# Botconf Lightning Talk on Qakbot

All research was performed together with João Gouveia (@jgouv).

It was performed using data from AnubisNetworks' Cyberfeed.

# Qakbot?

Looks over your shoulders when you do your online banking. Especially if you're in the US.

Had its 15 minutes of fame around 2011.

Became active again late in 2013.

# C&C protocol

`v=[VERSION]&c=[REQUEST]`

`[REQUEST]` is Base64-encoded information about machine.

# Protocol versions

Version 2: plaintext

Version 3,4,5: keysize|key|payload
uses XOR ‘encryption’

Version 8: random data

# Completely random?

No. There's a small bias in the $18^{th}$ byte.

# RC4

First 16 bytes likely used for the key. Any ideas?

# C&C protocol version 8