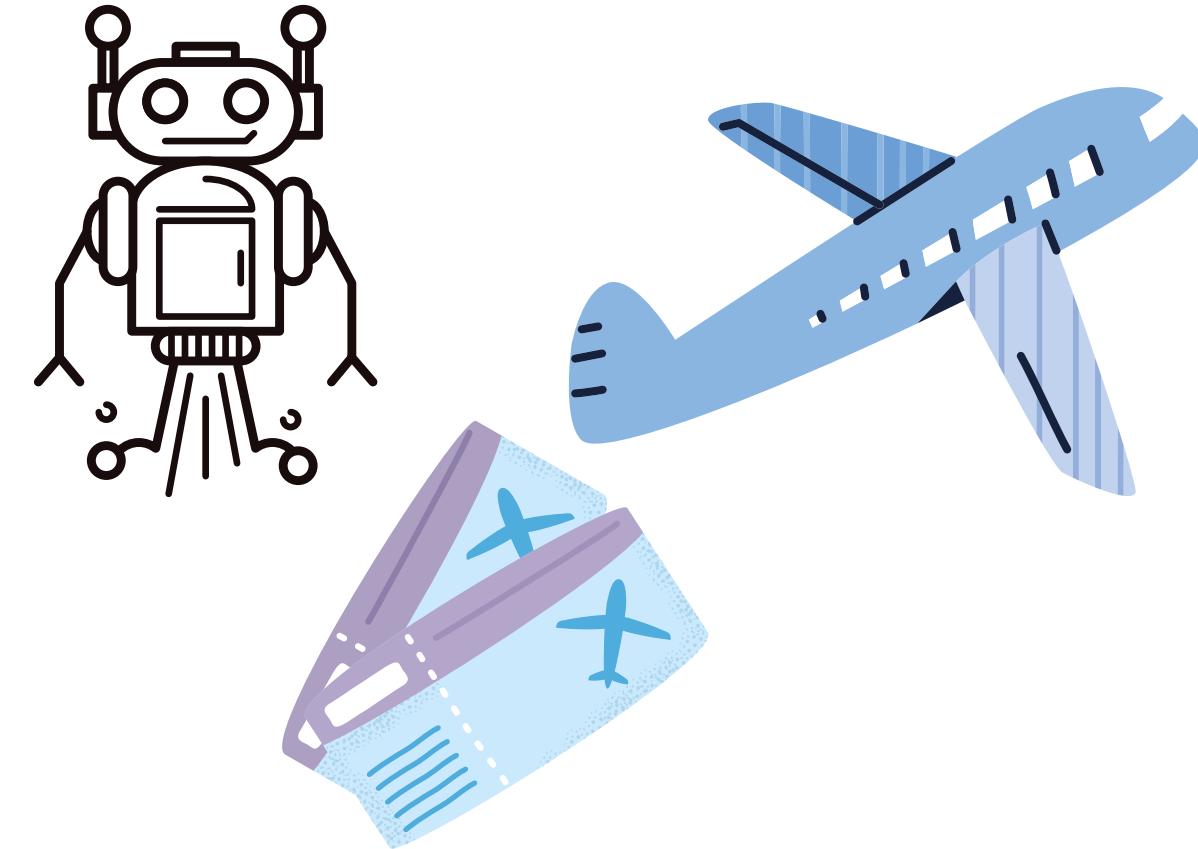


# Botnet ecosystems and airlines websites

PhD student: Elisa Chiapponi

EURECOM Supervisor: Prof. Marc Dacier

Project in collaboration with Amadeus IT Group



# Amadeus IT Group

▲ IT provider for the travel industry



# Amadeus IT Group

- ▲ IT provider for the travel industry
- ▲ Fares calculation and booking engines for airlines

# Amadeus IT Group

- ▲ IT provider for the travel industry
- ▲ Fares calculation and booking engines for airlines
  - ▲ Different booking solutions

# Amadeus IT Group

- ▲ IT provider for the travel industry
- ▲ Fares calculation and booking engines for airlines
  - ▲ Different booking solutions
  - ▲ Huge number of processed requests

# Amadeus IT Group

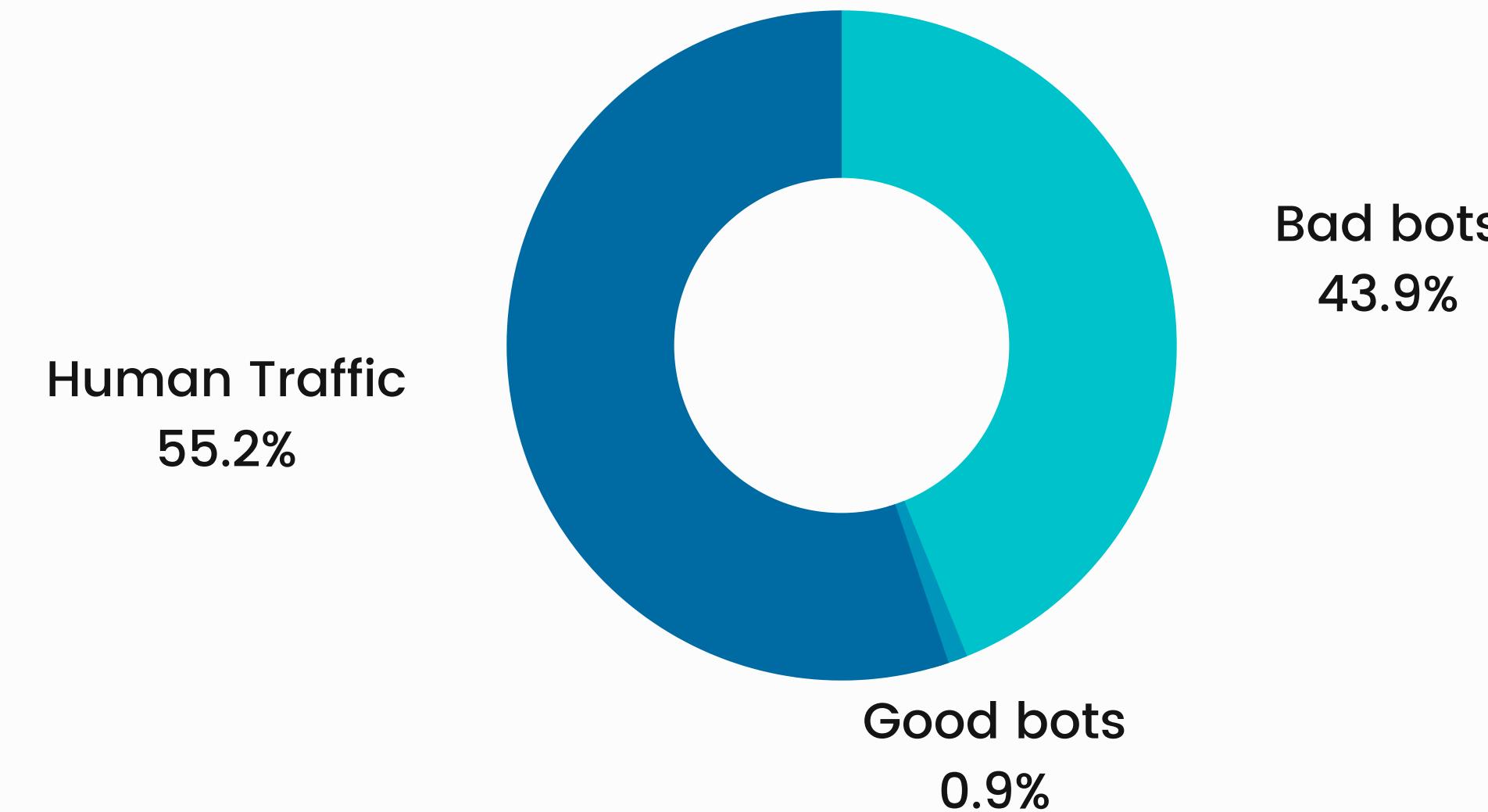
- ▲ IT provider for the travel industry
- ▲ Fares calculation and booking engines for airlines
  - ▲ Different booking solutions
  - ▲ Huge number of processed requests
    - ▲ Medium size airline, 1 million requests per day (2019)

# Amadeus IT Group

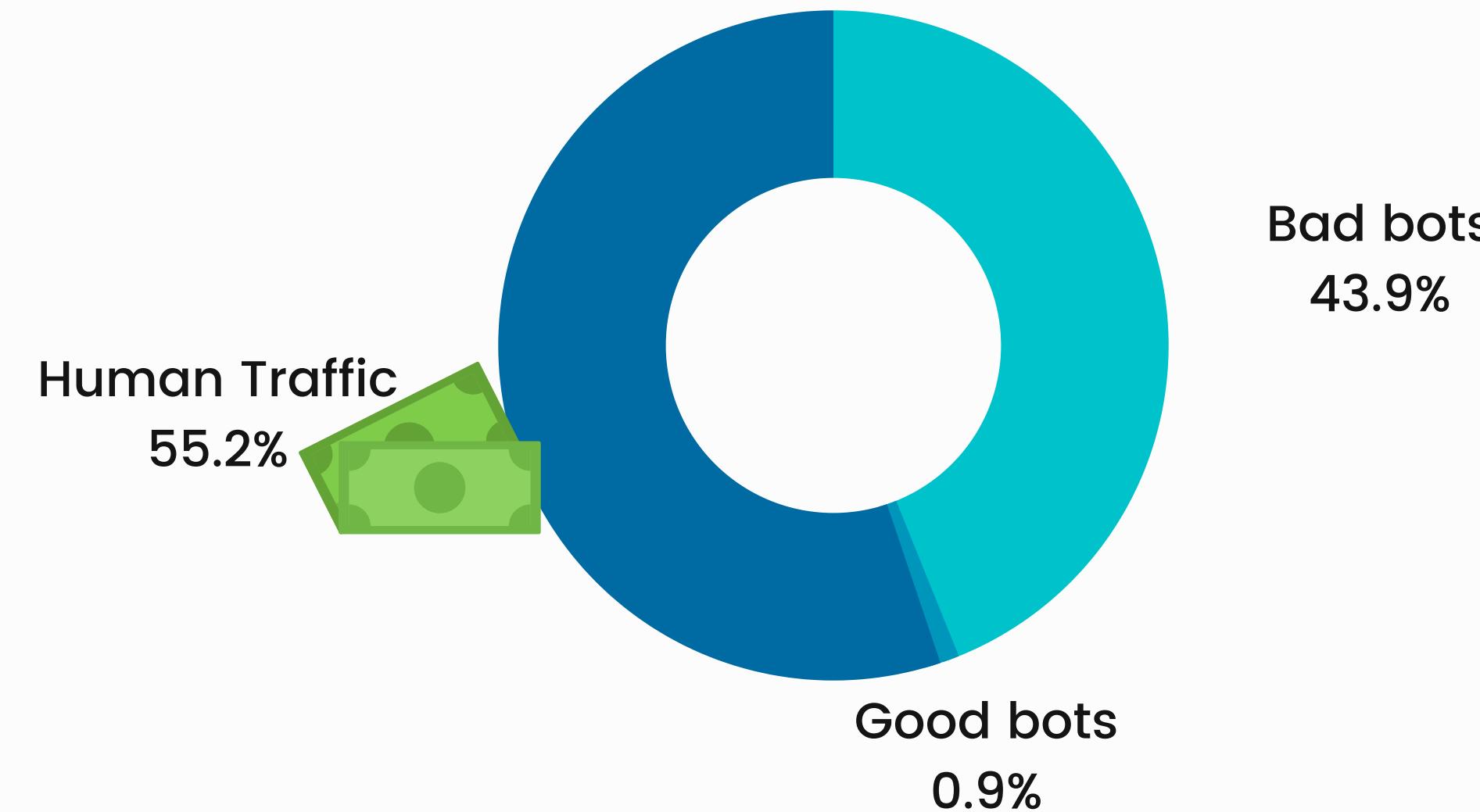
- ▲ IT provider for the travel industry
- ▲ Fares calculation and booking engines for airlines
  - ▲ Different booking solutions
  - ▲ Huge number of processed requests
    - ▲ Medium size airline, 1 million requests per day (2019)
    - ▲ 1,994,000 passengers borded in 2019

# Scraping bots and airlines

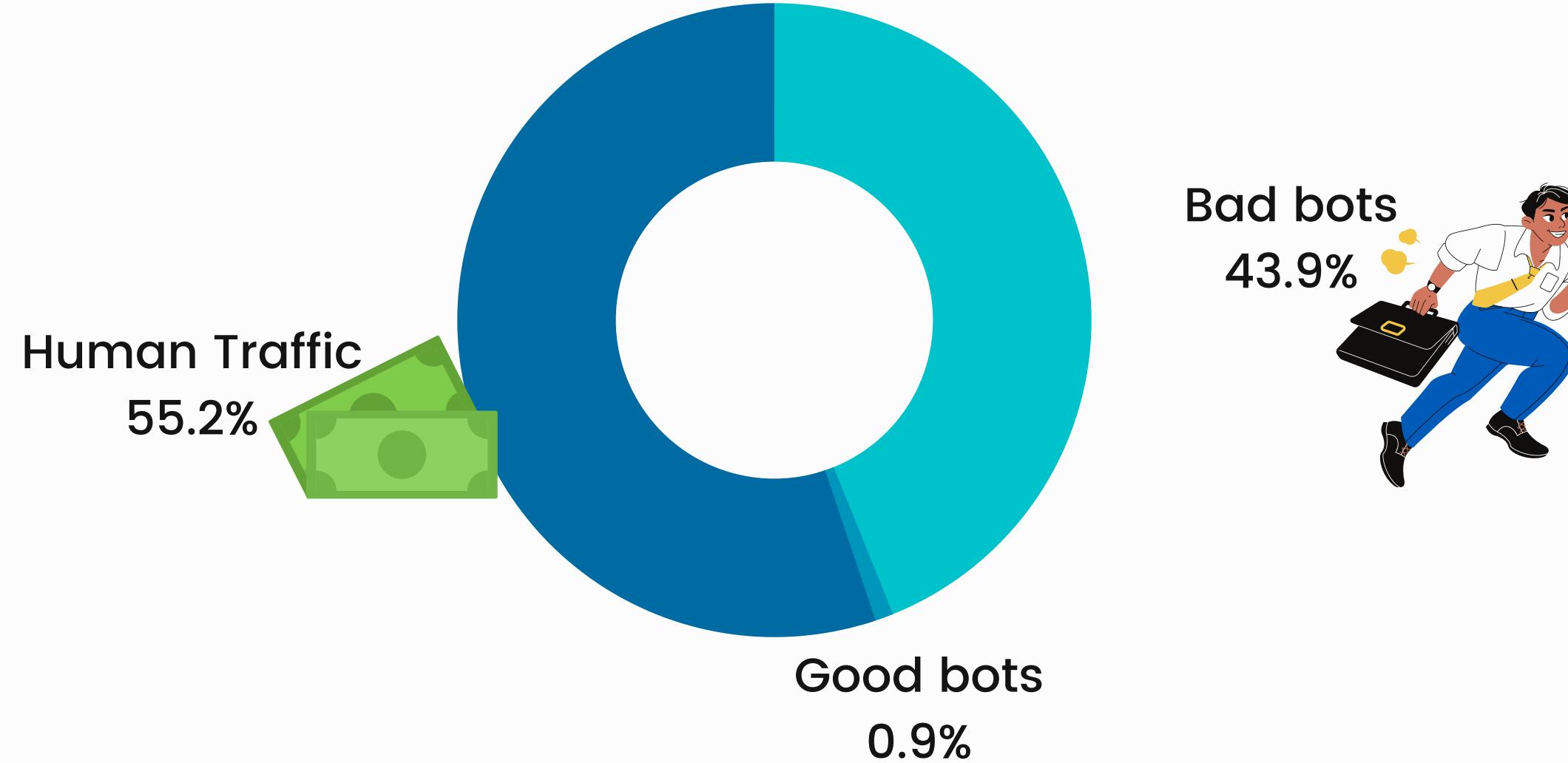
Scraping bot traffic analysis



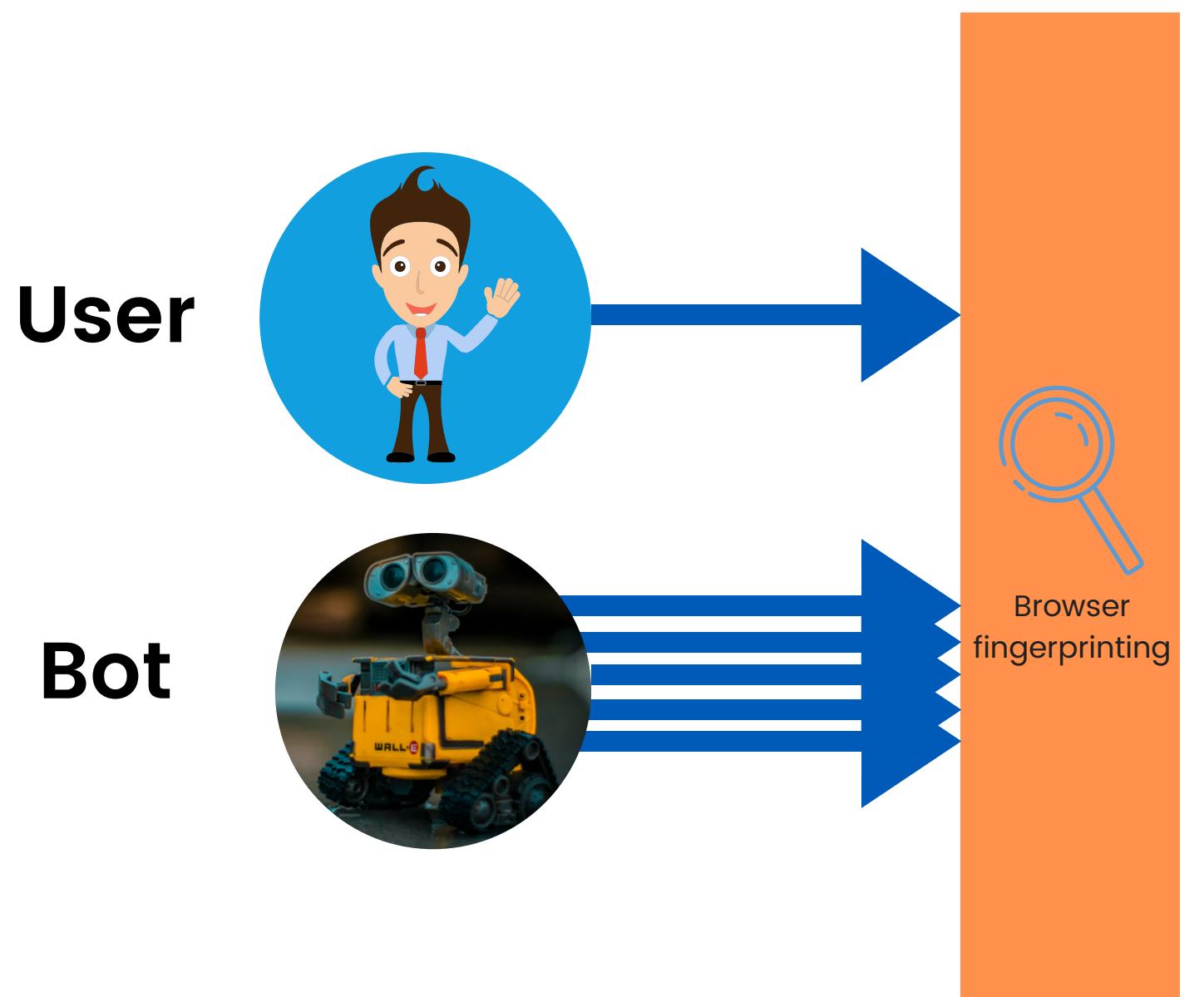
# Scraping bots and airlines



# Scraping bots and airlines

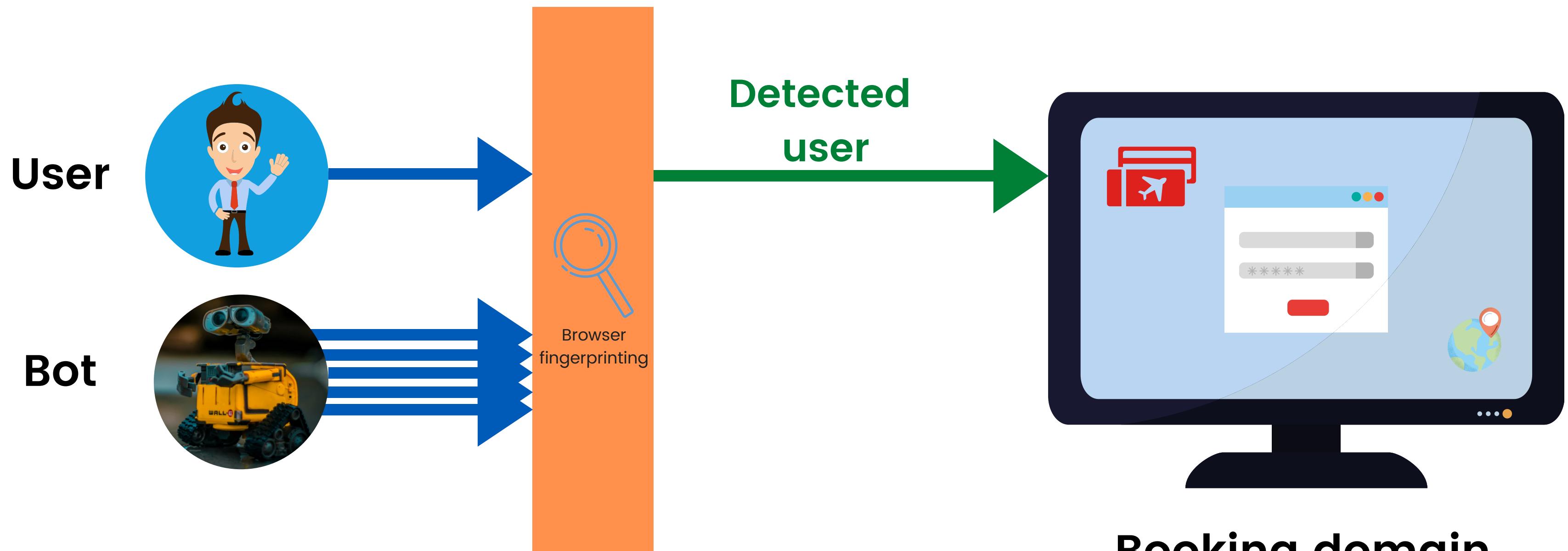


# Anti-bot solutions

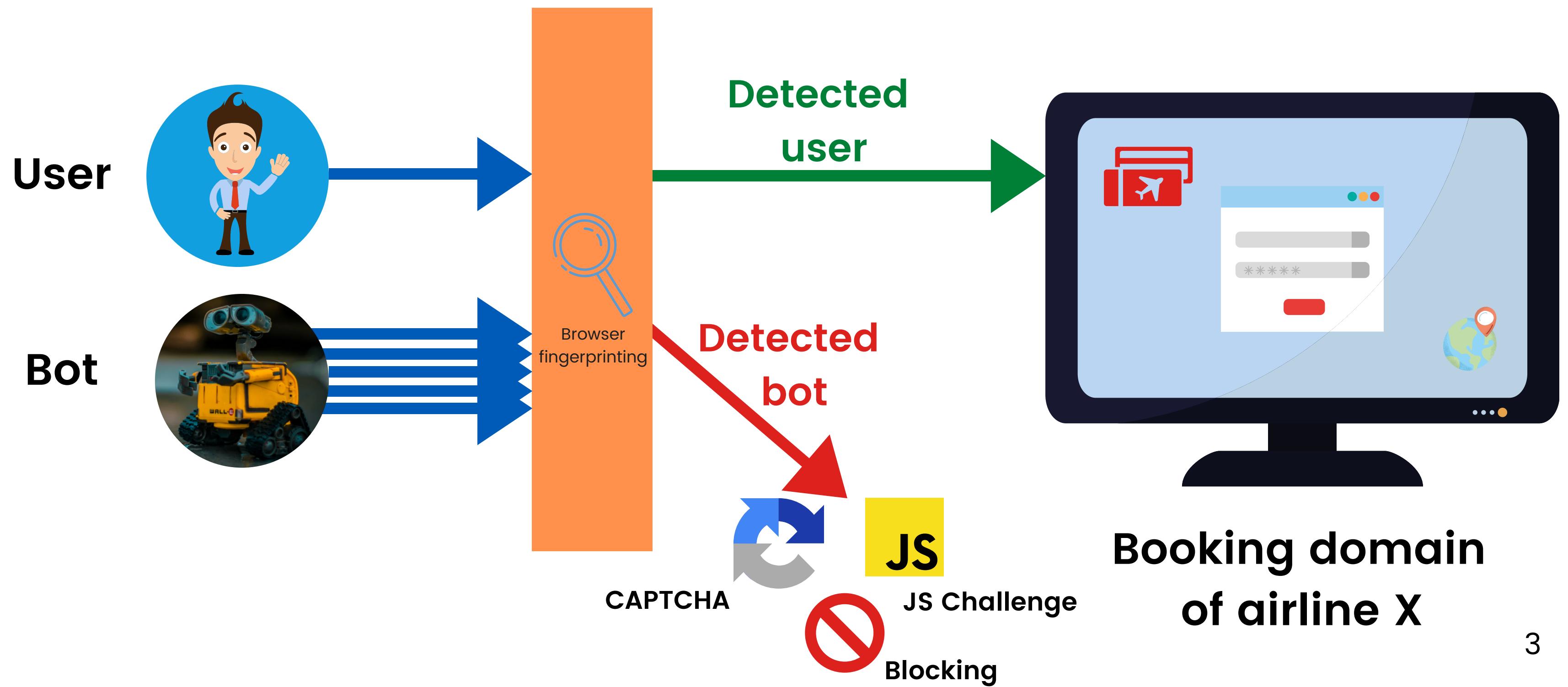


**Booking domain  
of airline X**

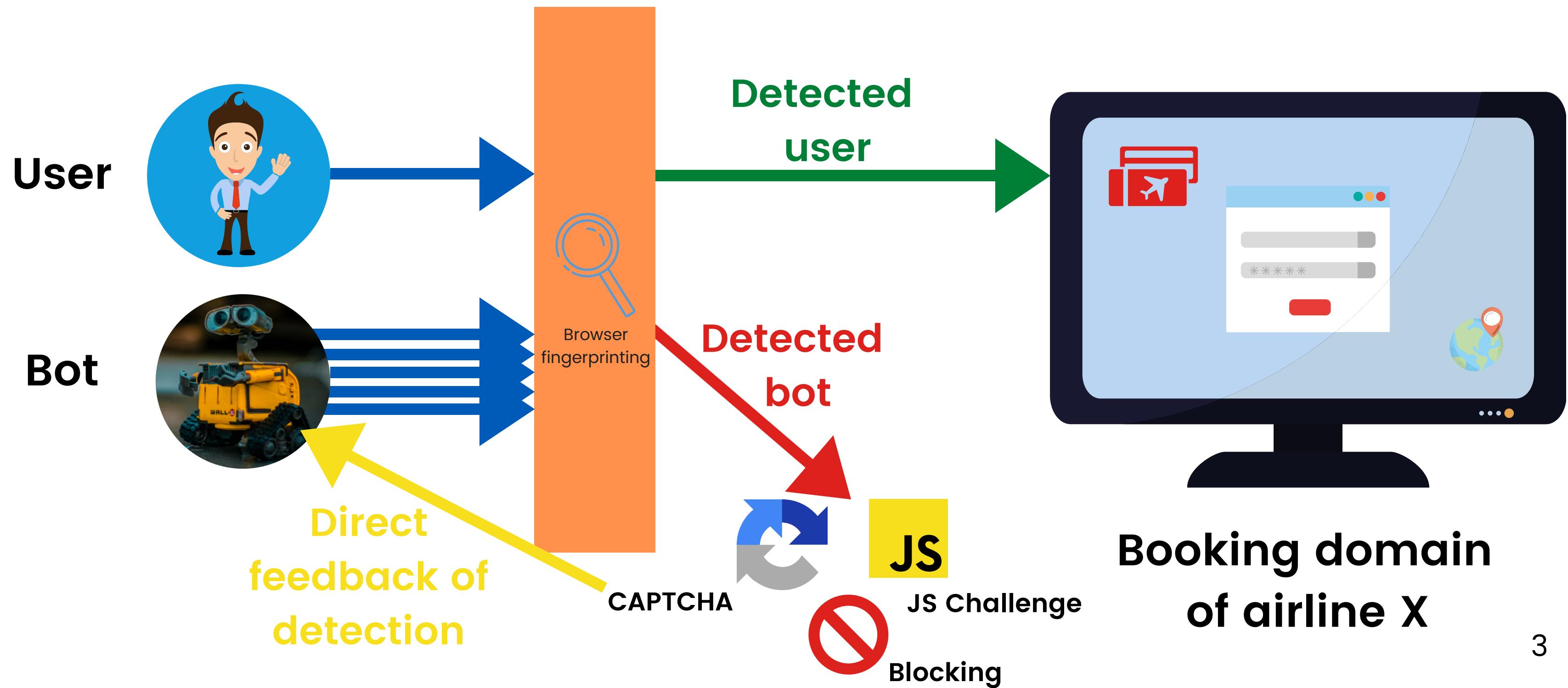
# Anti-bot solutions



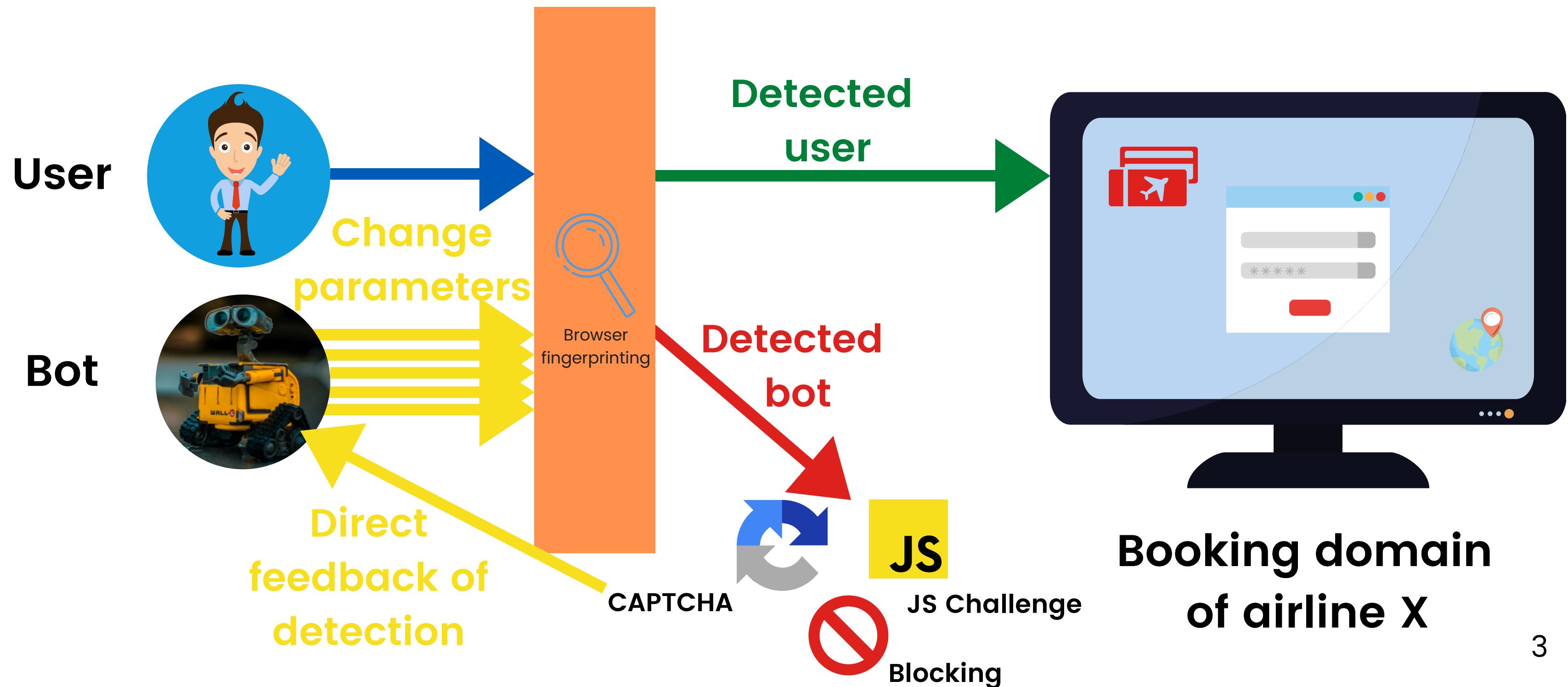
# Anti-bot solutions



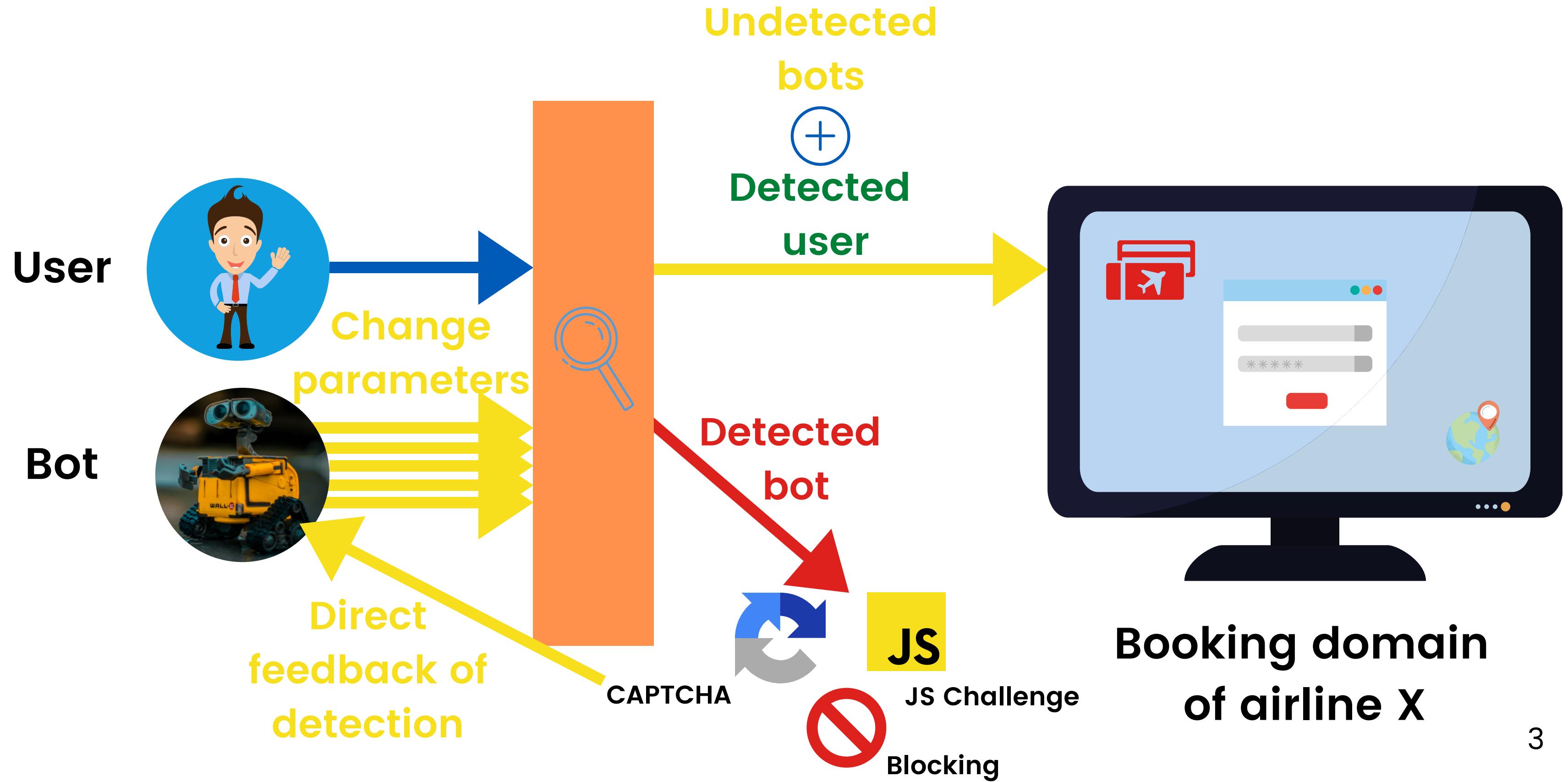
# Anti-bot solutions



# Anti-bot solutions



# Anti-bot solutions



# What do we **want** to do?

Understanding the bots business model and invariants in their requests to make it more difficult to evade detection

# What have you **done** so far



Honeypot

# What have you **done** so far



Lure attackers



Honeypot

# What have you **done** so far

Lure attackers

Study behavioral patterns



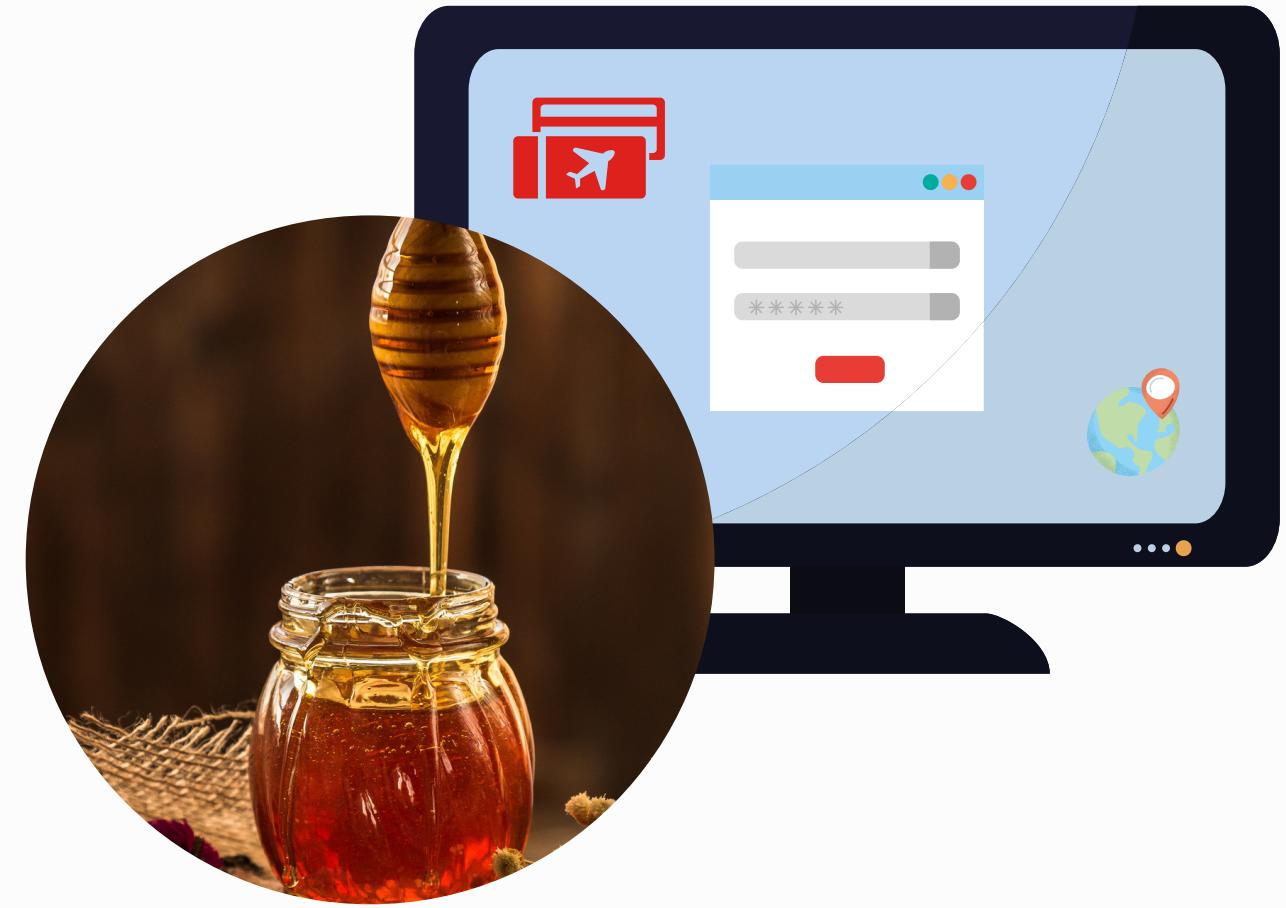
Honeypot

# What have you **done** so far

 Lure attackers

 Study behavioral patterns

 Statistics on IP addresses



Honeypot

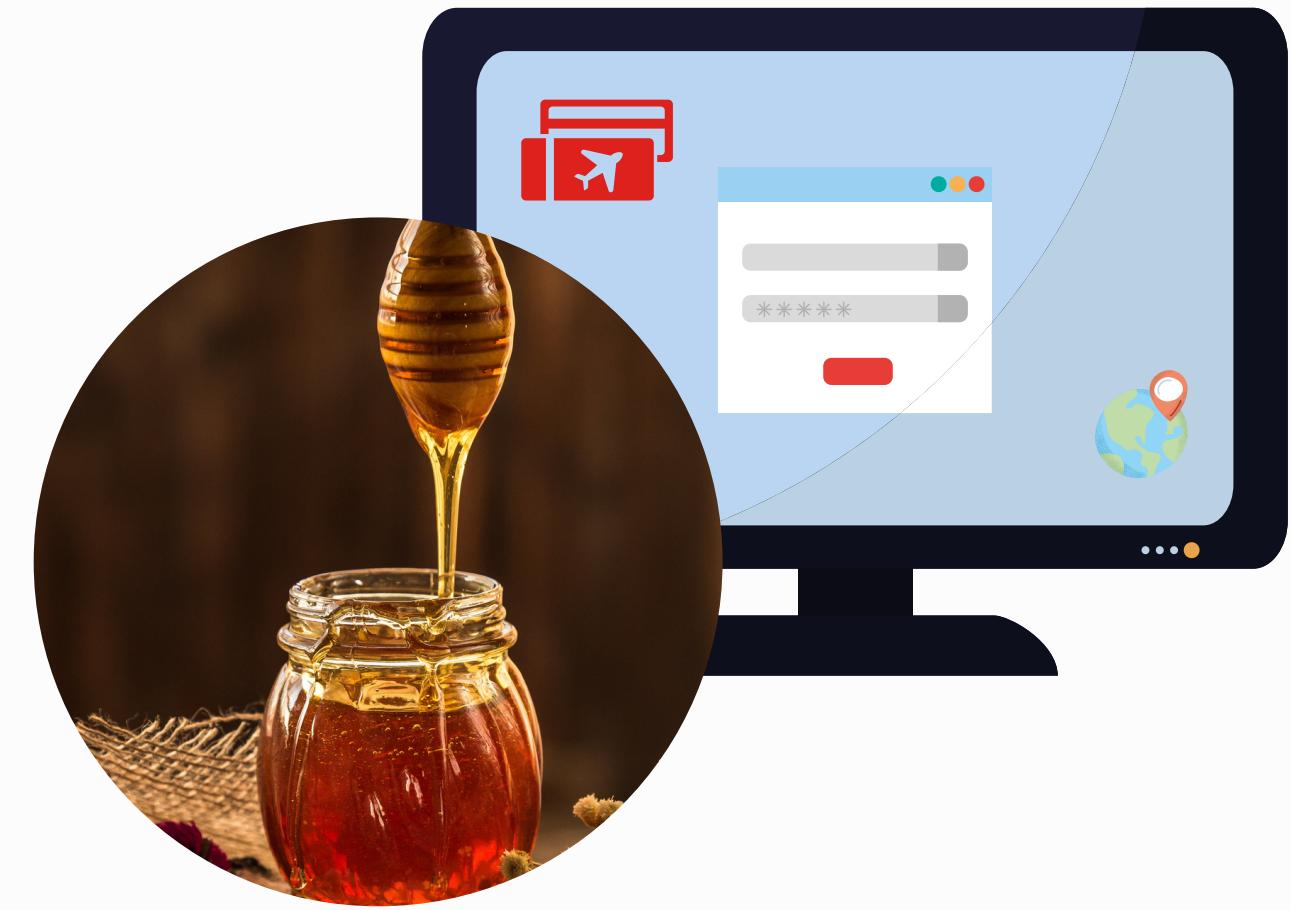
# What have you **done** so far

Lure attackers

Study behavioral patterns

Statistics on IP addresses

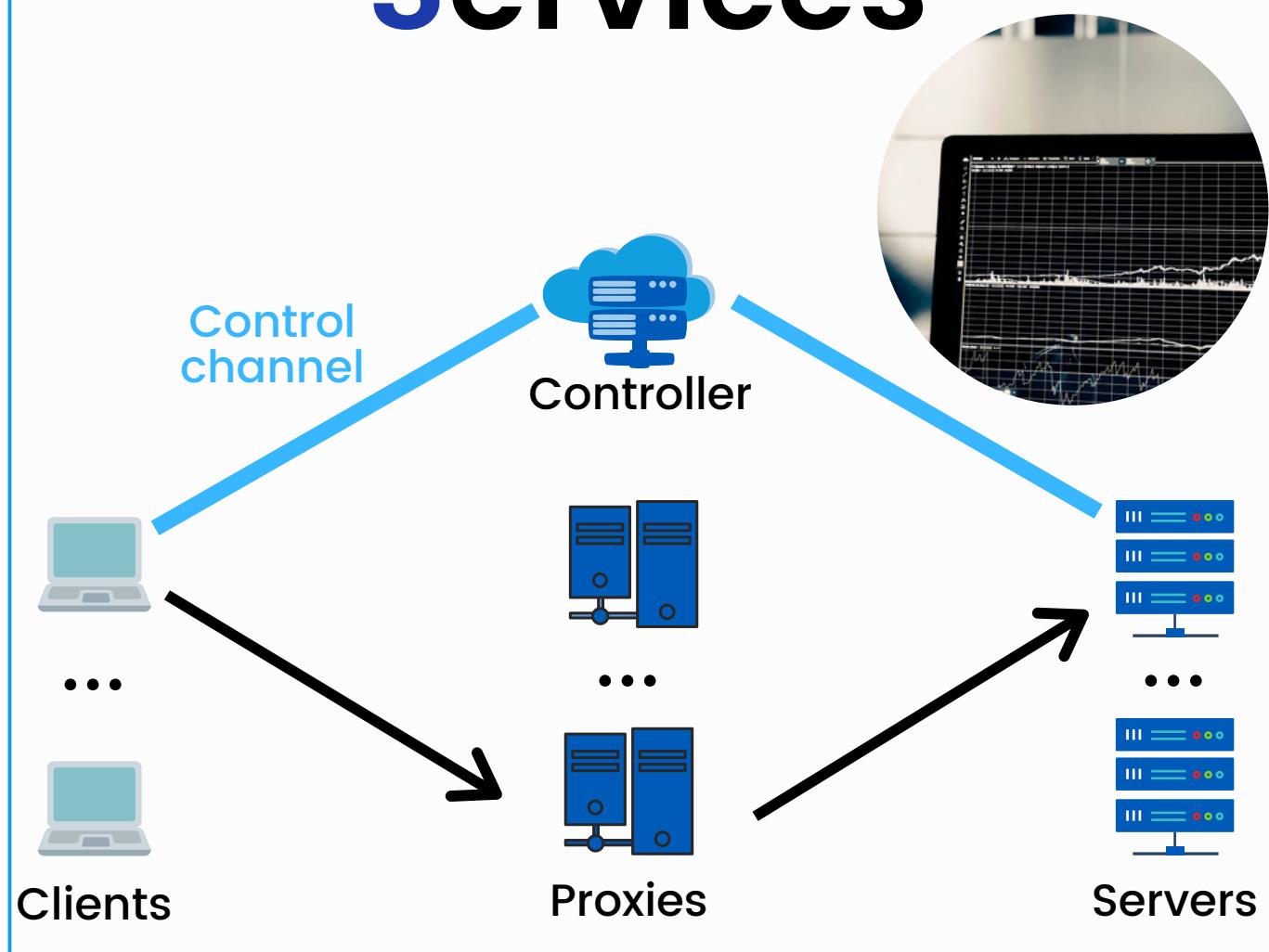
Modeling of IP picking process



Honeypot

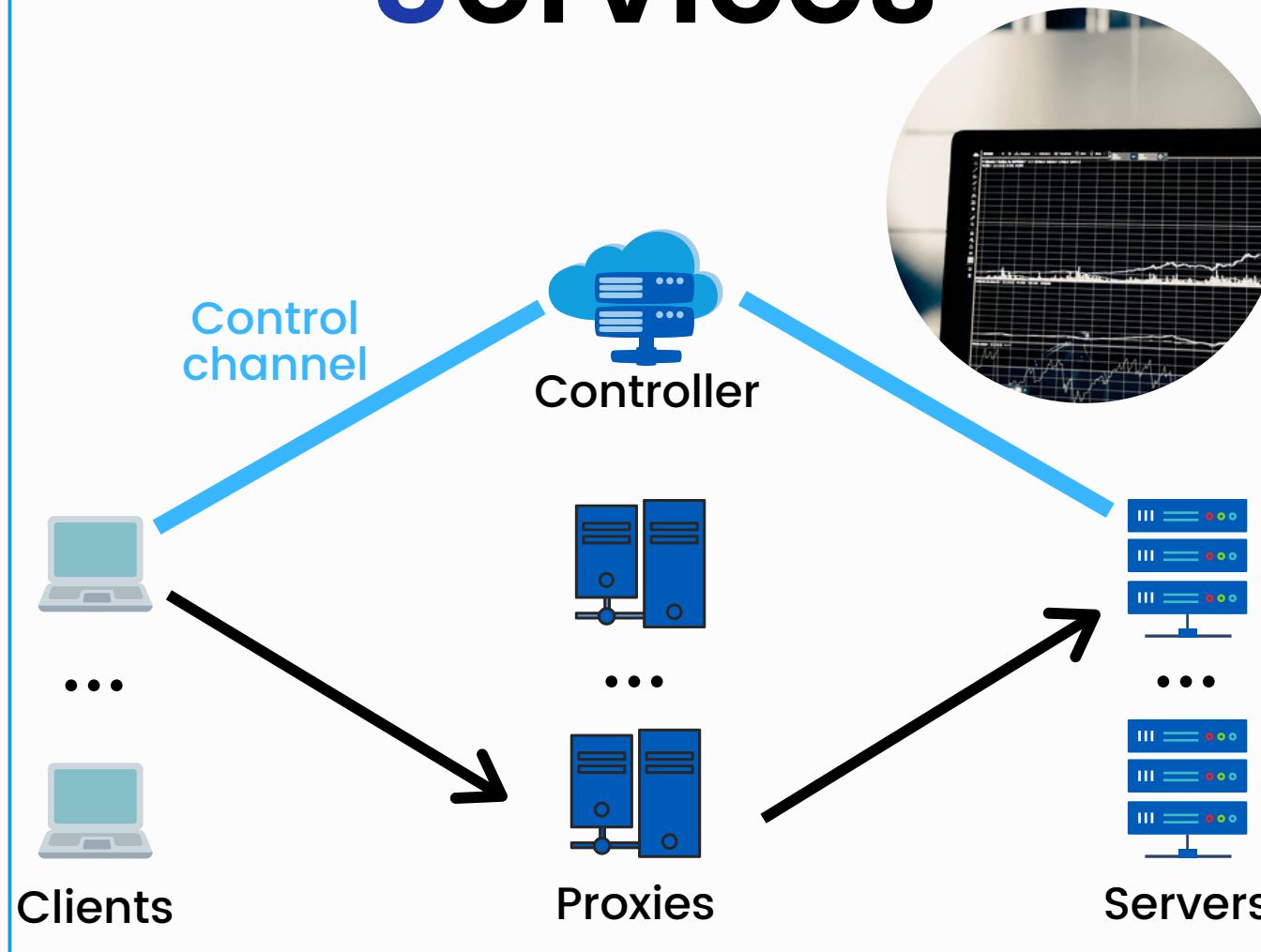
# Next steps

**BAD PASS: Bots  
taking ADvantage  
of Proxy AS a  
Services**



# Next steps

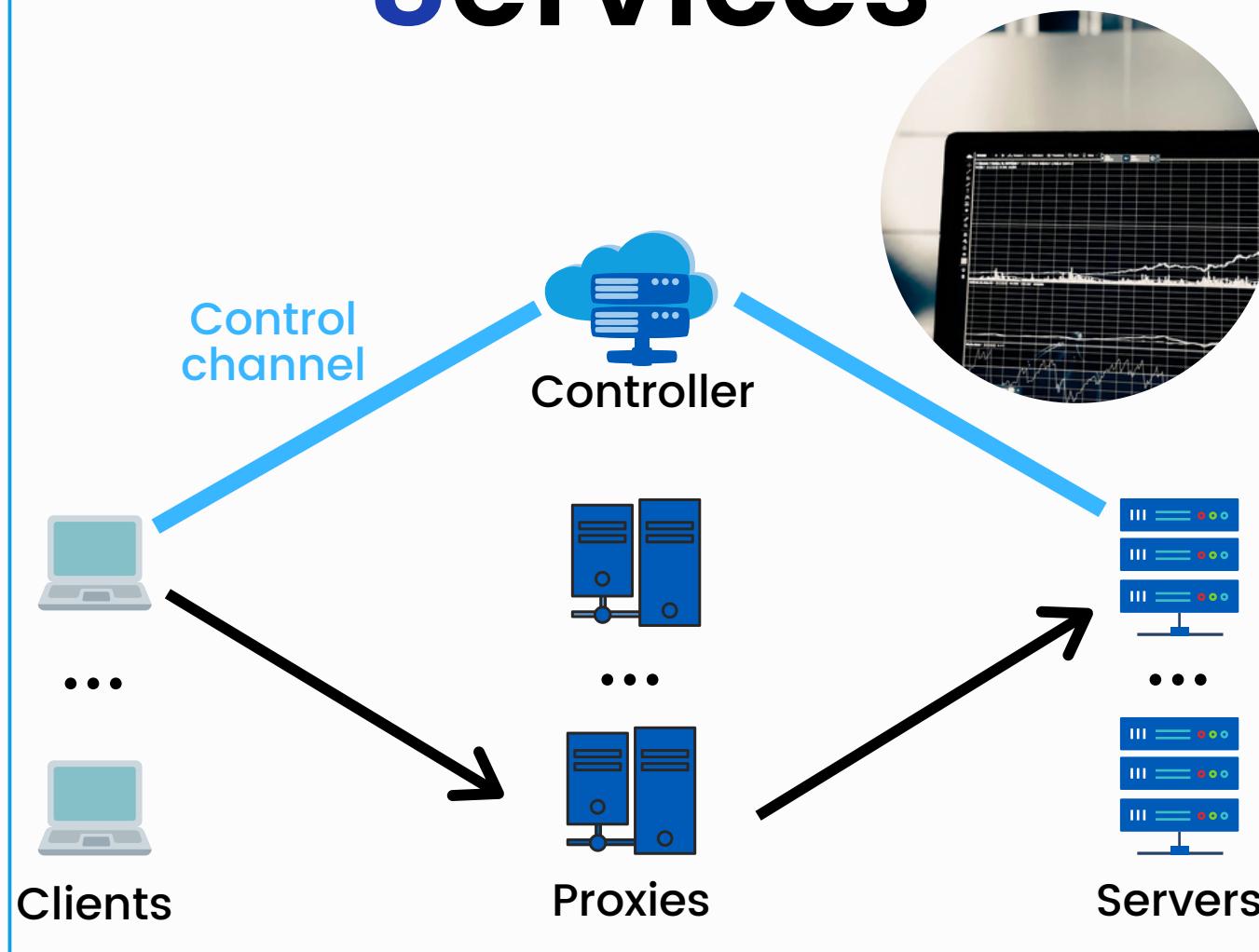
## BAD PASS: Bots taking ADvantage of Proxy AS a Services



- IPs at Proxy Services disposal
- Availability factor
- Geo-localization

# Next steps

## BAD PASS: Bots taking ADvantage of Proxy AS a Services



- IPs at Proxy Services disposal
  - Availability factor
  - Geo-localization
- 
- Proxy changes in the requests

# Thank You

## **Our works:**

- Chiapponi, E., Catakoglu, O., Thonnard, O., Dacier, M.: HoPLA: a Honeypot Platform to Lure Attackers. In: C&ESAR 2020, Computer & Electronics Security Applications Rendez-vous, Deceptive security Conference, part of European Cyber Week. Rennes, France (2020)
- Chiapponi, E., Dacier, M., Todisco, M., Catakoglu, O., Thonnard, O., : Botnet sizes: when maths meet myths. In: CFTIC 2020, 1st International Workshop on Cyber Forensics and Threat INvestigations Challenges in Emerging Infrastructures, held in conjunction with the 18th International Conference on Service Oriented Computing (ICSOC 2020), 14-17 December 2020, Dubai, UAE (virtual Conference) / Also to be published in Lecture Notes in Computer Science (LNCS)