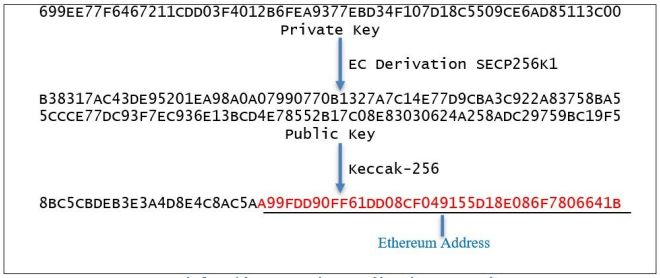
Key-guessing blockchain banditry is discovered in security research

25 April 2019, by Nancy Cohen



Example flow of deriving an Ethereum address from a private key. Credit: Independent Security Evaluators

A bandit story of the cryptocurrency kind was a popular item on tech sites this week, with staggering amounts of money scooped up by some blockchain bandit, and spotted by security consultants, Independent Security Evaluators.

The weakness comes from poorly implemented private key generation, facilitating cryptocurrency theft. The bandit is guessing private keys— and the bandit is scoring millions.

Researchers spotted 732 actively used private keys on the Ethereum blockchain. "Our research sought to locate Ethereum addresses based on the use of weak keys, and to examine how those addresses are used," the team said in their paper. (The Ethereum project uses elliptic curve cryptography to generate the public/private key pair.)

In the process, and detailed by Andy Greenberg in *Wired*, the researchers found that cryptocurrency users have in the last few years stored their crypto treasure with hundreds of easily guessable private keys. They also uncovered a bandit.

How did the researchers find the keys? Programming errors in software that generated the private keys. "These private keys are not sufficiently random which makes it trivial for a computer to brute force and eventually guess," said the ISE blog.

"A single Ethereum account seems to have siphoned off a fortune of 45,000 ether—worth at one point more than $50 million—using those same key-guessing tricks."

Their video notes: "While researching key generation on Ethereum's blockchain we discovered funds from weak private key addresses are being pilfered by someone. On 01/13/18, this blockchain bandit held a balance of 37,926 ETH valued at $54 million."

ISE discovered 732 private keys as well as their corresponding public keys. They wrote about their method in their paper. They said, "instead of attempting to brute force search random private keys, we devised ways to discover keys that may have been generated using faulty code, faulty random number generators, or a combination of both."

Adrian Bednarek, security consultant, as quoted in *Wired*. "Whoever this guy or these guys are, they're spending a lot of computing time sniffing for new wallets, watching every transaction, and seeing if they have the key to them."

ISE issued a number of recommendations based on their research findings, including these. Use a cryptographically secure pseudo-random number generator instead of just any pseudo-random number generator; audit source code and resulting compiled code to verify randomly generated keys are not truncated or become malformed by faulty workflows that interact with them; do not generate private keys based from passphrases, aka brain wallets — as people tend to use easily guessable passphrases.

As important, this is not a one-off escapade. The thefts are ongoing.

ISE's blog said, "the bandit seems to be operating an ongoing campaign to loot cryptocurrencies from wallets derived from weak private keys. ISE researchers intentionally placed one U.S. dollar worth of ETH in a weak private key derived wallet and witnessed that within seconds, the ETH was transferred out and into the bandit's wallet."

Who could be doing this? Bednarek has no real idea of who the blockchain bandit might be, wrote Greenberg. "I wouldn't be surprised if it's a state actor, like North Korea, but that's all just speculation," said Bednarek.

More information:
www.securityevaluators.com/cas …
tudies/ethercombing/

© 2019 Science X Network
APA citation: Key-guessing blockchain banditry is discovered in security research (2019, April 25) retrieved 25 June 2022 from https://techxplore.com/news/2019-04-key-guessing-blockchain-banditry.html

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.