Anthropic Claude Code Leak | ThreatLabz

By Manisha Ramcharan Prajapati, Jithin Prajeev Nair, Avinash Kumar, Mallikarjun Piddannavar

Published: 2026-04-01 · Archived: 2026-05-06 02:01:01 UTC

ThreatLabz discovers “Claude Code leak” lure that distributes Vidar and GhostSocks

While monitoring GitHub for threats, ThreatLabz came across a “Claude Code leak” repository published by idbzoomh (links located in the IOC section). The repository looks like it’s trying to pass itself off as leaked TypeScript source code for Anthropic’s Claude Code CLI. The README file even claims the code was exposed through a `.map` file in the npm package and then rebuilt into a working fork with “unlocked” enterprise features and no message limits.

The repository link appears near the top of Google results for searches like “leaked Claude Code,” which makes it easy for curious users to encounter, as shown in the figure below.

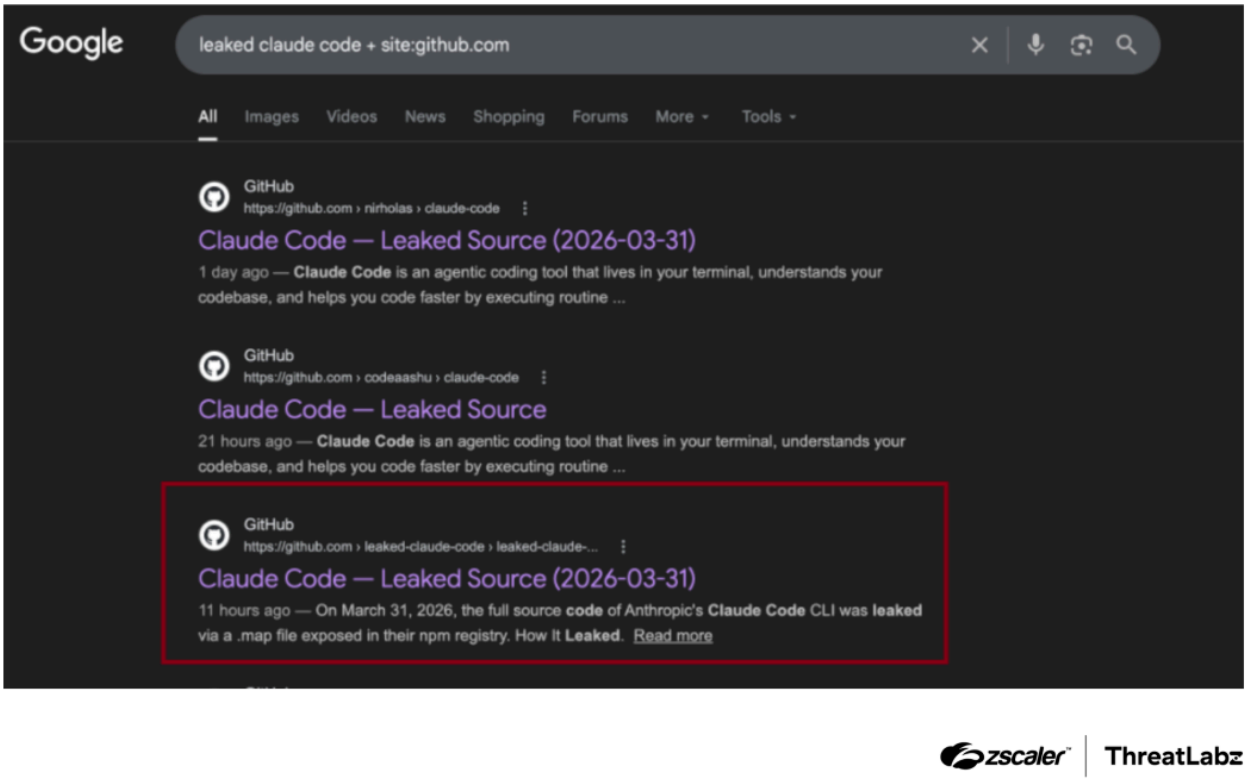


Figure 1: Google search results for leaked Claude Code on GitHub returning a malicious repository.

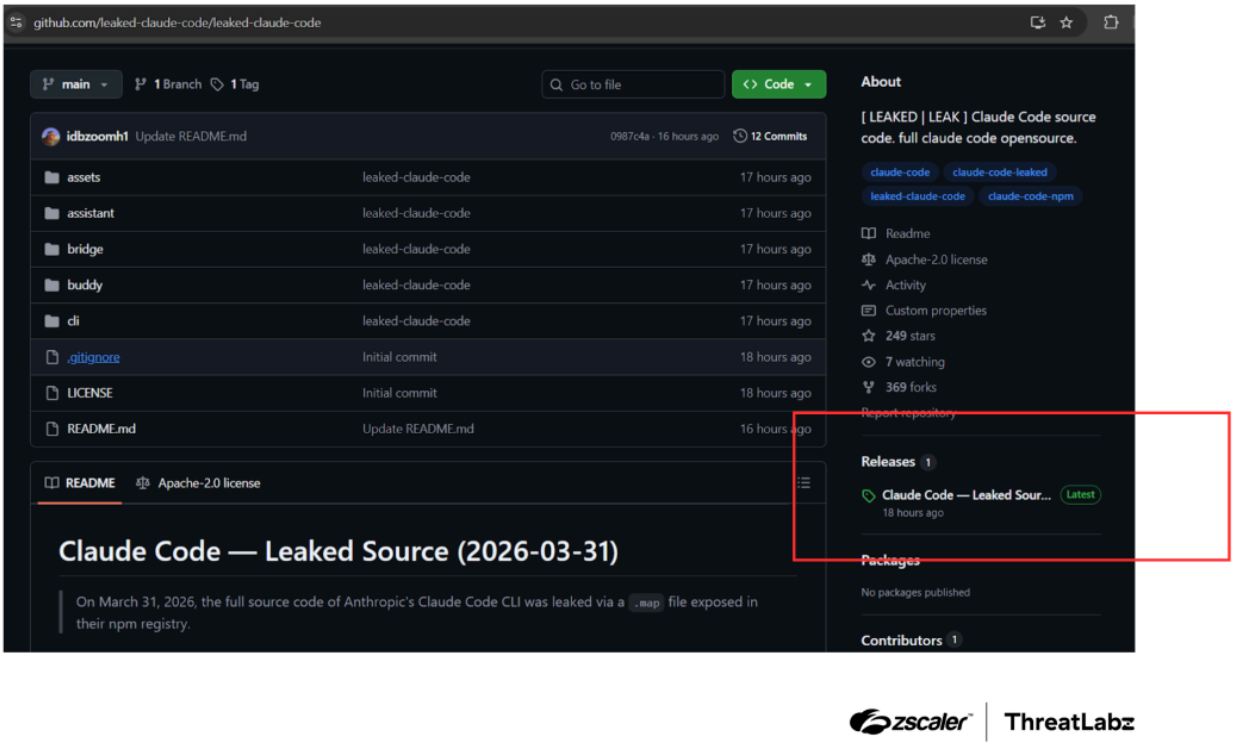
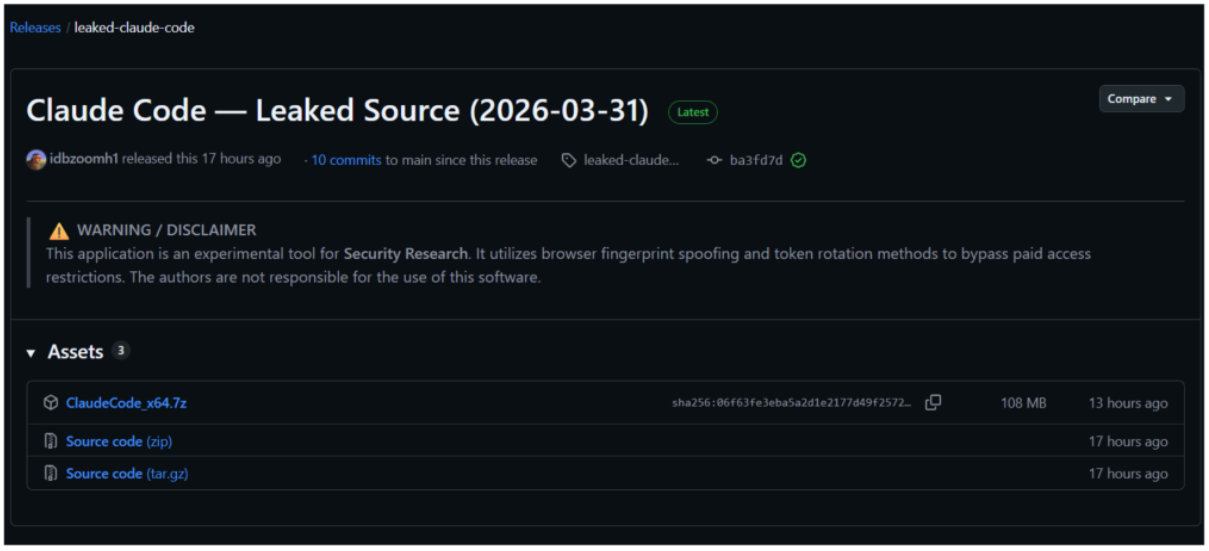


Figure 2: Malicious GitHub repository using the leaked Claude Code source as a lure.

The malicious ZIP archive in the repository's releases section is named *Claude Code - Leaked Source Code* (.7z). The archive includes *ClaudeCode_x64.exe*, a Rust-based dropper. On execution, the ClaudeCode_x64.exe drops Vidar v18.7 and GhostSocks. Vidar is an information stealer and GhostSocks is used to proxy network traffic. In early March, another security vendor reported a similar campaign where GitHub was being used to deliver the same payload.

The threat actor keeps updating the malicious ZIP archive in short intervals. At the time of analysis, ThreatLabz observed that there were two ZIP archives updated in the releases section in a short timeframe. The figure below shows the first ZIP archive ThreatLabz encountered which was updated about 13 hours ago.



zscaler | ThreatLabz

Figure 3: GitHub repository using the Claude Code leak as a lure to distribute malicious ZIP archives.

ThreatLabz also identified the same GitHub repository hosted under another account (located in the IOC section) that contains identical code and appears to be committed by the same threat actor, idbzoomh.

Unlike the earlier repository, this one does not include a releases section. The README file displays a prominent “Download ZIP” button. However, it does not link to any compiled binary or an archive and was non-functional at the time of analysis. The figure below shows the repository and non-functional button.

Figure 4: Additional GitHub repository hosting the same Claude Code leak lure with a “Download ZIP” button.

Source: https://www.zscaler.com/blogs/security-research/anthropic-claude-code-leak