

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

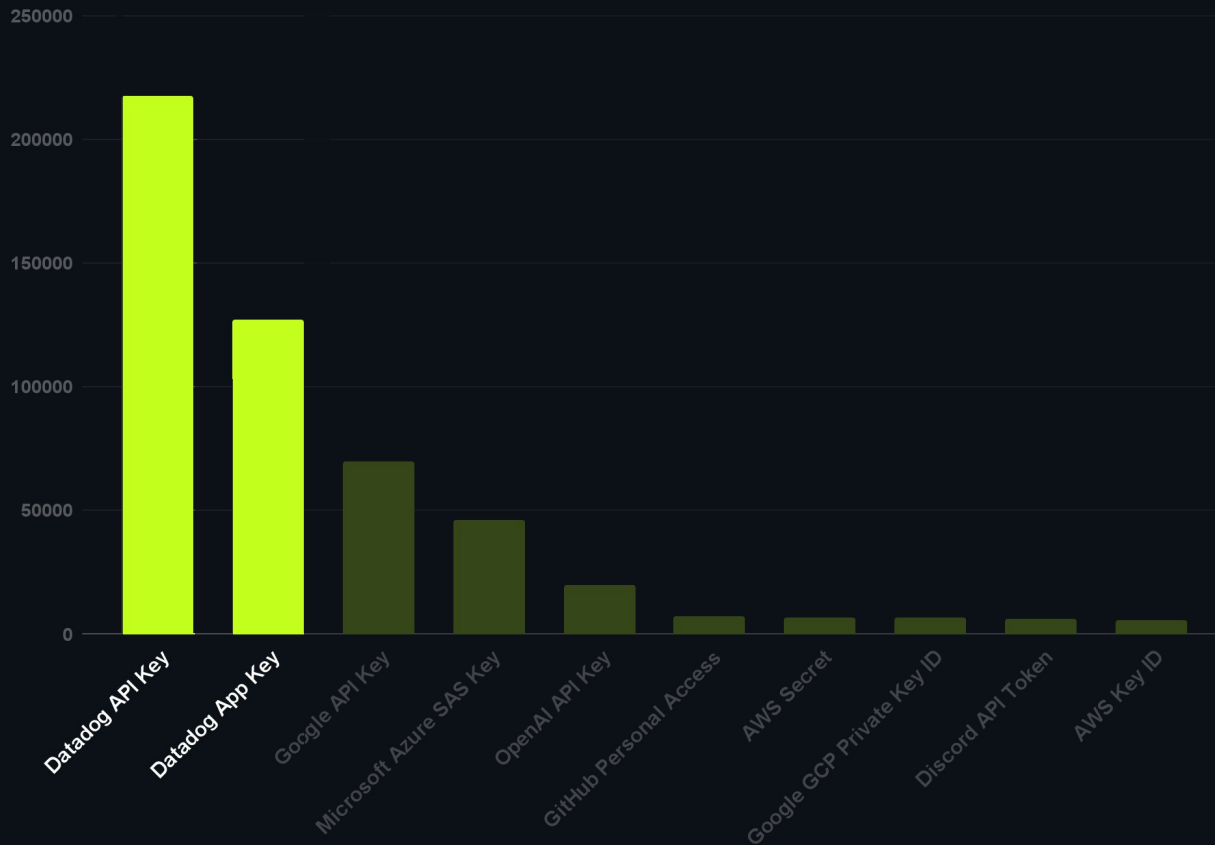


**AWS credentials are
written to GitHub public
repos _____ times a
month**

**AWS credentials are
written to GitHub public
repos 7000 times a
month** 

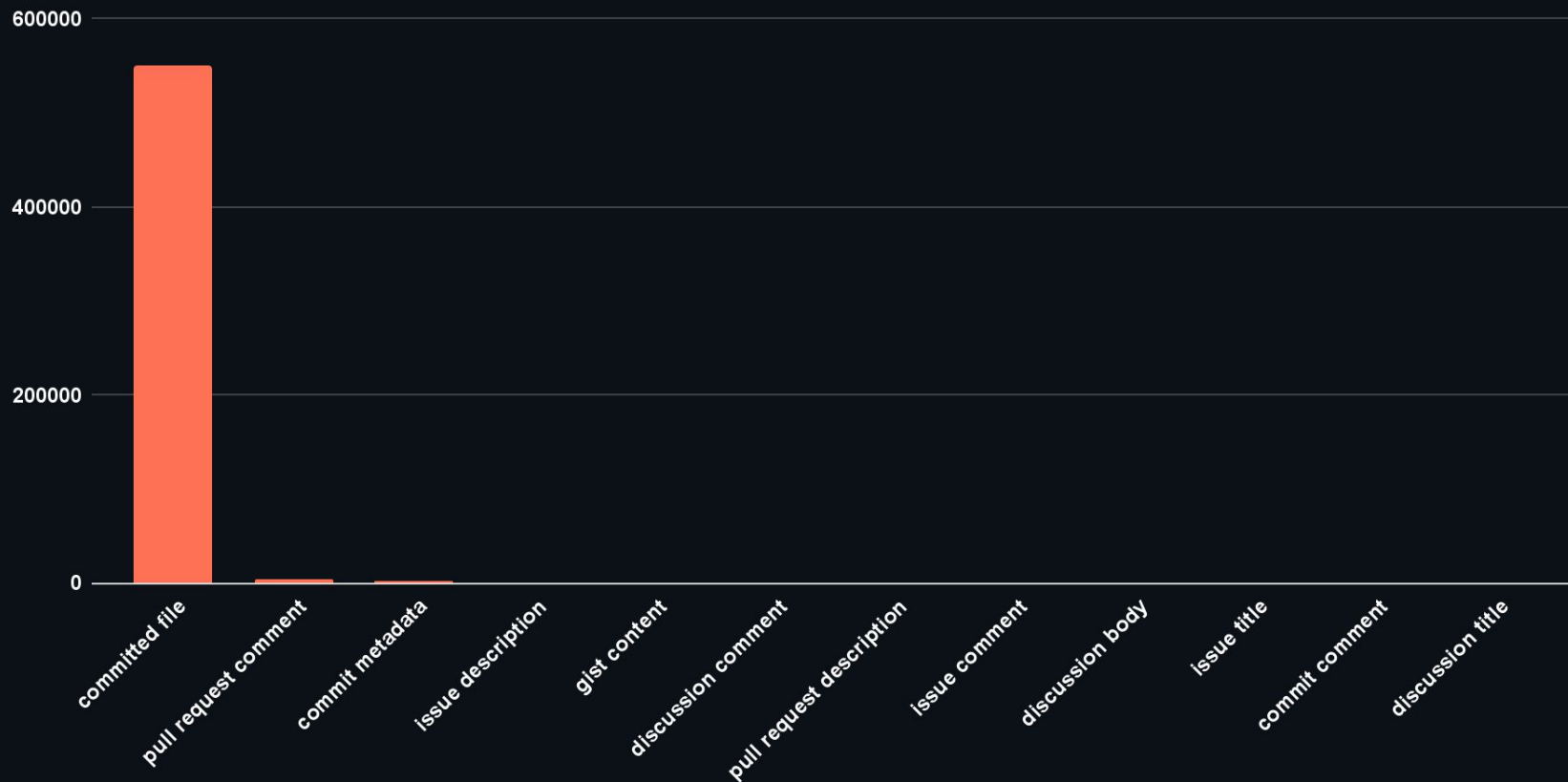
Top 10 Credential Types

GitHub public repositories - Feb. 2024



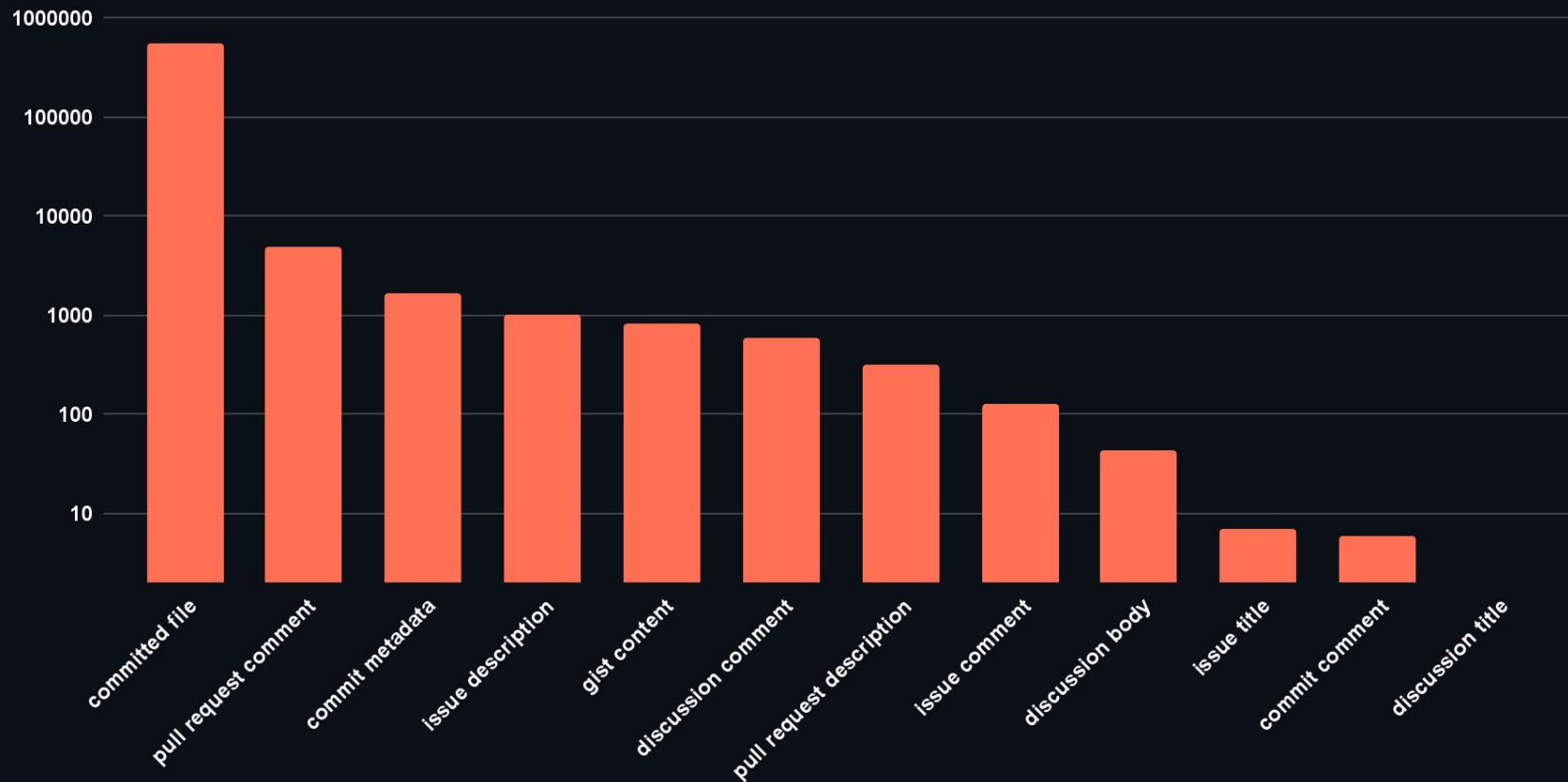
Credential Leak Locations

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

aws Services			Search for services, features, blogs, docs, and more	[Option+S]			Global	Jose's AWS Account
Cost allocation tags	AWS Service Charges		\$81.84					
Free Tier	▶	Data Transfer	\$0.00					
Billing Conductor	▼	Elastic Compute Cloud	\$81.84					
Cost Management	▶	Asia Pacific (Mumbai)	\$1.50					
Cost Explorer	▶	Asia Pacific (Osaka)	\$3.42					
Budgets	▶	Asia Pacific (Seoul)	\$2.75					
Budgets Reports	▶	Asia Pacific (Singapore)	\$2.81					
Savings Plans	▶	Asia Pacific (Sydney)	\$3.20					
Preferences	▶	Asia Pacific (Tokyo)	\$3.07					
Billing preferences	▶	Canada (Central)	\$2.68					
Payment methods	▶	EU (Frankfurt)	\$2.78					
Consolidated billing	▶	EU (Ireland)	\$2.75					
Tax settings	▶	EU (London)	\$2.91					
	▶	EU (Paris)	\$2.91					
	▶	South America (Sao Paulo)	\$3.77					
	▶	US East (N. Virginia)	\$2.46					
	▶	US East (Ohio)	\$2.46					

What is GitHub doing?



Secret Scanning

Regex-based search of every commit

Find deeply nested in the history

Searches repo metadata

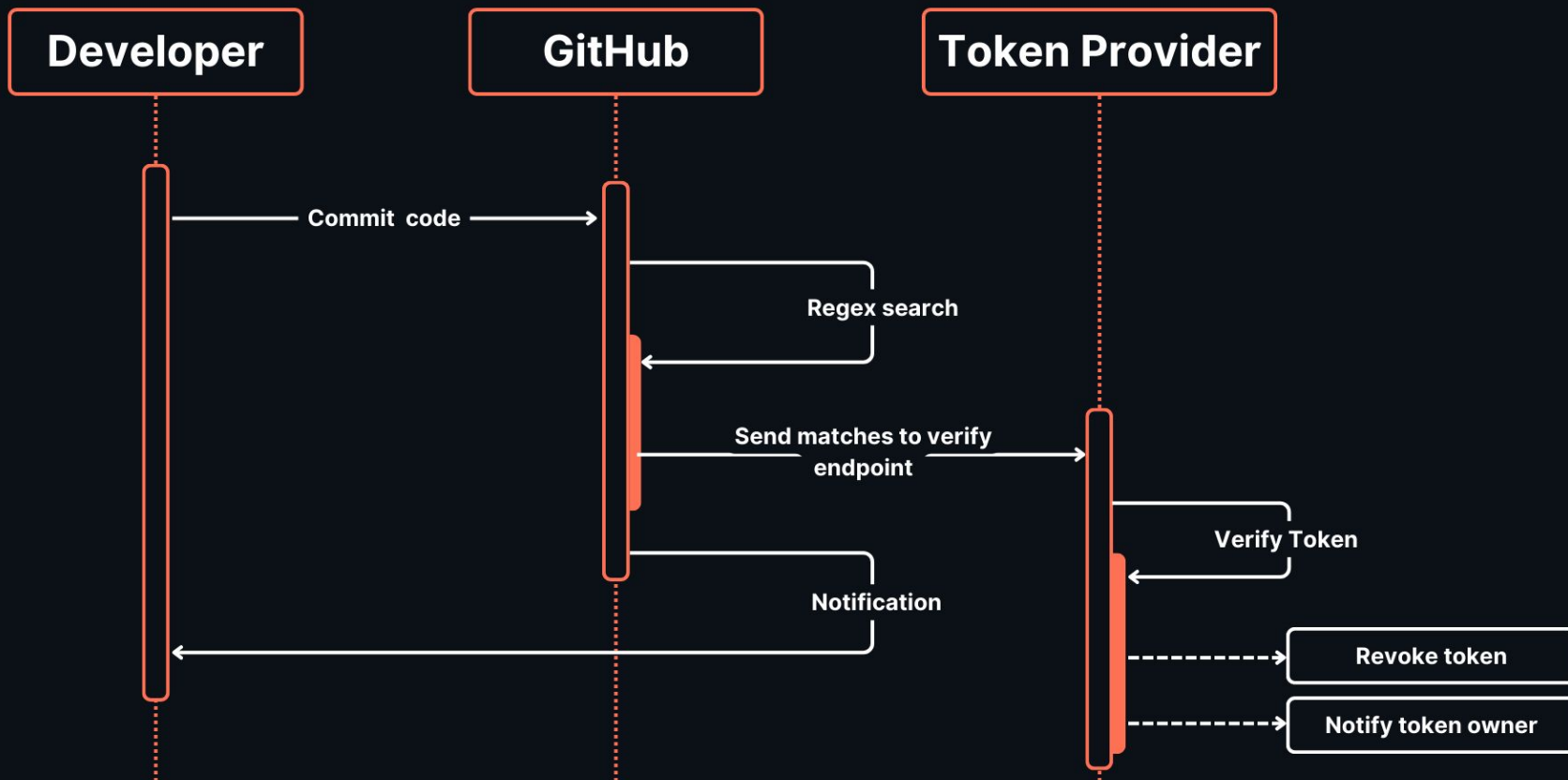
Issues, PR comments, Gists, etc.

The screenshot shows the GitHub web interface for the repository `burrito-party / beat-bot`. The top navigation bar includes links for Code, Issues, Pull requests, Actions, Projects, Wiki, Security (with 116 alerts), and Insights. The left sidebar shows the 'Secret scanning' section as active, with a count of 1 alert. The main content area is titled 'Secret scanning alerts' and displays a list of detected secrets. The list includes:

- GitHub Personal Access Token** (ghp_Zn4uMZLaHmTLlJwQRUhL...): #4 opened 23 seconds ago. Detected secret in `.aws/credentials:7`.
- Amazon AWS Secret Access Key** (30ihNVxVXuHIm0KHIp0pss8...): #3 opened 23 seconds ago. Detected secret in `.aws/credentials:3`.
- Amazon AWS Access Key ID** (AKIA60DU5DHTRJ06UCJG): #2 opened 23 seconds ago. Detected secret in `.aws/credentials:2`.
- Google API Key** (AIzaSyAQfxPJiounkh0jODE0...): #1 opened on Jan 31. Detected secret in `env:1`.

At the top of the alert list, there is a summary: 4 Open, 0 Closed, and a 'Bypassed' dropdown menu. A search bar at the top of the list shows the filter `is:open`.

How secret scanning works



Secret Scanning Push Protection

The screenshot shows a GitHub repository interface for 'leftleftleft / AWS-manager'. The top navigation bar includes links for Code, Issues, Pull requests, Actions, Projects, Wiki, Security (with 16 alerts), Insights, and Settings. The repository path is 'main' and the file 'AWS-manager/' is selected. A search bar is present with the text 'Go to file'. Below the navigation bar, a commit history table is displayed, showing the last commit message and date for each commit. The table has three columns: Name, Last commit message, and Last commit date. The first commit is for '.aws' with the message 'Create credentials' and was committed 32 minutes ago. The second commit is for 'README.md' with the message 'Update README.md' and was committed 3 days ago. The third commit is for 'infrastructure.tf' with the message 'Rename basic.tf to infrastructure.tf' and was committed last week. Below the table, the README file is shown, titled 'AWS-manager', with the content: 'I'm just a demo app that includes some Terraform for deploying applications.'

Name	Last commit message	Last commit date
.aws	Create credentials	32 minutes ago
README.md	Update README.md	3 days ago
infrastructure.tf	Rename basic.tf to infrastructure.tf	last week

AWS-manager

I'm just a demo app that includes some Terraform for deploying applications.



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.

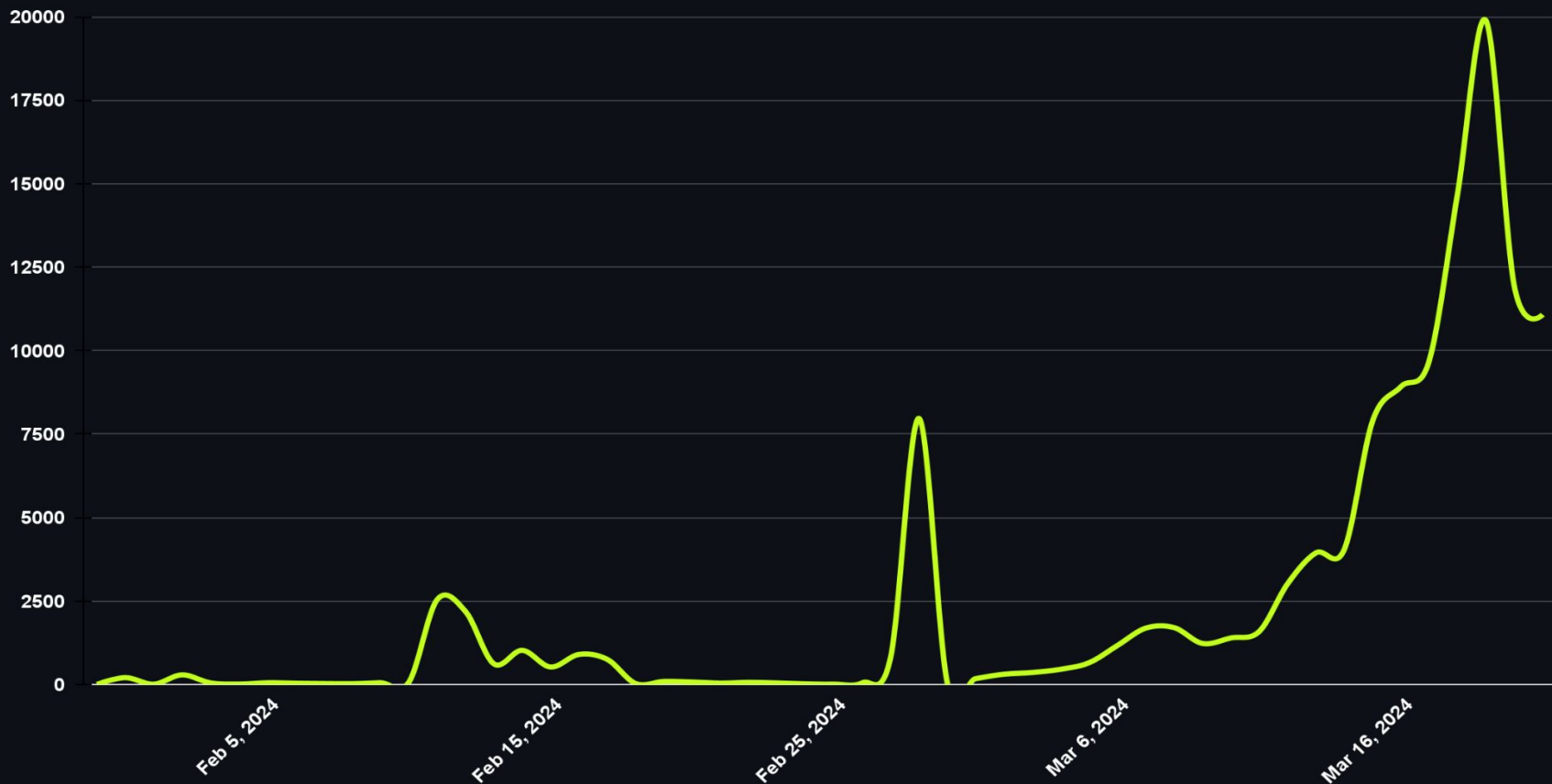
If a secret is detected in any push to a public repository, your push will be blocked. You will have the option to remove the secret from your commits or, if you deem the secret safe, bypass the block.

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?



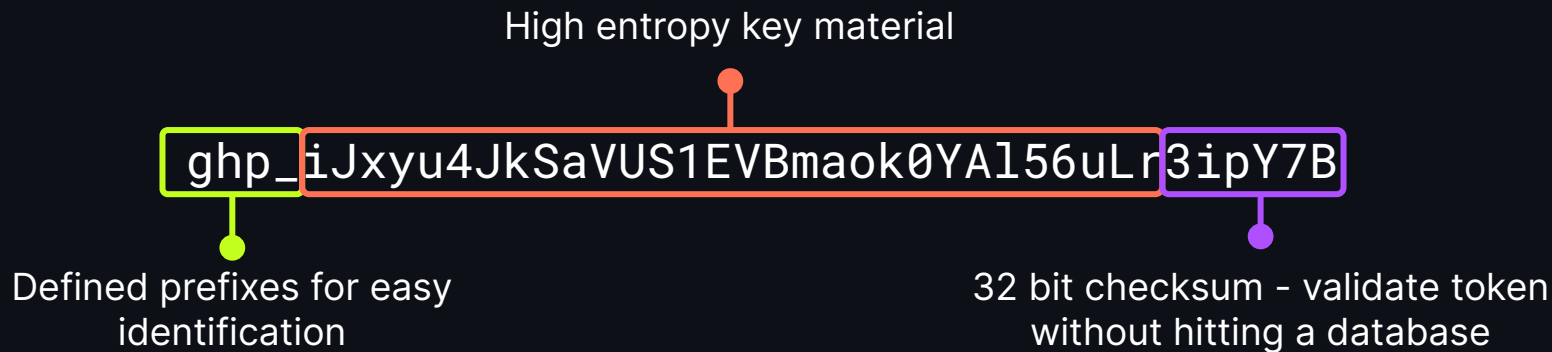
My company creates API tokens

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

