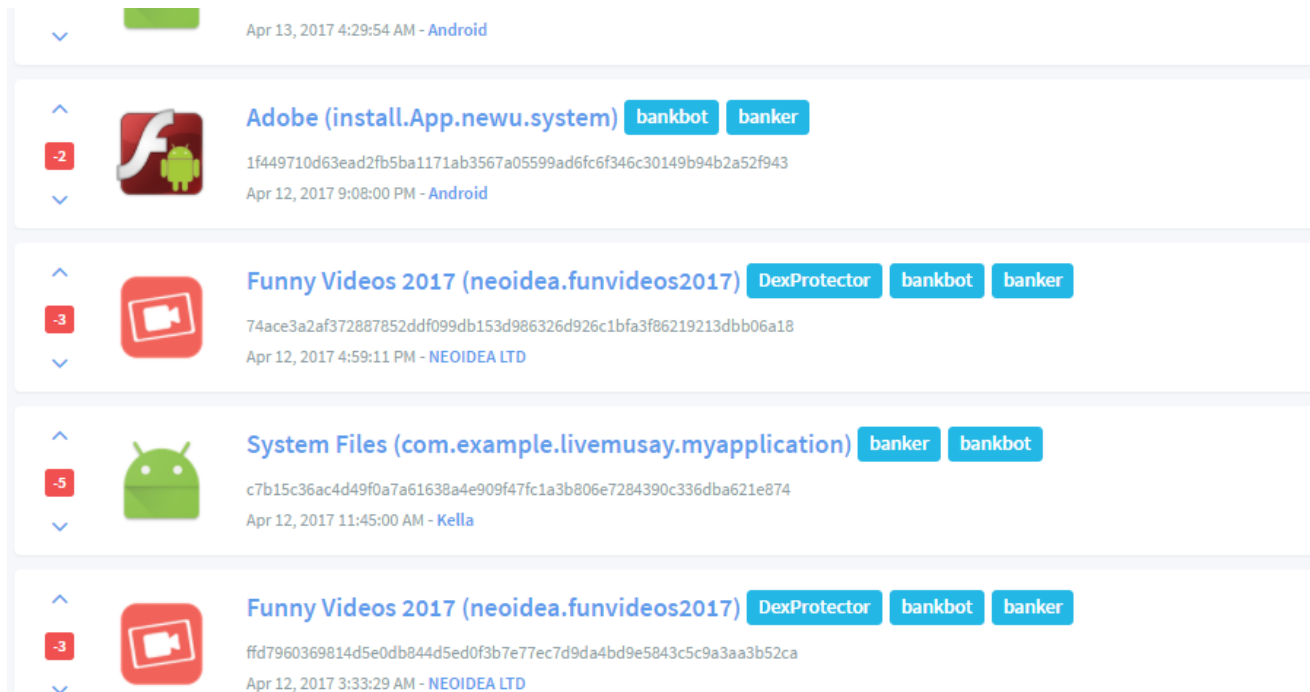


Decrypting Bankbot communications.

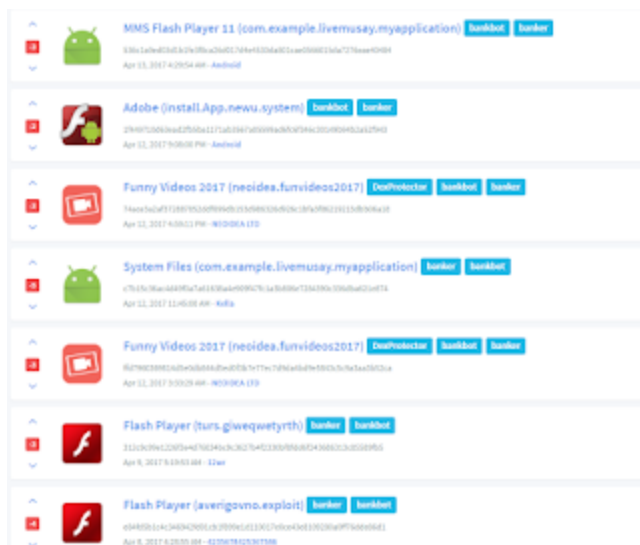
 blog.koodous.com/2017/04/decrypting-bankbot-communications.html



The screenshot shows a list of applications on an Android app store. Each entry includes a rating, an icon, the app name, a list of security tags, and the package name. The applications listed are:

- Adobe (install.App.newu.system)**: Rating -2, tags: bankbot, banker. Package: 1f449710d63ead2fb5ba1171ab3567a05599ad6fc6f346c30149b94b2a52f943. Date: Apr 12, 2017 9:08:00 PM - Android.
- Funny Videos 2017 (neoidea.funvideos2017)**: Rating -3, tags: DexProtector, bankbot, banker. Package: 74ace3a2af372887852ddf099db153d986326d926c1bfa3f86219213dbb06a18. Date: Apr 12, 2017 4:59:11 PM - NEOIDEA LTD.
- System Files (com.example.livemusay.myapplication)**: Rating -5, tags: banker, bankbot. Package: c7b15c36ac4d49f0a7a61638a4e909f47fc1a3b806e7284390c336dba621e874. Date: Apr 12, 2017 11:45:00 AM - Kella.
- Funny Videos 2017 (neoidea.funvideos2017)**: Rating -3, tags: DexProtector, bankbot, banker. Package: ffd7960369814d5e0db844d5ed0f3b7e77ec7d9da4bd9e5843c5c9a3aa3b52ca. Date: Apr 12, 2017 3:33:29 AM - NEOIDEA LTD.

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.



The screenshot shows a list of applications on an Android app store. Each entry includes a rating, an icon, the app name, a list of security tags, and the package name. The applications listed are:

- MMS Flash Player 11 (com.example.livemusay.myapplication)**: Rating -4, tags: bankbot, banker. Package: 8361a7e40348329a39ba30c3234f1120a8e31ae0588126a72736ae0304. Date: Apr 13, 2017 4:20:54 AM - Android.
- Adobe (install.App.newu.system)**: Rating -4, tags: bankbot, banker. Package: 2f907c0069ad2f8a61171a209af00599a6c0f346c30149b94b2a52f943. Date: Apr 12, 2017 9:08:00 PM - Android.
- Funny Videos 2017 (neoidea.funvideos2017)**: Rating -4, tags: DexProtector, bankbot, banker. Package: 74ace3a2af372887852ddf099db153d986326d926c1bfa3f86219213dbb06a18. Date: Apr 12, 2017 4:59:11 PM - NEOIDEA LTD.
- System Files (com.example.livemusay.myapplication)**: Rating -4, tags: banker, bankbot. Package: c7b15c36ac4d49f0a7a61638a4e909f47fc1a3b806e7284390c336dba621e874. Date: Apr 12, 2017 11:45:00 AM - Kella.
- Funny Videos 2017 (neoidea.funvideos2017)**: Rating -4, tags: DexProtector, bankbot, banker. Package: ffd7960369814d5e0db844d5ed0f3b7e77ec7d9da4bd9e5843c5c9a3aa3b52ca. Date: Apr 12, 2017 3:33:29 AM - NEOIDEA LTD.
- Flash Player (turs.giveqwertyrh)**: Rating -4, tags: bankbot, banker. Package: 313c394c22054e702463c327642339f90a68543663c303039f5. Date: Apr 8, 2017 8:00:00 AM - Kira.
- Flash Player (xerigovno.exploit)**: Rating -4, tags: bankbot, banker. Package: 69498104c44022951b2896c1120c79046e12020a9f7000042. Date: Apr 8, 2017 8:00:00 AM - KIRASIRI201708.

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:

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

Some samples:

- [74ace3a2af372887852ddf099db153d986326d926c1bfa3f86219213dbb06a18](#)
- [2dfde3d394b7eaf3a45693dc95f9c5540c9fd2b3bc7e89e9ebc9d12963c00bee](#)