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”?!
Credential Honeypots. reposted +50 times by crackers themselves.

Hunted a Cracked RU Info-stealer as a service

Top-performing hacking business modules, architecture, and techniques
Agenda

01 Syntax

How to define '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. Success rate = \( \frac{\text{Successful checkouts/logins}}{\text{Total attempts}} \)
   - 80% Successful Logins/Checkouts
   - 20% Top Performers

Top-performing hacking business modules, architecture, and techniques
Brute-force ATO Preconditions

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

---

**ATO Preconditions**

Top-performing hacking business modules, architecture, and techniques
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!
- [007,632,234] 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!
Mail Validation

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

- UI OSINT
- API exploitation

ATO Preconditions

Ban List

Top-performing hacking business modules, architecture, and techniques
Password Cracking Predictabilities

**Pattern**
- Your password must include the following:
  - 8-10 characters
  - Upper & lowercase letters
  - At least one number or special character
- 8-10 characters
- Upper-case prefix
- 1, 5, or 7 suffix
- Enumeration based on keys attached to each other on the keyboard

**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

ATO Preconditions

Top-performing hacking business modules, architecture, and techniques
ATO Preconditions

Password Enumeration Flow

Use Password Generator to compose a hyper-targeted wordlist

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

Password enumeration based on:
- victim PII
- breached passwords
- Password policy

Top-performing hacking business modules, architecture, and techniques
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 Preconditions
ATO Attack Cycle

5. combo Recycling
   - 93k Private Combolist
   - Type: Mail Pass
   - From: All
   - good for Shopping sites
   - #Combolist #Combo
   - #email_Combo
   - #emailpass_Combo
   - #Fresh_Combolist

4. 90% to costumers
   - Walmart
   - Sign in
   - Sellix
   - Shoppy
   - ATSHOP
   - Sally

3. 10% to prospects
   - N
   - Letterbox
   - REACTOR

1. Mail validation
2. Wordlist Gen
3. Super Proxy
4. ATO Attack Cycle

Top-performing hacking business modules, architecture, and techniques.
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

Top-performing hacking business modules, architecture, and techniques
Scalping Intro

Limited Edition Scalping

High Demand
Low Supply

Opportunist Scalping

Standard Demand
Temporary Low Supply

Top-performing hacking business modules, architecture, and techniques
Retail Scalping Preconditions

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

1. Target site’s valid aged accounts
2. Cook-group
3. Bot & Bot manager toolkit
4. Product Release Monitoring Service

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.
Dedicated Servers

Minimize Bot’s ping to the target server

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

<table>
<thead>
<tr>
<th>SERVER CPU</th>
<th>RAM</th>
<th>SSD</th>
<th>BANDWIDTH</th>
<th>PMI</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES.3XLarge</td>
<td>64GB</td>
<td>480GB</td>
<td>100Gbps</td>
<td></td>
<td>London, UK</td>
</tr>
<tr>
<td>ES.3XLarge</td>
<td>64GB</td>
<td>480SSD</td>
<td>100Gbps</td>
<td></td>
<td>Ashburn, VA</td>
</tr>
</tbody>
</table>
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
Scalping Attack

1. Remote connection
2. ZephyrMonitors
3. Top-performing hacking business modules, architecture, and techniques
4. Returns with PID
5. Ship your purchase to your US address at Viabox warehouse
   Viabox combines & forwards boxes to you in any country

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

---

Top-performing hacking business modules, architecture, and techniques
Summary

What mindsets differentiates top performing actors?

1. Think DevOps
   Minimize request TTL by adjusting architecture to the target sites

2. Leverage OSINT
   Using OS Osint scripts

- Dedicated servers from closest possible Geo to the target datacenter
- Mobile emulation for maximizing IP limit rate
- Validate breached emails by exploiting API or UI intelligence
- Intelligent emulation of wordlists based on victim’s PII
What mindsets differentiate top performing actors?

3. **Time resourceful**

- Outsource code when needed
- Developed a deep understanding of debugging, web-testing, and obfuscation techniques.

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

Summary

Top-performing hacking business modules, architecture, and techniques
Q&A

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

arikatar.defcon30@gmail.com

Top-performing hacking business modules, architecture, and techniques