# Android/Flubot: preparing for a new campaign?

cryptax.medium.com/android-flubot-preparing-for-a-new-campaign-2f7563fc6c06

@cryptax March 29, 2021


@cryptax

Mar 29, 2021

.

4 min read

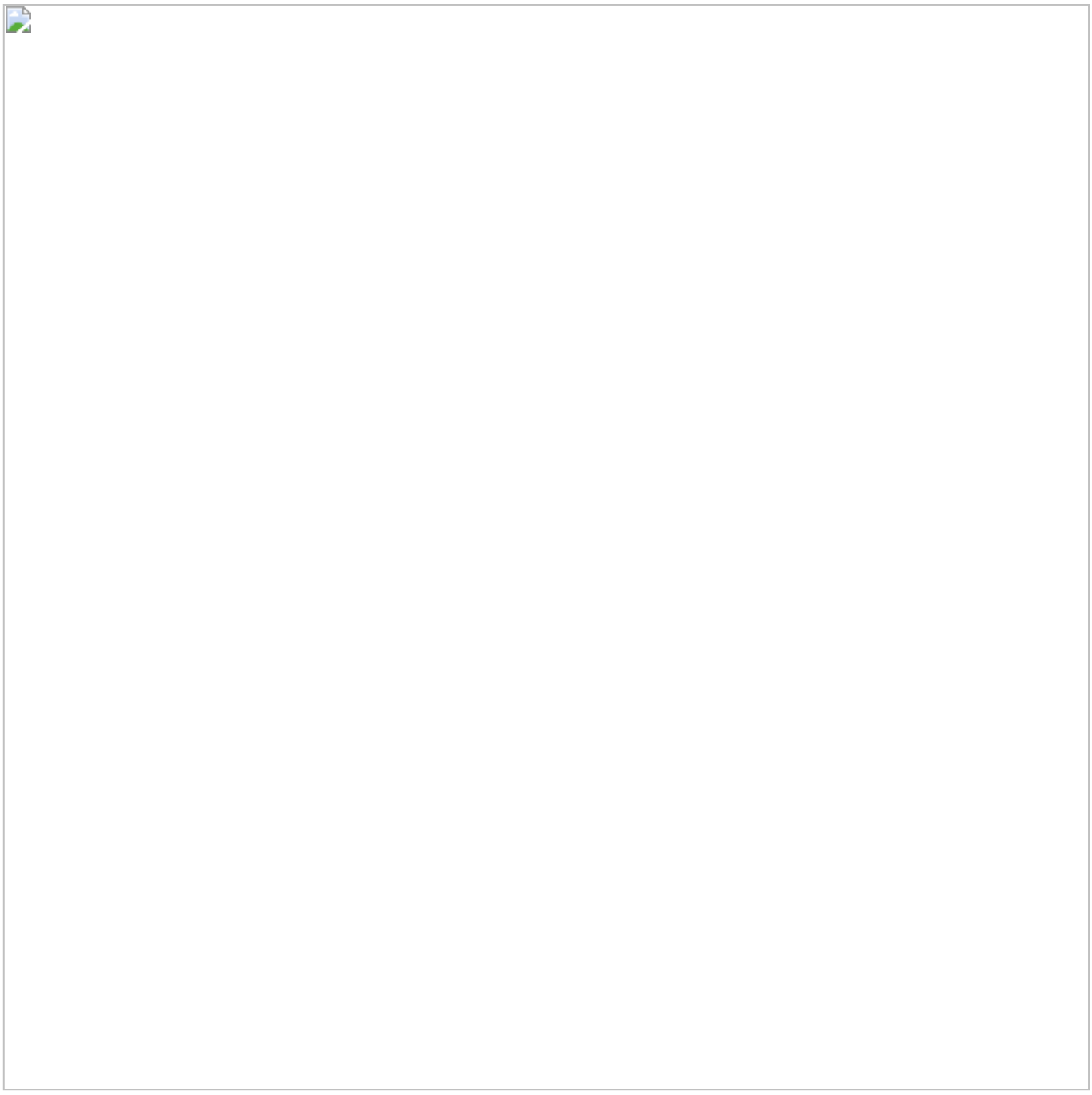
*Update March 29, 2021: . See. It looks like the version 3.7 I analyzed wasn't totally finished, because in the one I analyze, the campaign number nor the DGA haven't been updated, while the tweet shows a version 3.7 where all modifications have been made.*

*March 29, 2nd update: this is moving rapidly, version 3.8 is already out: see .*

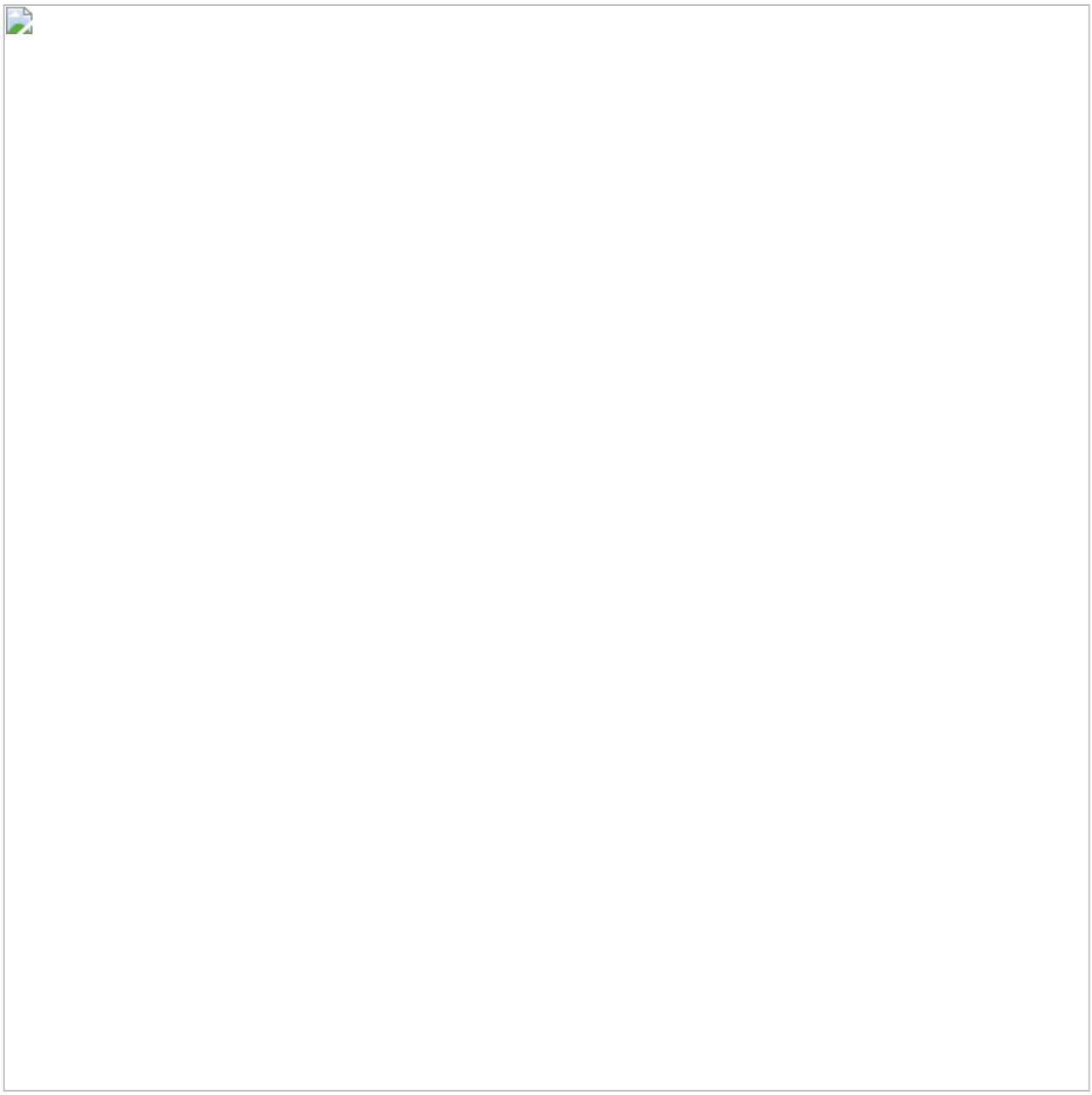
Since Friday (March 26, 2021), Android/Flubot is **propagating a new version, v3.7**. For reminder, Android/Flubot is an Android **banking malware**, which surfaced in November 2020. In short, the malware abuses yet and again Android's *Accessibility Services*. For example, to disable Play Protect, or display overlay windows to grab credit card info. But it also abuses the Accessibility Services for features I had not seen in other malware before like *automatically accepting to send SMS messages*. Read this analysis from Prodaft for more details. I won't repeat what's in the report and only focus on differences.

## New version 3.7 is currently distributing!

This video shows Flubot 3.6 in action, and communicating with a live C&C. The name of the C&C is generated via a proprietary algorithm. The communication with the C&C is encrypted : we use a Frida hook to display the messages before encryption or after decryption. The video captures the C&C requesting list of contacts, SMS, disabling Play Protect and asking to propagate malware via SMS with links to infected sites. Those infected sites currently propagate v3.7.
The **list of APK distribution domains is long** (see at the end of this article in section "IoCs") and changes frequently. The websites check the browser's user agent matches an Android platform, and won't respond to other platforms (i.e you have to append a fake Android user agent to get the pages). The served page is the same as in Prodaft's report, except we currently view the **German campaign**.



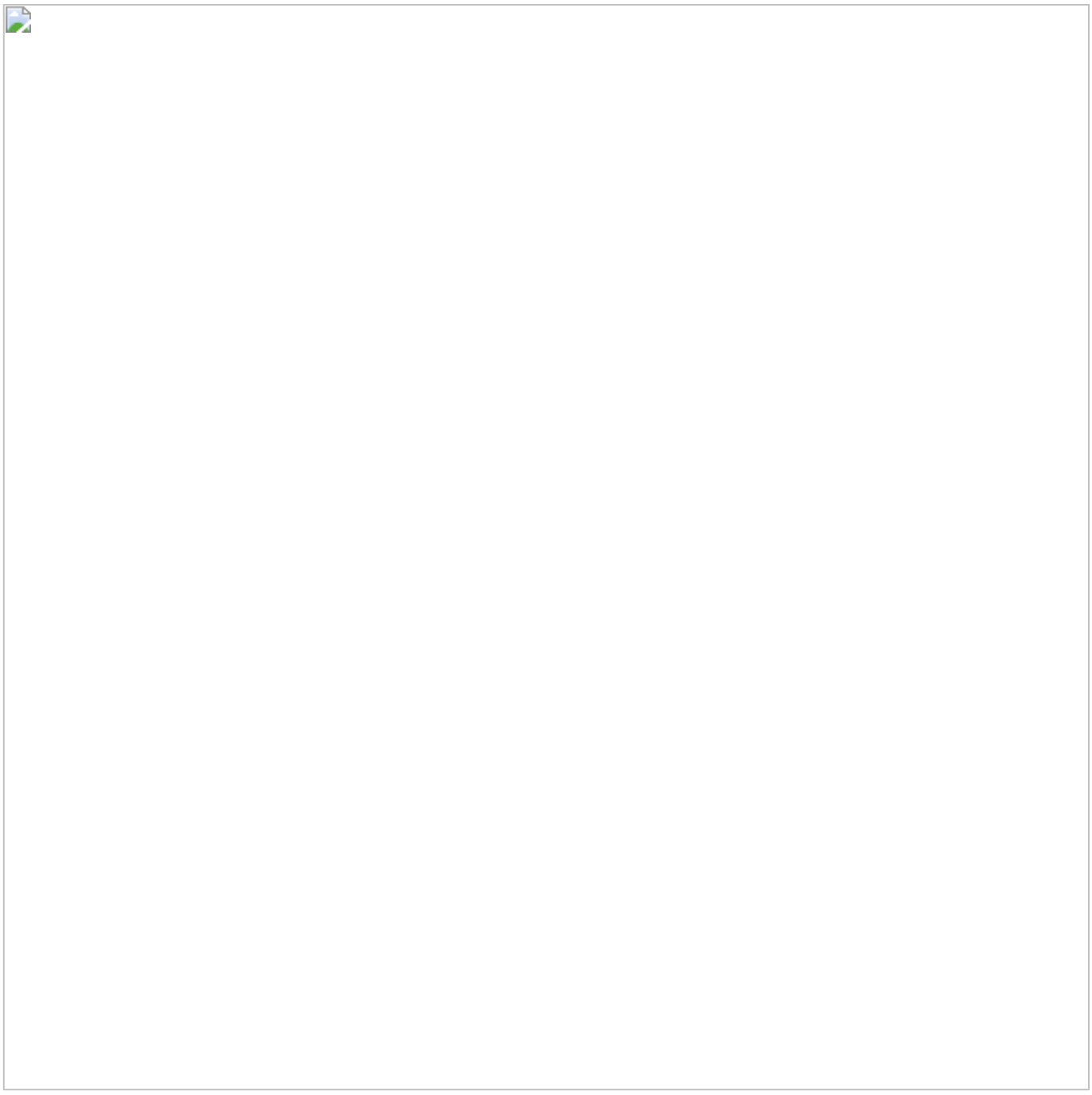
When you click to download the application, you get a recent version of the malware.
Several of these domains currently serve an APK sha256 `e4d70de608d9491119bacd0729a5a2f55ce477227bd7b55d88fa2086486e886d` which an even more *recent version* of Flubot. This sample is packed (like others) and **is a new version, 3.7, of Flubot**.



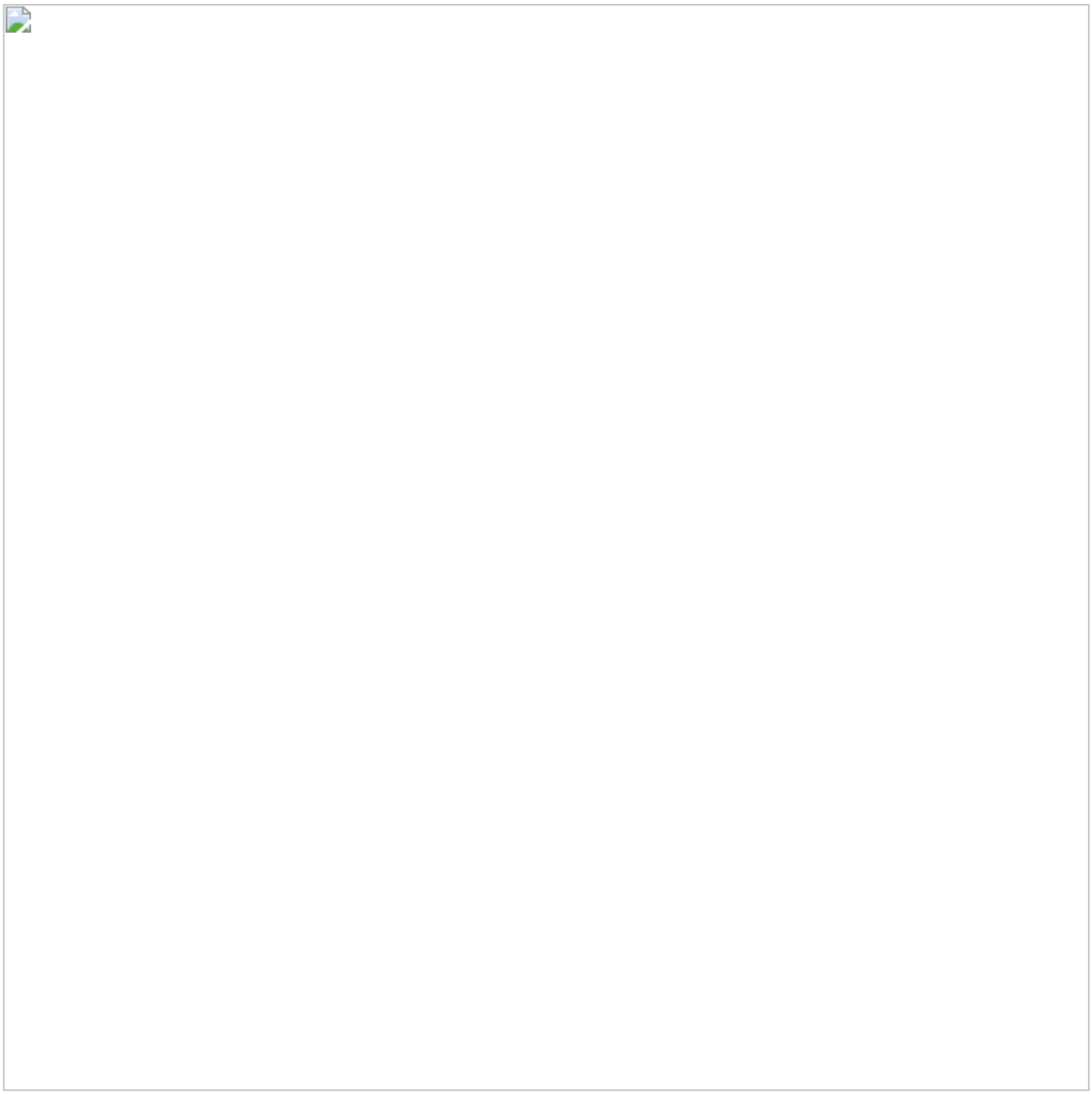
New version of the day for Android/Flubot: 3.7 (March 26, 2021)

## What's new in v3.7?

Actually, **close to nothing** both in the code and obfuscated strings. Reminder: strings are obfuscated using "paranoid" Java library. You can de-obfuscate all strings of v3.6 and v3.7 with my stand-alone source code.



De-obfuscated strings of v3.6 left, and v3.7 right. There are close to no difference.
The only difference lies in preparing support for the hungarian language.



The code shows new localized strings for Hungary in v3.7.

**Does this mean the next campaign of Flubot is going to target Hungarian end-users?** It's quite uncertain currently, especially because although the `HU_TEXT` entry is present, hungarian strings haven't been added yet, and the rest of the code does not support `.hu` locale. In addition, the campaign indicator `ProgConfig.CAMP_NUM_PREF` is still set to Germany (49).

## Take away summary

- Because of string obfuscation, the . However, the de-obfuscated content is very similar. Actually, the only notable change in 3.7 looks like . Yet, the current campaign still targets german speaking end-users.

- You can watch a (see beginning of article). The communication flow with the C&C thanks to a Frida hook which displays text before encryption.
- If you wish to work on Flubot, (obfuscation, domain name generation, Frida hooks) are available: see References below
- An updated is provided in Appendix.

## References

- .
- hook by Prodaft. My versions .

Unpacking Flubot with House. Actually, this is a bit overkill for this sample as it simply sits in a private directory of the app…

## The Brief Glory of Cabassous/FluBot — a private Android banking botnet

### A new botnet has surfaced in late 2020, take a look at the details about this criminal operation targeting banking…

medium.com

## IoCs

## List of active C&Cs:

Both domains have changed since Prodaft's report and currently go to the following (March 26, 2021):

- u
-

## List of APK distribution domains:

hxxp://jfourtshirtmart.com/track/?4pbmxy24vzwhxxp://trace-eye-d.com/track/?
59wrgdjd4g1e4d70de608d9491119bacd0729a5a2f55ce477227bd7b55d88fa2086486e886dhxxp://trace-
eye-d.com/track/?v0nlimrsvmqhxxp://cowdigital.co.uk/pkge/?
va37j7103ykshxxp://beautycenter.yourprofitguru.com/pkge/?
3ziq0yiu3t6hxxp://cowdigital.co.uk/pkge/?vh7xoxjd1jrhxxp://senanginsta.com/trck/?
0q3wnaqrmpehxxp://webridgeinnovation.com/trck/?1zv9yaumiv5hxxp://cpap-sales.com/pkg/?
xi10u7rea8o4hxxp://trace-eye-d.com/track/?ge2om10nbk7zhxxp://humberto-
cardenas.com/pkge/?4z9m9y511010rhxxp://webridgeinnovation.com/trck/?
dcxd2d5u477hxxp://jfourtshirtmart.com/track/?xsst9rx6j1xhxxp://cpap-sales.com/pkg/?
xzutci86kfhhxxp://jfourtshirtmart.com/track/?bg9de9wp779hxxp://trace-eye-d.com/track/?
5wy9ly108m6mhxxp://jfourtshirtmart.com/track/?iuenfwdd45khxxp://humberto-
cardenas.com/pkge/?210z3djromp2hxxp://cowdigital.co.uk/pkge/?o0tqs8kaj1rhxxp://cpap-
sales.com/pkg/?nsnh10rlc10tshxxp://gainsuperno1.com/pkg/?
10vbdlci8h9xhxxp://gainsuperno1.com/pkg/?g10kupbvsrlhxxp://jfourtshirtmart.com/track/?
6ix9i10tf84bhxxp://humberto-cardenas.com/pkge/?
52q79dwav2hhxxp://jfourtshirtmart.com/track/?
xudbym9103pthxxp://webridgeinnovation.com/trck/?
jzvjzp10qnnphxxp://webridgeinnovation.com/trck/?
amjx83vgod4hxxp://jfourtshirtmart.com/track/?qmm1r3u63pxhxxp://trace-eye-d.com/track/?
4pob68ughz8hxxp://flamingocantina.com/pkge/?jayznpsswe0hxxp://humberto-
cardenas.com/pkge/?77681019vdjdhxxp://senanginsta.com/trck/?
ab99gza5z7bhxxp://jfourtshirtmart.com/track/?
sdwflwnnshehxxp://webridgeinnovation.com/trck/?j63bemodkm0hxxp://humberto-
cardenas.com/pkge/?yz4q79olg0rhxxp://trace-eye-d.com/track/?
ywiw102y8mr5hxxp://webridgeinnovation.com/trck/?tg7f56kvshkhxxp://gainsuperno1.com/pkg/?
7oqigahzjbyhxxp://cpap-sales.com/pkg/?42iu4srbp5chxxp://cowdigital.co.uk/pkge/?
pnmqknfkfcxhxxp://webridgeinnovation.com/trck/?v3vothul1r5hxxp://cowdigital.co.uk/pkge/?
1muij0wwi5jhxxp://gainsuperno1.com/pkg/?iluyttg0kv4hxxp://senanginsta.com/trck/?
510mh70eqe85hxxp://humberto-cardenas.com/pkge/?
q101xpppyahhhxxp://cowdigital.co.uk/pkge/?tg10yhuo57g6hxxp://gainsuperno1.com/pkg/?
wdmdec0t4r3hxxp://humberto-cardenas.com/pkge/?x0adna53w5uhxxp://senanginsta.com/trck/?
9qxruq8bm9ehxxp://cpap-sales.com/pkg/?dnoeswgaxvohxxp://cowdigital.co.uk/pkge/?
noldlm17punhxxp://gainsuperno1.com/pkg/?n34b53n7v810hxxp://cpap-sales.com/pkg/?
lirc2arb10s1hxxp://cowdigital.co.uk/pkge/?sg9dvijrol1hxxp://humberto-cardenas.com/pkge/?
x4vlm4dgiichxxp://gainsuperno1.com/pkg/?waex6qenhzmhxxp://cowdigital.co.uk/pkge/?
7q5th1smnmahxxp://cpap-sales.com/pkg/?
401ewt94dbohxxp://beautycenter.yourprofitguru.com/pkge/?2uejxu4e0oihxxp://humberto-
cardenas.com/pkge/?jk54ogi6geihxxp://gainsuperno1.com/pkg/?
yp9iezvpxxnhxxp://webridgeinnovation.com/trck/?
azk6xlt1orfhxxp://jfourtshirtmart.com/track/?im6g3uwrgiqhxxp://trace-eye-d.com/track/?
wvftkbhkq8ohxxp://senanginsta.com/trck/?vy310n5x4syrhxxp://senanginsta.com/trck/?
vuszj6mhpixhxxp://cpap-sales.com/pkg/?1310igiio7cfhxxp://gainsuperno1.com/pkg/?
qt10108u8ia80hxxp://trace-eye-d.com/track/?h8m92b66i18hxxp://cpap-sales.com/pkg/?
i68mh31gr0hhxxp://humberto-cardenas.com/pkge/?hoct5ed9na9hxxp://cowdigital.co.uk/pkge/?
knpzykweo6ihxxp://gainsuperno1.com/pkg/?jr09puq4efhxxp://cpap-sales.com/pkg/?gnhf81a3m8e

— Cryptax