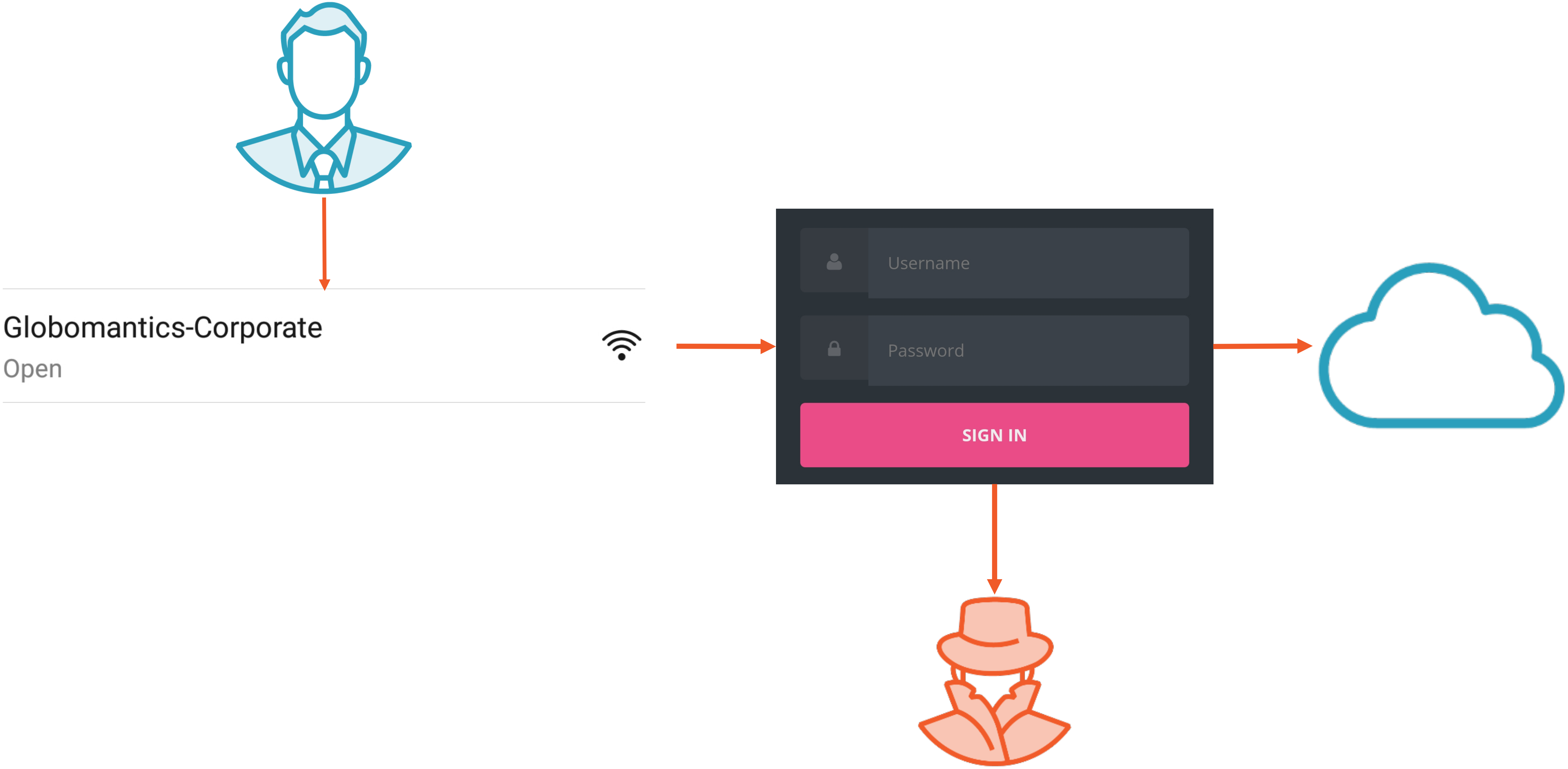
Initial Access with WiFi-Pumpkin

Ricardo Reimao
CYBER SECURITY CONSULTANT



Globomantics-Corporate

Open

WiFi
WiFi-Pumpkin
Framework for Rogue Wi-Fi Access Point Attack

Founder: Marcos Bomfim (mh4x0f) – P0cL4bs

A rogue access point framework to easily create fake WiFi networks. Includes several modules, such as transparent proxy, ARP poisoning, phishing manager, and much more.

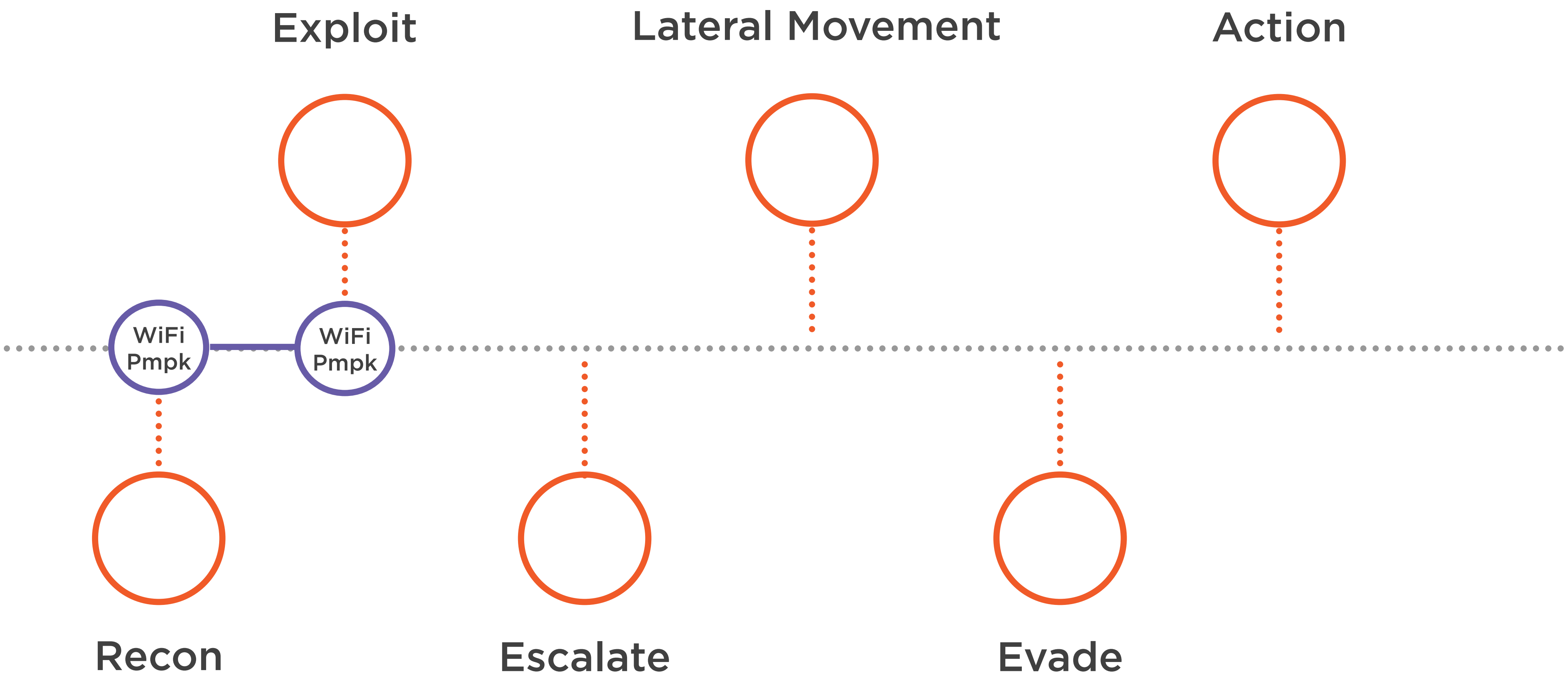
Open source tool (GNU v3.0)
https://github.com/P0cL4bs/WiFi-Pumpkin

Easy to install and use

Includes several attacks out of the box

- Packet injection
- HTTP credential monitoring
- ARP poisoning and DNS spoofing
- Fake captive portals

Kill Chain

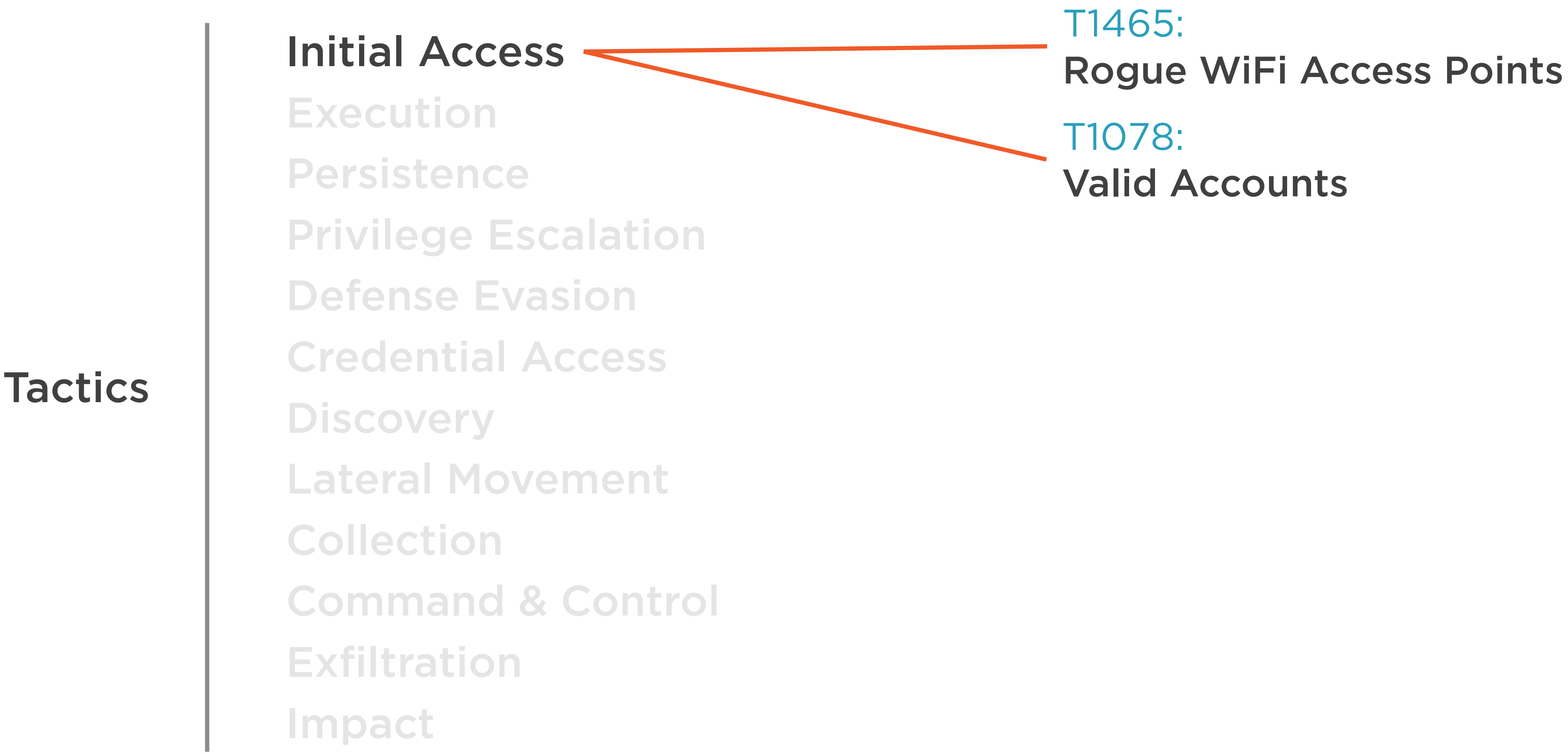

Exploit
Lateral Movement
Action
WiFi Pmpk
WiFi Pmpk
Recon
Escalate
Evade

MITRE ATT&CK

Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

MITRE ATT&CK



Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

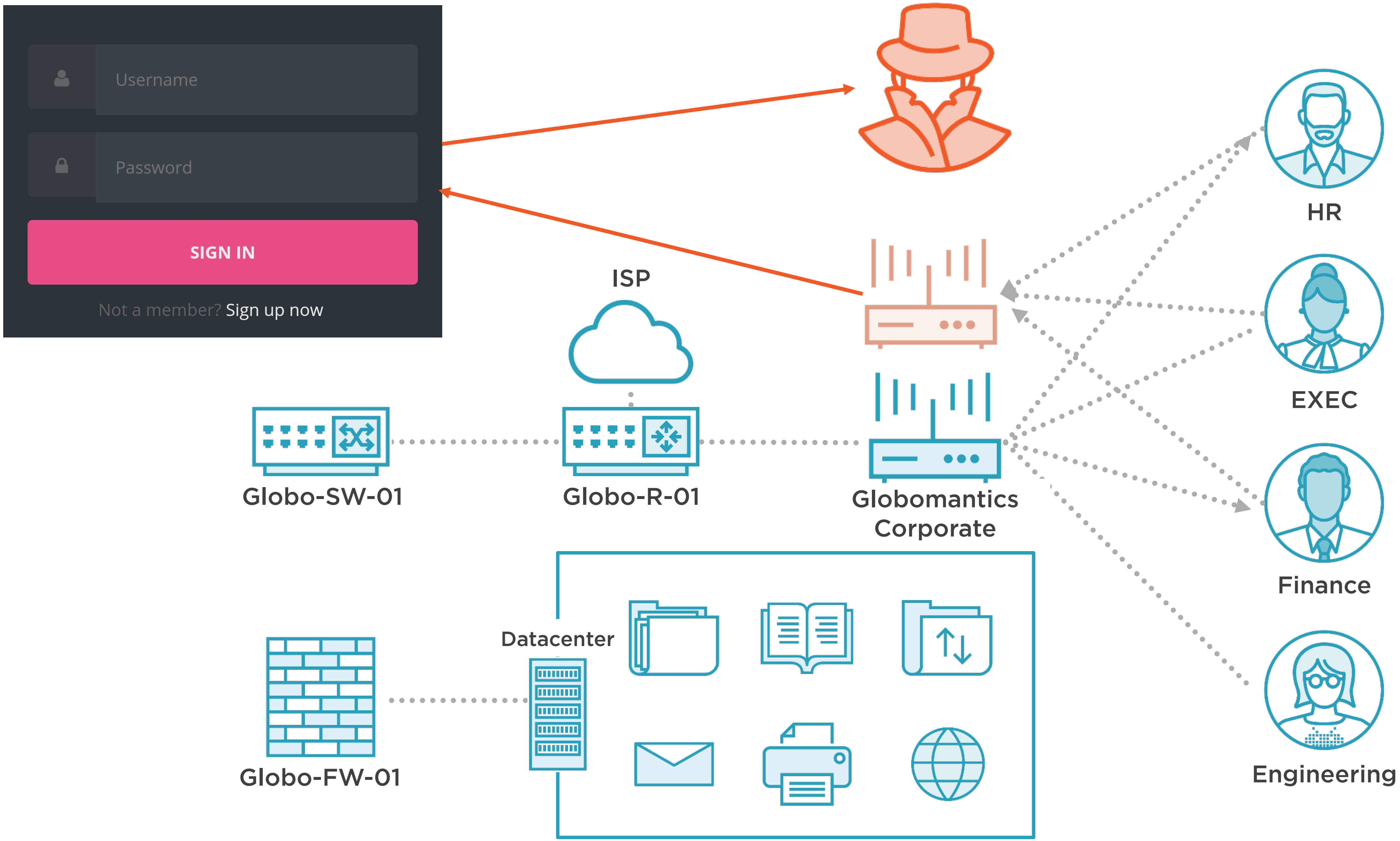
Command & Control

Exfiltration

Impact

T1465:
Rogue WiFi Access Points

T1078:
Valid Accounts


Username
Password
SIGN IN
Not a member? Sign up now
ISP
Globo-SW-01
Globo-R-01
Globomantics Corporate
HR
EXEC
Finance
Engineering
Datacenter
Globo-FW-01

Staying Legal

Stealing credentials without authorization is ILLEGAL in most countries

Letter of engagement, detailing dates and scope of what will be executed

Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network

Prerequisites

KALI

BY OFFENSIVE SECURITY

Kali Linux

Version: 2020.1 or superior

Up to date:
```
$ apt-get update
$ apt-get upgrade
```

WiFi Network Card

Must support “Monitor Mode”

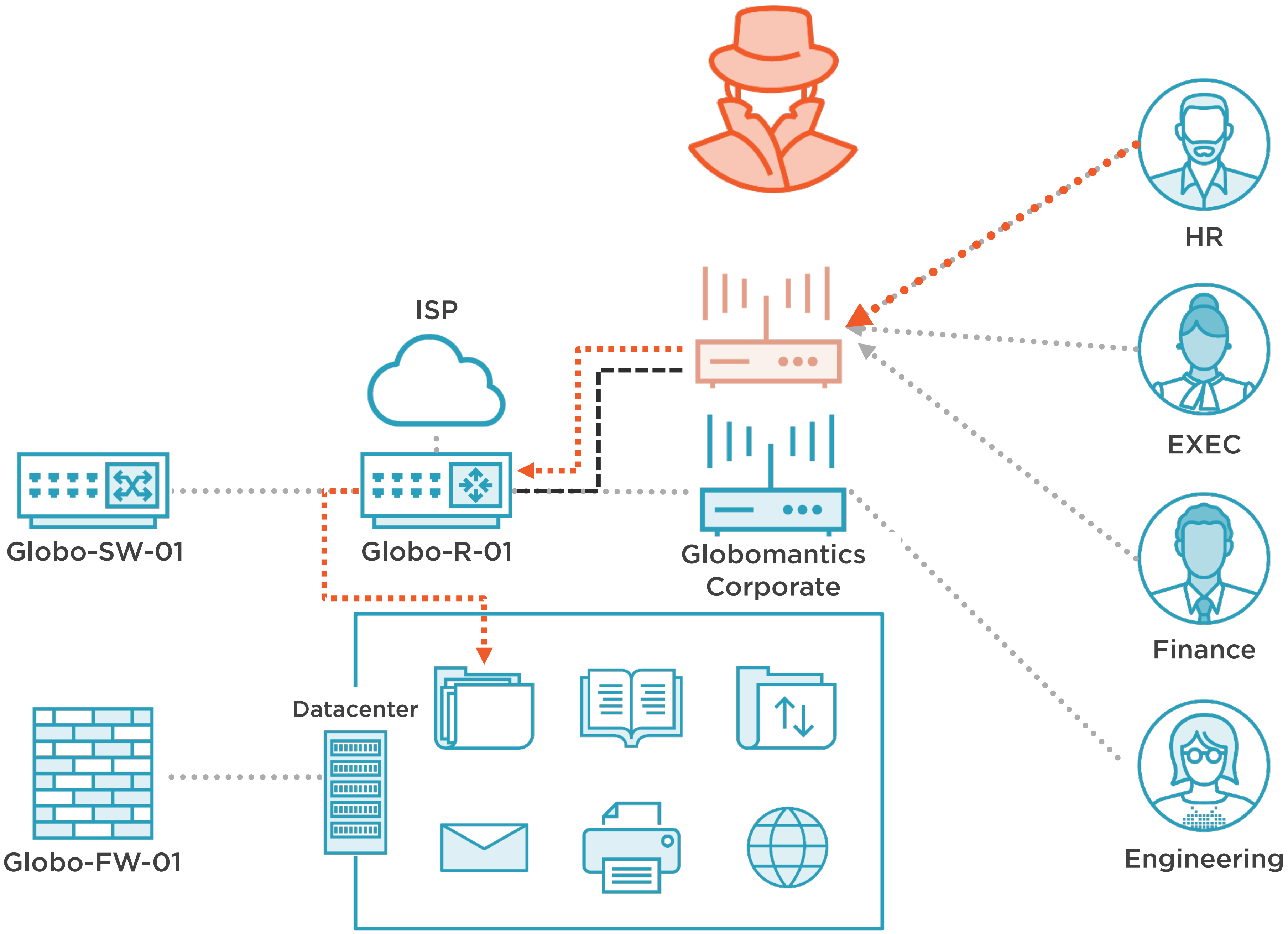
Suggested models:
- TP-LINK: TL-WN722N
- Alfa: AWUS036NH

Demo Place Holder

1. Installation Tips and Tricks

2. First use instructions and common usage syntax

3. Use of main features on live targets or in live environment


HR
EXEC
Finance
Engineering
ISP
Globo-SW-01
Globo-R-01
Globomantics Corporate
Datacenter
Globo-FW-01

How to Increase Your Success Rate

Use a convincing WiFi SSID
- "Globomantics Corporate Secure"
- "Globomantics Employees"

Create a convincing login page
- Use the target logo and colors

Generate a failed authentication
- Edit the template JavaScript

Cause DoS (if authorized)
- Use Aireplay-ng

```
# aireplay-ng --deauth 0 -a [real_ap_mac] -c [victm_mac] wlan0mon
```

More Information

Official Documentation

Several other capabilities, such as WiFi Proxy, SSL decryption, image capture, credential capture and much more.
https://github.com/P0cL4bs/WiFi-Pumpkin

DoS tool: Aircrack-ng

https://www.aircrack-ng.org/

Initial Access with Aircrack-ng
https://app.pluralsight.com/library/courses/initial-access-aircrackng/

More Courses in Pluralsight on Wireless Penetration Testing

Wireless Penetration Testing
https://app.pluralsight.com/library/courses/wireless-network-penetration-testing/

Wireless Network Penetration Testing Advanced Techniques
https://app.pluralsight.com/library/courses/wireless-network-penetration-testing-advanced-techniques/

Thank you!

Ricardo Reimao
Cyber security consultant