Open in app ↗

Sign up

Sign in

Medium

Search

Write

Understanding & Detecting C2 Frameworks — BabyShark

Nasreddine Bencherchali · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

BabyShark

UnkL4b/BabyShark

This is a basic C2 generic server written in Python and Flask. This code has based ideia to GTRS, which uses Google…

github.com

> *This is a basic C2 generic server written in Python and Flask.*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Before we dive into the source code, we first need to understand how can google translate be used as a proxy.

Google translate is used typically to translate words, paragraphs or documents. But it can also be used to translate web pages. By simply visiting the following URL and providing the web page we want to translate.

```
https://translate.google.com/translate?&anno=2&u=[URL OF WEB PAGE]
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

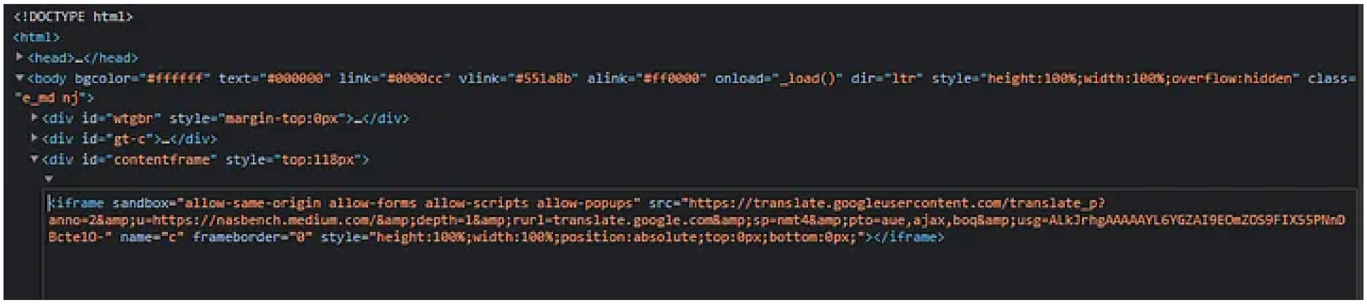
Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Simple right ? If we inspect the source of this page we'll find that the content is loaded inside of an "iframe". This "iframe" points to another URL.



```
<!DOCTYPE html>
<html>
▸ <head>…</head>
▾<body bgcolor="#ffffff" text="#000000" link="#0000cc" vlink="#551a8b" alink="#ff0000" onload="_load()" dir="ltr" style="height:100%;width:100%;overflow:hidden" class=
"e_md nj">
  ▸<div id="wtgbr" style="margin-top:0px">…</div>
  ▸<div id="gt-c">…</div>
  ▾<div id="contentframe" style="top:118px">
    ▾
     <iframe sandbox="allow-same-origin allow-forms allow-scripts allow-popups" src="https://translate.googleusercontent.com/translate_p?
     anno=2&amp;u=https://nasbench.medium.com/&amp;depth=1&amp;rurl=translate.google.com&amp;sp=nmt4&amp;pto=aue,ajax,boq&amp;usg=ALkJrhgAAAAAYL6YGZAI9EOmZOS9FIX5SPNnD
     Bcte1O-" name="c" frameborder="0" style="height:100%;width:100%;position:absolute;top:0px;bottom:0px;"></iframe>
```

Inspecting the source

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

We got our original web page now “hosted” on a google domain. If you’re thinking what if instead of doing this we insert a link to a C2 server? Well, that’s exactly the idea behind the GTRS project and BabyShark example agent.

C2 Server (app.py)

The server portion of “BabyShark” is composed of a web interface where the operators can send commands and visualize the output. These commands and results are stored inside of a database.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The server defines 5 web routes that we can see in the screenshot below.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

“/” Route

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

function simply parse and store the results in the database. Either way (If there are results or not) the page will send the next command(s) to be executed by the agent.

Below is an example of commands embedded within the page when requesting “/momyshark” with the correct key.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

“create” Function

The create function is linked to the “/create-task” path and accepts only post requests. This function will simply register the commands sent by the operators from the interface in the database.

done & delete

Both of these functions are simple wrappers to delete / update the state of a command. If we take a look at the database schema we’ll see that there are two tables with the following columns.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

We can see that the results have been stored and the command changed its “done” value to “1” meaning “completed”. The “done” function will simply inverse the state of a command in the command table.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

As stated in their GitHub introduction. The “BabyShark” C2 does not generate agents. Fortunately for us they provide an example inspired by GTRS agent that we’re going to look at.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
Safari/537.36"
data="Content-Hype: "
c2server="http://babyshark/momyshark?key=$secretkey"
result=""
input="/tmp/input"
output="/tmp/output"
```

It then defines some functions

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

main

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

functions are called.

getfirsturl

“getfirsturl” Function

The “getfirsturl” function will make a call to the google translate domain and

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

“getsecondurl” Function

This function will perform the same action as “getfirsturl” but this time it requests the URL extracted from the “iFrame” of the previous request. It also follows any redirections that google may throw at it by using the “-L” argument from curl.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

With this the agent returns to main with the command to execute in hand (or should i say in variable…).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The result will be concatenated to the User-Agent as follow

```
result="$user_agent | $outputb64 | $idcommand "

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36 |
L2hvbWUvbi90b29scy9CYWJ5U2hhcmsK | 1
```

To send the results back to the C2 the agent will call the ***"talktotranslate"*** function but this time with the newly generated user-agent. The C2 server

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

8. Request the *"google-translate"* server using the newly generated USER-AGENT.
9. Repeat until it receives *"exit"* command.

. . .

Conclusion

That's it for Baby Shark doo, doo, doo, doo, doo, doo *(sorry not sorry)*. I hope

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- **T1041 — Exfiltration Over C2 Channel**
- **T1059.004 — Command and Scripting Interpreter: Unix Shell**
- **T1071.001 — Application Layer Protocol: Web Protocols**

Infosec · Blue Team · Red Team · Detection Engineering · Command And Control

--

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app