CONFIDENTIAL & RESTRICTED

Web Bots: A Growing Threat to Your Business

How to Protect Your Organization's Digital Assets

Elisa Chiapponi
elisa.chiapponi@amadeus.com

Azur Tech Summer 2025

Sophia Antipolis, France

3rd July 2025

amadeus
Global Security Operations

Who am I

- Security Researcher in the **Global Security Operations** of Amadeus
  - Protection of web domains linked to the travel industry
- Expertise in **Network** and **Application** Security
- Work based on current and Ph.D. research and collaborations

amadeus
Global Security Operations

RESCUE – Resilient Cloud for Europe
IPCEI – Germany
Amadeus Germany GmbH

Funded by the European Union NextGenerationEU

Supported by: Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag

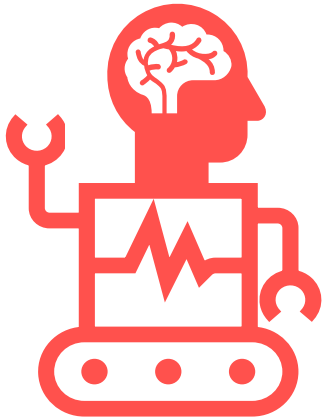
EURECOM Sophia Antipolis

SORBONNE UNIVERSITÉ

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Resilient Computing and Cybersecurity Center

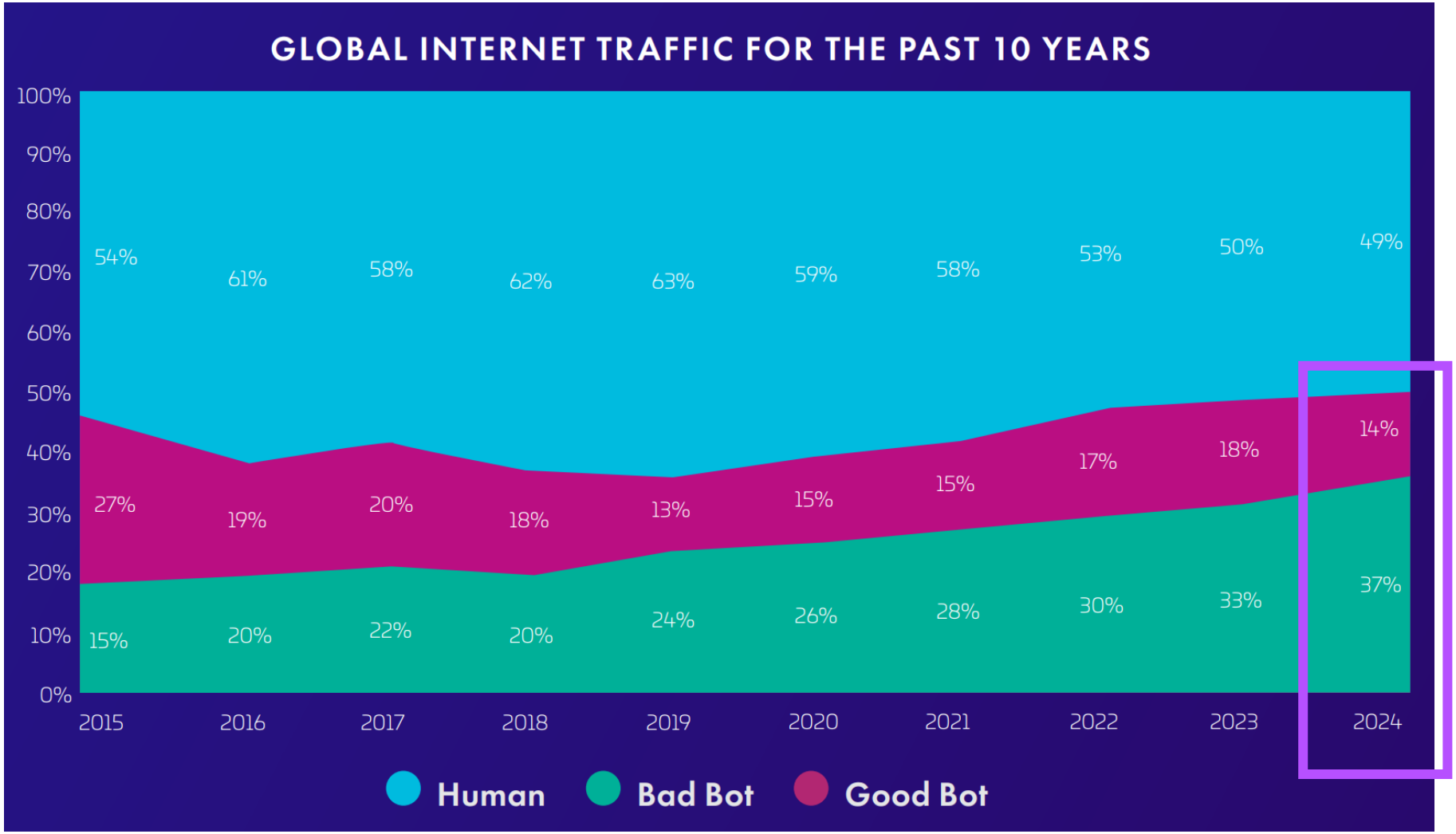
© Amadeus IT Group and its affiliates and subsidiaries



Sophisticated bots

Mimic of **human interaction** to reach their goals

© Amadeus IT Group and its affiliates and subsidiaries



51% of traffic was robotic in 2024

© Amadeus IT Group and its affiliates and subsidiaries

amadeus [1] Imperva a Thales company, “Bad Bot Report: The Rapid Rise of Bots and the Unseen Risk for Business”, 2025

Today it’s easier to have access to bots…

GenAI helps evading anti-bot protection [1]

You

could you create in python a bot that enters in a website and clicks on a button called submit simulating human-like mouse movements?

Copilot

Absolutely! Here’s a Python script that uses Selenium and `pyautogui` to simulate human-like mouse movements and click on a button called “submit”:

1. **Install the necessary libraries**:

```
pip install pyautogui
pip install selenium
```

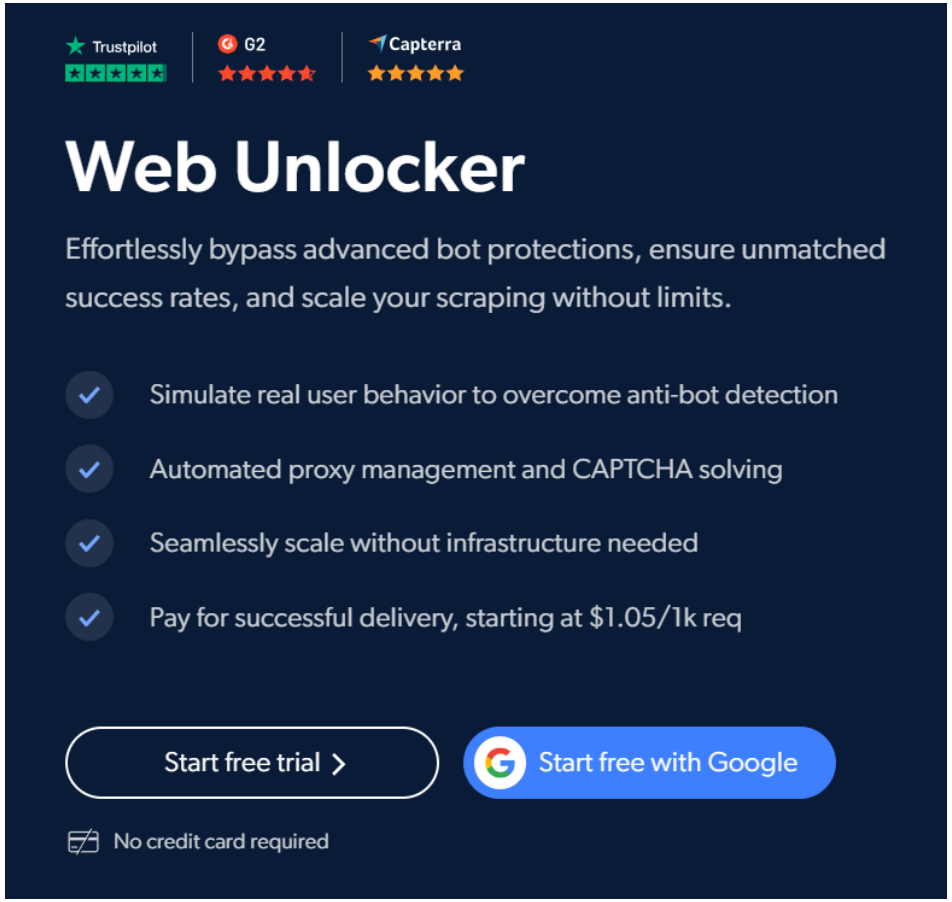
2. **Write the script**:

Python

```python
import pyautogui
import time
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC

# Set up the Selenium WebDriver
driver = webdriver.Chrome()  # Make sure you have the ChromeDriver installed
driver.get('http://example.com')  # Replace with your target website

# Wait for the submit button to be clickable
```



All-in-one solutions for not experienced users

© Amadeus IT Group and its affiliates and subsidiaries

[1] Imperva a Thales company, “Bad Bot Report: The Rapid Rise of Bots and the Unseen Risk for Business”, 2025

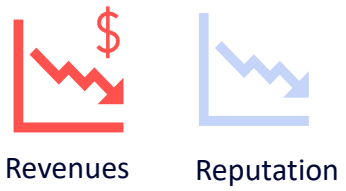
Sophisticated Bot Attacks – Functional Abuse

Denial Of Inventory

- Disrupt supply and demand
- Impact revenues and operations
- Defeat the competition
- Holding cheapest fares

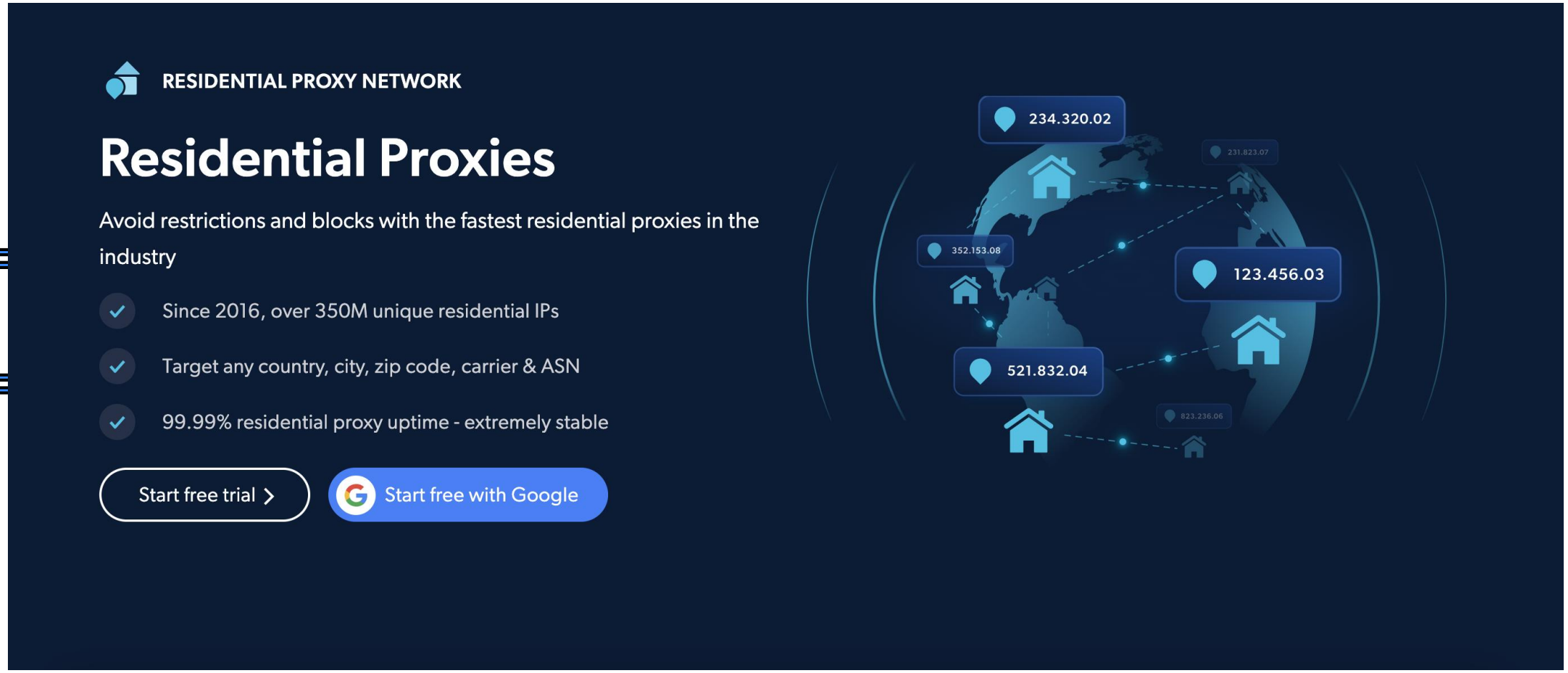
SMS Pumping

- Impact revenues
- Generate revenue through network operators



© Amadeus IT Group and its affiliates and subsidiaries

Arms race



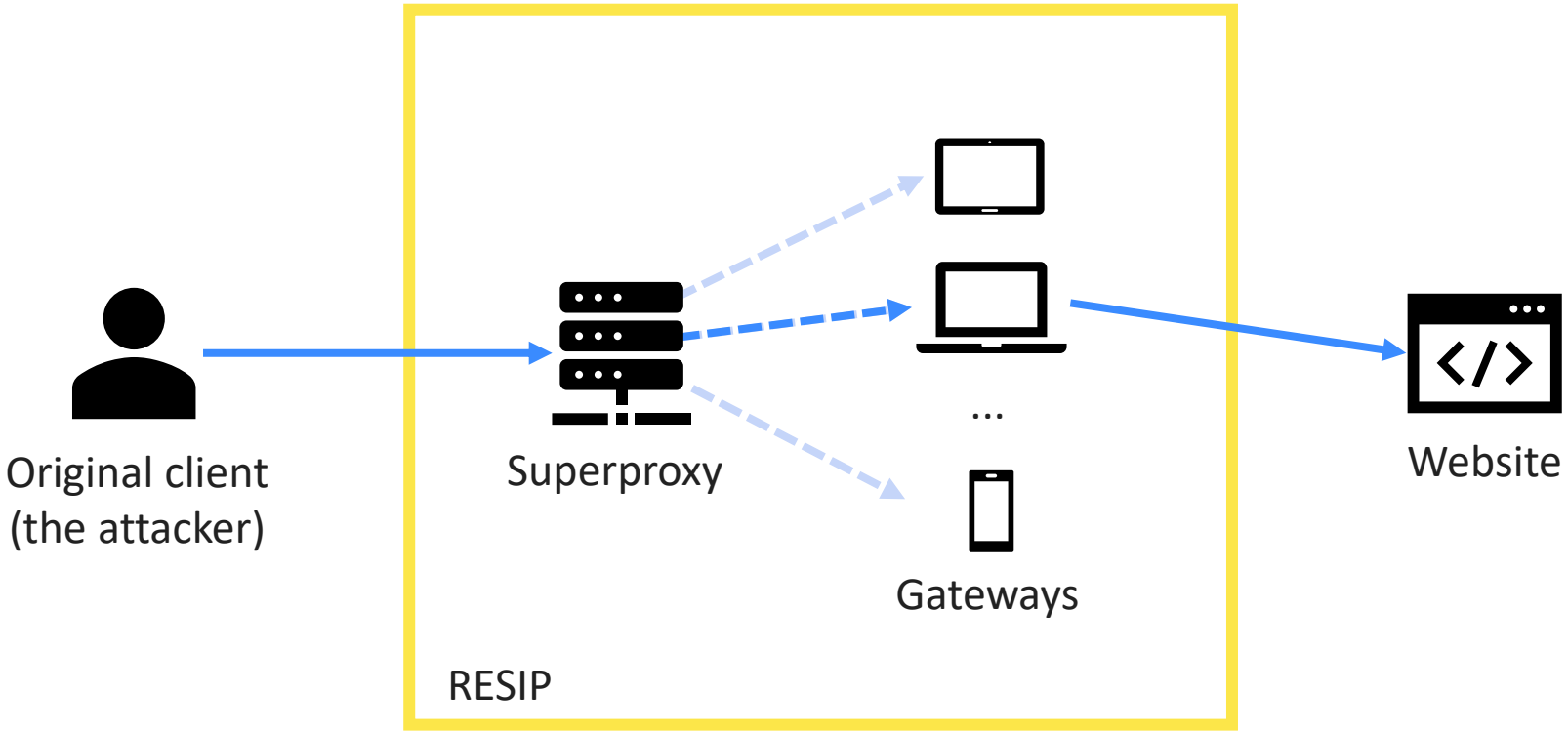
© Amadeus IT Group and its affiliates and subsidiaries

Residential IP Proxies (RESIPs)

- Large networks of **residential devices** (smartphones, laptops, tablets,…)
- Devices **owned** by genuine users who **share** their usage
- No application layer information about being proxied
  - **Indistinguishable** from the requests sent directly by the residential devices at this layer
  - **High probability of false positives** for the traditional server-side bot detection techniques
- Advanced bot traffic **heavily rely** on RESIPs

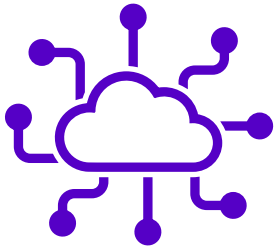
© Amadeus IT Group and its affiliates and subsidiaries

RESIP infrastructure



© Amadeus IT Group and its affiliates and subsidiaries

Advantages for the attacker



Tens of millions of residential IPs

No private distributed infrastructure

Not only malicious reputation IPs

No direct traceability

© Amadeus IT Group and its affiliates and subsidiaries

Recruitment process

Free services (e.g. VPN)

Bandwidth payment

Mobile SDKs included by app developers

Infected devices (IoT)

[2] M. Frappier et al., Illegitimate residential proxy services: the case of 911.re and its IOCs, 2022.
[3] X. Mi et al., “Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks,” in NDSS 2021.
[4] A. Vastel. “Ever wonder how proxy providers & BaaS providers obtain residential proxies?”, 2022.

© Amadeus IT Group and its affiliates and subsidiaries

Legitimate but…

- **Shady** Device Recruitment

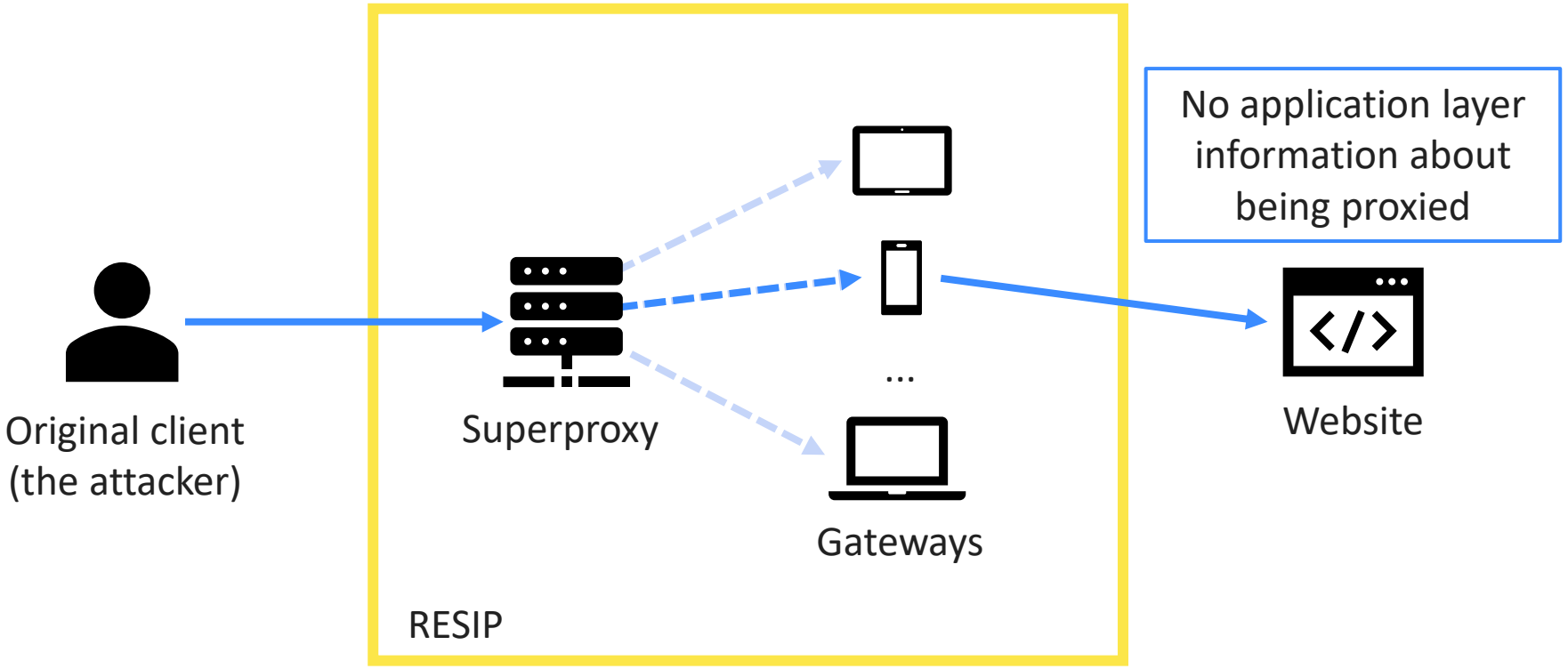
- Research works **showed** involvement in:
  - Credential and stuffing attacks
  - Cryptojacking
  - Financial Scams
  - …

- **More expensive** than common VPNs
  - 7$/GB vs 6$/month unlimited traffic

[2] M. Frappier et al., Illegitimate residential proxy services: the case of 911.re and its IOCs, 2022.
[5] B. Krebs, The Rise of “Bulletproof” Residential Networks, 2019.
[6] X. Mi et al. Resident Evil: Understanding Residential IP Proxy as a Dark Service, IEEE S&P 2019.
[7] M. Yang et al., An Extensive Study of Residential Proxies in China. ACM SIGSAC CCS 2022.
[8] E. Khan et al. A First Look at User-Installed Residential Proxies From a Network Operator's Perspective, CNSM 2024

© Amadeus IT Group and its affiliates and subsidiaries

RESIP infrastructure

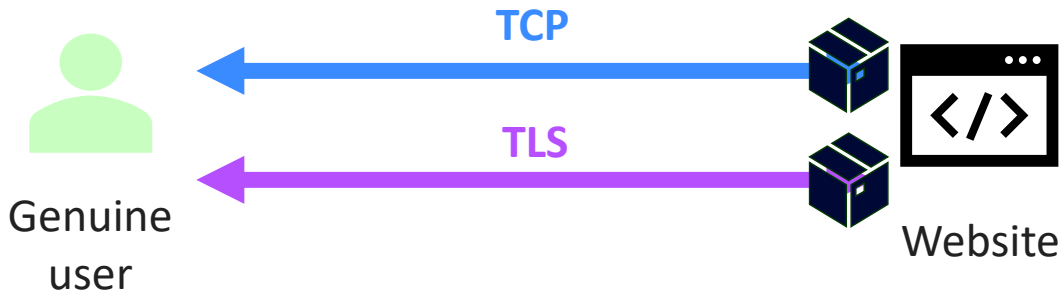


© Amadeus IT Group and its affiliates and subsidiaries

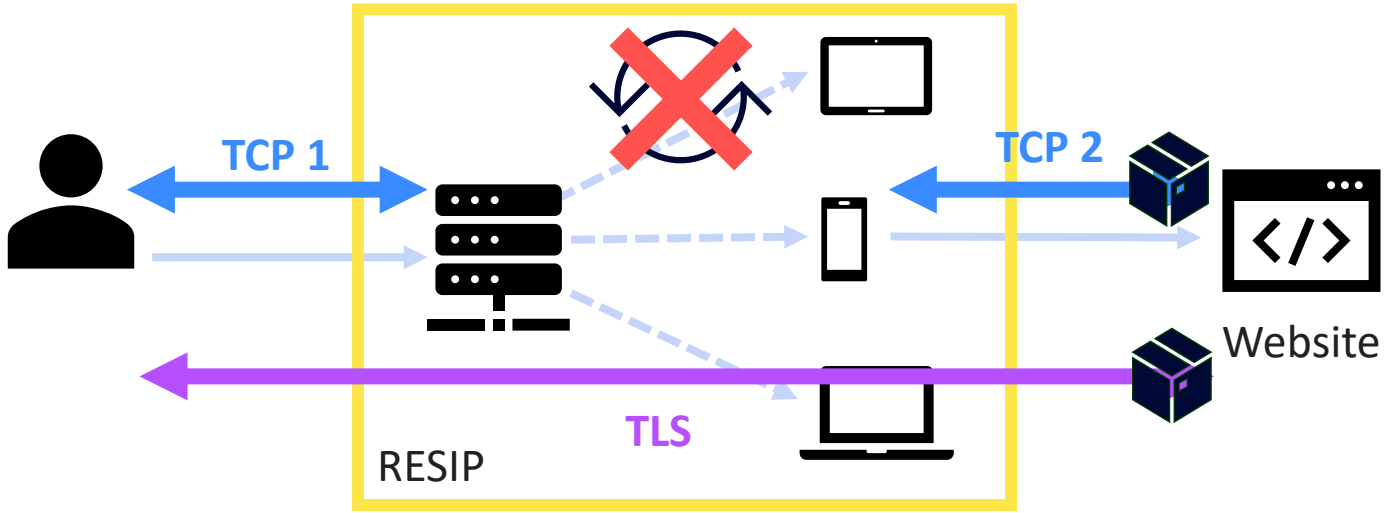
What do we do in Amadeus to protect against RESIPs?

Network Measurements

Direct connection



RESIP connection



We can measure the **Round Trip Time** in the TCP and TLS layer at the server side and understand when a RESIP is used

Request by request approach and linked to their **infrastructure management**

False Positives: Specific Mobile Carriers and VPNs

Whitelisting

Technique **integrated** in our anti-bot protection

© Amadeus IT Group and its affiliates and subsidiaries

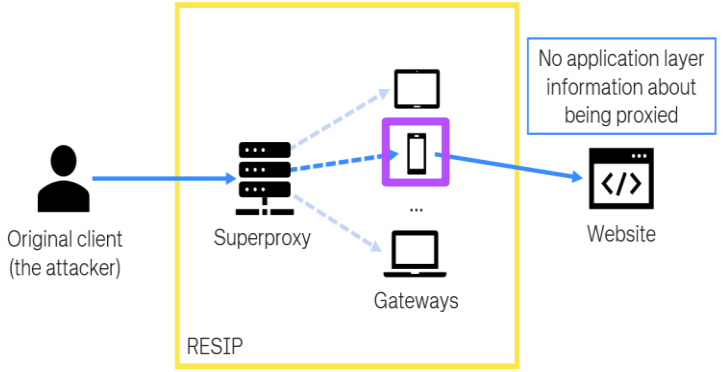
TCP= Transport Control Protocol

TLS=Transport Layer Security

What do we do in Amadeus to protect against RESIPs?

IP Intelligence

- **69M+** RESIP connection from **4** major RESIP providers
- Each provider **reuses** IPs among different paths (and possibly users)
- Different providers **share** pools of IPs
- The total amount of RESIP IPs is **smaller** than advertise values
- IP changes, **/24 vary less**
- Can we **leverage** this information?
  - **Tracking /24** and associate the ones where RESIPs appear to a **risk score**
  - Genuine users **share** their devices -> **Whitelisting** to reduce FPs
    - Association of IPs completing a **confirmed human action** (e.g. booking) to the corresponding **fingerprint**



© Amadeus IT Group and its affiliates and subsidiaries

Conclusion

- A significant portion of current Internet traffic consists of bots
  - GenAI and all-in-one solutions enable to build complex bots
- Bots can execute sophisticated functional attacks
  - Financial losses, damage to reputation, and service interruptions
- Residential Proxies are being exploited for bot attacks
  - Not recognized by conventional defenses
- Amadeus leverage network measurements and tailored IP intelligence
  - Protection while ensuring a seamless user experience

© Amadeus IT Group and its affiliates and subsidiaries

Thank you for your attention!

amadeus

More questions?
elisa.chiapponi@amadeus.com
or here in person

Check our published works here:

© Amadeus IT Group and its affiliates and subsidiaries