

A hands-on approach on *botnets* for a learning purpose

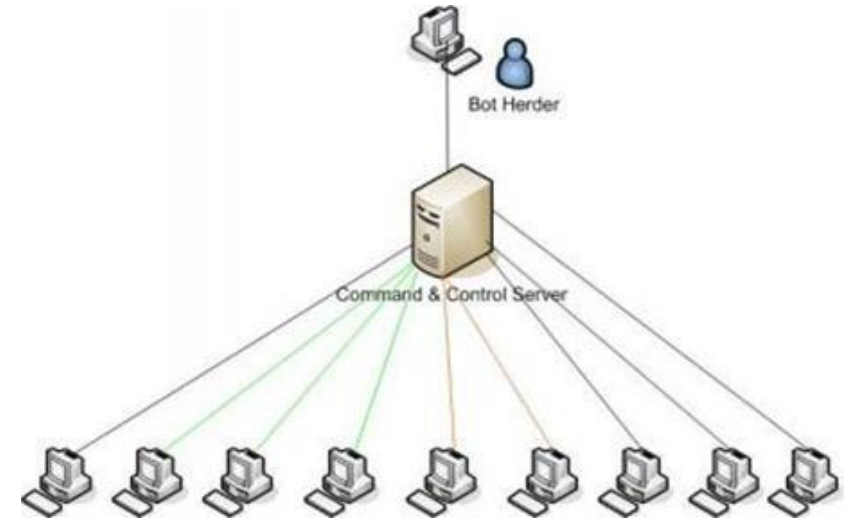
ØxO P O S E C Møetup

28/04/2016

Botnet

- A **botnet** is a number of Internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C) or by passing messages to one another.

In Wikipedia



What's the problem?

- There is a lack of a simple way to learn about botnets, what they are, how they work and what we can do about it.
- A safe and open-source experimental kit to analyze and modify the behavior of botnets. Built in an easy way.

What we built.

- Botnet *wiki*
 - A wiki with information regarding botnets, its anatomy, typical architecture and impact on the technological world.
- Botnet *lab*
 - A laboratory with a simple and open-source botnet kit with a set of built-in functionalities.
 - Easily expanded and modifiable.
 - Built for anyone who is interested in botnets and want to setup a laboratory at home and play with it.

Botnet lab - Technologies

- Python 2.7.3  python™

- IRC communication protocol



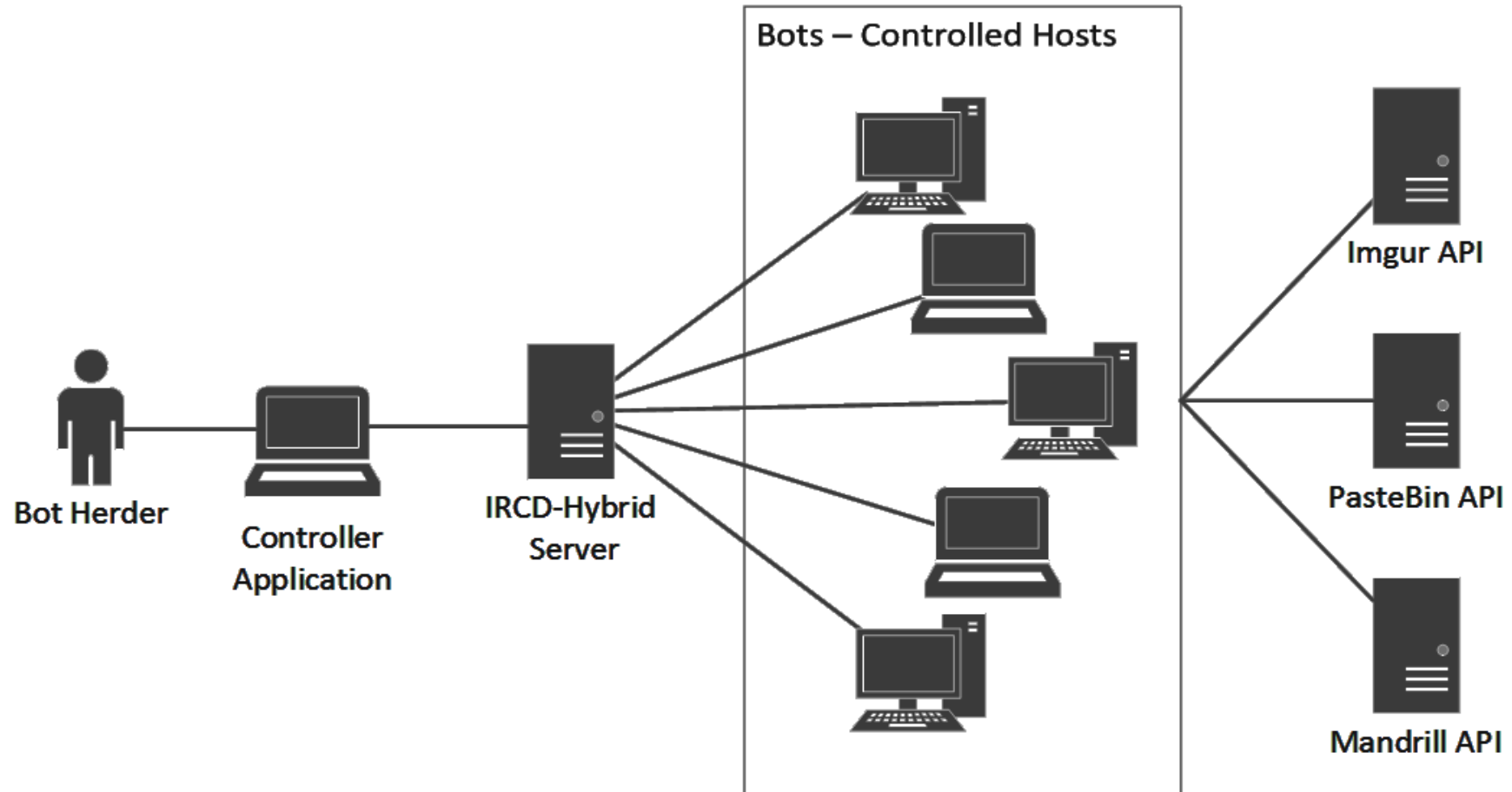
- Several external API's



imgur

freegeoip.net

Botnet lab - Architecture




Demo

- **Riley's Rule of Software Demonstrations**
- The probability of failure of a software demonstration is directly proportional to the product of the number of people attending and the importance of the demo.

Team

- João Pedro Dias
 - <http://jpdias.me/>
 - <http://twitter.com/jpd1as/>
- José Pedro Pinto
 - <http://josepinto.me/>
 - <http://twitter.com/jppint0/>

- GitHub repo: 
 - <https://github.com/jpdias/botnet-lab>
- Documentation:
 - <http://jpdias.me/botnet-lab/>

