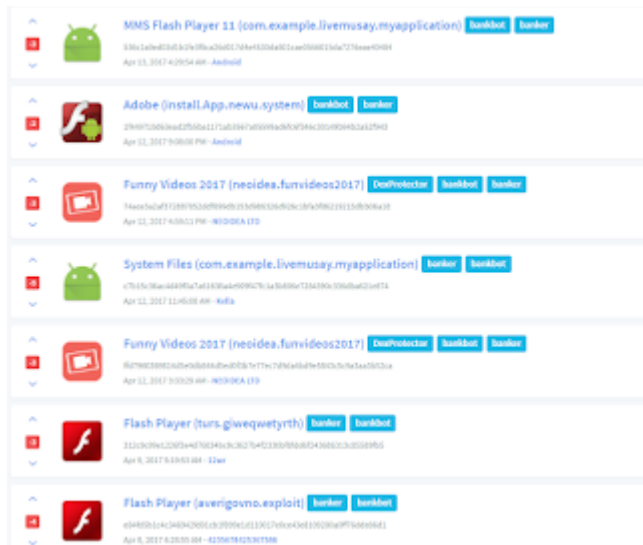


Decrypting Bankbot communications.

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 communications 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:

```

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 12 Apr 2017 21:46:51 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: PHP/5.4.16
Content-Length: 46513

ctagpyy kkk kay or kae yg kko yg kka kkr kat or yy kkk kkl kkt kkg yk kkk kkt kat eg ta ga yy kkk
kay or kae yg kko yg kka kkr kat or yy kkk kkl yk yk kka kag eg ta ga yy kkk kay or kkl kkk kll kat
kkr kko kkk kka or kat kkt yy kkk kkl eg ta ga yy kkk kay or kkt kkk kkl kkr kkr kay yy kko or kat
kkt yk yg kka kag yg kkt kat eg ta ga yy kkk kay or kkr kkr yk eg ta ga yy kkk kay or yg kag yk yg
kka kag or yg kka kka kkk kat kat kae or yg kkl kkl kkt or yg kag yk yg kka kag yt kae kat kko kkk
kag kkr or ta ga yy kkk kay or yg kag yk yg kka kag or kkt kkk kkl kkr kkr kkl eg ta ga yy kkk
kay or yg kag yk yg kka kag or yg kka kka kkk kat kae or yg kkl kkl kkt or yg kag yk yg kka kag
yt kae kat kko kag kat kkr yt kkr yg yk kkk kkk kkr eg ta ga yy kkk kay or kll kag yk or yg kka kka
kka kkt kat kae or kyy kkk yk kat kkk kkk kkk yk kll eg ta ga yy kkk kay or kat kat kka yg kka kkt yk
yg kka kag or kkk kka kkl yg kko yg eg ta ga yy kkk kay or kkr kay kkk yk kkr kkk yy kko or kae yg kag
kag yk yg kka kag eg ta ga yy kkk kll or kkr kll or kyy kkk yk kat kka kat kka or yg kka kka kko kkk kat
kae or kll kll kll kll or yy kkk kkl ye kkt kat kll kko kkk kay yk kkr kat kag eg ta ga yy kkk kay or
kll yk kag kat kll yk yg kka kag or kyy kkk yk kat kkk kkk eg ta ga yy kkk kay or kat kka kka yk
yg kka kag kkr kko or kat kka kka kkk yk kat kag eg ta ga yy kkk kay or kkr kay kkk yk or kaa kaa
kka kat kll yk yg kka kag eg ta ga kkr kko or yy kkk kay or kkt kag kag kkk kko yk kat kkk kat kkt
kat kay or kyy yk yg kka kag eg ta ga yy kkk kay or kll kat kko yg yk kkr or kll kat kka yg yk kkr
kay kkk yk kat kag eg ta ga yy kkk kay or kat kka kkr kkk kkr kkr kkr yk kae or kyy kkk yk kat kag
kag yk yg kka kag eg ta ga yy kkk kll kat kko or yy kkr kat kkk kko or yy kkr kat kkk kat kkr kll eg ta ga yy
kll kay or kag kag kkk kkk kll kkr kkr kkr kko kag or kyy kkk yk kat kkk kkk eg ta ga yy kkk kay or kyy
or kll kkr yg kko kat kka yg kka kll or kkr kay kkk yk or yg kka kka kkk kat kae or kll kat
kat kka yg kka kll kll kkr yk kkr kkk kkt eg ta ga yy kkk kay or kkr kkr yk kko kat kka yk kka
kll or kll kay kkk yk or yg kka kka kko kkk kat kae or kkt yk yg kka kag kat kka kae eg ta ga kaa
kag or kat kat kaa kkk yk kat yk or kkt kay yk kko kkr kll kaa kkk kka kkr or yg kka kka kkk
kat kae or yk yg kka kag kat kka kae or kll kko eg ta ga yy kkk kay or kaa yk or kay kay or kaa kaa

```

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

```

com.android.providers.calendar/com.android.providers.calendar.Calendar$1
com.android.providers.calendar/com.android.providers.calendar.Calendar$2
com.android.providers.calendar/com.android.providers.calendar.Calendar$3
com.android.providers.calendar/com.android.providers.calendar.Calendar$4
com.android.providers.calendar/com.android.providers.calendar.Calendar$5
com.android.providers.calendar/com.android.providers.calendar.Calendar$6
com.android.providers.calendar/com.android.providers.calendar.Calendar$7
com.android.providers.calendar/com.android.providers.calendar.Calendar$8
com.android.providers.calendar/com.android.providers.calendar.Calendar$9
com.android.providers.calendar/com.android.providers.calendar.Calendar$10
com.android.providers.calendar/com.android.providers.calendar.Calendar$11
com.android.providers.calendar/com.android.providers.calendar.Calendar$12
com.android.providers.calendar/com.android.providers.calendar.Calendar$13
com.android.providers.calendar/com.android.providers.calendar.Calendar$14
com.android.providers.calendar/com.android.providers.calendar.Calendar$15
com.android.providers.calendar/com.android.providers.calendar.Calendar$16
com.android.providers.calendar/com.android.providers.calendar.Calendar$17
com.android.providers.calendar/com.android.providers.calendar.Calendar$18
com.android.providers.calendar/com.android.providers.calendar.Calendar$19
com.android.providers.calendar/com.android.providers.calendar.Calendar$20
com.android.providers.calendar/com.android.providers.calendar.Calendar$21
com.android.providers.calendar/com.android.providers.calendar.Calendar$22
com.android.providers.calendar/com.android.providers.calendar.Calendar$23
com.android.providers.calendar/com.android.providers.calendar.Calendar$24
com.android.providers.calendar/com.android.providers.calendar.Calendar$25
com.android.providers.calendar/com.android.providers.calendar.Calendar$26
com.android.providers.calendar/com.android.providers.calendar.Calendar$27
com.android.providers.calendar/com.android.providers.calendar.Calendar$28
com.android.providers.calendar/com.android.providers.calendar.Calendar$29
com.android.providers.calendar/com.android.providers.calendar.Calendar$30
com.android.providers.calendar/com.android.providers.calendar.Calendar$31
com.android.providers.calendar/com.android.providers.calendar.Calendar$32
com.android.providers.calendar/com.android.providers.calendar.Calendar$33
com.android.providers.calendar/com.android.providers.calendar.Calendar$34
com.android.providers.calendar/com.android.providers.calendar.Calendar$35
com.android.providers.calendar/com.android.providers.calendar.Calendar$36
com.android.providers.calendar/com.android.providers.calendar.Calendar$37
com.android.providers.calendar/com.android.providers.calendar.Calendar$38
com.android.providers.calendar/com.android.providers.calendar.Calendar$39
com.android.providers.calendar/com.android.providers.calendar.Calendar$40
com.android.providers.calendar/com.android.providers.calendar.Calendar$41
com.android.providers.calendar/com.android.providers.calendar.Calendar$42
com.android.providers.calendar/com.android.providers.calendar.Calendar$43
com.android.providers.calendar/com.android.providers.calendar.Calendar$44
com.android.providers.calendar/com.android.providers.calendar.Calendar$45
com.android.providers.calendar/com.android.providers.calendar.Calendar$46
com.android.providers.calendar/com.android.providers.calendar.Calendar$47
com.android.providers.calendar/com.android.providers.calendar.Calendar$48
com.android.providers.calendar/com.android.providers.calendar.Calendar$49
com.android.providers.calendar/com.android.providers.calendar.Calendar$50
com.android.providers.calendar/com.android.providers.calendar.Calendar$51
com.android.providers.calendar/com.android.providers.calendar.Calendar$52
com.android.providers.calendar/com.android.providers.calendar.Calendar$53
com.android.providers.calendar/com.android.providers.calendar.Calendar$54
com.android.providers.calendar/com.android.providers.calendar.Calendar$55
com.android.providers.calendar/com.android.providers.calendar.Calendar$56
com.android.providers.calendar/com.android.providers.calendar.Calendar$57
com.android.providers.calendar/com.android.providers.calendar.Calendar$58
com.android.providers.calendar/com.android.providers.calendar.Calendar$59
com.android.providers.calendar/com.android.providers.calendar.Calendar$60
com.android.providers.calendar/com.android.providers.calendar.Calendar$61
com.android.providers.calendar/com.android.providers.calendar.Calendar$62
com.android.providers.calendar/com.android.providers.calendar.Calendar$63
com.android.providers.calendar/com.android.providers.calendar.Calendar$64
com.android.providers.calendar/com.android.providers.calendar.Calendar$65
com.android.providers.calendar/com.android.providers.calendar.Calendar$66
com.android.providers.calendar/com.android.providers.calendar.Calendar$67
com.android.providers.calendar/com.android.providers.calendar.Calendar$68
com.android.providers.calendar/com.android.providers.calendar.Calendar$69
com.android.providers.calendar/com.android.providers.calendar.Calendar$70
com.android.providers.calendar/com.android.providers.calendar.Calendar$71
com.android.providers.calendar/com.android.providers.calendar.Calendar$72
com.android.providers.calendar/com.android.providers.calendar.Calendar$73
com.android.providers.calendar/com.android.providers.calendar.Calendar$74
com.android.providers.calendar/com.android.providers.calendar.Calendar$75
com.android.providers.calendar/com.android.providers.calendar.Calendar$76
com.android.providers.calendar/com.android.providers.calendar.Calendar$77
com.android.providers.calendar/com.android.providers.calendar.Calendar$78
com.android.providers.calendar/com.android.providers.calendar.Calendar$79
com.android.providers.calendar/com.android.providers.calendar.Calendar$80
com.android.providers.calendar/com.android.providers.calendar.Calendar$81
com.android.providers.calendar/com.android.providers.calendar.Calendar$82
com.android.providers.calendar/com.android.providers.calendar.Calendar$83
com.android.providers.calendar/com.android.providers.calendar.Calendar$84
com.android.providers.calendar/com.android.providers.calendar.Calendar$85
com.android.providers.calendar/com.android.providers.calendar.Calendar$86
com.android.providers.calendar/com.android.providers.calendar.Calendar$87
com.android.providers.calendar/com.android.providers.calendar.Calendar$88
com.android.providers.calendar/com.android.providers.calendar.Calendar$89
com.android.providers.calendar/com.android.providers.calendar.Calendar$90
com.android.providers.calendar/com.android.providers.calendar.Calendar$91
com.android.providers.calendar/com.android.providers.calendar.Calendar$92
com.android.providers.calendar/com.android.providers.calendar.Calendar$93
com.android.providers.calendar/com.android.providers.calendar.Calendar$94
com.android.providers.calendar/com.android.providers.calendar.Calendar$95
com.android.providers.calendar/com.android.providers.calendar.Calendar$96
com.android.providers.calendar/com.android.providers.calendar.Calendar$97
com.android.providers.calendar/com.android.providers.calendar.Calendar$98
com.android.providers.calendar/com.android.providers.calendar.Calendar$99
com.android.providers.calendar/com.android.providers.calendar.Calendar$100

```

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>