

Why Did you lose the last PS5 restock to a bot?

Top-performing app-hackers business modules,
architecture, and techniques

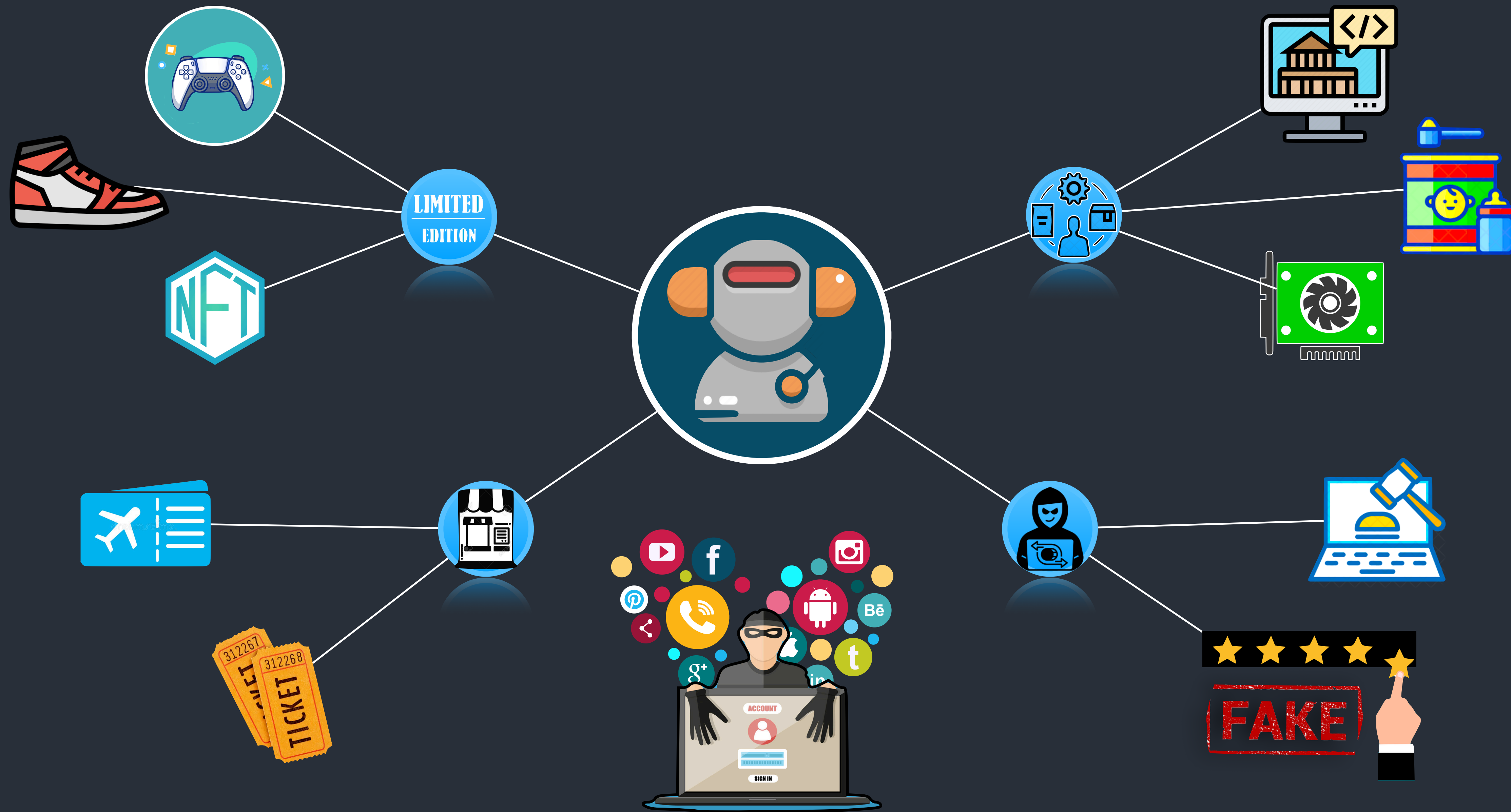
Arik Atar
Threat Intelligence Researcher



+



Intro

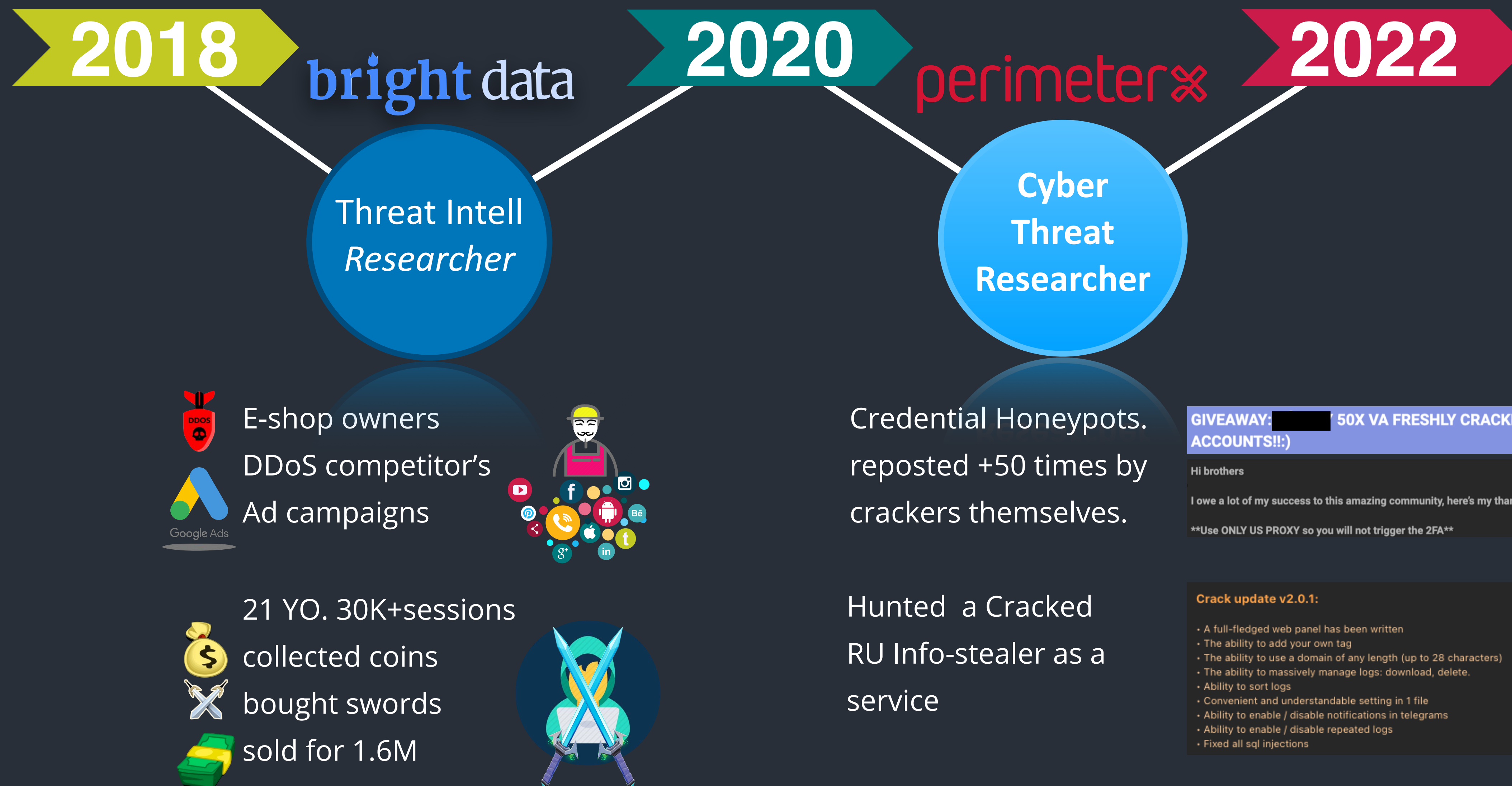


Bio



What do you mean
"I questioned her husband
For stealing millions from
the bank"?!





Agenda

01

Syntax

How to defined 'top performing' hackers

02

ATO Preconditions
& Attack Cycle

Behind the scenes of the breached accounts
economy

03

Scalping
Preconditions
& Architecture

Deep dive to a fascinating zero-sum-game

04

TTPs summary

The mindsets that makes a hacker a pro

05

Q&A

Promise not to answer like a bot

Syntax

1

Two malicious automation use cases:

- Account-take-over using brute force
- **Retail scalping** - using automation to buy stock

2

Top performing:

- Sustainable Business module
- Active for 6+ months
- Top 20%

3

$$\text{Success rate} = \frac{\text{Successful checkouts/logins}}{\text{Total attempts}}$$



80%



20%

Top
Performers

Successful
Logins/checkouts

Bruteforce ATO Preconditions

1 What do ATO hackers need before making the first request?

1

Brute-force tool

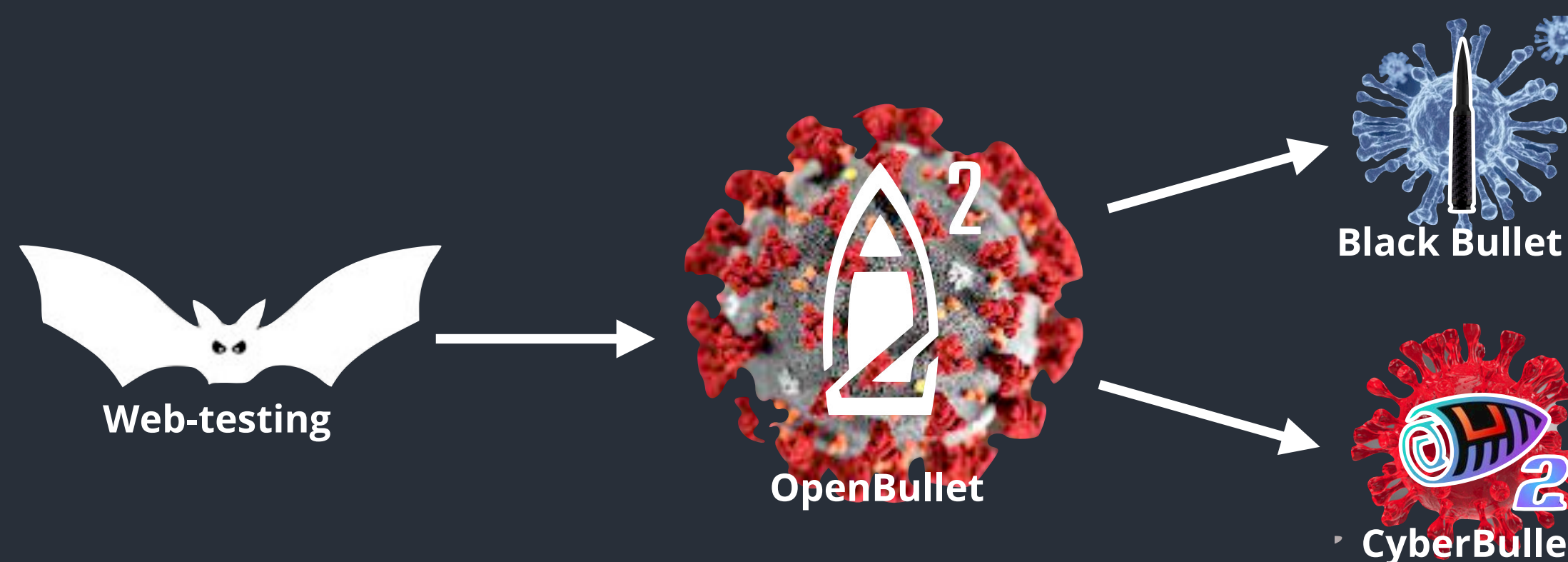
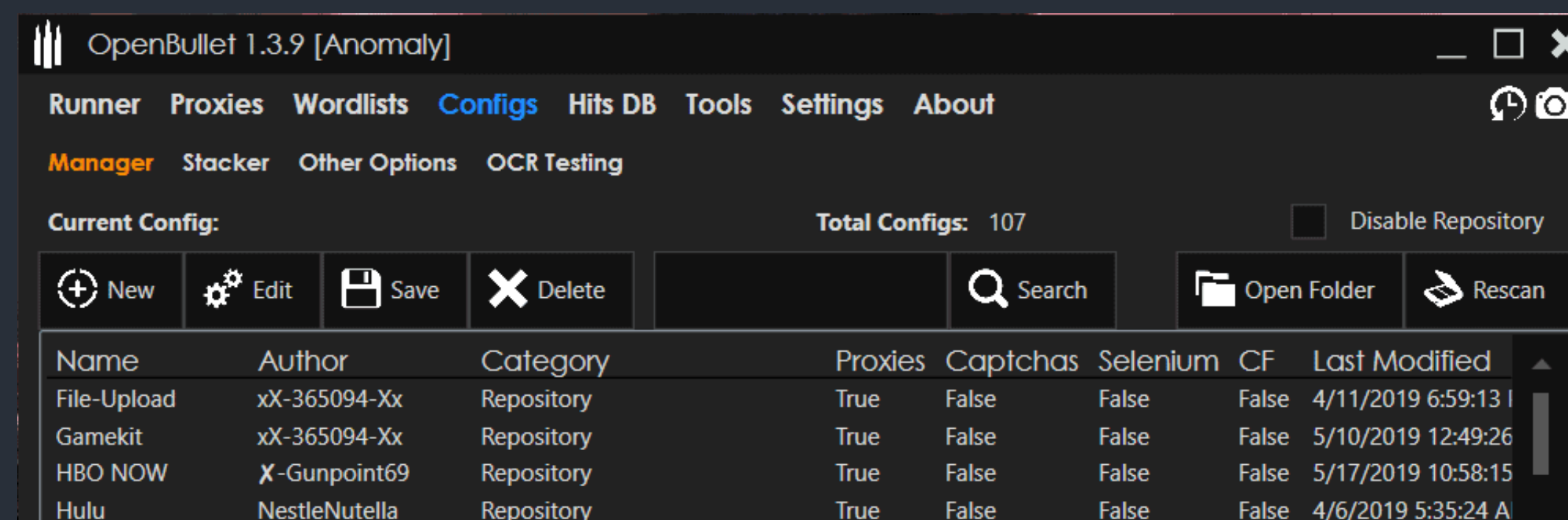
OpenBullet and its variants



Camouflage concurrent sessions as real login attempts



- One stop shop for cracker architecture.



2 Attack config



The attack's recipe.

Outsource attack planning to a developer



- Payload manipulation
- Replay attack
- Legit services spoofing
- API spoofing

```
#LOGIN REQUEST POST "https://www.████████.com/api-2.0/auth/████████-auth/login/?fields[
user]=title,image_100x100,is_fraudster,num_subscribed_courses,name,access_token"
CONTENT "email=<USER>&password=<PASS>"
CONTENTTYPE "application/x-www-form-urlencoded"
HEADER "Accept: */*"
HEADER "User-Agent: okhttp/3.8.0 ██████████ Android 4.2.0(192) (phone)"
HEADER "Pragma: no-cache"
HEADER "X-Client-Name: ██████████-Android"
HEADER "X-Version-Name: 4.2.0"
HEADER "X-Mobile-Client-Id: REM6RUY6Q0E6Mzc6Mzg6NzA="
HEADER "X-Mobile-Visit-Enabled: true"
HEADER "Accept-Language: en_US"
HEADER "Cache-Control: private, max-age=0, no-cache"
HEADER "Authorization: Basic YWQxMmVjYmUxN2FmYWZmMjU5ZmU1ZDk4NDcxYTY6YTdjNmMwNjQ2MzA4ODI0YjIz
MDFmZGI2MGVjZmQ4YTA5NDdlODJkNQ=="
HEADER "X-████████-Client-Secret: a7c630646308824b2301fdb60ecfd8a0947e82d5"
HEADER "X-████████-Client-Id: ad12eca9cbe17afac6259fe5d98471a6"
```

```
75
76 FUNCTION Translate
  StopAfterFirstMatch=FALSE
77 KEY "1" VALUE "Noah"
78 KEY "2" VALUE "Unlimited Screens"
79 KEY "3" VALUE "Enhanced Cloud"
80 KEY "4" VALUE "PSL"
81 KEY "5" VALUE "Multi Stream"
82 KEY "6" VALUE "Live Stream"
83 KEY "7" VALUE "Lunchbox"
84 "<capture>" -> CAP "Features"
85
86 FUNCTION Translate
  StopAfterFirstMatch=FALSE
87 KEY "14" VALUE "No Commercials"
88 KEY "15" VALUE "Showtime"
89 KEY "16" VALUE "Live TV"
90 KEY "17" VALUE "HBO"
91 KEY "18" VALUE "Cinemax"
92 KEY "19" VALUE "Starz"
93 KEY "21" VALUE "Entertainment"
94 KEY "23" VALUE "Spanish Add-on"
95 "<Sub>" -> CAP "Subscriptions"
96
```

✨ ██████████ Config ✨

Name: ██████████

CPM: depends on proxy service + recaptcha service

Combolist Type: Email:Pass

Captcha: Yes (compatible with capmonster)

Capture: CC and GC

ONLY 5 COPIES WILL BE SOLD

First copy: \$250

Second - Fifth copy: \$300

PM me on discord or on here to buy: ██████████

S: Any leakage of the config results in a scam report and a \$1500 fee.

3 Credentials:



Get access to target accounts



- collect credential combos from Hacking platforms/private sellers
- Build credential DB on VPS
- Share it with others
- Scan it for old victim passwords

We have a total of **10,947,482,245** Records from the following **540** Datasets, free for download once you unlock them.

[014,936,670] | 2015 - (000webhost.com) 000webhost Database ⇒ Download Here!
[007,476,940] | 2021 - (datpiff.com) DatPiff Database ⇒ Download Here!
[007,633,234] | 2018 - (blankmediagames.com) BlankMediaGames Database ⇒ Download Here!
[015,003,961] | 2021 - (epik.com) Epik Database ⇒ Download Here!
[000,819,478] | 2014 - (warframe.com) Warframe Database ⇒ Download Here!
[004,105,095] | 2018 - (avvo.com) Avvo Database ⇒ Download Here!
[000,018,131] | 2017 - (crackingitaly.com) CrackingItaly Database ⇒ Download Here!
[010,604,307] | 2019 - (armorgames.com) Armor Games Database ⇒ Download Here!



4 Mail Validation



Clean non-relevant users that are not signed up on the target site



- UI OSINT
- API exploitation

Forgot [password?](#)

Password Reset

Enter your email into the box below to have a new password sent to you.

RESET PASSWORD

The information that you have provided does not match our records. Please check your details and try again.

Ban List

```
[SCRIPT]
#Check_mail REQUEST POST "https://[REDACTED].com/auth/_ajax/auth/v1/
checkusername?clientId=[REDACTED]&EncodeContent=TRUE"
```

```
KEYCHECK
KEYCHAIN Success OR
  KEY "That email already exists on [REDACTED]"
KEYCHAIN Failure OR
  KEY "{\"result\":{\"log_session\":\"\"}"
KEYCHAIN Ban OR
  KEY "<RESPONSECODE>" EqualTo "403"
```

5 Password Cracking Predictabilities



Pattern ✓

Your password must include the following:

8–100 characters

Upper & lowercase letters

At least one number or special character



- 8-10 characters
- Upper-case prefix
- 1,5 or 7 suffix



Content ✓

Most of users Use PII:

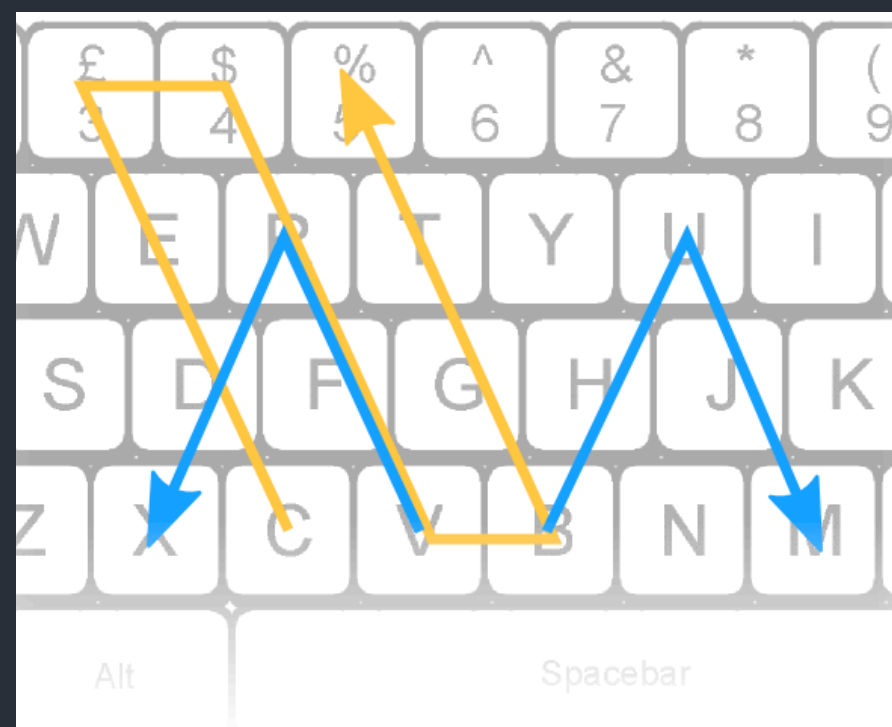
50% Old passwords

33% Pets names and birthdate

22% Their own name

15% Spouse's bd/names

14% Child(ren)'s name



**Enumeration based on keys
attached to each other on the
keyboard**

Password Enumeration Flow



Use Osint OS repos and
breached DB to enrich The
victim PII.



Use Password Generator to
compose a hyper-targeted wordlist



Password enumeration based on:

- victim PII
- breached passwords
- Password policy



```

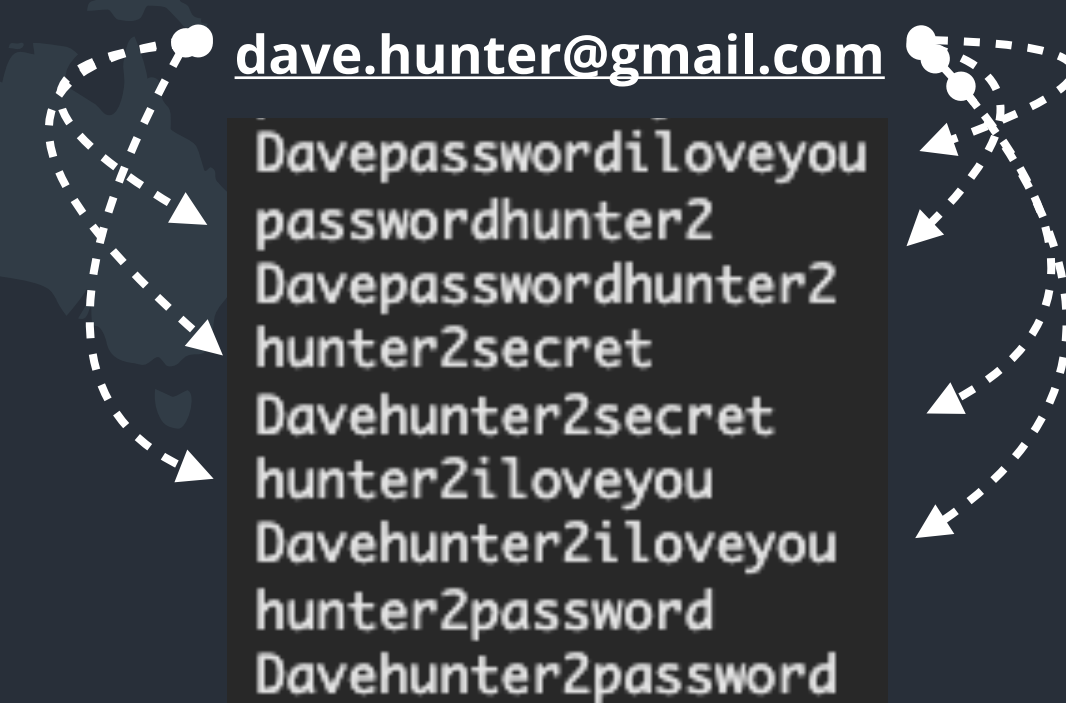
pydictor
2.1.0#dev

Social Engineering Dictionary Builder
Build by LandGrey

-----[ command ]-----
[+]help desc          [+]exit/quit          [+]clear/cls
[+]show option        [+]set option arguments [+]rm option
[+]len minlen maxlen  [+]head prefix        [+]tail suffix
[+]encode type        [+]occur L d s         [+]types L d s
[+]regex string       [+]level code         [+]leet code
[+]output directory   [+]run

-----[ option ]-----
[+]cname              [+]ename              [+]sname
[+]birth              [+]usedpwd            [+]phone
[+]uphone             [+]hphone             [+]email
[+]postcode           [+]nickname           [+]idcard
[+]jobnum              [+]otherdate          [+]usedchar

pydictor SEDB>>
  
```



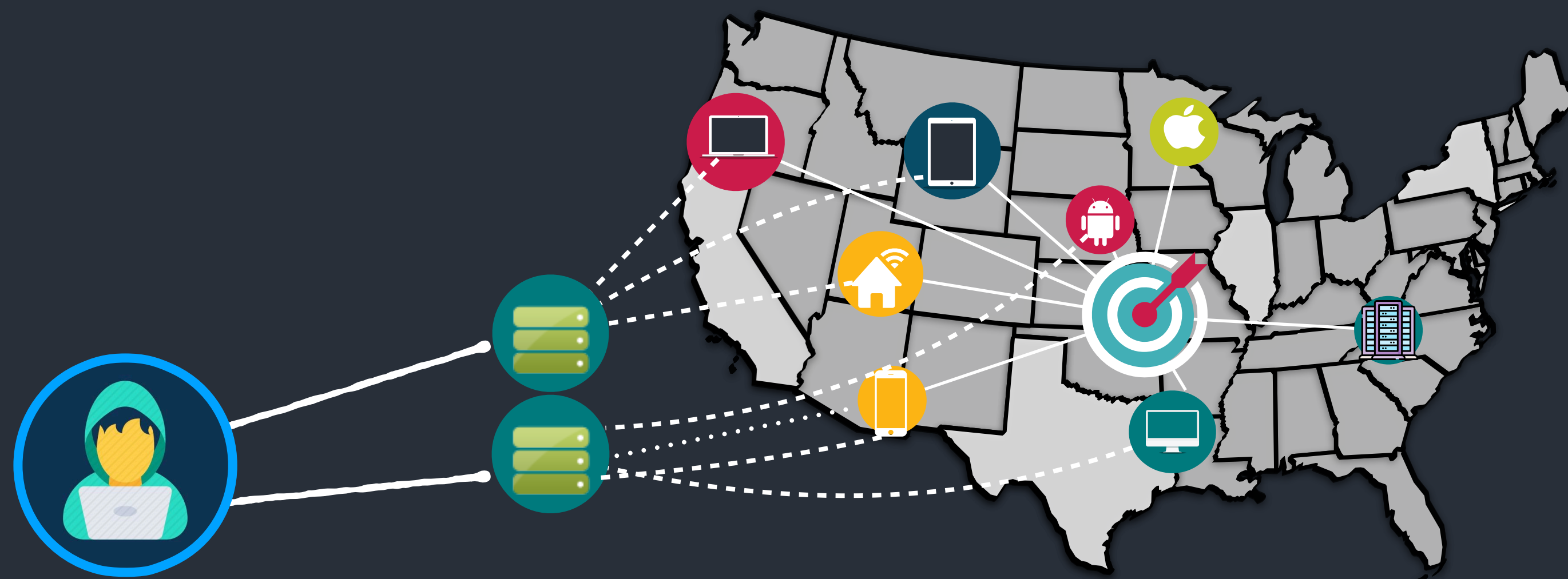
6 Proxy network



- Concurrent Sessions
- Maximizing IP/rate limit
- Hide attacker's IP



Using a dynamic pool of rotating residential IPs from reputable ISPs

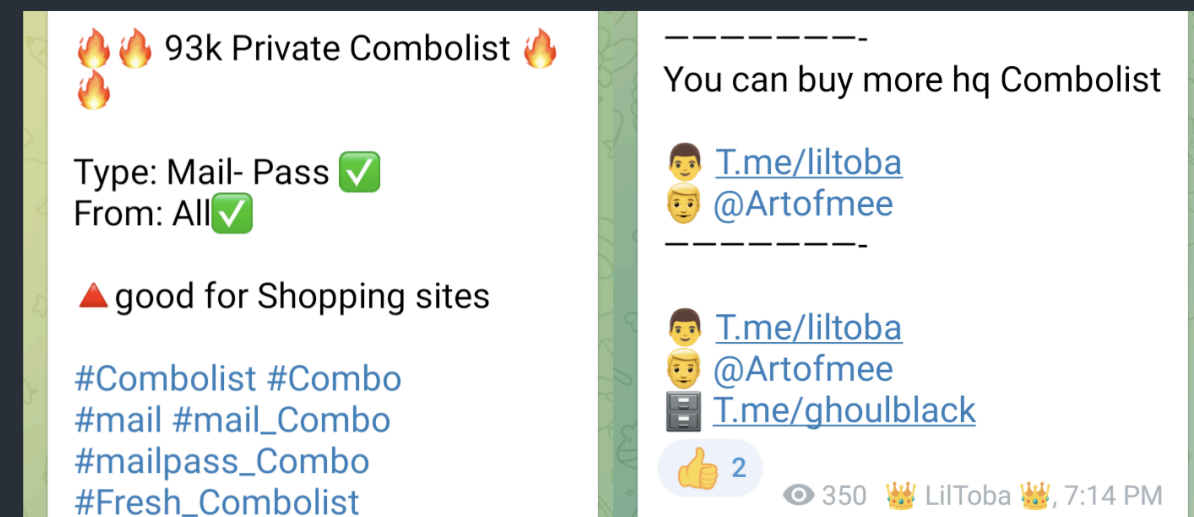


- ➡ Unlimited concurrent sessions
- ➡ Pay per bandwidth, infinite IP pool.
- ➡ Auto-rotate+start new session when captcha
- ➡ contains peers from all ASNs, ISPs, and Geos (city resolution) > impossible to IP block without FP

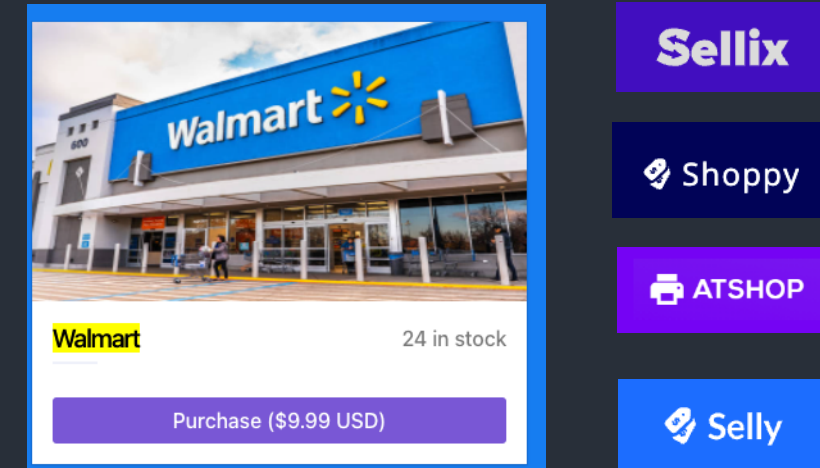
ATO Attack Cycle

13

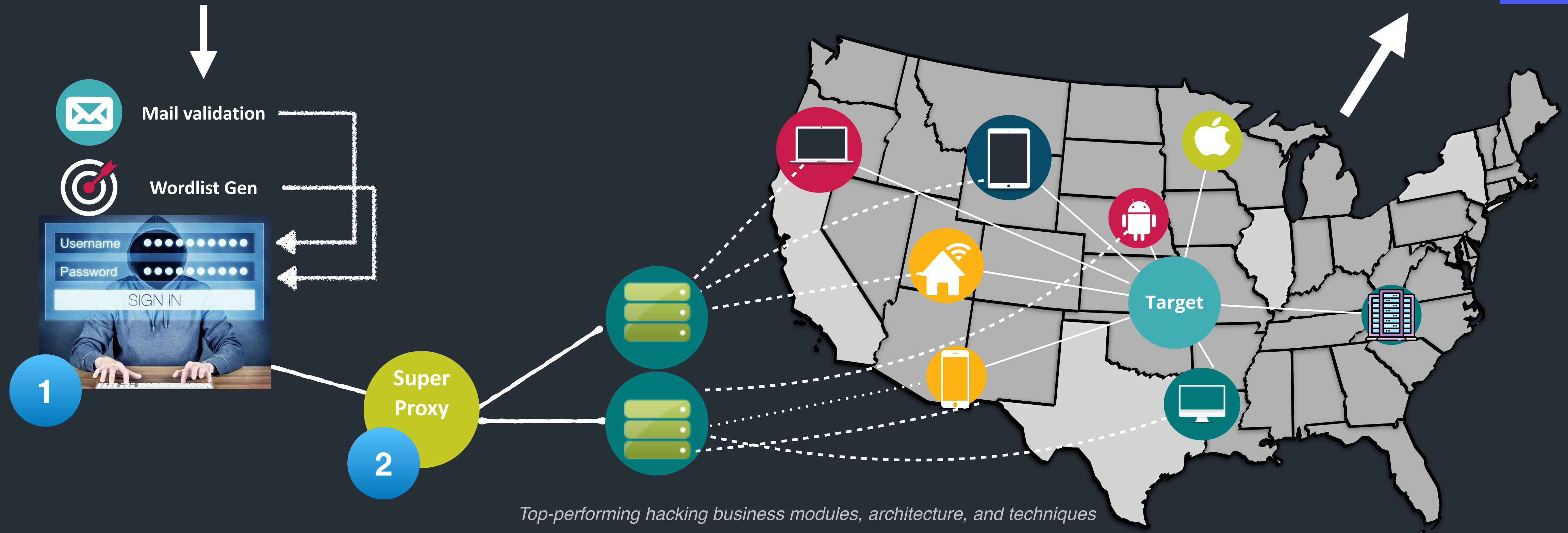
5 combo Recycling



4 90% to costumers



3 10% to prospects



Sustainable cracking

How credentials are being recycled on the dark automation economy

01

Cracker releases uncracked credential



02

Opportunists repost credentials on Deep and DW platforms to harvest marketplace credits



03

Thousands of crackers run their latest config to catch as much account as they can.



2

Minutes until malicious traffic arrives after publication



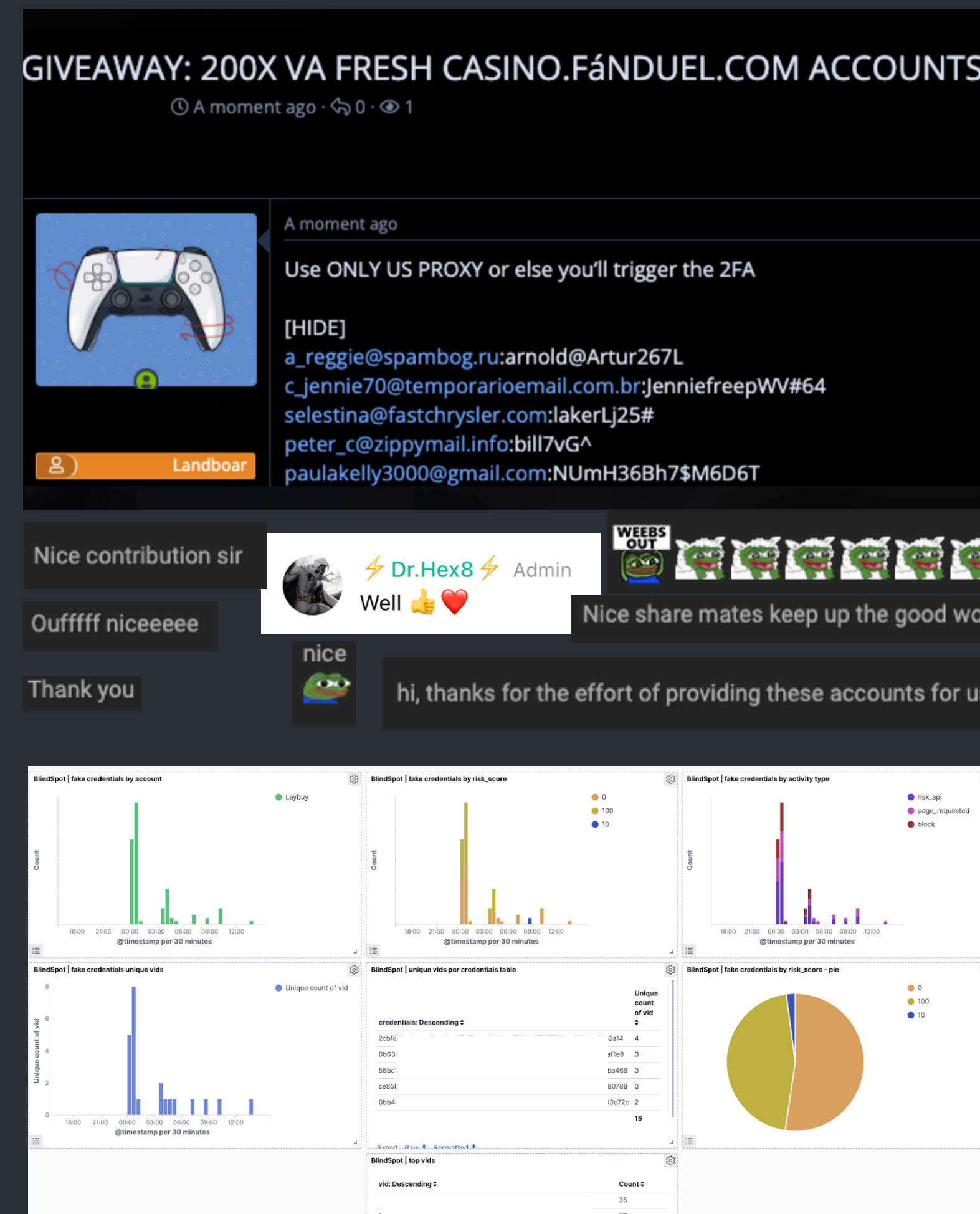
50+

Reposting of the honeypots in 24h



600

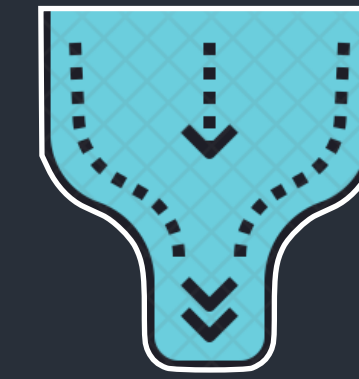
Attackers were exposed to the honeypot publications across the web



Scalping Intro



**Limited Edition
Scalping**



**Opportunist
Scalping**

High Demand
Low Supply

Standard Demand
Temporary Low Supply



Retail Scalping Preconditions

What do retail bot operators need to pay for before making the first request?

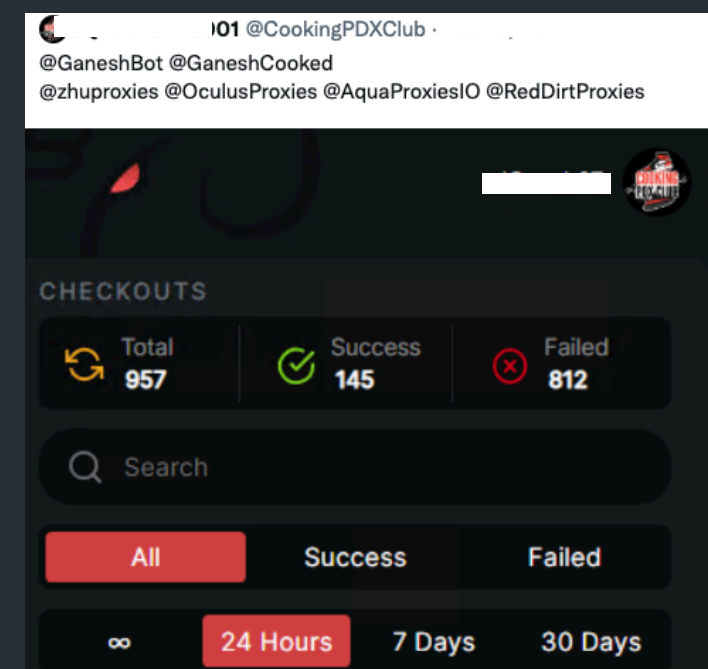


Target site's valid aged accounts

Need stockx accounts, need to be aged for at least a year, more the better, but have to be no recent activity (at least in the past half year). Selling and buying history is preferred too. Mail access needed. HMU with pictures



Cook-group



Backdoors
Sneaker backdoors for off white drops

Bots
Free sneaker bot rentals for all users

Partnerships
Get access to sold-out bots through our partnerships

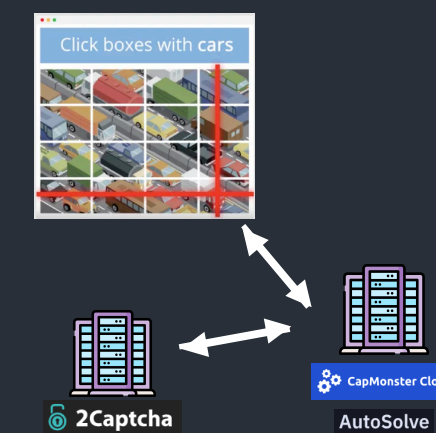
Monitors
Receive notifications for product restocks on over 1000 websites

Support
In-depth help articles & 1 to 1 support staff

Automation
An inhouse chrome autofill that works on 100s of sites



Bot & Bot manager toolkit



Accounts Proxies AutoSolve Settings						
File	Edit	Selected Items: 1		OneClicks: 278 / 300	Running: 20 / 300	Scheduled: 280 / 300
Categories		Name	Proxy	Action Log	Status	Enabled One Click
All		aycdtest1@gmail.com	91.10...	Reading Technology News	Good	✓ Yes
Yeezy v3 Accounts		aycdtest2@gmail.com	91.10...	Viewing a Product	Good	✓ Yes
Supreme Accounts						



Product Release Monitoring Service



Yeet Monitors
14/07/2022, 09:00:02

Competitor 1
MISSED

Competitor 2
MISSED

Competitor 3
MISSED

Yeet Monitors
29/06/2022, 13:42:36

Competitor 1
29/06/2022, 13:44:54

Competitor 2
29/06/2022, 13:44:54

Competitor 3
29/06/2022, 14:03:46

5 Dedicated Servers

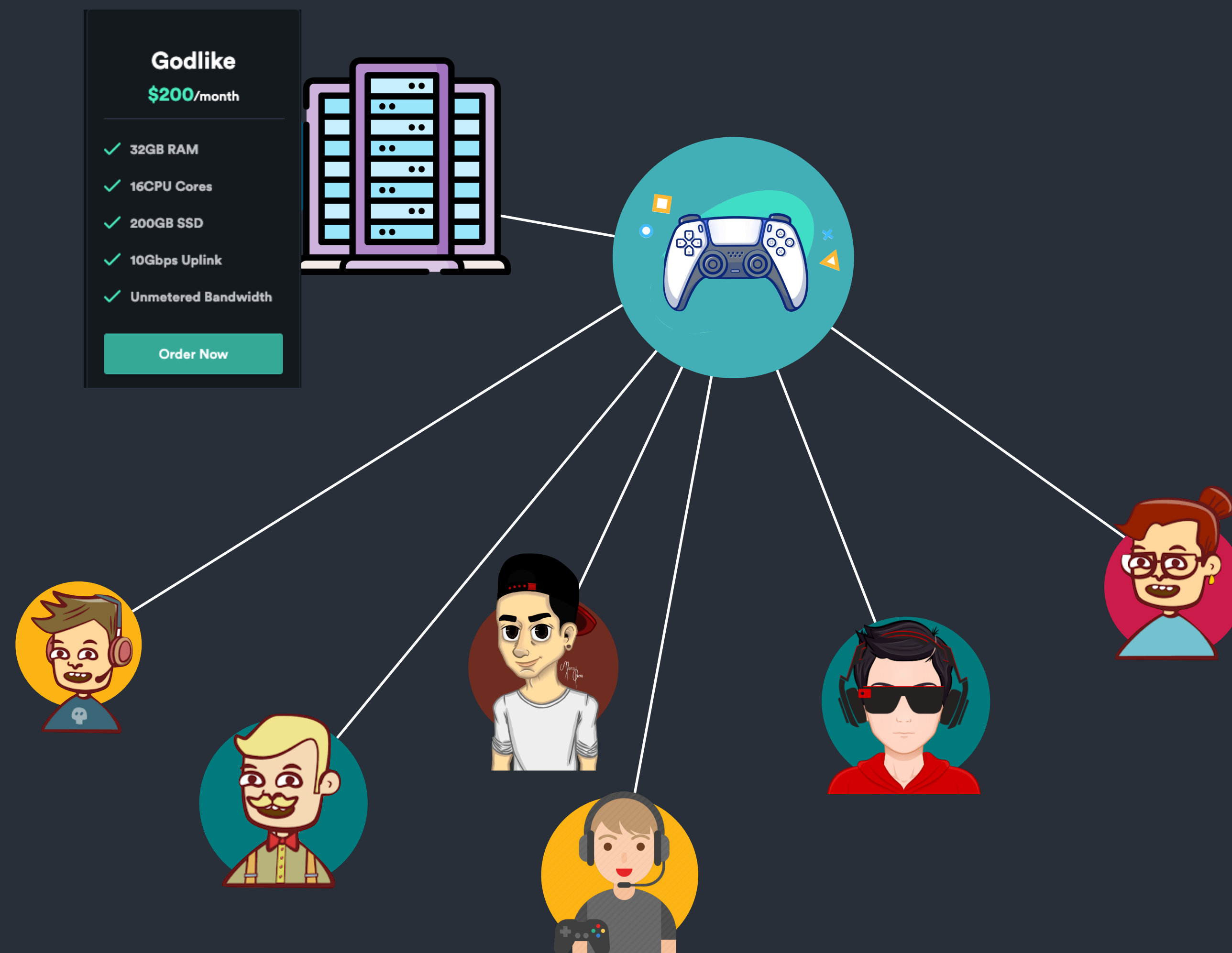


Minimize Bot's ping to the target server



Sends the requests from the closest possible Geo to the target datacenter

SERVER CPU	RAM	HDD	BANDWIDTH	IPMI	LOCATION
4 in stock E5-2680v4 x2	64GB DDR4	480G SSD	10Gbps	✓	London, UK
2 in stock E5-2680v4 x2	64GB DDR4	480 SSD	10Gbps	✓	Ashburn, VA



6 Residential Proxy Network access



- Concurrent Sessions
- Bypass IP/rate limit
- Decrease ping to target platform



Using mobile emulation and dynamic pool of rotating mobile IPs

Release Premium

5% Off

✓ Location: Ashurn, Virginia

✓ 10 GBPS Speed

✓ ISP Proxies

✓ Locked for Optimization on key sites

Optimized sites

YeezySupply

Footsites

Retail

Supreme

SNKRS

Shopify

1 W

1 M

2 M

3 M

Retail Residential

50GB

Valid for 3 Months

Bandwidth

50GB

✓ 10000 IPs per Generation

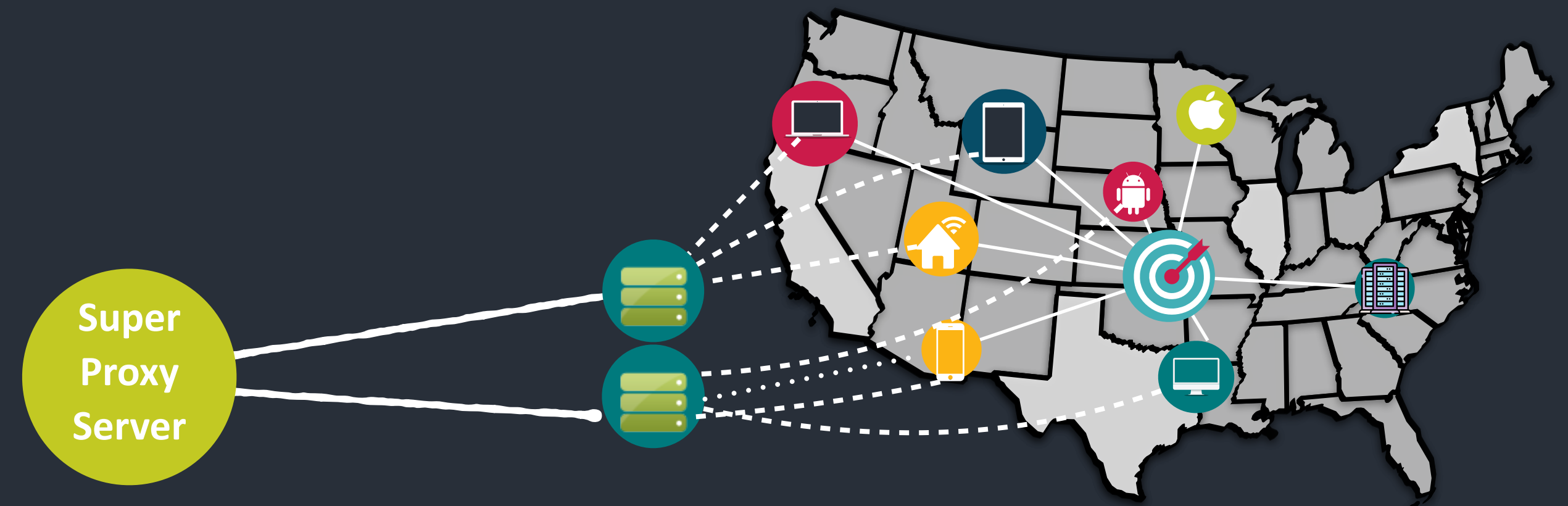
✓ Global IPs

✓ KYC Verification

✓ Advanced Network Routing

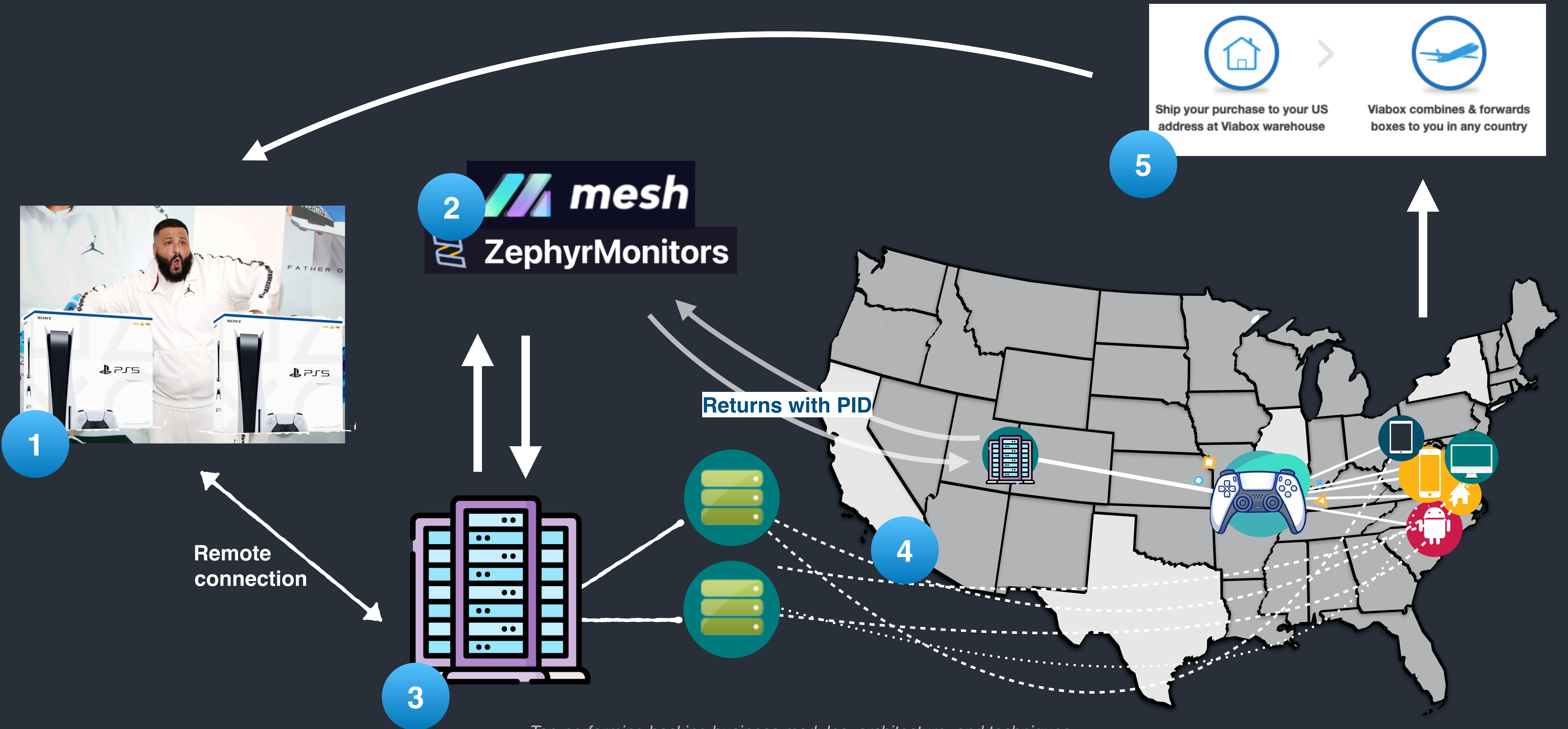
✓ Exclusive IP Pool

✓ Mobile IPs



Scalping Attack

19



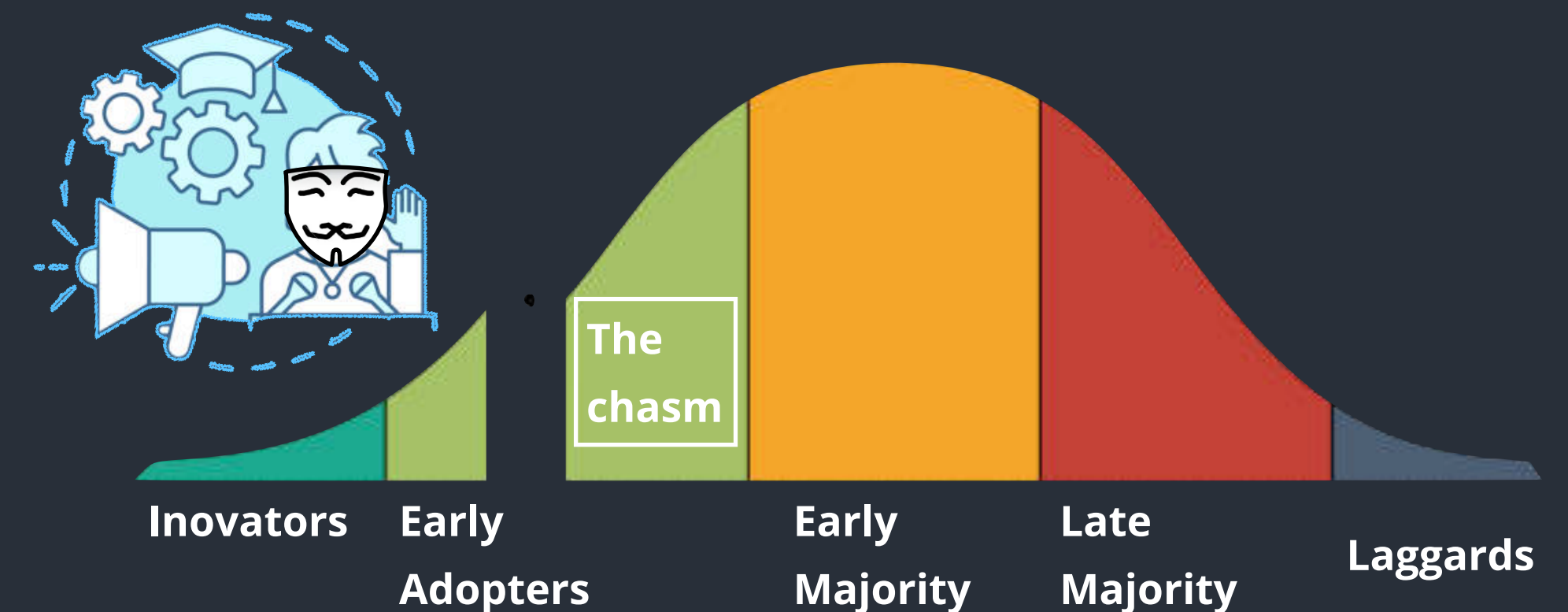
Top-performing hacking business modules, architecture, and techniques

The Future Of Automation

What mindsets differentiates top performing actors?

1

Top performers are the **early adopters** of new cracking tools and techniques



2

Every retail supply chain bottleneck is a **business opportunity** for bots operators



Summary

What mindsets differentiates top performing actors?

1

Think DevOps

Minimize request TTL by adjusting architecture to the target sites



mobile emulation for maximizing IP limit rate

Dedicated servers from closest possible Geo to the target datacenter

2

Leverage OSINT

Using OS Osint scripts



Validate breached emails by exploiting API or UI intelligence

Intelligent emulation of wordlists based on victim's PII

What mindsets differentiates top performing actors?

3

Time resourceful

Scalper's biggest asset is not his money, but his time.

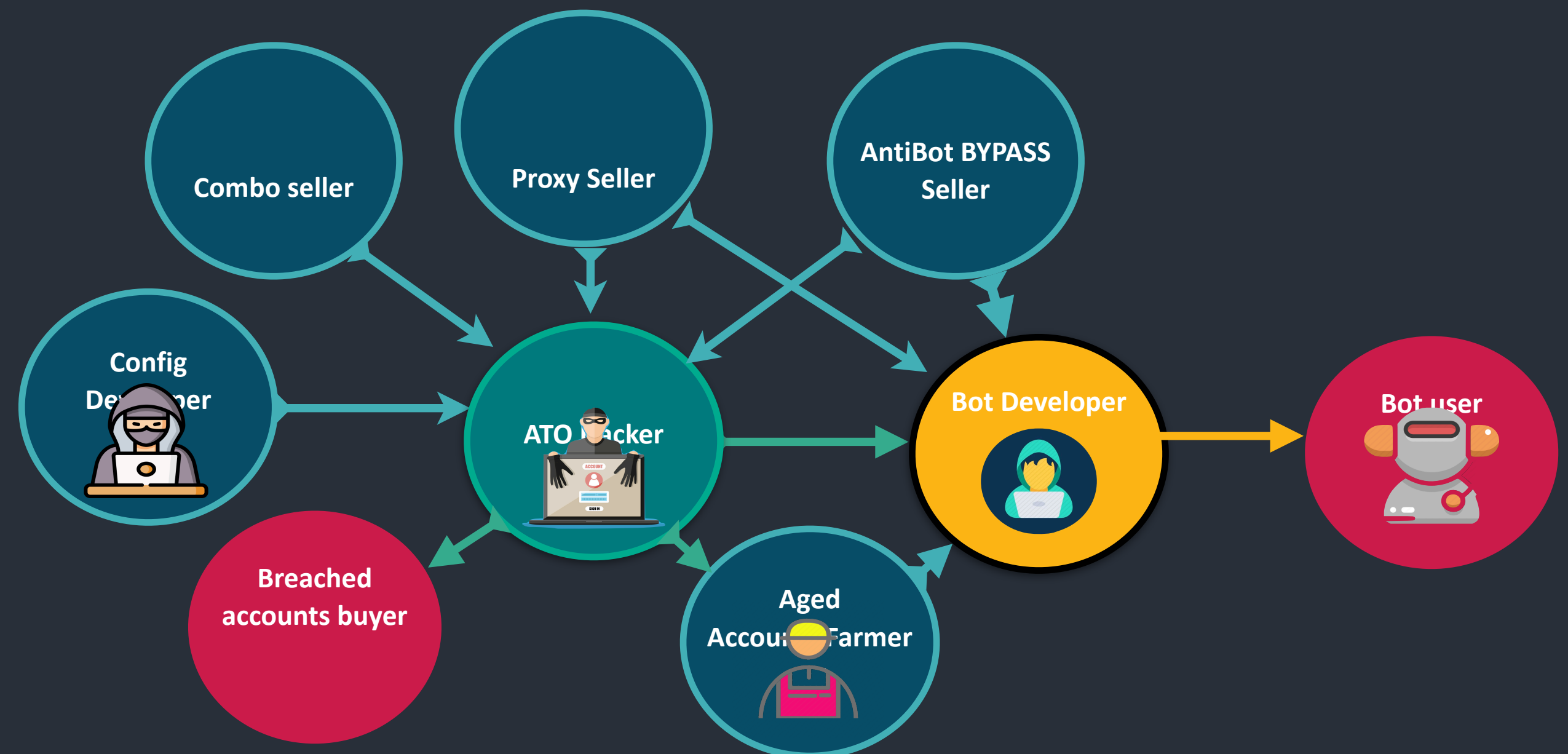
- Outsource code when needed

The promotion paradox

All tickets will be answered in the next few days, sorry for the delays, wrote 3 exams last week, this week will be my last 2, then ill be fully back 🤖

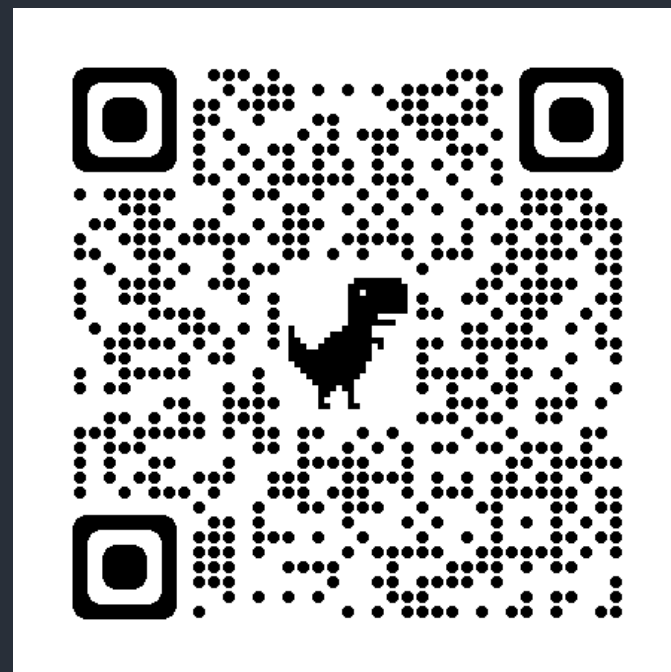
✓ 3

- Developed a deep understanding of debugging, web-testing, and obfuscation techniques.



Q&A

Anything you wanted to ask about Bots and was too shy to ask



arikatar.defcon30@gmail.com

