How to *accidentally* host a crypto mining operation in less than 3 minutes

PRESENTED BY

Dan Shanahan

The problem
What is GitHub doing?
What can I do?

AGENDA

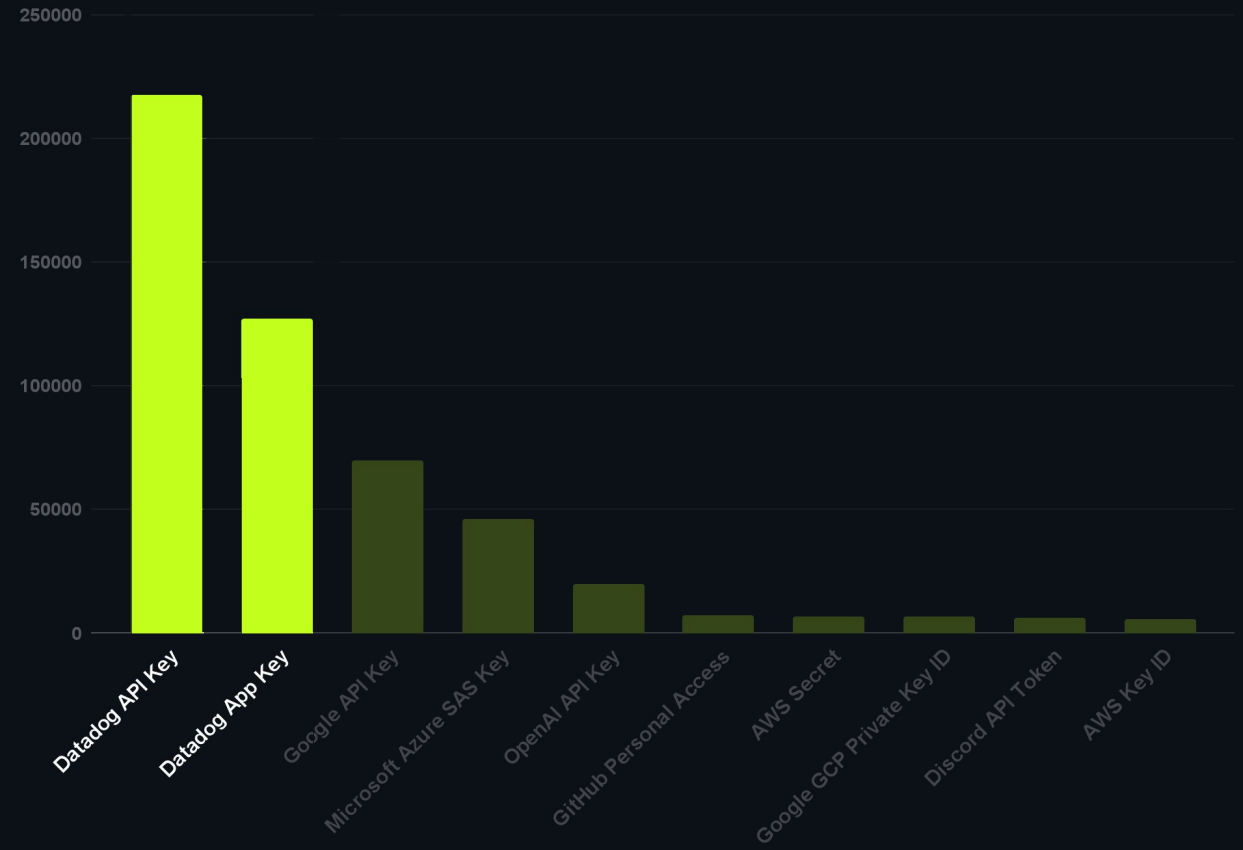
The problem

AWS credentials are written to GitHub public repos ____ times a month

AWS credentials are written to GitHub public repos 7000 times a month ¯_(ツ)_/¯

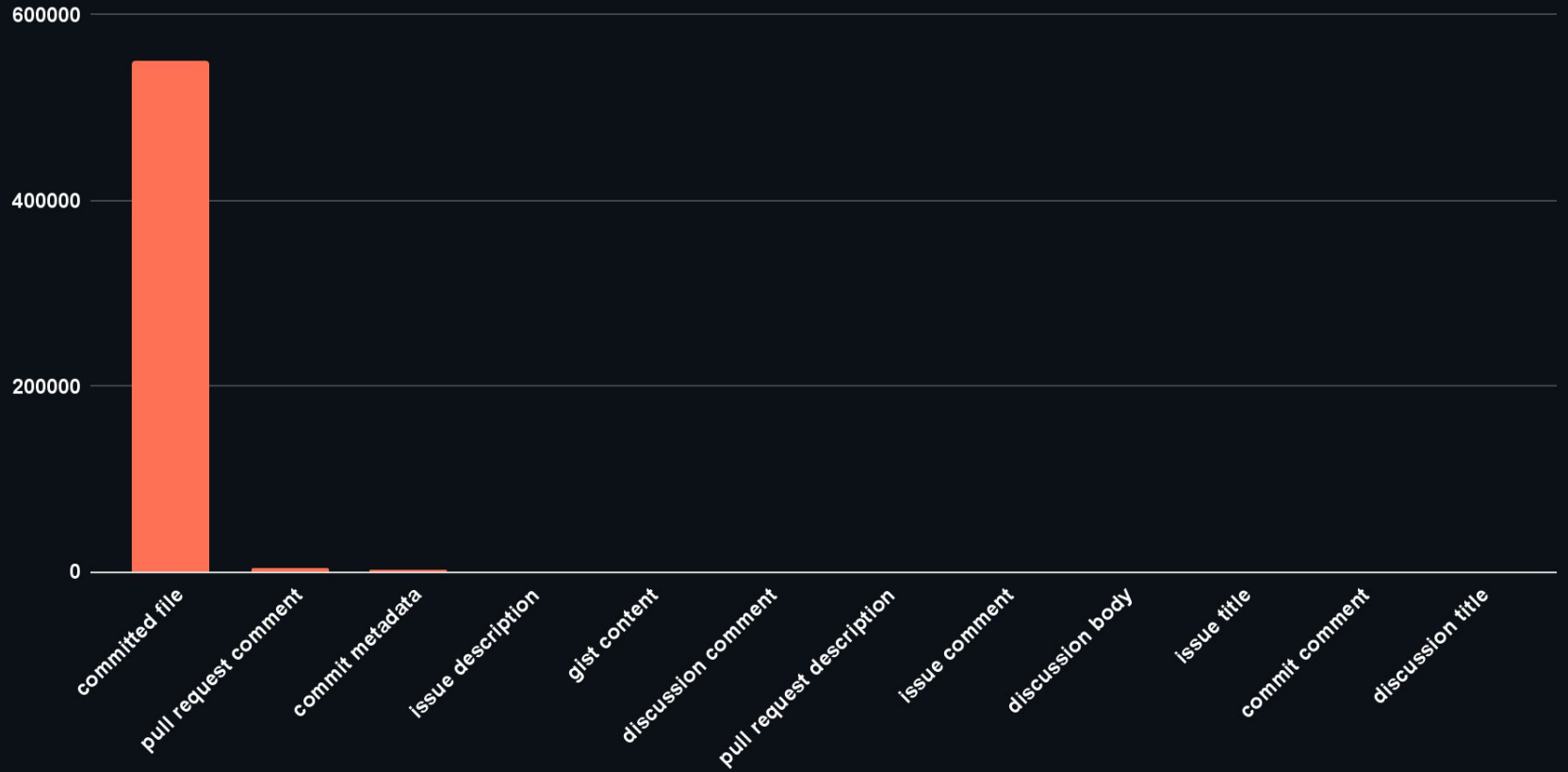
Top 10 Credential Types

GitHub public repositories - Feb. 2024



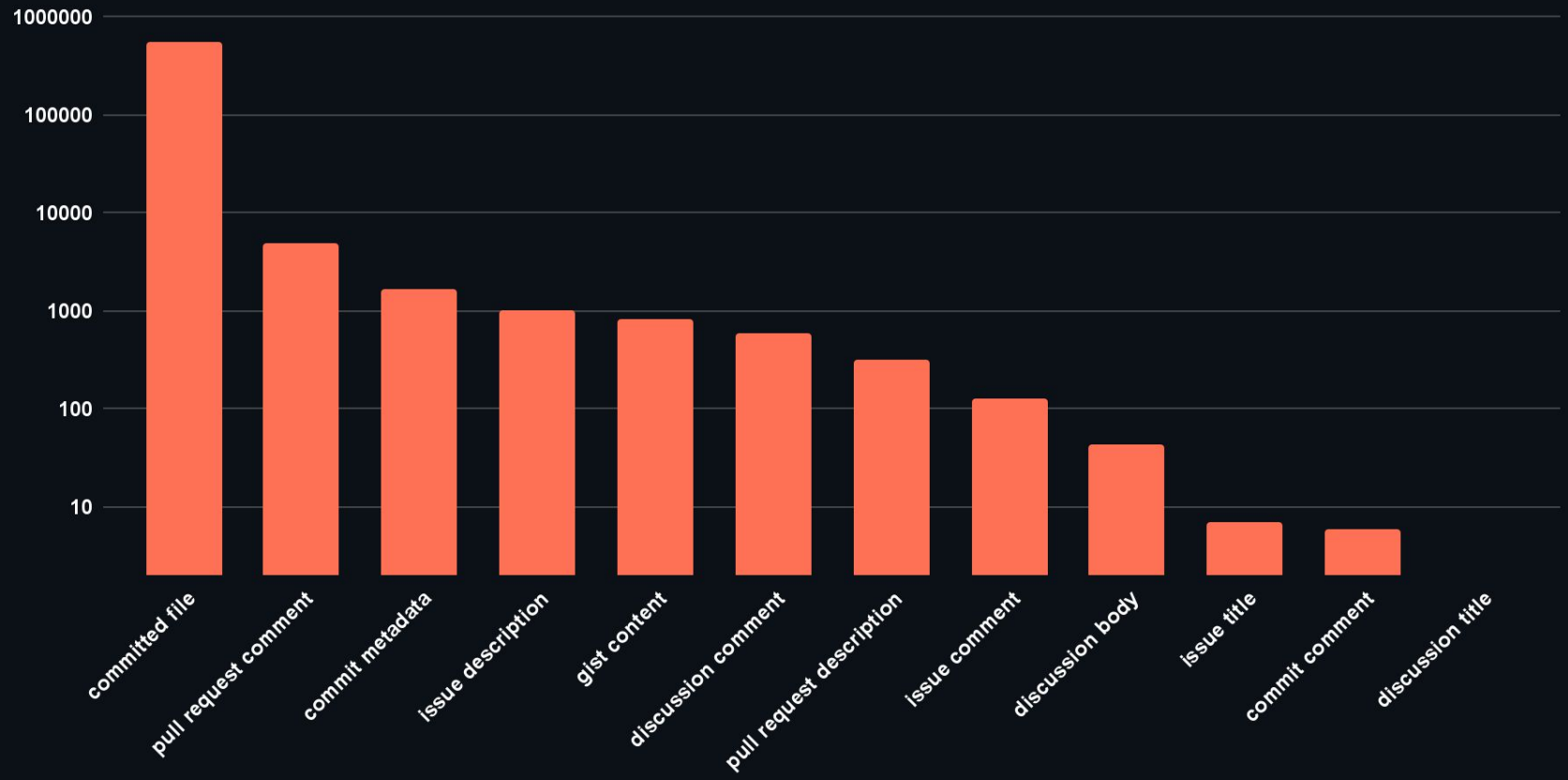
Credential Leak Locations

GitHub public repositories - Feb. 2024



Credential Leak Locations

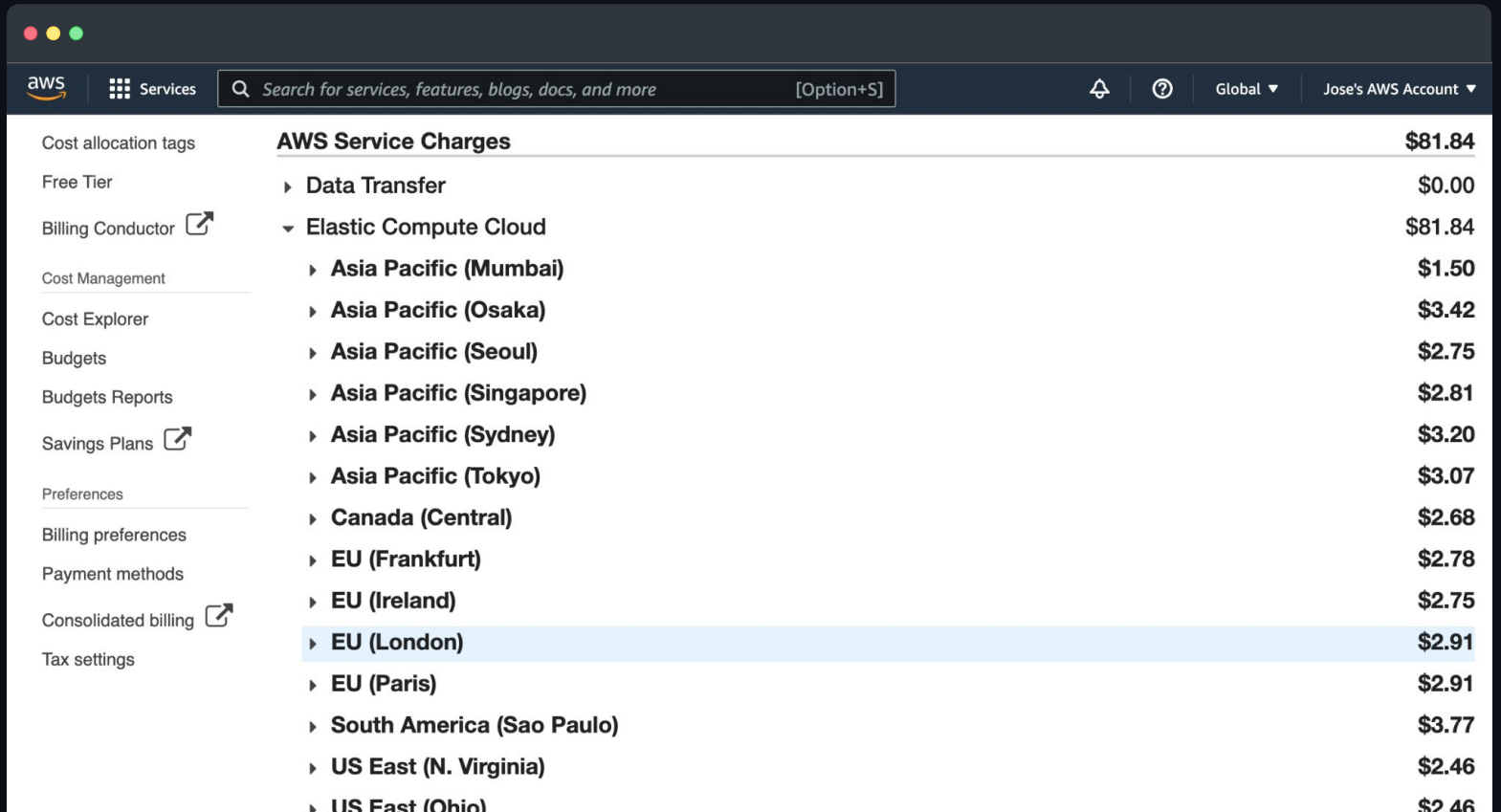
GitHub public repositories - Feb. 2024
(logarithmic)



10.2 million

Secrets identified in 2023

Crypto Miners at work



What is GitHub doing?

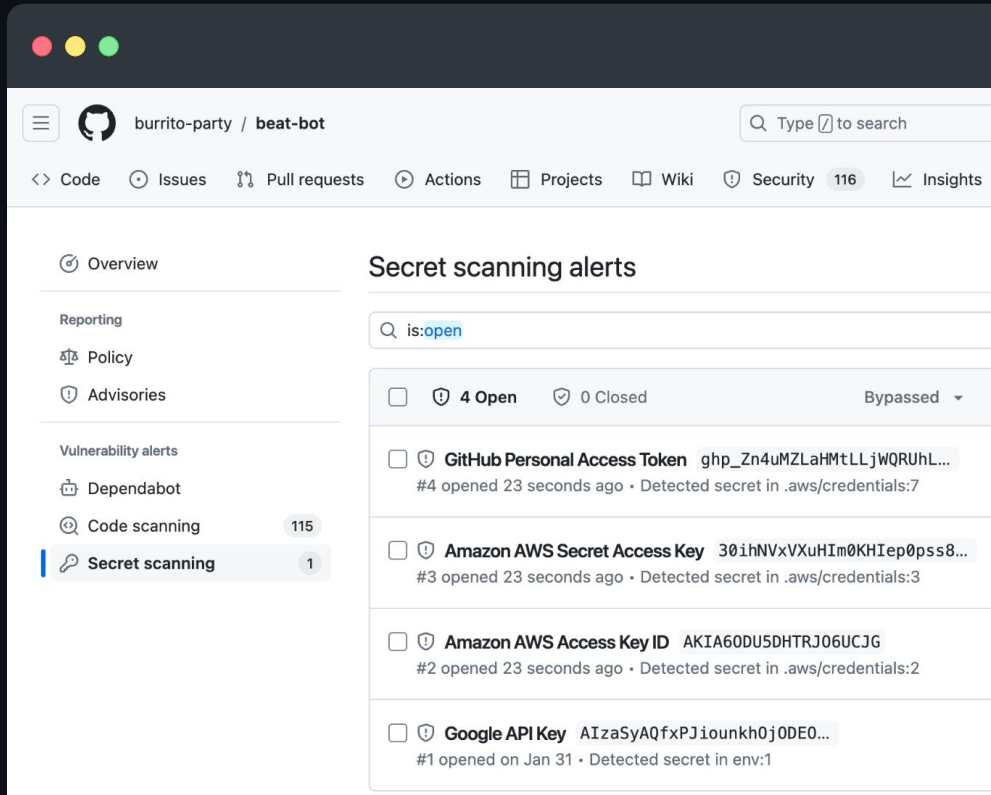
Secret Scanning

Regex-based search of every commit

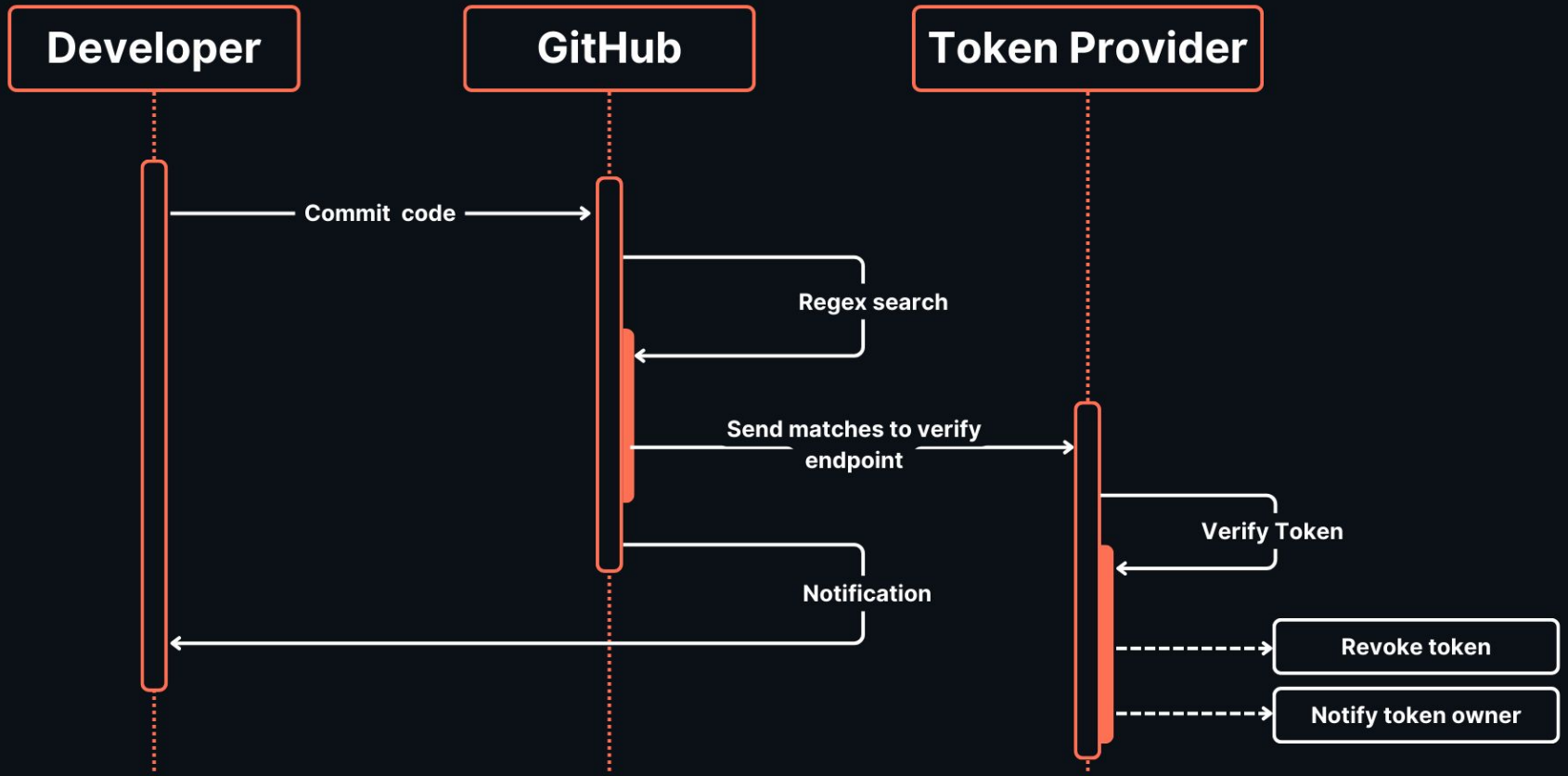
Find deeply nested in the history

Searches repo metadata

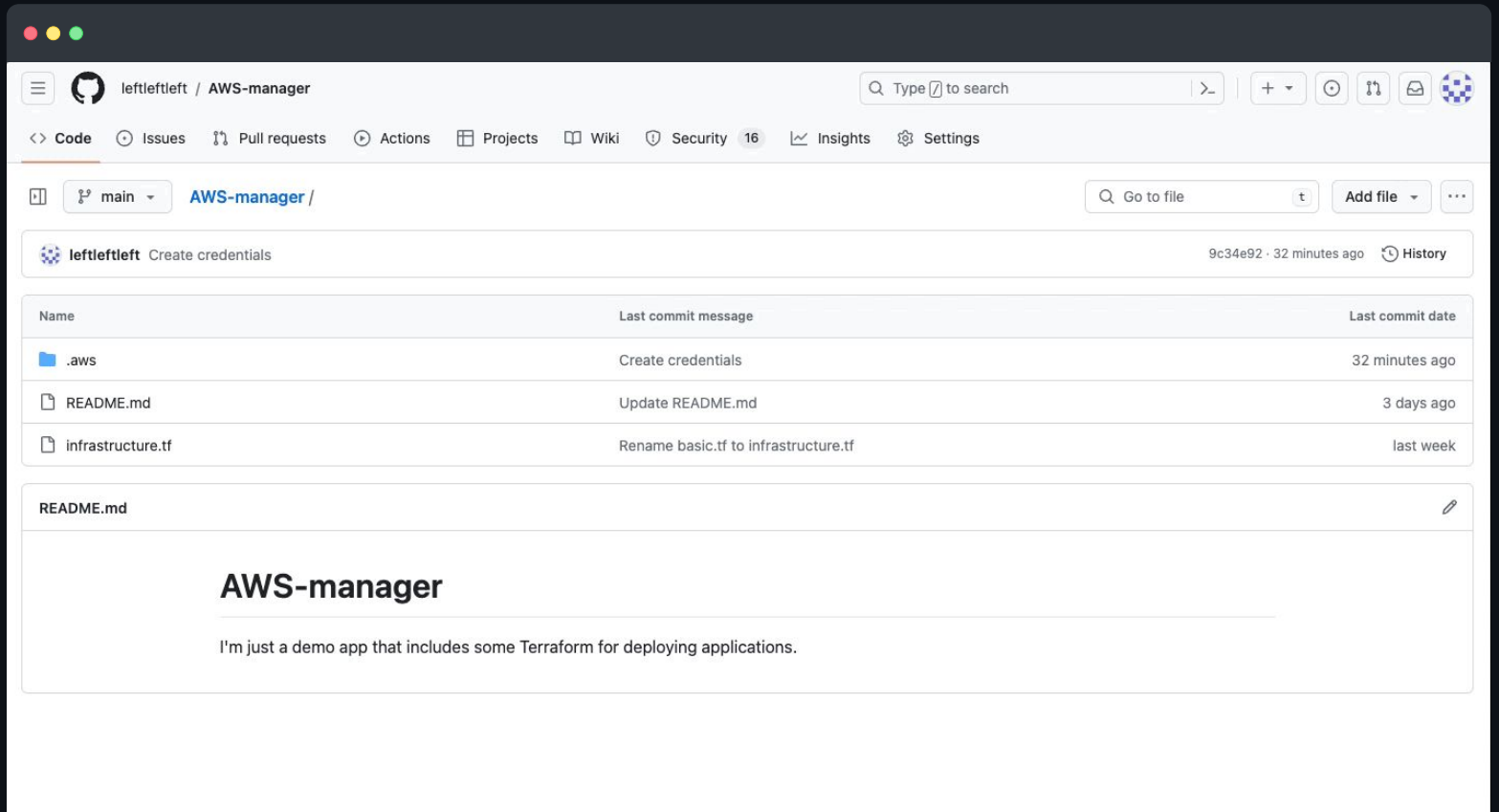
Issues, PR comments, Gists, etc.



How secret scanning works



Secret Scanning Push Protection



Push protection is enabled for free users on GitHub

secret-scanning security

February 29, 2024

We've started the rollout for enabling push protection on all free user accounts on GitHub. This automatically protects you from accidentally committing secrets to public repositories, regardless of whether the repository itself has secret scanning enabled.

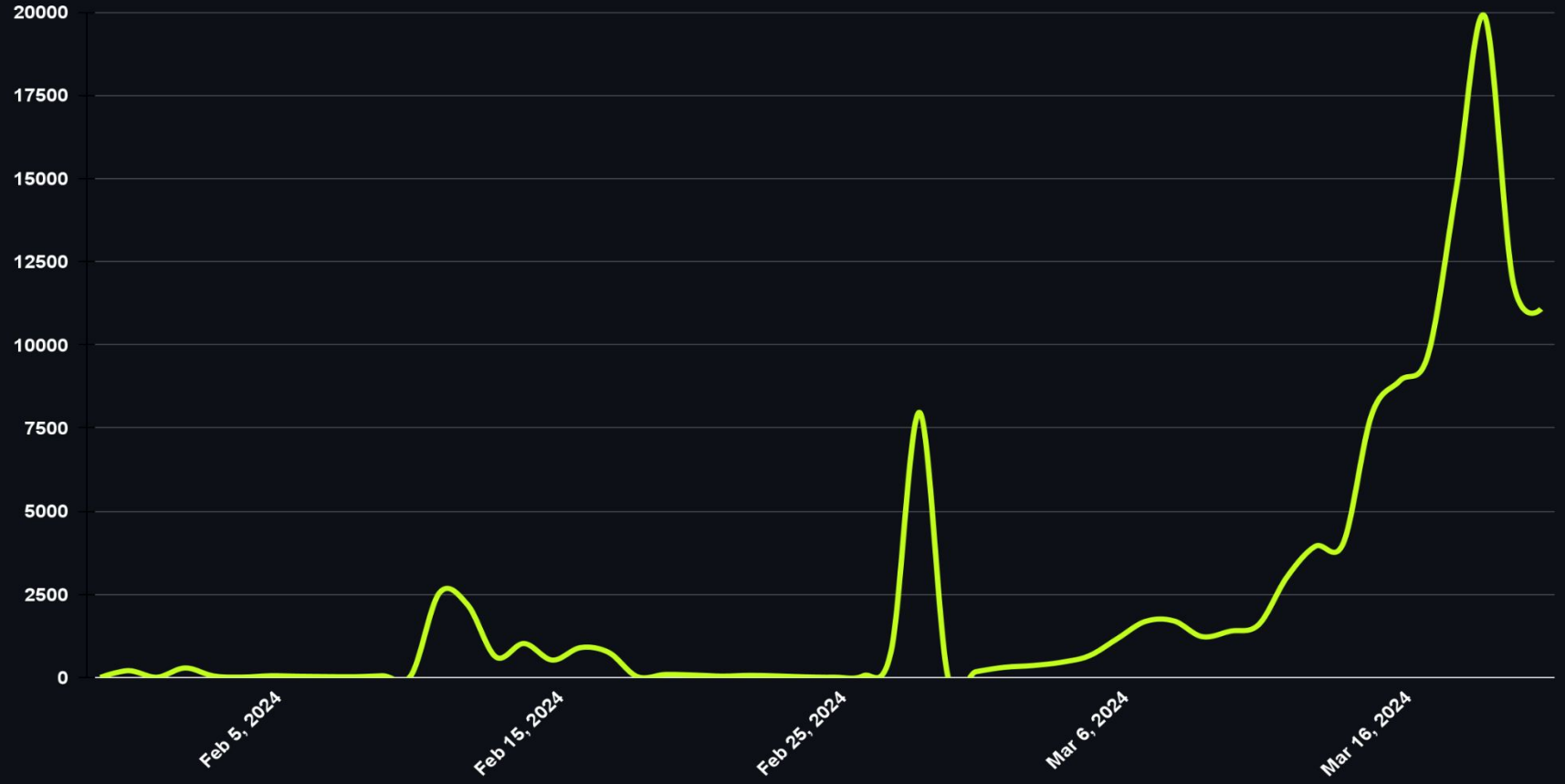
If a secret is detected in any push to a public repository, your push will be blocked. You will have the option to remove the secret from your commits or, if you deem the secret safe, bypass the block.

It might take a week or two for this change to apply to your account; you can verify status and opt-in early in your code security and analysis settings. Once enabled, you also have the option to opt-out. Disabling push protection may cause secrets to be accidentally leaked.

- Read the blog post

Push Protection Blocks

GitHub public repositories - Jan. 30 2024 - Mar. 21 2024



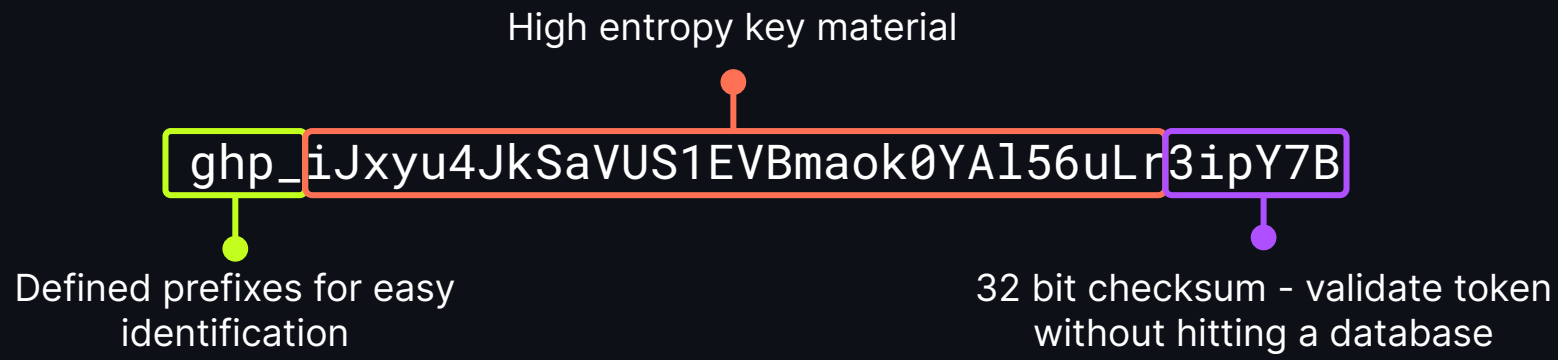
What can I do?

My company creates API tokens
What can I do?

Join the secret scanning program
Help us identify keys on GitHub by becoming a partner

Create identifiable credentials
Make the job of detecting lost credentials easier by generating identifiable keys

Highly identifiable secret patterns



I work on open source projects

What can I do?

Enable secret scanning for your communities

Encourage your communities to enable secret scanning on their projects.

Don’t turn off secret scanning 🙃

Secret scanning is on by default for your account.

I care about security at work
What can I do?

- Provide a secrets management tool - and make it easy
- Be clear about your credential policies
- Make rotation and revocation an automated process
- Secrets don’t just live in your source code. Be broad with your secret scanning program
- Accidents will happen. Be cool when they do 😎

Thank you

PRESENTED BY

Dan Shanahan @ BSidesSD 2024