The GitHub Black Market: Gaming the Star Ranking Game

By Yehuda Gelb

Published: 2024-07-25 · Archived: 2026-04-05 22:22:42 UTC

7 min read

Nov 30, 2023

Press enter or click to view image in full size

As the world’s top Version Control System, GitHub has evolved well beyond its original purpose of simply storing and sharing code. Today it has become a digital portfolio for developers, showcasing their talents, contributions, and collaborations.

However, the growing demand for artificially boosting one’s presence in this thriving community has led to the emergence of a massive black market, with online stores and chat groups openly selling GitHub stars. This underground market undermines the authenticity of GitHub stars, falsely inflating a repository’s perceived value and popularity. This blog explores the manipulation of GitHub stars and provides a method to help you determine if a repository has been subjected to such deceptive practices.

Key Points

- GitHub Stars are an important metric that serves as a key indicator of a repository’s credibility and popularity.

- Individuals with malicious intent and those with deceptive practices may inflate star counts, misleading users about a repository's true worth.

The Role and Impact of GitHub Stars

GitHub stars play a crucial role in indicating the usefulness and quality of a repository. They serve as a measure of visibility, which can have various positive outcomes. For instance, repositories with more stars tend to attract more contributions from developers, opening up opportunities for collaboration and improvement.

Additionally, maintainers of highly-starred repositories may receive better job offers due to the recognition and validation of their work.

Moreover, in certain cases, a repository's star count can even lead to funding opportunities, providing financial support for further development and innovation.

The Dark Side of Star Inflation

While GitHub stars are generally a reliable indicator, it is essential to acknowledge the existence of unethical practices aimed at manipulating star counts. This deceptive behavior can mislead users and create a false impression of a repository's true value and popularity.

Users should be aware of these possible manipulations and exercise caution when evaluating repositories solely based on their star count, particularly for recent ones with a relatively high star count.

The GitHub Black Market

The underground market for GitHub stars is a testament to the lengths some will go to fake their way to popularity. As revealed in a study titled "Understanding Promotion-as-a-Service on GitHub", there are online stores and chat groups openly selling GitHub stars, posing serious challenges to the platform's integrity. The research identified over 63,872 suspected promotion accounts, generating millions of dollars in profit. This underground market undermines the authenticity of GitHub stars, falsely inflating a repository's perceived value and popularity.

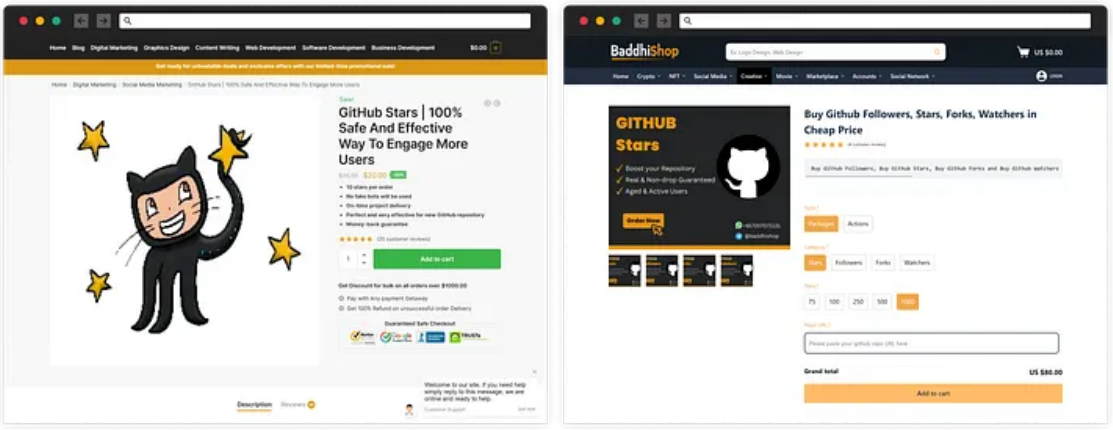
After learning about the existence of this massive black market for GitHub stars, I decided to dig deeper and investigate the services offered by these providers. I reached out to several service providers and asked them about their GitHub star services. I inquired about the number of stars they could provide, the cost and the timeframe for delivery.

The responses I received varied significantly. Some providers claimed that they could deliver a few hundred stars within a span of weeks, while one even offered to provide the stars within 1–2 days and suggested spreading out the delivery to make it appear more organic. The cost of these services also varied greatly, ranging from $80 for 1000 stars to a staggering $3000 for the same number of stars.

It's worth noting, though, that it wasn't just stars that were up for sale but also additional metrics such as followers, forks, and watchers.

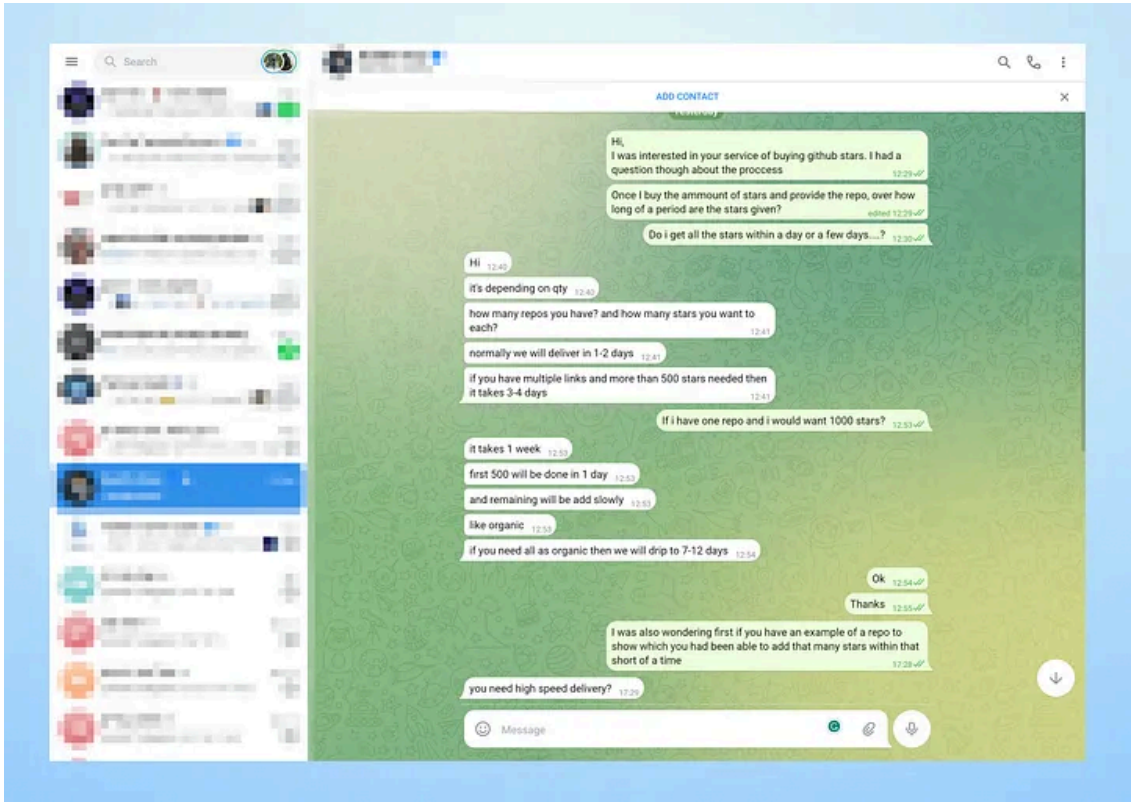
By exploring these services and their offerings, it became evident that the black market for GitHub stars is a thriving industry with significant financial implications. These practices undermine the authenticity and reliability of GitHub metrics, making it increasingly challenging to evaluate repositories based solely on their popularity metrics.

Press enter or click to view image in full size



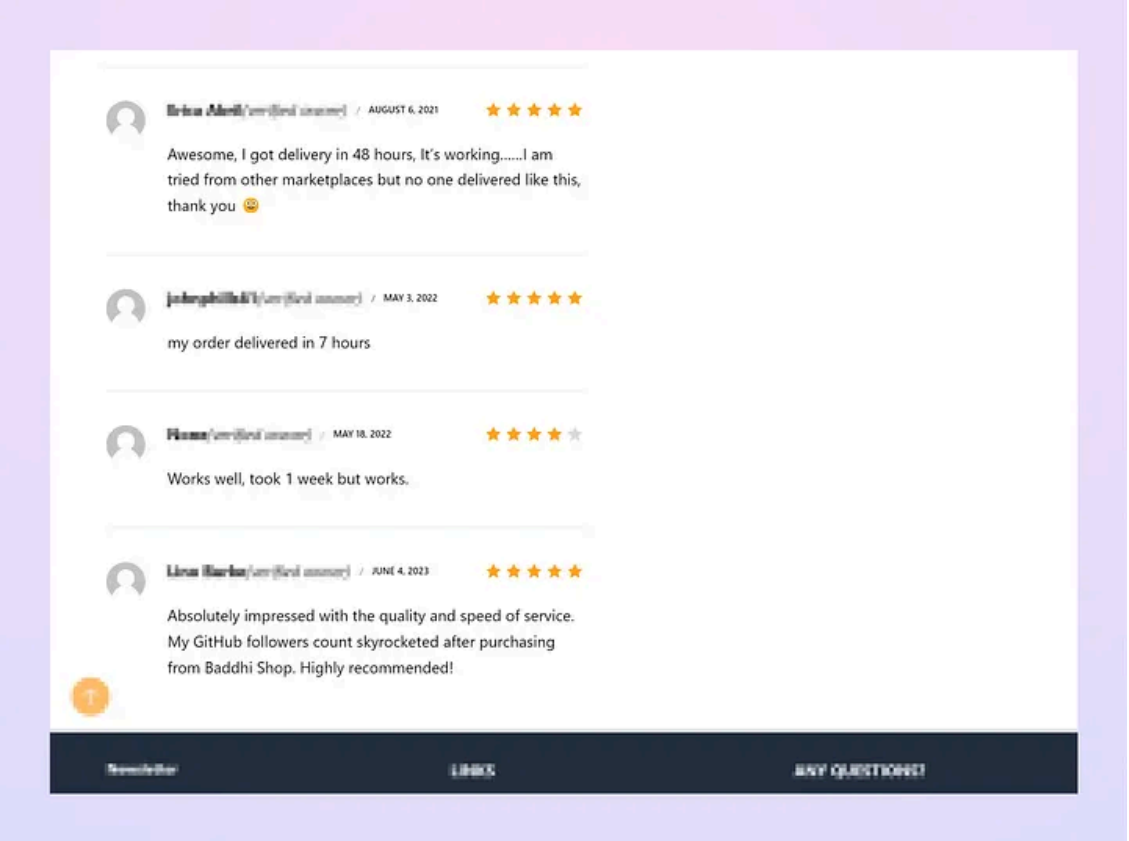
Just a couple of the many examples of star inflation services

Press enter or click to view image in full size



Conversation with one of the black market sellers

Press enter or click to view image in full size



Some happy customers

The Far-Reaching Implications of Star Inflation

The manipulation of GitHub stars doesn't just inflate numbers; it has tangible effects on how projects are perceived and utilized.

Get Yehuda Gelb's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Repositories that amass a high number of stars, particularly those that receive them in sudden bursts, often find their way into GitHub's trending section. They may also get featured in emails to subscribers of the GitHub Explore daily newsletter. This visibility can lead to genuine user engagement, as the project appears to be backed by a robust community.

This phenomenon has significant implications, especially for startups and tech companies. These entities often rely on GitHub stars as a barometer for choosing technologies, under the assumption that a high star count equates to widespread community support and reliability. However, when these stars are the result of artificial inflation rather than genuine interest, it can lead to misguided decisions.

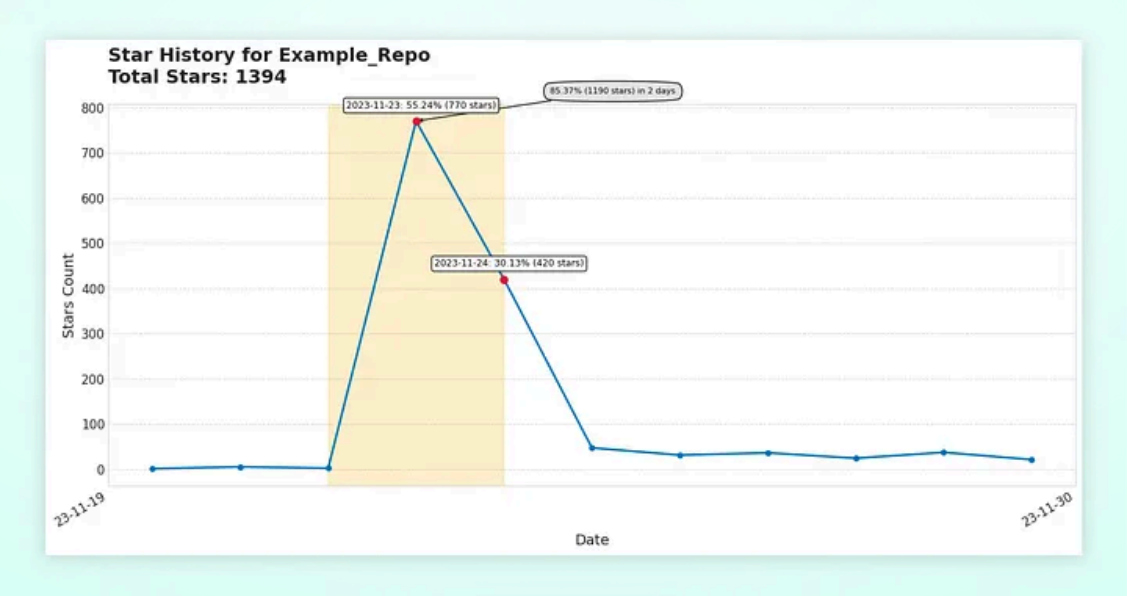
Verify their Stars.

If you come across a GitHub repository and want to take precautions, we offer a free Python tool called fake_star_check. This tool, available on GitHub, can help you examine repositories for suspicious star activities. It focuses on two main aspects: identifying unusual star patterns and suspicious fake user profiles within the repository. By using this tool, you can gain better insights into the repository's overall health and reliability, enabling you to make informed decisions before engaging with it. We also welcome collaboration and contributions from the community to improve the tool.

1. Star Time Patterns

The tool examines the timing and distribution of GitHub stars to identify abnormal patterns indicative of artificial popularity. It analyzes when each star is awarded to a repository and searches for any possible red flags. These red flags may include a sudden spike in stars within a brief period, particularly when a significant portion of the repository's total stars are accumulated during that spike. This suggests artificial inflation by bots or paid services.

Press enter or click to view image in full size



An example of a repository that could be considered suspicious due to the large number of stars it received in a very short period, especially considering its recent creation date.

2. User Profile Analysis

Beyond star pattern analysis, the tool also delves into the profiles of users who have starred the repository. It examines different aspects, such as the dates of account creation, levels of activity, and the diversity of interactions on GitHub. Legitimate users typically have a track record of contributions and varied interactions across multiple repositories. In contrast, profiles involved in manipulating stars often exhibit limited activity, with profiles that are very similar to each other, and their engagement is predominantly confined to starring repositories, frequently overlapping with other similar profiles, and lacking in genuine contributions.

Beyond Fake Stars

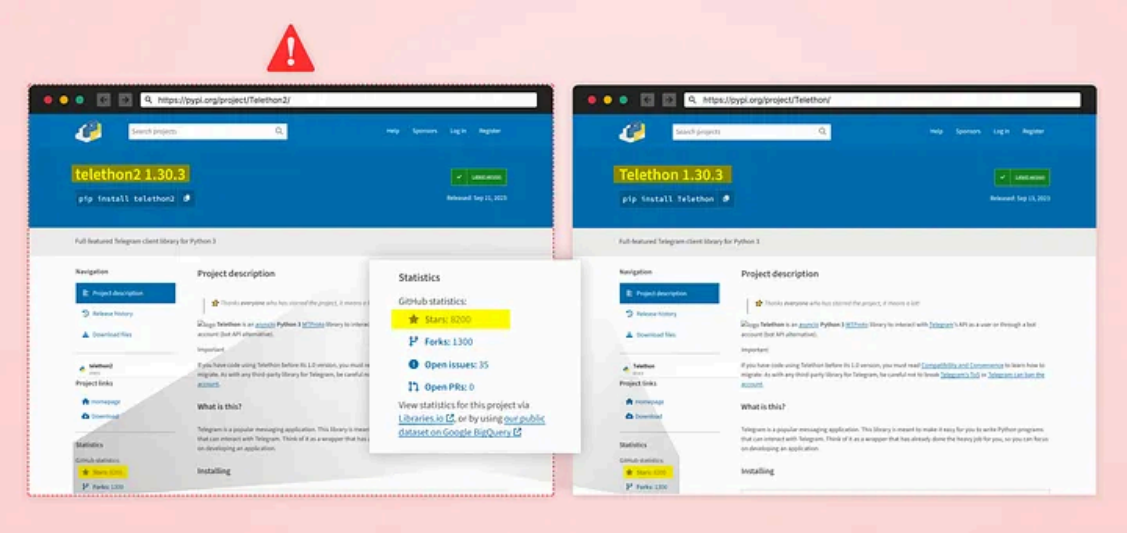
The manipulation of GitHub stars directly on GitHub is not the only method used by individuals to fake their way to popularity.

The Issue of Starjacking

Some package managers allow packages to be linked to GitHub repositories, which enables the package's homepage on the package manager to display popularity metrics from the linked GitHub repo.

Another technique, known as "Starjacking," involves linking a package hosted on a package manager (typically PyPi) to an unrelated repository on GitHub. By doing this, the popularity metrics of the original package, including the stars, are displayed on the unethical person's repository, deceiving others into thinking it is a popular package. Since the statistics displayed by package managers do not go through any validation process and this process is relatively simple to execute, attackers often employ it in their attacks. [A recent example of such an attack targeted users of Telegram, AWS, and Alibaba Cloud.]

Press enter or click to view image in full size



GitHub Profile manipulation

Fake stars are just one facet of deception on GitHub; consider checking out our recent series on [How Attackers Manipulate Their GitHub Profiles to Deceive you.]

Summary

In an ecosystem as vast and influential as GitHub, where stars often serve as an indication of a project's popularity and credibility, it's essential to remember that these metrics do not always tell the whole story. While star counts can generally offer a glimpse into a project's community support and visibility, they do not guarantee the quality or suitability of the software. It's crucial, therefore, to go beyond surface-level metrics.

A thorough assessment, which includes code quality reviews, community engagement, documentation, and update frequency, provides a more comprehensive understanding of a project's value.

Furthermore, nowadays, there is a wealth of tools and resources available that assist in evaluating these open-source projects.

Remember, not all is as it seems…

As part of the Checkmarx Supply Chain Security solution, our research team continuously monitors suspicious activities in the open-source software ecosystem. We track and flag “signals” that may indicate foul play and promptly alert our customers to help protect them.
