never delivering any mining equipment—specialized computer processors and electronic devices for mining Bitcoin. These retailers typically endure for 145 days, much longer than Ponzi schemes. Vasek and Moore looked at Labcoin, Active Mining Corp., AsicMiningEquipment.com and Dragon-Miner.com.

—Victims make deposits into [scam](#) wallets under the promise the service offers greater transaction anonymity. If the deposit is small, scammers leave the money, but if it rises above a threshold, scammers move the money into their wallet. Services such as Onion Wallet, Easy Coin and Bitcoinwallet.in each surfaced with transfers from victims siphoned to one address held by a scammer.

—Exchange scams, such as BTC Promo, CoinOpend and Ubitex, offer PayPal and credit card processing, but at a better exchange rate than competitors. Customers soon find out, however, they never get Bitcoin or cash after making payment. Longer-lived exchange scams survived about three months. Wallet and exchange scams exploit the difficulty in judging the legitimacy of web services.

The study is not a comprehensive review, the researchers note, as they were limited to those scams for which they could determine a minimum estimate of the prevalence and criminal profits of the scams after analyzing the public ledger of all Bitcoin transactions ever executed.

The researchers conservatively estimate that \$11 million has been taken by scams, while only \$4 million has ever been returned. Most of the successful scams catch a few "big fish," say the researchers, who pay the bulk of the money into the scam.

"Bitcoin scams pose a problem for more than the victims who directly lose money," Moore said. "They threaten to undermine trust in this

promising technology, and cast a chilling effect on those interested in trying out new services. By mining the public record for fraudulent transactions, we hope to deter would-be scammers and assist law enforcement in cracking down on the bad actors."

Provided by Southern Methodist University

Citation: Bitcoin scams steal at least \$11 million in virtual deposits from unsuspecting customers (2015, January 28) retrieved 21 May 2024 from <https://phys.org/news/2015-01-bitcoin-scams-million-virtual-deposits.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--