Pedro Gomes

4 July 2022

CarBridge

Security Analysis

This report is an over simplified version of a security analysis.

The report tries to access the cyber security risks and implications of the software "CarBridge" usage.

The analysis is based on: Open source intelligence information.

1. What is CarBridge

CarBridge is an application that allows two iOS apps to be simultaneously opened. One in the media display screen of a car, and another in the iOS device. In order to this CarBridge uses both mirroring and screen bridging techniques. Mirroring is used as an alternative when bridging is not possible due to compatibility issues.

2. Analysis

There seems to be a lot of SCAM websites about CarBridge. After searching for awhile, the site https://carbridge.app seems to be the legitimate one.

That are several factors that conducted me to think this is the legitimate website.

1. WHOIS info:

   Domain Name: carbridge.app

```
Registry Domain ID: 4155ACF01-APP
Registrar WHOIS Server: 
whois.google.com
Registrar URL: https://
domains.google.com
Updated Date: 2022-04-24T13:58:57Z
Creation Date: 2020-02-05T03:38:27Z
Registrar Registration Expiration 
Date: 2023-02-05T03:38:27Z
```

As we can see the domain was register in 2020 and the registrar was Google. This is the oldest registered domain I found for CarBridge. Here is an example of the whois of a similar domain.

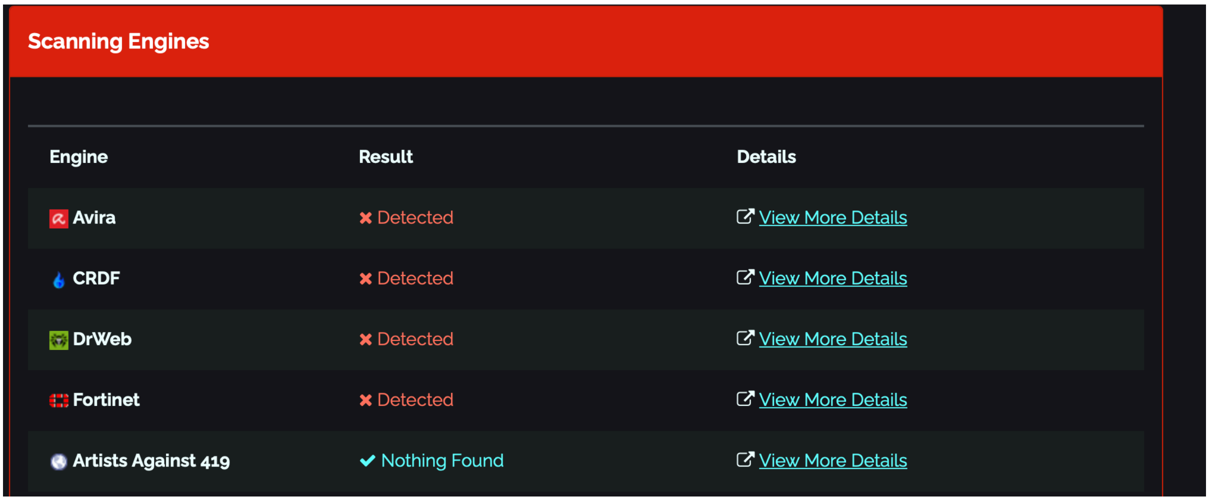
Domain Name: CARBRIDGEAPP.COM

```
   Registry Domain ID: 
2600147627_DOMAIN_COM-VRSN
   Registrar WHOIS Server: 
whois.namecheap.com
   Registrar URL: http://
www.namecheap.com
```

```
    Updated Date:
2022-02-22T06:31:04Z
    Creation Date:
2021-03-24T05:14:18Z
    Registry Expiry Date:
2023-03-24T05:14:18Z
    Registrar: NameCheap, Inc.
```

Here we can see that the domain was registered one year after the first domain and the registrar is NameCheap. A commonly used registrar by threat actors due to advantageous registration prices.

When downloading the said CarBridge on the NameCheap registered domain website, there is a redirection to a suspicious website: https://www.locked1.com/cl.php?id=25eb6720d3ef5fae1336b224f075140e, which is flagged as malicious by 5 different antivirus engines in the URLvoid:



Scanning Engines

Engine	Result	Details
Avira	✖ Detected	View More Details
CRDF	✖ Detected	View More Details
DrWeb	✖ Detected	View More Details
Fortinet	✖ Detected	View More Details
Artists Against 419	✓ Nothing Found	View More Details

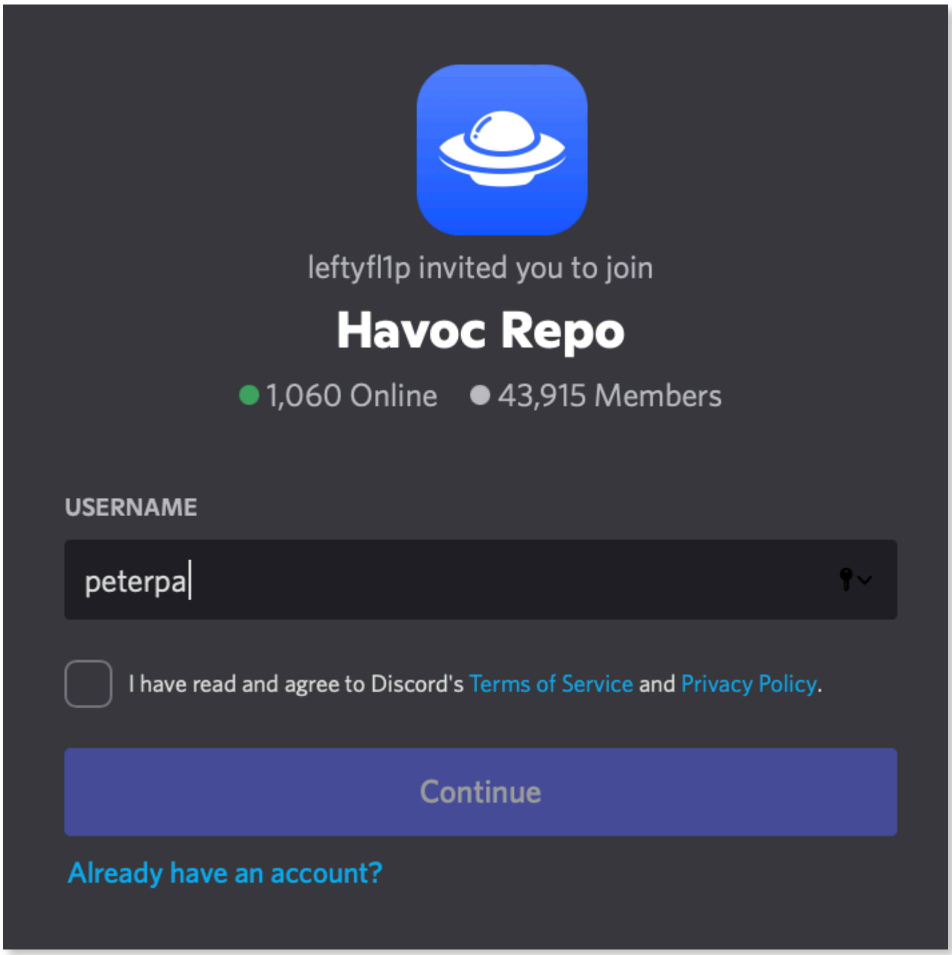
On the carbridge.app website, the authors state the following:

> *Please note: CarBridge or any other 'unsupported CarPlay app loaders' will always require a jailbreak because of Apple limitations and the nature of how this type of software works. Any such software that claims to not require a jailbreak is 100% a scam. This is the only official site for CarBridge.*

The reason for this is because, quoting from the side load channel of a reddit post[0]:

> *CarBridge requires access to the root directory of an iPhone (since it needs access to all apps on the springboard), which is impossible without a jailbreak. A sandbox exists which keeps apps from accessing other apps, and only a jailbreak stops that. It also requires access to write the data of the unauthorized apps onto the CarPlay screen, also impossible without a jailbreak.*

This makes sense from a technical perspective and is consistent with the Apple iOS security practises[1]. In the same website there are also 2 further indicators of legitimacy. The 1st is the discord channel with 43k participants and the 2nd one is the official twitter account of the CarBridge creator. I did not found any CarBridge web pages with discord channel with so many member, nor with twitter profiles providing regular and specific technical updates and support.



leftyfl1p invited you to join

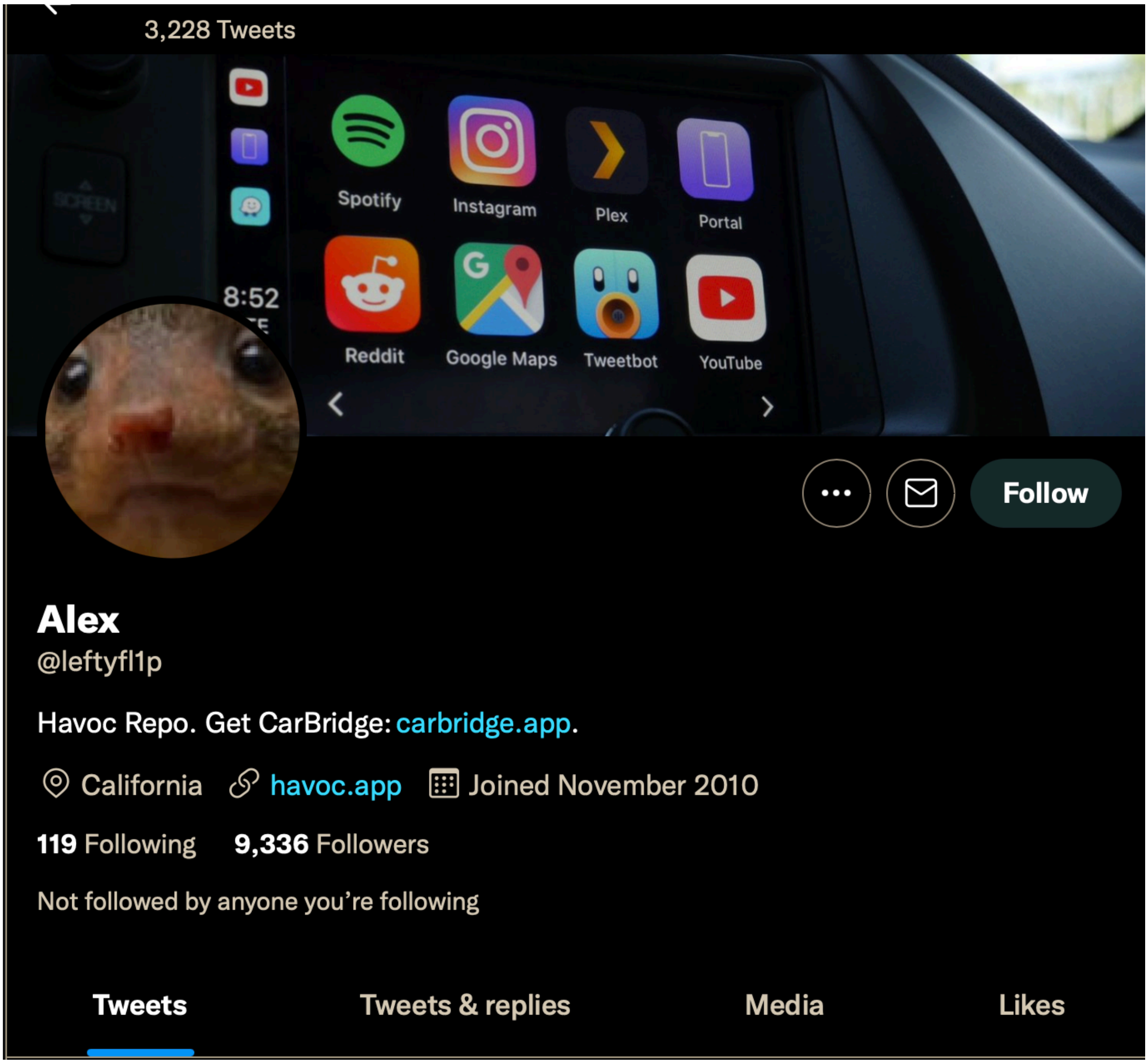
Havoc Repo

● 1,060 Online ● 43,915 Members

USERNAME

peterpa

□ I have read and agree to Discord's Terms of Service and Privacy Policy.



Alex
@leftyfl1p

Havoc Repo. Get CarBridge: carbridge.app.

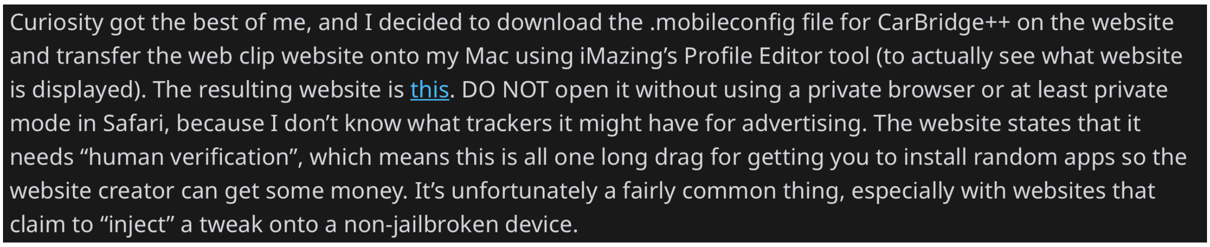
California havoc.app Joined November 2010

119 Following 9,336 Followers

Not followed by anyone you're following

I went on and accessed the Discord Channel. There is a sub-channel called "CarBridge" with a very active community behind and people helping each other trying to solve technical problems.

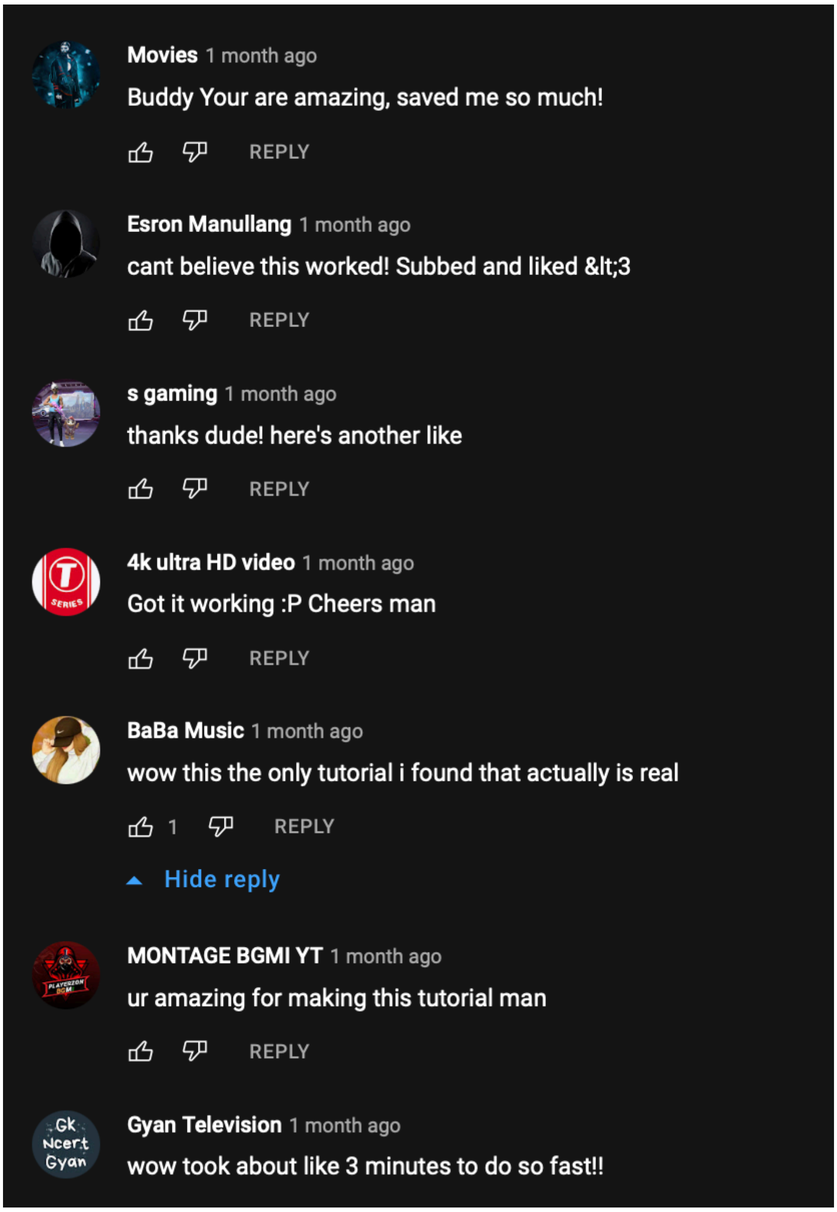
On the reddit post from [0], we can also see that the author actually download a SCAM CarBridge app and shared with us the results. The skips the need to a dynamic manual analysis.



Curiosity got the best of me, and I decided to download the .mobileconfig file for CarBridge++ on the website and transfer the web clip website onto my Mac using iMazing's Profile Editor tool (to actually see what website is displayed). The resulting website is this. DO NOT open it without using a private browser or at least private mode in Safari, because I don't know what trackers it might have for advertising. The website states that it needs "human verification", which means this is all one long drag for getting you to install random apps so the website creator can get some money. It's unfortunately a fairly common thing, especially with websites that claim to "inject" a tweak onto a non-jailbroken device.

Finally on YouTube there are many videos of people claiming they can install CarBridge without jailbreak and using an IPA only. Or videos about similar CarBridge software. Examples of such YouTube videos:

However, after a quick analysis, we can see that the comments of those videos are just bots. The comments were written in the very same period and are very generic. The YouTube profiles of the people commenting do not have any playlists, history, nor followers, which shows evidence they were created not long ago for the purpose of the video. Example



Movies 1 month ago
Buddy Your are amazing, saved me so much!

Esron Manullang 1 month ago
cant believe this worked! Subbed and liked <3

s gaming 1 month ago
thanks dude! here's another like

4k ultra HD video 1 month ago
Got it working :P Cheers man

BaBa Music 1 month ago
wow this the only tutorial i found that actually is real

MONTAGE BGMI YT 1 month ago
ur amazing for making this tutorial man

Gyan Television 1 month ago
wow took about like 3 minutes to do so fast!!

It seems the ultimate goal of the majority of the scammers is to make a potential victim install third-party IPAs with apps containing advertisement and to ask additional purchases during the installation process.

3. Conclusion

Given that is technically impossible to use CarBridge without jailbreak or any other similar mirroring software, I do not recommend the installation of any other CarBridge software, or similar, that is not officially stated in https://carbridge.app.

4. References

[0] : https://www.reddit.com/r/sideloaded/comments/q3b4c1/question_can_i_trust_the_carbridge_ios_app_no/

[1] : https://developer.apple.com/library/archive/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html