2023

Uncovering Sybils in the Beta Round

GRAY

Abstract

This report outlines a methodology for identifying sybils in the Gitcoin Beta Round using post-mortem analysis of the Alpha Round data. Our focus is on identifying patterns of address usage that are too specific to be coincidences and are indicative of scripted behavior. We demonstrate how cosine similarity can be used to group together similar address patterns, and set a threshold for identifying groups of addresses that are likely to be controlled by the same entity. By applying this methodology, we were able to identify a significant number of sybils in the Beta Round and provide insight into the extent of scripted behavior

Keywords: Cosine Similarity, Repetition

Introduction

The Gitcoin platform is a popular platform for crowdfunding open-source software development projects. However, the platform is vulnerable to attacks from Sybils, which are fake identities created by a single entity to manipulate the system. The Gitcoin team conducted a beta round to identify and remove Sybils from the platform. In this project, we perform a post-mortem analysis of the beta round data to identify Sybils based on their address patterns. Specifically, we focus on a project that latched onto the scripted nature of Sybils and their similarities within address patterns that are too specific to be coincidences. Our goal is to provide insights that can help improve the detection of Sybils in future Gitcoin rounds and enhance the platform's security

Methodology

Data Collection

The data collection process involved the use of two APIs: the Etherscan API and the Covalent API. The Etherscan API was used to collect transaction information, including wallet age, timestamps for the first and last transactions, TDD metric, last wallet sent to and sent from, first wallet sent to and sent from, and the number of transactions, including the count of to and from transactions on both regular ETH transactions and the ERC-20 tokens. The Covalent API was used to gather additional data related to token balances and transaction history.

Data Processing and Feature Engineering

The data was cut down to include only addresses that funded less than 5 grants or funded 5 times, which was the 75th percentile. The project title column was merged to form one value containing one entry for all grants funded by an address, and these were the chosen features to be used in the cosine similarity analysis. The selected features included 'Funding count', 'No. Grants Funded', 'token', 'amount', 'passport score', 'passport pass', 'project title sorted', 'first from', 'first to', 'last from', 'last to', 'transaction count', 'Wallet Age', 'Wallet Age (Erc20)', 'to count', 'from count', 'erc to', and 'erc from'.

Sybil Attack Detection/Similarity Analysis

The Sybil Attack Detection/Similarity Analysis was performed using cosine similarity grouping to identify potential Sybils in the Gitcoin Beta round. The data was pre-processed and selected features were used to calculate the cosine similarity matrix. A threshold of 0.9996 was set for

grouping together similar rows. The resulting list of similar supporter wallets are identified as Sybils in the Alpha/Beta round. In order to accurately group together similar supporter wallets using cosine similarity, a threshold needed to be set. However, due to the encoded data points, setting the threshold too low would result in the grouping of unsimilar data. To avoid this, a high threshold of 0.9996 was set for each round, ensuring that only highly similar wallets were grouped together.

Note: All clusters where manually checked to validate similarity metrics

Results and Analysis

The analysis using the Sybil attack detection and similarity analysis identified a total of 125 Sybils in the Gitcoin Beta round. The team investigated further and found that in the alpha round, there were 205 Sybils identified in the eth_infra and climate categories. The team set the threshold for grouping similar data at 0.9996 to avoid grouping unsimilar data, and the results showed that the identified Sybils used similar address patterns.

The majority of the identified Sybils funded less than five grants or funded five times, which is the 75th percentile.By detecting and mitigating Sybil attacks, the platform can ensure the integrity of the Gitcoin ecosystem and continue to serve as a reliable and trustworthy space for funding open-source projects.