GitHub API, your mistakes belong to us!

Frederick Kaludis

Quarkslab

Summary

Quarkslab

SUMMARY

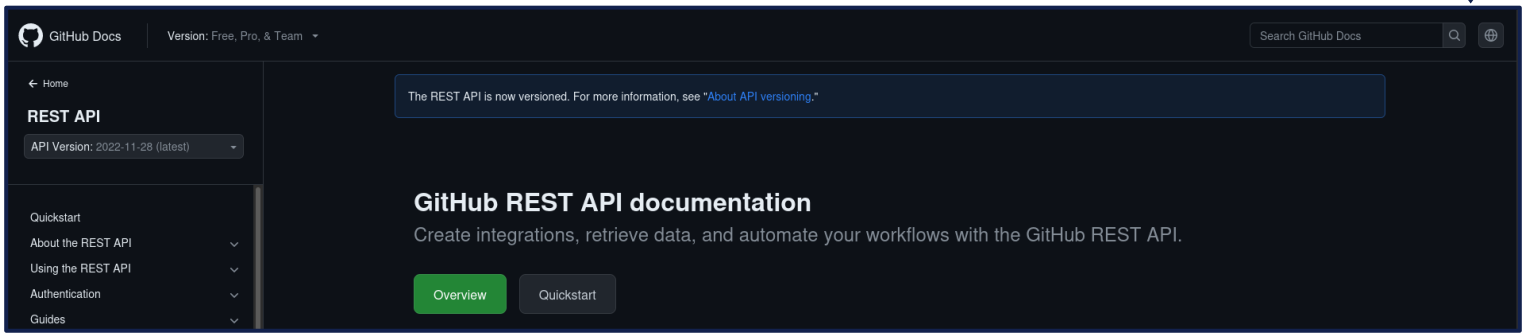
- Introduction to three API routes (*events*, *tarball* & *zipball*).
- Presentation of a real-life case study.
- Concluding remarks.

GitHub API, interesting routes

Quarkslab

GITHUB API, INTERESTING ROUTES

- Documentation:
  - https://docs.github.com/en/rest
- 2 (minimum) or 3 (according to your taste) API routes will be useful:
  - REST API endpoints for events:
    - List repository events
  - REST API endpoints for repository contents:
    - Download a repository archive (tar)
    - Download a repository archive (zip)



REST API ENDPOINTS FOR EVENTS

- The documentation for this route specifies that:
  - "This endpoint can be used without authentication or the aforementioned permissions if only public resources are requested."
- As a result, the request presented in the documentation can be simplified from:

- To:

curl https://api.github.com/repos/OWNER/REPO/events

REST API ENDPOINTS FOR REPOSITORY CONTENTS

- The documentation for this route specifies that:
  - "Gets a redirect URL to download a zip/tar archive for a repository. If you omit `:ref`, the repository's default branch (usually `main`) will be used."
- In addition, for the same reasons as the previous API route, the requests presented in the documentation can be simplified from:

- To:

curl https://api.github.com/repos/OWNER/REPO/tarball/REF
curl https://api.github.com/repos/OWNER/REPO/zipball/REF

Real-life case study

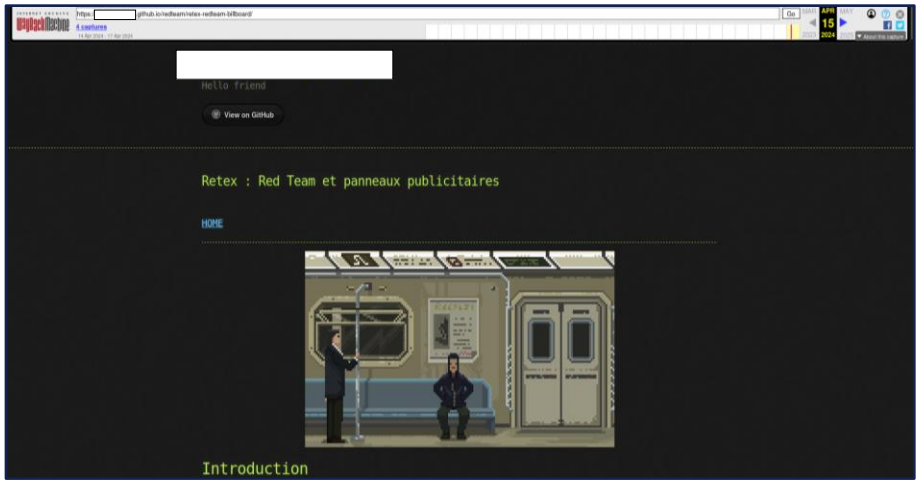
THE MISSING BLOGPOST

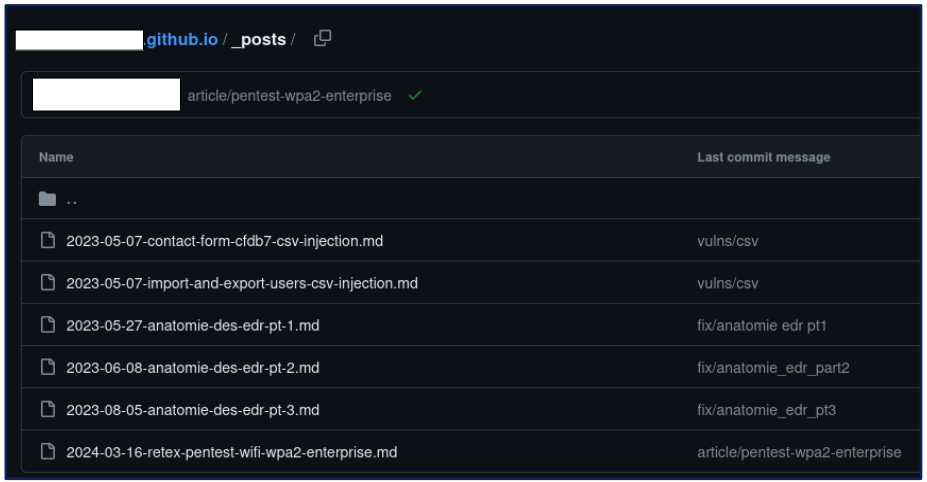
- 12 April 2024 - A link to a blog post about a Red Team engagement is published on .
- Lacking time, I chose to read it later.
- The week goes by normally …
- 17 April 2024 - I wanted to read the article but unfortunately the blog post was deleted without any announcement.

/redteam/retex-redteam-billboard/

RELATED GITHUB REPOSITORY

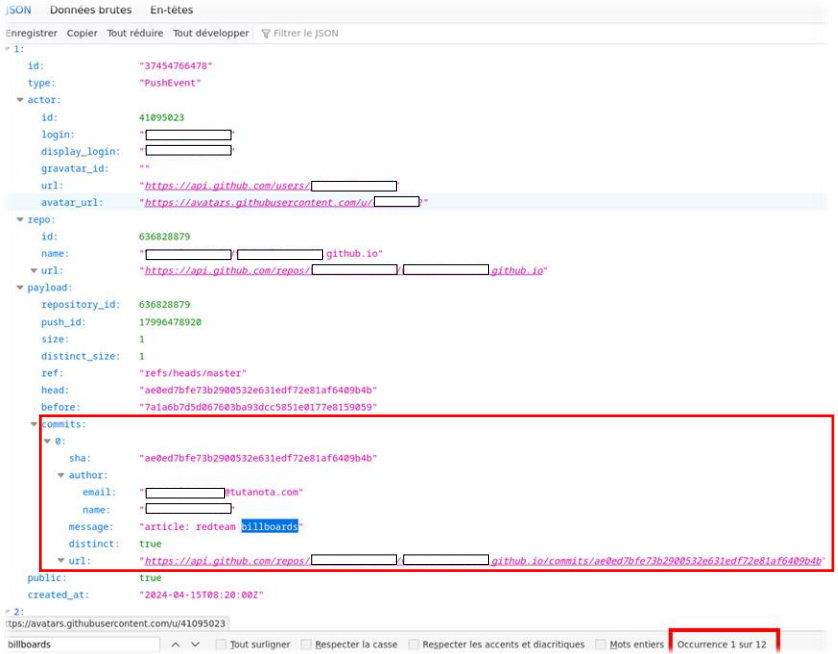
- The Wayback Machine makes it possible to retrieve the article:
  - http://web.archive.org/web/20240415[redacted]/https://[redacted].github.io/redteam/retex-redteam-billboard/
- The file related to the blog post is no longer available on the associated GitHub repository.





USING THE GITHUB API

- Some events in the repository (push operations) took place on dates more recent than those displayed by the GUI.
  - “Wouldn't the front end lie to us?”



FIRST FLAG

```
wget https://api.github.com/repos/AAAA/BBBB.github.io/zipball/ae0ed7...409b4b -O ae0ed7bfe73b409b4b.zip
unzip ae0ed7...409b4b.zip
cd AAAA-BBBB.github.io-ae0ed7b/_posts
```

ALL THE OTHER FLAGS

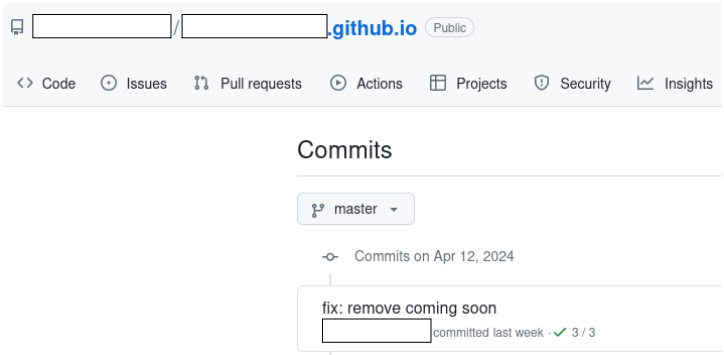
Bash Kung Fu (grab all the events).

- cat events.json | jq ".[] | .payload, .created_at"

- Analyze the dates.

- Recreate our own git repository.

3559cb3a89fedce0285e48088b4c3819785654c5

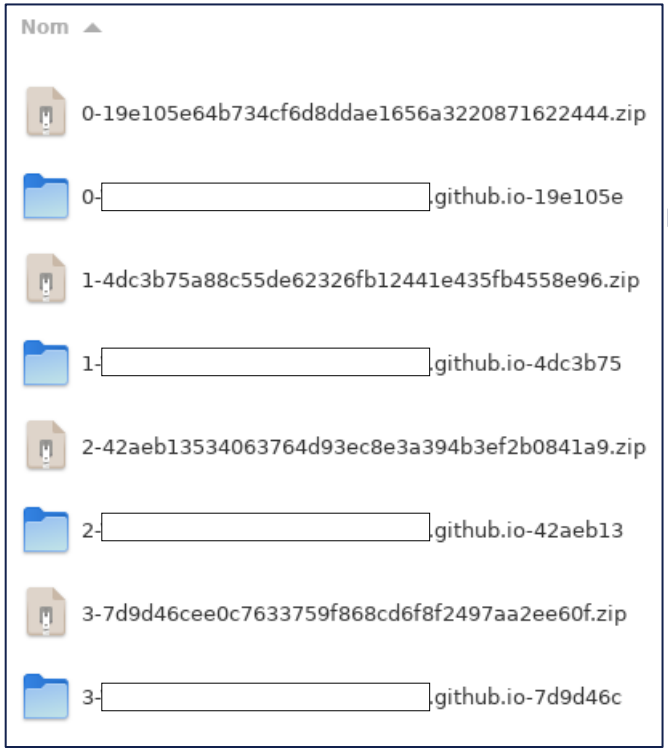



```
{
  "repository_id": 636828879,
  "push_id": 17967408461,
  "size": 1,
  "distinct_size": 1,
  "ref": "refs/heads/master",
  "head": "3559cb3a89fedce0285e48088b4c3819785654c5",
  "before": "13eb712c81c41393f7aaec7f8c29b96aa243d205",
  "commits": [
    {
      "sha": "3559cb3a89fedce0285e48088b4c3819785654c5",
      "author": {
        "email": "[redacted]@tutanota.com",
        "name": "[redacted]"
      },
      "message": "fix: remove coming soon",
      "distinct": true,
      "url":
"https://api.github.com/.../3559cb3a89fedce0285e48088b4c3819785654c5"
    }
  ]
}
"2024-04-12T09:44:13Z"
```



```
$ cat events.json|jq ".[] | .payload.head"
"3559cb3a89fedce0285e48088b4c3819785654c5"
"ae0ed7bfe73b2900532e631edf72e81af6409b4b"
"7a1a6b7d5d067603ba93dcc5851e0177e8159059"
"230f906a518ff5aa3c70577061f8f092362c0558"
"3559cb3a89fedce0285e48088b4c3819785654c5"
"639bb68cfb2b451b223311912eb3359442784bb7"
"7e9b47e954a17b17eb64f2b286d9830970442392"
"10ed622d6ed088a9d1643bd68b77e7d7ac3b4269"
"dad25351cdc8d73b8b777efc7cdd81f6d288e538"
"3559cb3a89fedce0285e48088b4c3819785654c5"
"f577d7f4dbde0e58e3e267028cb696a0676120d3"
null
"db638e6c283cece39e6f35ca2e89986f139e282d"
"4158de5041d98554d03c709e740c4b0c246566c2"
"06c4f0d1d3695ce7a89f166adfdbfcdf98ae5370"
"589e76b3c1401d6ccedc27f428ab56a19eacee4b"
"3559cb3a89fedce0285e48088b4c3819785654c5"
null
null
"13eb712c81c41393f7aaec7f8c29b96aa243d205"
"7d9d46cee0c7633759f868cd6f8f2497aa2ee60f"
"42aeb13534063764d93ec8e3a394b3ef2b0841a9"
"4dc3b75a88c55de62326fb12441e435fb4558e96"
"19e105e64b734cf6d8ddae1656a3220871622444"
```

ALL THE OTHER FLAGS



Look for the first commit related to the missing blogpost (sorted by ascendant creation date).

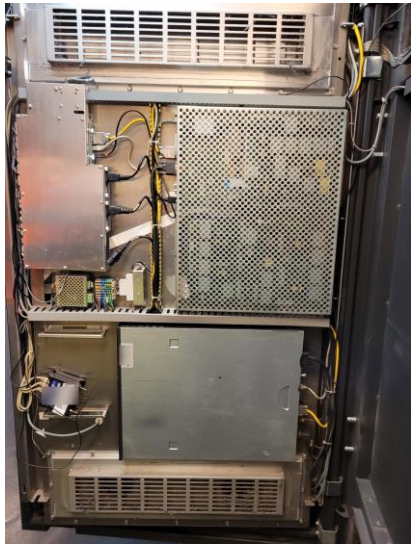
```
[ 2:10][ego@alter:~/Téléchargements/Resources/Archives]
 $ find ./ -iname "*billboard.md"|sort -u
./10-[redacted].github.io-f577d7f/_posts/2024-04-12-retex-redteam-billboard.md
./14-[redacted].github.io-639bb68/_posts/2024-04-12-retex-redteam-billboard.md
./15-[redacted].github.io-230f906/_posts/2024-04-12-retex-redteam-billboard.md
./17-[redacted].github.io-ae0ed7b/_posts/2024-04-12-retex-redteam-billboard.md
/6-[redacted].github.io-589e76b/_posts/2024-04-12-retex-redteam-billboard.md
./7-[redacted].github.io-06c4f0d/_posts/2024-04-12-retex-redteam-billboard.md
./8-[redacted].github.io-4158de5/_posts/2024-04-12-retex-redteam-billboard.md
./9-[redacted].github.io-db638e6/_posts/2024-04-12-retex-redteam-billboard.md
```

DID THE AUTHOR TRY TO HIDE...

Poor blurring?

u serveur principal via internet et récupère les campagne
rogrammées pour les transmettre aux panneaux publicitaire
anneaux publicitaires : également situés dans la station.
ls affichent les campagnes publicitaires.

anneaux existent sous différentes tailles et sont mainten
fogérés par une entreprise tierce.



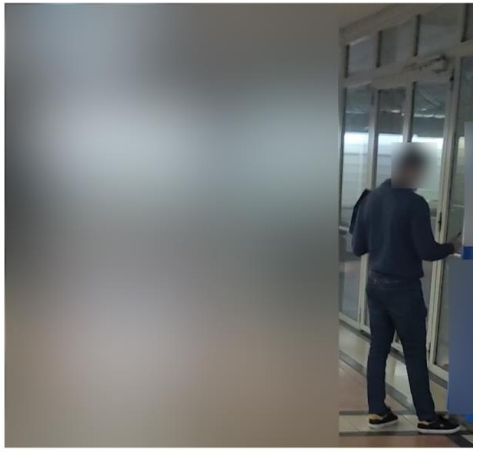
Technical data?

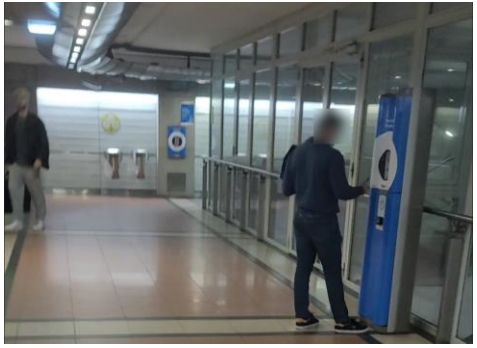
DID THE AUTHOR TRY TO HIDE...

Information concerning access?

deux catégories de personnes :

>> Les collaborateurs de l'entreprise munis d'un
>> Les externes qui doivent se présenter à l'int



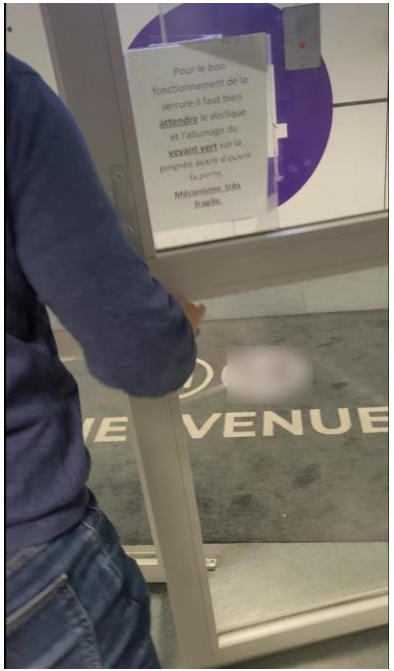


Très souvent les personnes externes se présentaie
l'interphone en déclinant une identité et un moti
aux locaux.

On a donc opté pour ce scénario et on a envoyé un
l'équipe, ordinateur et téléphone à la main pour
tant que technicien du support informatique d'une

vérrouillage automatique.

N'ayant aucune connaissance des lieux, on s'est pe
locaux mais après quelques minutes de recherche, c
réussi à trouver un local technique et dont la por
entrouverte.



WHO WAS THE CLIENT?

RATP

Conclusion

Quarkslab

CONCLUSION

- If you inadvertently publish a secret in a commit, **delete the repository and recreate a new one**.
  - However, it's important to remember that **the secret will still be in the possession of Microsoft** (and therefore of US government agencies).

- This presentation is not intended to mock or attack the author of the blog, it's a preventive measure to make you realize that the GitHub GUI doesn't tell you everything.

Thank you

Quarkslab

TO GO FURTHER (BUILD YOUR TOOL/SCRIPT)

- Compare */commits* and */events* :
  - In order to identify which commits have been deleted, simply compare the hashs obtained from the list of */commits* and */events*.
  - Once the comparison has been made, it will be possible to identify deleted elements and consequently regenerate the associated tarball/zipball archives.

- About pagination:
  - When a response from the REST API would include many results, GitHub will paginate the results and return a subset of the results. For example, GET `/repos/octocat/Spoon-Knife/issues` will only return 30 issues from the *octocat/Spoon-Knife* repository even though the repository includes over 1600 open issues. This makes the response easier to handle for servers and for people.
  - You can use the `link` header from the response to request additional pages of data. If an endpoint supports the `per_page` query parameter, you can control how many results are returned on a page.

TO GO FURTHER (BUILD YOUR TOOL/SCRIPT)

- Using link headers:
  - When a response is paginated, the response headers will include a link header. If the endpoint does not support pagination, or if all results fit on a single page, the link header will be omitted.
  - The link header contains URLs that you can use to fetch additional pages of results. For example, the previous, next, first, and last page of results.