Android/Flubot: preparing for a new campaign?

By @cryptax

Published: 2021-03-29 · Archived: 2026-04-05 20:55:39 UTC

4 min read

Mar 29, 2021

Update March 29, 2021: ***a new campaign is confirmed, in Hungary****. See this tweet. 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 here.

Get @cryptax's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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 *excellent* 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**.

Press enter or click to view image in full size

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**.

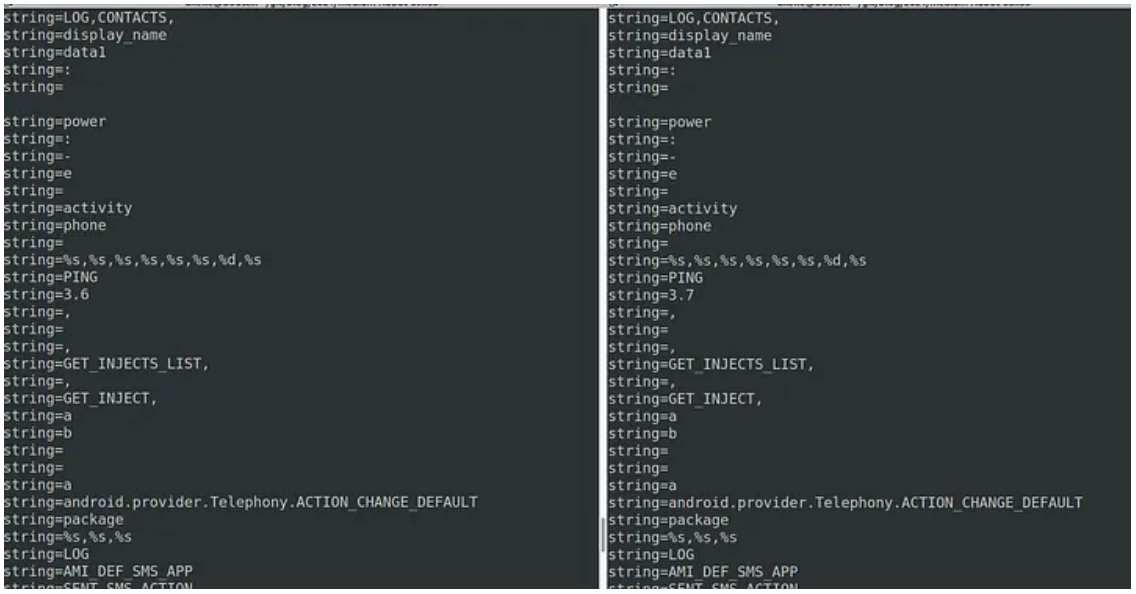
```
static {
    ProgConfig.VERSION = "3.7";
    ProgConfig.SERV_PATH = "/poll.php";
    ProgConfig.BOT_ID_KEY = "a";
```

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.

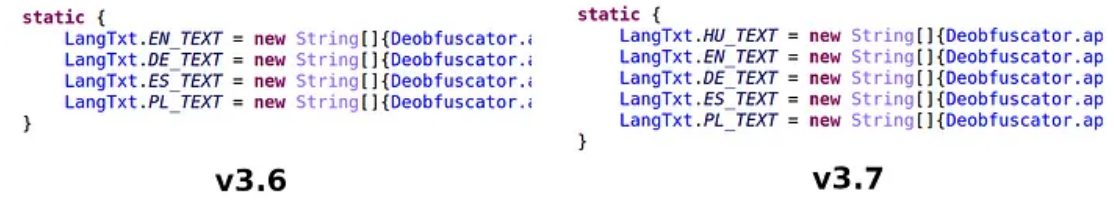
Press enter or click to view image in full size



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.

Press enter or click to view image in full size



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 *obfuscated chunks change for each version of Flubot*. However, the de-obfuscated content is very similar. Actually, the only notable change in 3.7 looks like **preparation for support of the hungarian language**. Yet, the current campaign still targets german speaking end-users.
- You can watch a **video of Flubot in action** (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, **several scripts** (obfuscation, domain name generation, Frida hooks) are available: see References below
- An updated **list of active C&Cs and distribution hosts** is provided in Appendix.

References

- Flubot Malware Analysis Report. **A must-read!**
- DGA standalone algorithm, Frida hook by Prodaft. My versions here.

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

IoCs

List of active C&Cs:

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

- hxxp://nwjkvblqxgdafpu.ru
- hxxp://xnekrtnyfyoqwic.ru

List of APK distribution domains:

```
hxxp://jfourtshirtmart.com/track/?4pbmxy24vzw
hxxp://trace-eye-d.com/track/?59wrgdjd4g1e4d70de608d9491119bacd0729a5a2f55ce477227bd7b55d88fa2086486
hxxp://trace-eye-d.com/track/?v0nlimrsvmq
hxxp://cowdigital.co.uk/pkge/?va37j7103yks
hxxp://beautycenter.yourprofitguru.com/pkge/?3ziq0yiu3t6
hxxp://cowdigital.co.uk/pkge/?vh7xoxjd1jr
hxxp://senanginsta.com/trck/?0q3wnaqrmpe
hxxp://webridgeinnovation.com/trck/?1zv9yaumiv5
hxxp://cpap-sales.com/pkg/?xi10u7rea8o4
hxxp://trace-eye-d.com/track/?ge2om10nbk7z
hxxp://humberto-cardenas.com/pkge/?4z9m9y511010r
hxxp://webridgeinnovation.com/trck/?dcxd2d5u477
hxxp://jfourtshirtmart.com/track/?xsst9rx6j1x
hxxp://cpap-sales.com/pkg/?xzutci86kfh
hxxp://jfourtshirtmart.com/track/?bg9de9wp779
hxxp://trace-eye-d.com/track/?5wy9ly108m6m
hxxp://jfourtshirtmart.com/track/?iuenfwdd45k
hxxp://humberto-cardenas.com/pkge/?210z3djromp2
hxxp://cowdigital.co.uk/pkge/?o0tqs8kaj1r
hxxp://cpap-sales.com/pkg/?nsnh10rlc10ts
hxxp://gainsuperno1.com/pkg/?10vbdlci8h9x
hxxp://gainsuperno1.com/pkg/?g10kupbvsrl
hxxp://jfourtshirtmart.com/track/?6ix9i10tf84b
hxxp://humberto-cardenas.com/pkge/?52q79dwav2h
hxxp://jfourtshirtmart.com/track/?xudbym9103pt
hxxp://webridgeinnovation.com/trck/?jzvjzp10qnnp
hxxp://webridgeinnovation.com/trck/?amjx83vgod4
hxxp://jfourtshirtmart.com/track/?qmm1r3u63px
hxxp://trace-eye-d.com/track/?4pob68ughz8
hxxp://flamingocantina.com/pkge/?jayznpsswe0
```

```
hxxp://humberto-cardenas.com/pkge/?77681019vdjd
hxxp://senanginsta.com/trck/?ab99gza5z7b
hxxp://jfourtshirtmart.com/track/?sdwflwnnshe
hxxp://webridgeinnovation.com/trck/?j63bemodkm0
hxxp://humberto-cardenas.com/pkge/?yz4q79olg0r
hxxp://trace-eye-d.com/track/?ywiw102y8mr5
hxxp://webridgeinnovation.com/trck/?tg7f56kvshk
hxxp://gainsuperno1.com/pkg/?7oqigahzjby
hxxp://cpap-sales.com/pkg/?42iu4srbp5c
hxxp://cowdigital.co.uk/pkge/?pnmqknfkfcx
hxxp://webridgeinnovation.com/trck/?v3vothul1r5
hxxp://cowdigital.co.uk/pkge/?1muij0wwi5j
hxxp://gainsuperno1.com/pkg/?iluyttg0kv4
hxxp://senanginsta.com/trck/?510mh70eqe85
hxxp://humberto-cardenas.com/pkge/?q101xpppyahh
hxxp://cowdigital.co.uk/pkge/?tg10yhuo57g6
hxxp://gainsuperno1.com/pkg/?wdmdec0t4r3
hxxp://humberto-cardenas.com/pkge/?x0adna53w5u
hxxp://senanginsta.com/trck/?9qxruq8bm9e
hxxp://cpap-sales.com/pkg/?dnoeswgaxvo
hxxp://cowdigital.co.uk/pkge/?noldlm17pun
hxxp://gainsuperno1.com/pkg/?n34b53n7v810
hxxp://cpap-sales.com/pkg/?lirc2arb10s1
hxxp://cowdigital.co.uk/pkge/?sg9dvijrol1
hxxp://humberto-cardenas.com/pkge/?x4vlm4dgiic
hxxp://gainsuperno1.com/pkg/?waex6qenhzm
hxxp://cowdigital.co.uk/pkge/?7q5th1smnma
hxxp://cpap-sales.com/pkg/?401ewt94dbo
hxxp://beautycenter.yourprofitguru.com/pkge/?2uejxu4e0oi
hxxp://humberto-cardenas.com/pkge/?jk54ogi6gei
hxxp://gainsuperno1.com/pkg/?yp9iezvpxxn
hxxp://webridgeinnovation.com/trck/?azk6xlt1orf
hxxp://jfourtshirtmart.com/track/?im6g3uwrgiq
hxxp://trace-eye-d.com/track/?wvftkbhkq8o
hxxp://senanginsta.com/trck/?vy310n5x4syr
hxxp://senanginsta.com/trck/?vuszj6mhpix
hxxp://cpap-sales.com/pkg/?1310igiio7cf
hxxp://gainsuperno1.com/pkg/?qt10108u8ia80
hxxp://trace-eye-d.com/track/?h8m92b66i18
hxxp://cpap-sales.com/pkg/?i68mh31gr0h
hxxp://humberto-cardenas.com/pkge/?hoct5ed9na9
hxxp://cowdigital.co.uk/pkge/?knpzykweo6i
hxxp://gainsuperno1.com/pkg/?jr09puq4ef
hxxp://cpap-sales.com/pkg/?gnhf81a3m8e
```

— Cryptax

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