

GitHub API, your mistakes belong to us!

Frederick Kaludis



VS



Summary



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

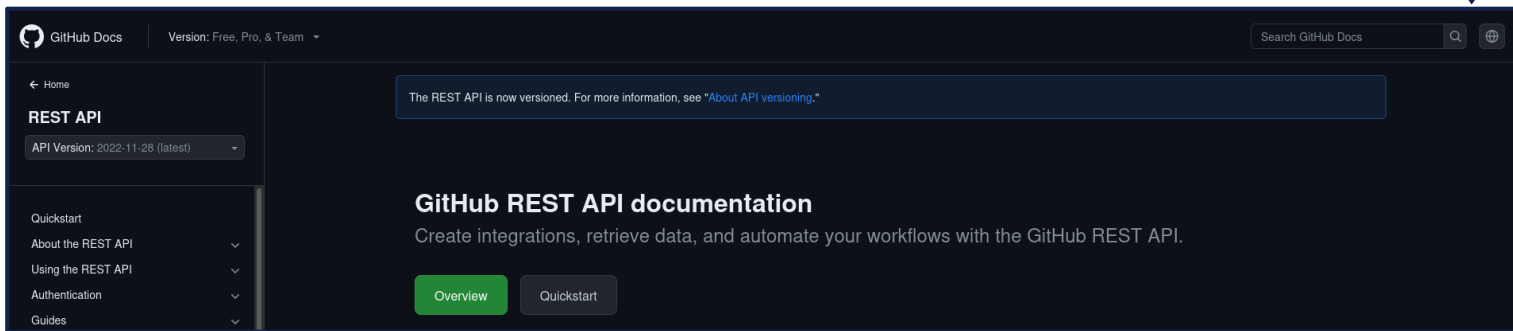
GitHub API, interesting routes



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:

```
GET /repos/{owner}/{repo}/events

cURL  JavaScript  GitHub CLI

curl -L \
-H "Accept: application/vnd.github+json" \
-H "Authorization: Bearer <YOUR-TOKEN>" \
-H "X-GitHub-API-Version: 2022-11-28" \
https://api.github.com/repos/OWNER/REPO/events
```



- 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:

```
GET /repos/{owner}/{repo}/tarball/{ref}

cURL JavaScript GitHub CLI

curl -L \
-H "Accept: application/vnd.github+json" \
-H "Authorization: Bearer <YOUR-TOKEN>" \
-H "X-GitHub-API-Version: 2022-11-28" \
https://api.github.com/repos/OWNER/REPO/tarball/REF
```

```
GET /repos/{owner}/{repo}/zipball/{ref}

cURL JavaScript GitHub CLI

curl -L \
-H "Accept: application/vnd.github+json" \
-H "Authorization: Bearer <YOUR-TOKEN>" \
-H "X-GitHub-API-Version: 2022-11-28" \
https://api.github.com/repos/OWNER/REPO/zipball/REF
```

- 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.

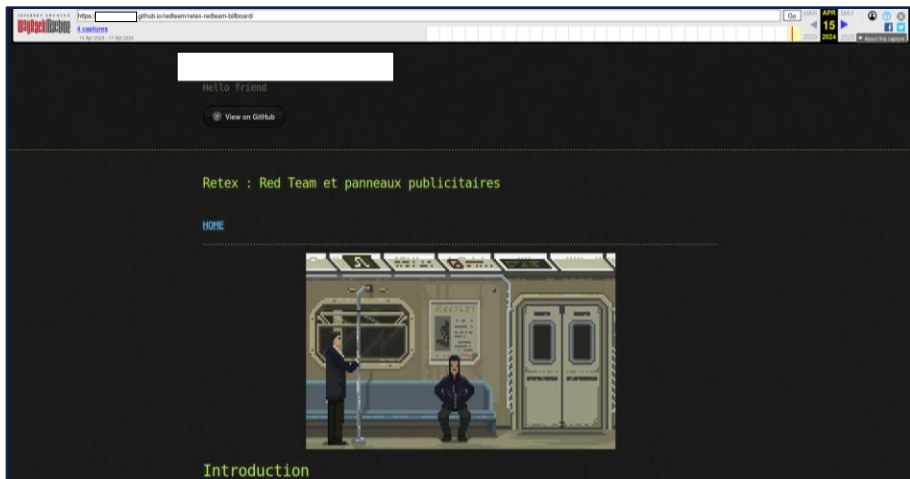


</redteam/retext-redteam-billboard/>

RELATED GITHUB REPOSITORY



- The Wayback Machine makes it possible to retrieve the article:
 - [http://web.archive.org/web/2024041517/https://\[redacted\].github.io/redteam/retex-redteam-billboard/](http://web.archive.org/web/2024041517/https://[redacted].github.io/redteam/retex-redteam-billboard/)
- The file related to the blog post is no longer available on the associated GitHub repository.



| Name | Last commit message |
|---|---------------------------------|
| .. | |
| 2023-05-07-contact-form-cfdb7-csv-injection.md | vulns/csv |
| 2023-05-07-import-and-export-users-csv-injection.md | vulns/csv |
| 2023-05-27-anatomie-des-edr-pt-1.md | fix/anatomie edr pt1 |
| 2023-06-08-anatomie-des-edr-pt-2.md | fix/anatomie_edr_part2 |
| 2023-08-05-anatomie-des-edr-pt-3.md | fix/anatomie_edr_pt3 |
| 2024-03-16-retex-pentest-wifi-wpa2-enterprise.md | article/pentest-wpa2-enterprise |

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?"



```
JSON  Données brutes  En-têtes
Enregistrer Copier Tout réduire Tout développer Filtre le JSON
1:
  id: "37454766478"
  type: "PushEvent"
  actor:
    id: 41095023
    login: "[redacted]"
    display_login: "[redacted]"
    gravatar_id: ""
    url: "https://api.github.com/users/[redacted]"
    avatar_url: "https://avatars.githubusercontent.com/u/[redacted]"
  repo:
    id: 636828879
    name: "[redacted] github.io"
    url: "https://github.com/repos/[redacted] github.io"
  payload:
    repository_id: 636828879
    push_id: 17996478920
    size: 1
    distinct_size: 1
    ref: "refs/heads/master"
    head: "aebed7bfe73b2900532e631edf72e81af6409b4b"
    before: "7a1a6b7d5d067603ba93dcc5851e0177e8159059"
  commits:
    0:
      sha: "aebed7bfe73b2900532e631edf72e81af6409b4b"
      author:
        email: "[redacted]@tutanota.com"
        name: "[redacted]"
        message: "article: redteam billboard"
        distinct: true
      url: "https://api.github.com/repos/[redacted] github.io/commits/aebed7bfe73b2900532e631edf72e81af6409b4b"
  public: true
  created_at: "2024-04-15T08:20:00Z"
2:
https://avatars.githubusercontent.com/u/41095023
billboards
^ v Tout surligner Respecter la casse Respecter les accents et diacritiques Mots entiers Occurrence 1 sur 12
```

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
```



```
--
layout: post
categories: redteam
title: "Retex : Red Team et panneaux publicitaires"
permalink: "/:categories/:title/"
---



# Introduction

Il y a quelques temps, on a eu la chance d'être sélectionnés par une entreprise pour réaliser un test d'intrusion interne qui s'est transformé en une mission Red Team sur son infrastructure.

Cette entreprise souhaitait évaluer la sécurité de son système de panneaux publicitaires dans les stations. L'objectif de la mission était de savoir si des attaquants pouvaient détourner l'affichage des panneaux pour y afficher des messages de propagande.

Pour commencer, on abordera rapidement l'architecture et le fonctionnement des panneaux publicitaires.

Ensuite, on verra comment des attaquants peuvent utiliser l'ingénierie sociale pour s'introduire dans des locaux techniques, notamment les salles informatiques.

Enfin, on va montrer comment, à partir d'un simple câble RJ45 et d'un accès à un commutateur, il est possible d'enchaîner plusieurs vulnérabilités pour prendre le contrôle de l'ensemble du système publicitaire.

"2024-04-12-retex-redteam-billboard.md" 211L, 13185B
```

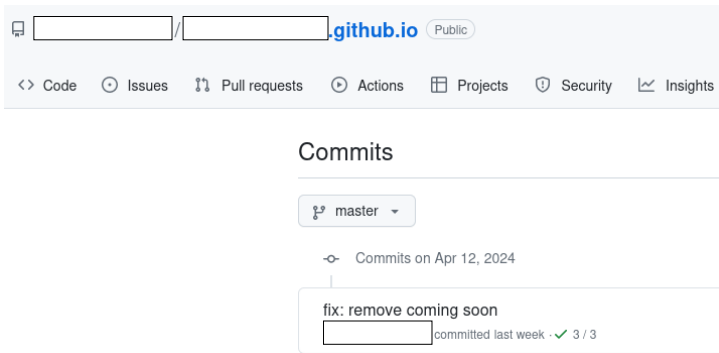
ALL THE OTHER FLAGS



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"
"06c4f0d1d3695ce7a89f166adfdbfcdcf98ae5370"
"589e76b3c1401d6cccd27f428ab56a19eace4b"
"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?

serveur intermédiaire : situé dans la station. Il se connecte au serveur principal via internet et récupère les campagnes programmées pour les transmettre aux panneaux publicitaires. Les anneaux publicitaires : également situés dans la station. Ils affichent les campagnes publicitaires.

Les anneaux existent sous différentes tailles et sont maintenant gérés par une entreprise tierce.



Technical data?

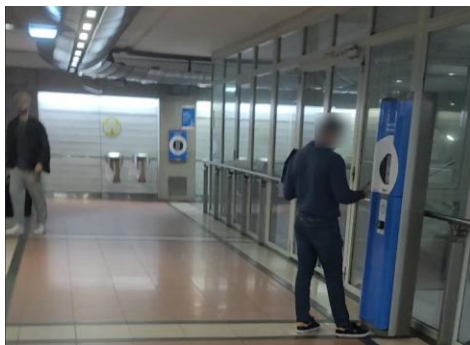
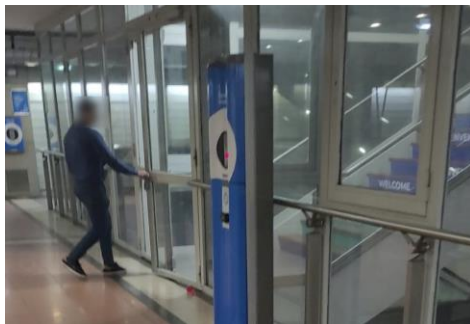
DID THE AUTHOR TRY TO HIDE...



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 présentaient à l'interphone en déclarant une identité et un motif aux locaux.

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

vérouillage automatique.



N'ayant aucune connaissance des lieux, on s'est présenté aux locaux mais après quelques minutes de recherche, on a réussi à trouver un local technique et dont la porte était entrouverte.

WHO WAS THE CLIENT?



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

TO GO FURTHER (BUILD YOUR TOOL/SCRIPT)



- Compare `/commits` and `/events`:
 - In order to identify which commits have been deleted, simply compare the hashes 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.

```
← → ↻ 🔍 https://api.github.com/repos/chamilo/chamilo-lms/events
ego
JSON Données brutes En-têtes
Copier
En-têtes de réponse
X-Firefox-Spdy h2
accept-ranges bytes
access-control-allow-origin *
access-control-expose-headers ETag, Link, Location, Retry-After, X-GitHub-OTP, X-RateLimit-Limit, X-RateLimit-Remaining, X-RateLimit-Used, X-RateLimit-Resource, X-RateLimit-Reset, X-OAuth-Scopes, public, max-age=60, s-maxage=60
cache-control
content-encoding gzip
content-security-policy default-src 'none', object-src blob: filesystem: *; frame-src blob: filesystem: *
content-type application/json; charset=utf-8
date Mon, 19 Aug 2024 09:53:56 GMT
etag W/"3002a9de5d674a54f378282637973ee13e204cc827421c6b1bc47216f552c1eb"
last-modified Sun, 18 Aug 2024 17:38:31 GMT
link <https://api.github.com/repositories/9103211/events?page=2>; rel="next", <https://api.github.com/repositories/9103211/events?page=10>; rel="last"
```