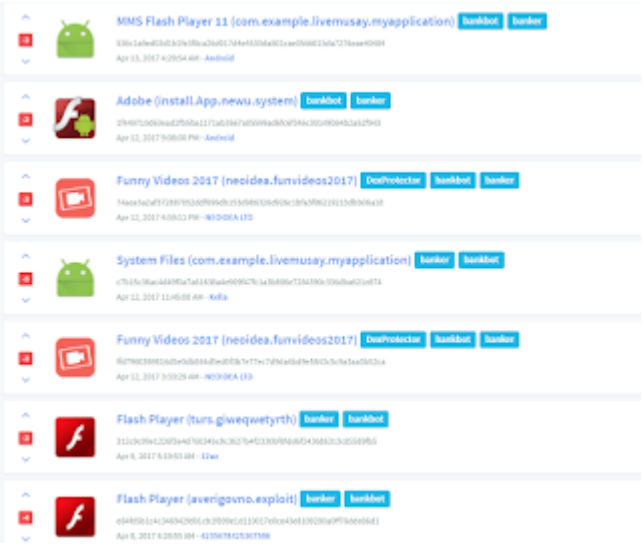
Decrypting Bankbot communications.

Archived: 2026-04-05 17:02:50 UTC

There's has been an increasing lately in the number of Bankbots found in the wild. The latest one, was seen on google play masked as a "fun" application. However, it downloaded a remote payload which contained this Malware.



Bankbot is an Android banking trojan that can be found in underground forums. It can be downloaded without paying a penny, so it's a choice for many people. This is why we see increasing numbers, with some variations but maintaining most of the original schema.

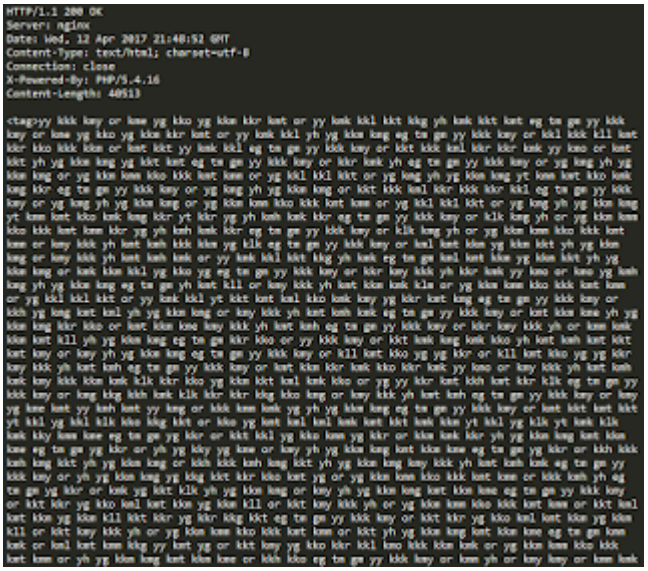
Its functionality covers a wide range:

- Get device data
- Intercept SMS
- Overlay applications
- Send stolen data to remote C&C

This looks like a normal setup for an Android banking trojan. However, these communactions are taking place under an 'encrypted' schema thus not allowing us to see them. We are releasing a script to decode them given the passwords after a few weeks of testing on different bankbots thanks to the encryption routine in the server-side. (Can be found at the end of the post)

The script requires 2 parameters, the first one being the password and the second one being the payload. Once we get this data, it's easy to retrieve the information.

Say this is our example payload:



And we are given the password *mkleotrghyua* then we just have to introduce this data in the script and we will recover the original information.

And this is it! All comms can be decrypted provided you have the password. You can now get this script HERE! It has another example payload with other key.

Decrypter: https://gist.github.com/ineedblood/01dd714d9dd786f3c05a73aae4dfbaef

Some samples:

- 74ace3a2af372887852ddf099db153d986326d926c1bfa3f86219213dbb06a18
- 2dfde3d394b7eaf3a45693dc95f9c5540c9fd2b3bc7e89e9ebc9d12963c00bee

---

Source: http://blog.koodous.com/2017/04/decrypting-bankbot-communications.html