

# **How CREDENTIAL STUFFING IS EVOLVING**

And where do we go from here?

Jarrod Overson

Director of Engineering at Shape Security

# CREDENTIAL STUFFING

cre·den·tial stuff·ing

/krə'den(t)SHəl 'stəfɪNG/

The testing of previously breached username  
and password pairs across sites to find  
accounts where passwords have been reused.

# Who am I?

And should you trust me?



- Director of Engineering at Shape Security
- Google Developer Expert.
- Old school video game hacker.
- @jsoverson everywhere



1

**Why credential stuffing is evolving**

2

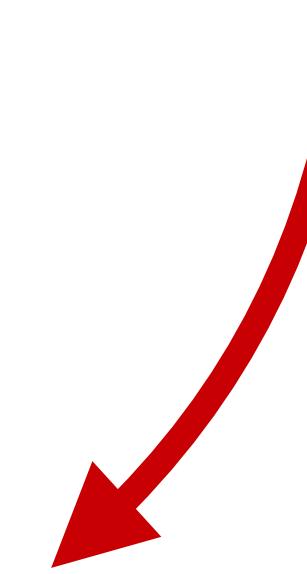
How credential stuffing has evolved

3

Where do we go from here?

1

## Why credential stuffing is evolving

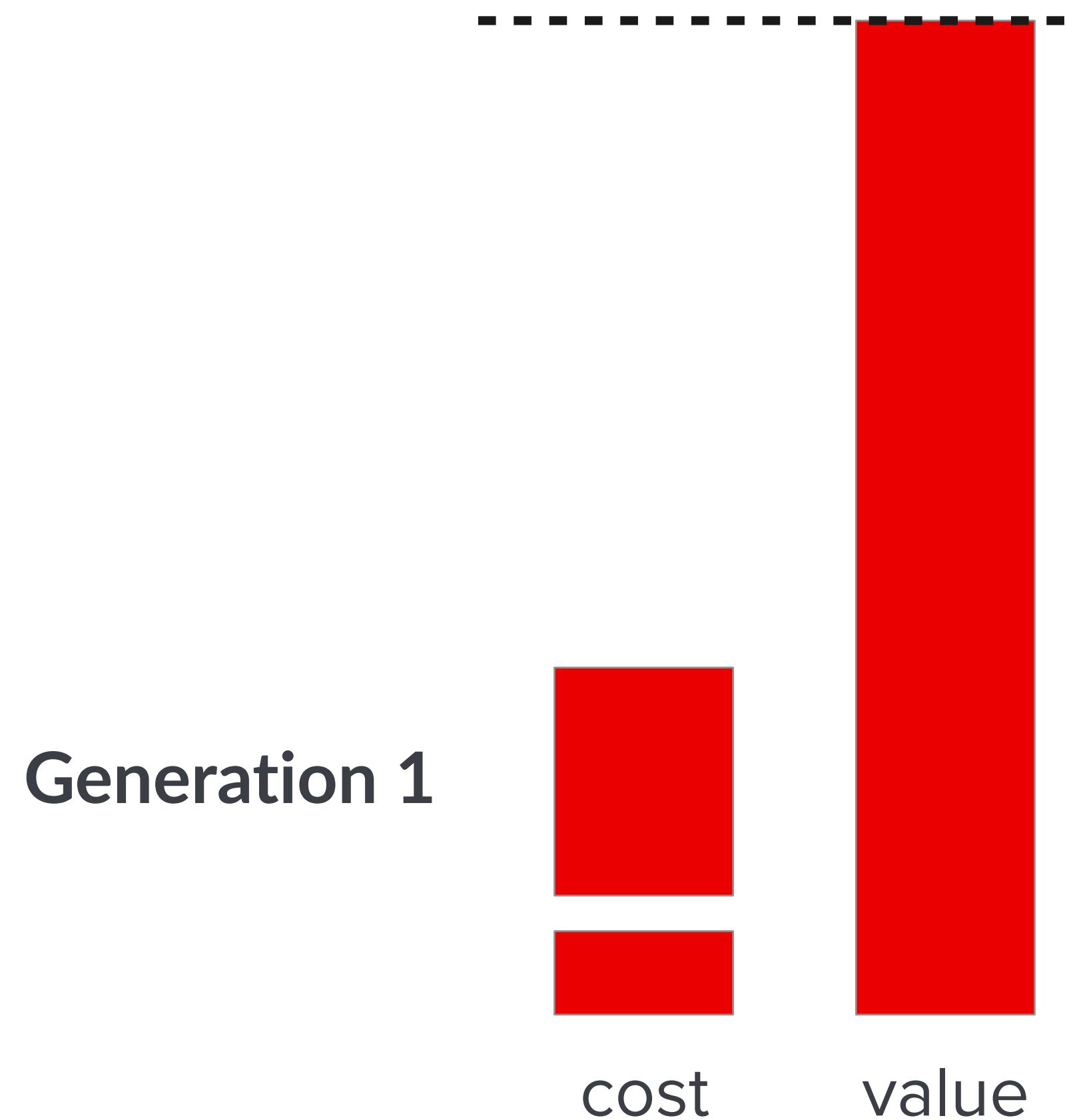


The same reason anything evolves. Incentive + adversity.

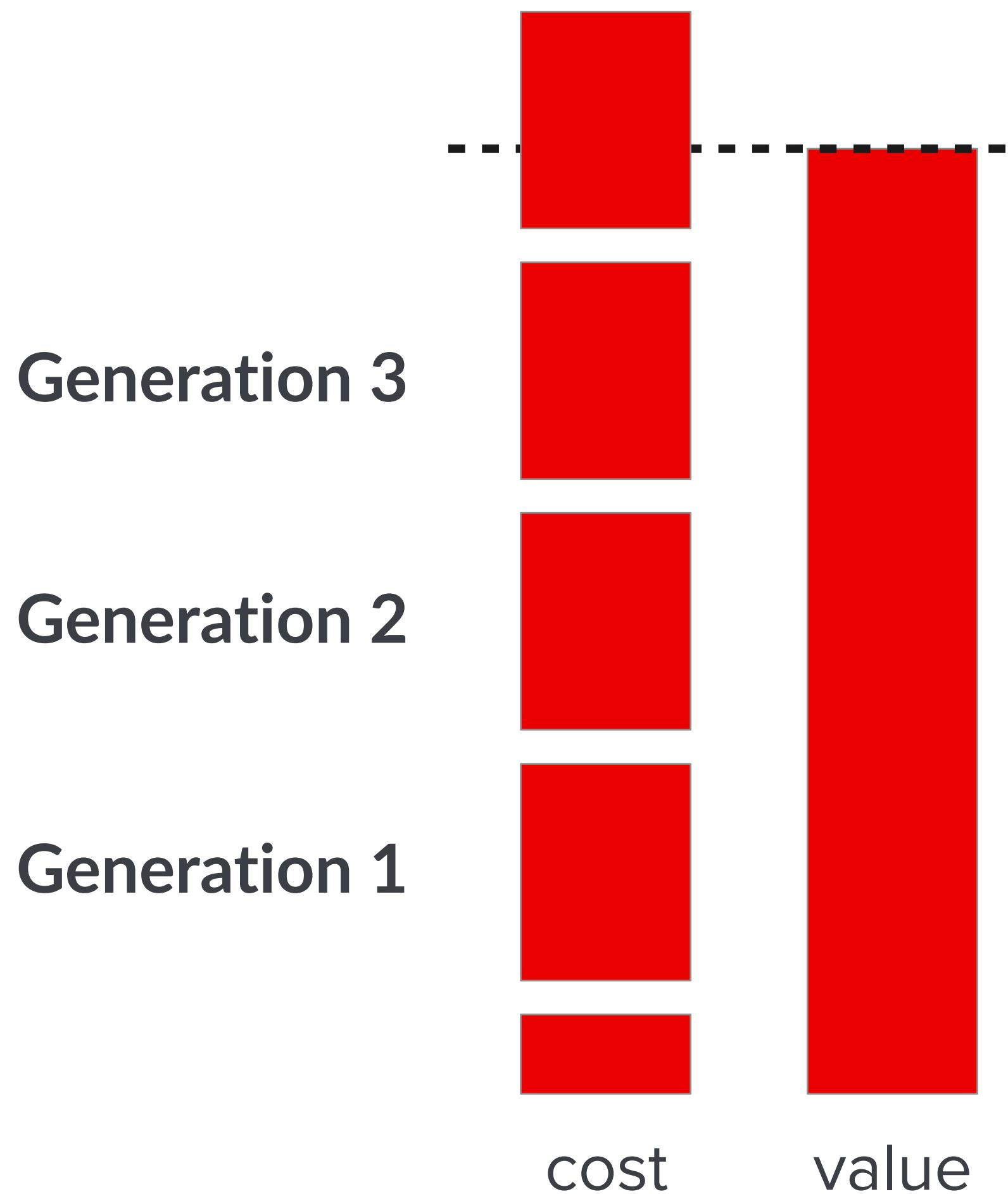
# If there are no defenses in place, the cost is nearly zero.



# Any defense increases the cost by forcing a generational shift.

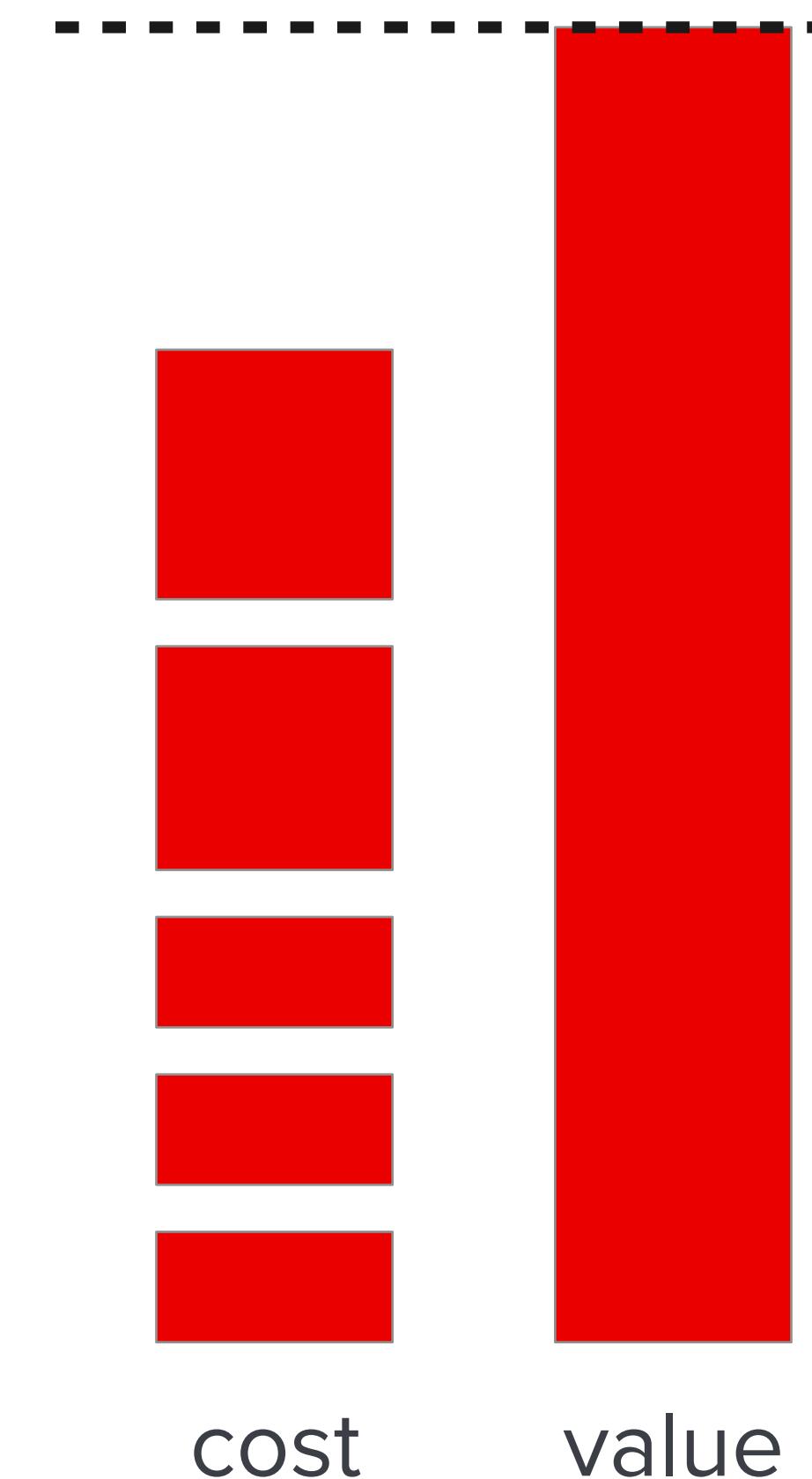


# Enough defenses will tip cost/value in your favor

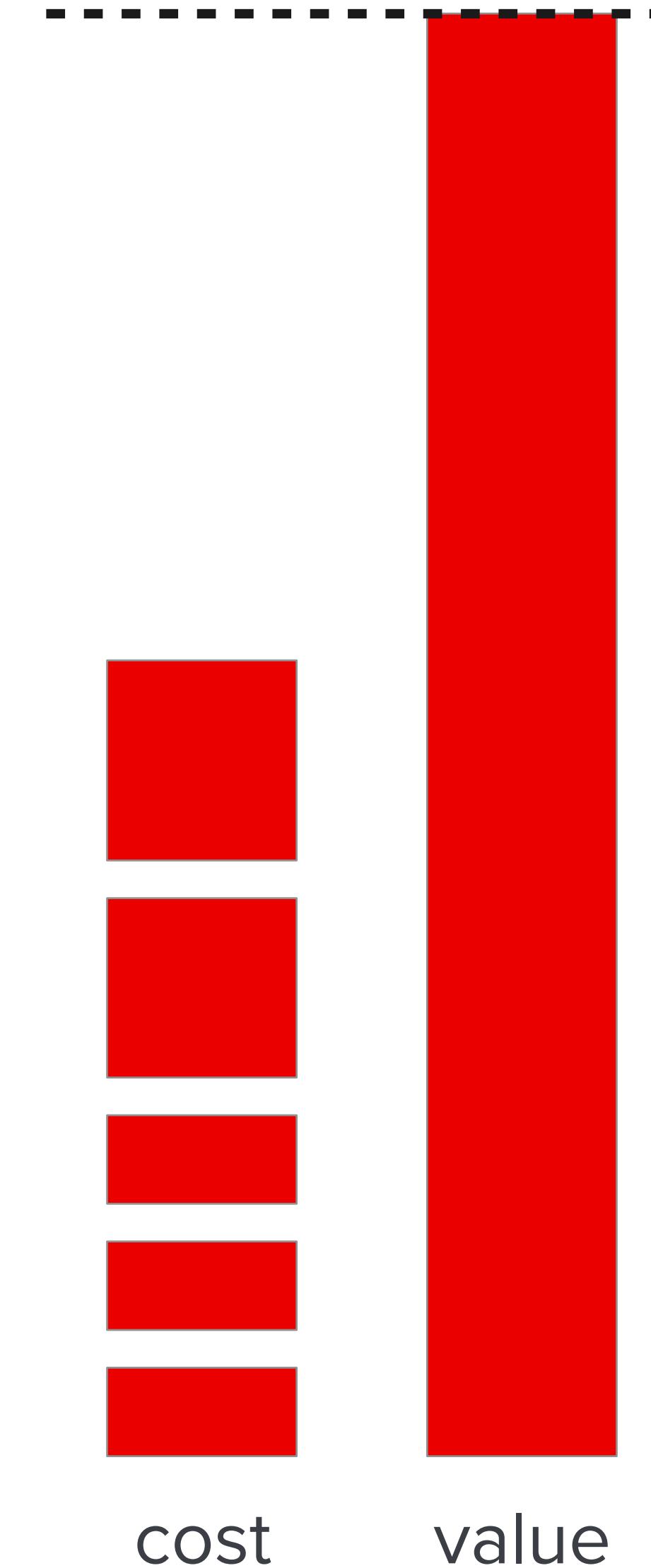


# The cost of entry for all technology decreases over time.

All technology gets cheaper as it becomes better understood and more generalized.



# While the value of successful attacks only goes up.



# MANUAL WORK

# AUTOMATION



# CREDENTIAL STUFFING: A HOW-TO GUIDE

- 1 Get Credentials
- 2 Automate Login
- 3 Defeat Existing Defenses
- 4 Distribute Globally

# CREDENTIAL STUFFING

Bookmarks People Window Help

RF Collection #1-5 & Zabagur & A... X +

https://raidforums.com/Thread-Collection-1-5-Zabagur-AntiPublic-Latest-120GB-1TB-TOTAL-Leaked-Download

f t g+ You p

Need proof? The layout is same as troys, size is same, + here's original sales thread from owner:

### Folders & Size

Collection	Size
Collection #1	87.18 GB
Collection #2	526.11 GB
Collection #3	37.18 GB
Collection #4	178.58 GB
Collection #5	42.79 GB
AP MYR&ZABUGOR #2	24.53 GB
ANTIPUBLIC #1	102.04 GB

(Blurred as the owner is under a lot of heat right now due to the exposure of this, so done out of respect, not that i care or anything just don't want drama).

Collection #1 to #5 in .torrent form thanks to user @neob and every seeder.

Hidden Content:  
Unlock for 8 credits.

# CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login

The image displays a complex software interface for automating tasks, likely a screenshot of a screenshot. The main area shows a workflow editor with various nodes connected by arrows:

- A top node displays statistics: Thread Number: {{threads}}, Success Number: 100000, Fail Number: 100000, and Selected: 2.
- Below it is a "Move And Click On Element" node with a "Sign in" button.
- An "For" loop node follows, with the condition 1 : {{clicks}}. It contains the instruction: Do clicks for {{clicks}} times. This action starts loop.
- Inside the loop:
  - An "Is Element Exists" node with the condition >CSS> a IS\_EXISTS. Description: Checking if there is any link on page.
  - An "If" node with the condition !IS\_EXISTS. Description: Break loop if there is no links.
  - A "Break" node.
  - A "Get Element Count" node with the condition >CSS> a LINK\_COUNT. Description: Get total link count.
  - A "Random Number" node with the condition LINK\_INDEX. Description: Get random link index.
  - A final "Move And Click On Element" node with the condition >CSS> a >AT> [[LINK\_INDEX]]. Description: Click on link.

The interface includes a toolbar at the bottom with icons for play, pause, stop, and refresh, along with a "Function:" dropdown set to "DoClicks". To the right of the workflow editor is a grid of tool icons:

- Browser (Chrome icon)
- Script logic (Puzzle piece icon)
- Tools (Wrench icon)
- Network (Wi-Fi icon)
- Waiters (Hourglass icon)
- Manual browser control (Power button icon)
- Filesystem (Folder icon)
- Fingerprint switcher (Fingerprint icon)
- Idle emulation (Clock icon)
- Image processing (Image icon)
- Regular expressions (Magnifying glass icon)
- Resources (AB) (Database icon)
- Script statistic (Pie chart icon)
- Receive sms (SMS icon)
- Telegram (Message icon)
- Timezone (Clock icon)

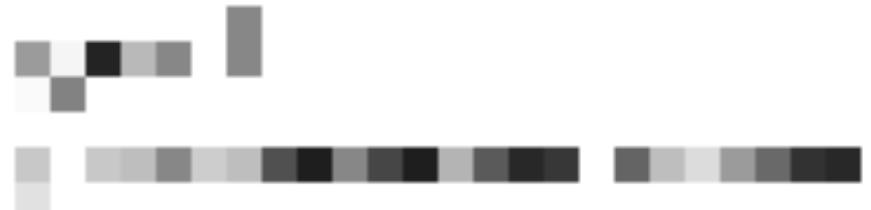
On the far right, a portion of a mobile Instagram login screen is visible, showing fields for "Mobile Number or Email", "Full Name", "Username", and "Password", along with "Sign up" and "Log in with Facebook" buttons.

# CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login

Upwork Global Inc. [US] | https://www.upwork.com/o/profiles/user... ☆ Incognito

≡ upwork



**Browser Automation Studio**

Automations like :

- + registrators on sites;
- + answering machines for messages;
- + sending e-mails;
- + work with text document (connection , disconnection text , etc.);
- + checking accounts of... [more](#)

**\$10.00**

Hourly rate

---

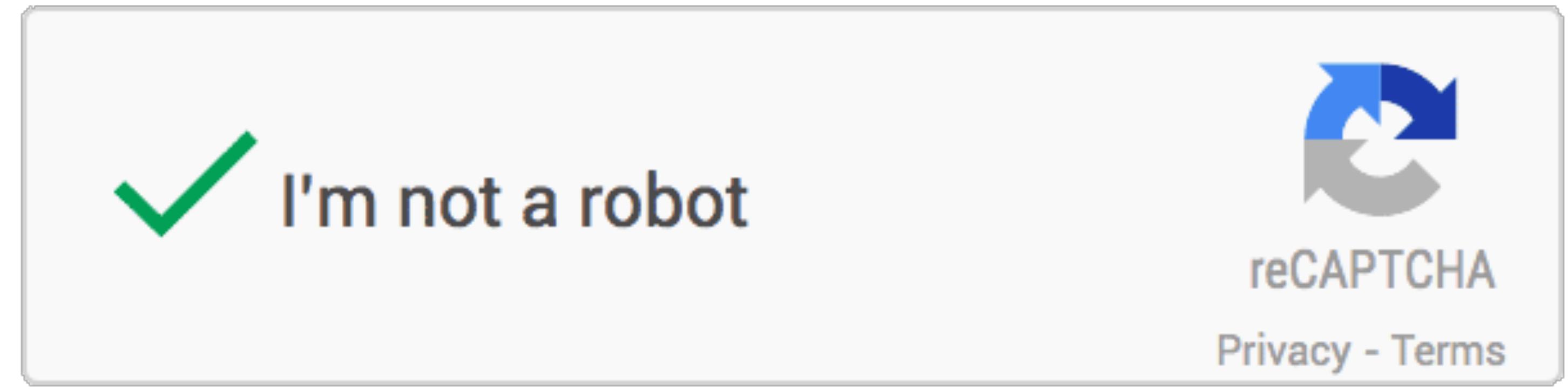
**Availability**

**Available**

More than 30 hrs/week

# CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login
3. Defeat Defenses



# CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login
3. Defeat Defenses

[Home](#)[F.A.Q.](#)[API](#)[Order CAPTCHAs](#)[DBC Points](#)[Testimonials](#)[Contact Us](#)

**STATUS: OK**

Average solving time 1 minute ago: 10 s  
5 minutes ago: 11 sec  
15 minutes ago: 11 sec  
Today's average accuracy rate: 90.5 %  
(updated every minute)

[Create a FREE account](#)

[Log In](#)

## Best CAPTCHA Solver Bypass Service

With Death by Captcha you can solve any CAPTCHA. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy!

Please note that our services should be used only for research projects and any illegal use of our services is strictly prohibited. Any bypass and CAPTCHA violations should be reported to [help@deathbycaptcha.com](mailto:help@deathbycaptcha.com)

Death By Captcha Offers:

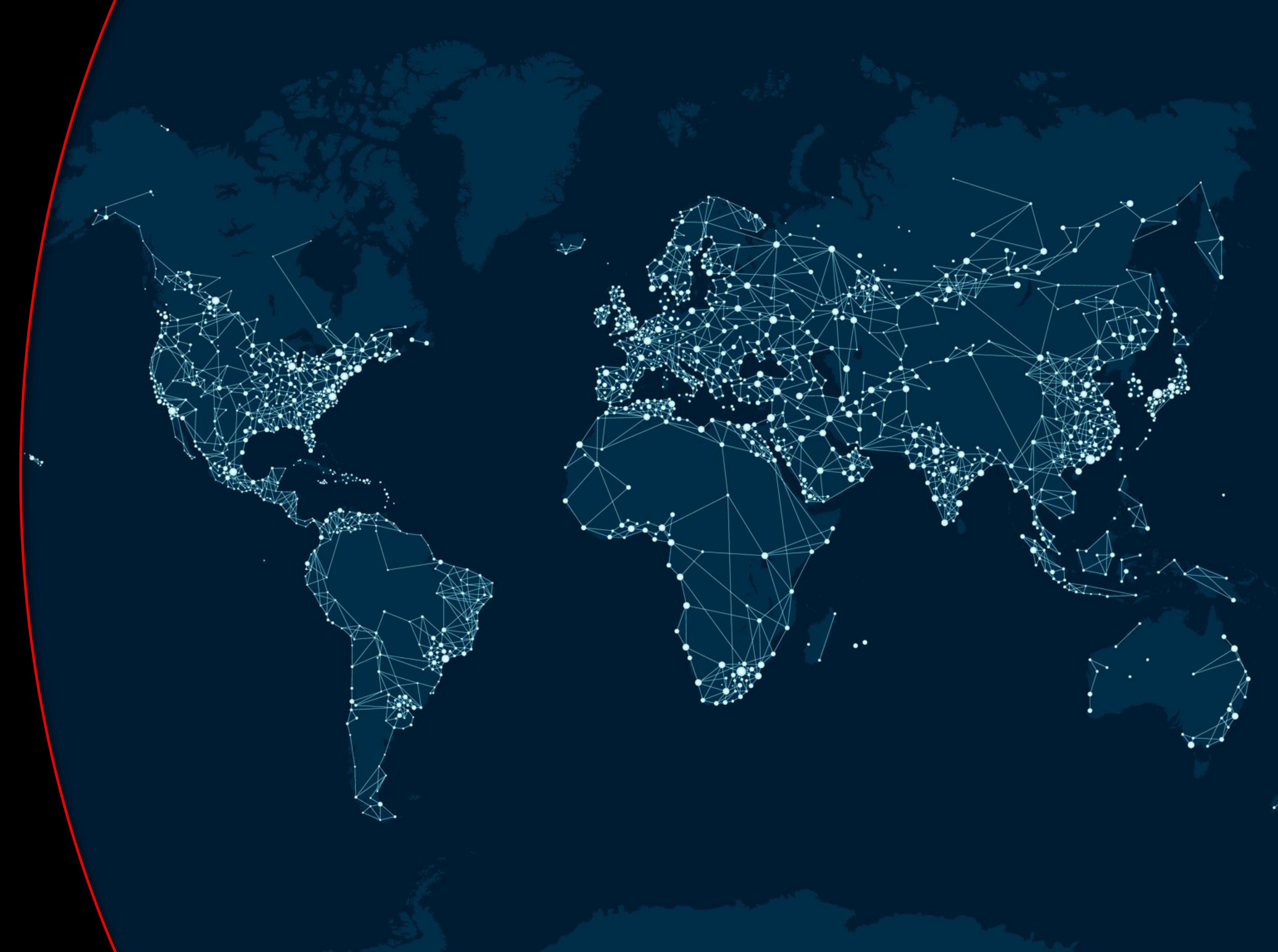
- Starting from an incredible low price of **\$1.39 (\$0.99 for Gold Members !)** for **1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.

Services CAPTCHA

- To meet TOS a user must be able to use services such as OCR based on the following methods:
  - A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.

# CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login
3. Defeat Defenses
4. Distribute



# 100,000 ATO attempts can be tried for less than \$200 USD

**\$0**

2.3 billion credentials

**\$0-50**

For tool configuration

**\$0-139**

For 100,000 solved  
CAPTCHAs

**\$0-10**

For 1,000 global IPs

**<\$0.002**

per ATO attempt.

# The rate of return is between 100% and 150,000%+

**\$2 - \$150+**

Typical range of account values.

**0.2% - 2%**

Success rate of a typical credential stuffing attack.

**\$0.002**

Cost per individual attempt.

$$\frac{\text{Value} * \text{Success Rate}}{\text{Cost}} - 100\% = \text{Rate of Return}$$

1

Why credential stuffing is evolving

2

**How credential stuffing has evolved**

3

Where do we go from here?

# Before Modern Era



# Generation 0: Basic HTTP requests with common tools

\$ |



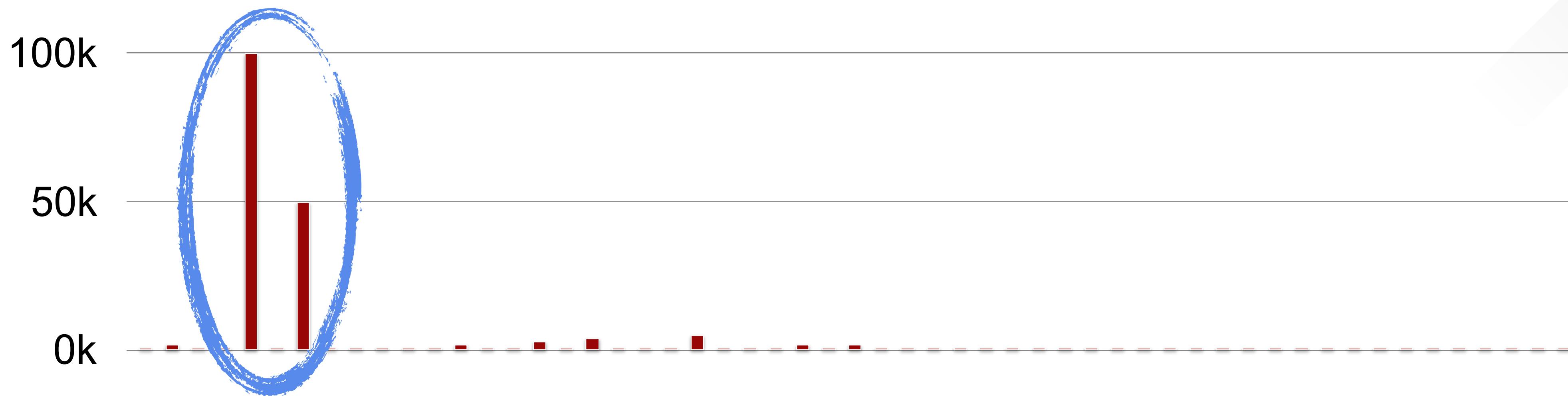
# SentryMBA

- Performs basic HTTP requests.
- Extensible and highly configurable.
- Tailored towards specific attack use cases.

The screenshot shows the SentryMBA application window. At the top, there's a toolbar with a 'Go !!' button (lightning bolt icon), an 'Abort' button (circle with a diagonal line), and a status bar showing 'Site: https://api-global.netflix.com/account/auth', 'Progress: 0%', and a 'List:' dropdown. Below the toolbar is a sidebar with a 'Settings' tab selected, containing links for General, HTTP Header, Proxy Settings, Fake Settings, and Keywords. The main configuration area is divided into several sections:

- Site Settings:** Timeout (s): 20, Bot relaunch delay (s): 0,  Resolve Hostname.
- Combo Settings:**  <USER>:<PASS> filter: Apply same rules for <USER> and <PASS>, Minimum Length: 6, Maximum Length: 8,  Letters,  Digits,  Alphanumeric,  Email, Forbidden Chars: [redacted], Allowed Chars: [redacted],  Lowercase and Uppercase,  Letter and Digit,  Special Character,  <EMAIL> filter: Must Be Email.
- General Settings:**  Save automatically valid usernames and expired combos,  Save automatically "To Check" combos,  Annoying sound on Hit -> [redacted] Browse,  Popup Memo containing Hit debug information,  Minimize to Tray,  Float Statistics in Progression,  Detect "network lost" conditions while bruteforcing, Progression updates: 0.
- Snap Shots:**  Enable Snap Shots,  Load Settings from Snap Shot (\*.ini),  Save Settings to Snap Shot.
- Images Database:**  Update Images Database from Directory,  Update Images Database from File.

# Early defense: IP Rate limiting.

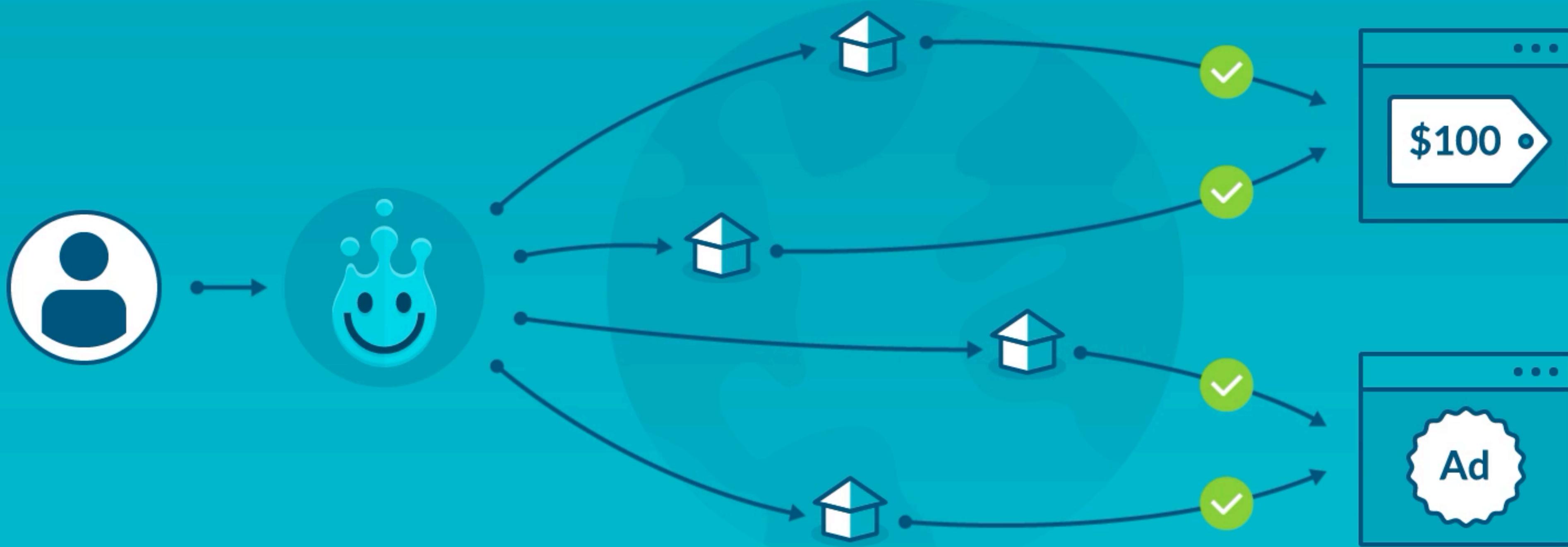


Free Proxy List						FREE PROXY	WEB PROXY	SOCKS PROXY	BUY PROXY	COMPANY	
Show 20 entries		Search all columns:									
IP Address	Port	Code	Anonymity	Https							
185.122.44.218	36805	IT	elite proxy	yes							
41.39.125.250	23500	EG	elite proxy	yes							
197.211.245.50	53281	ZW	elite proxy	yes							



Iteration 1 : Rotate through proxies

# Luminati – Residential proxy network



Every country and every city in the world



# Unblock any website

Used by over **190 million** people worldwide

Click to install Hola VPN

Start

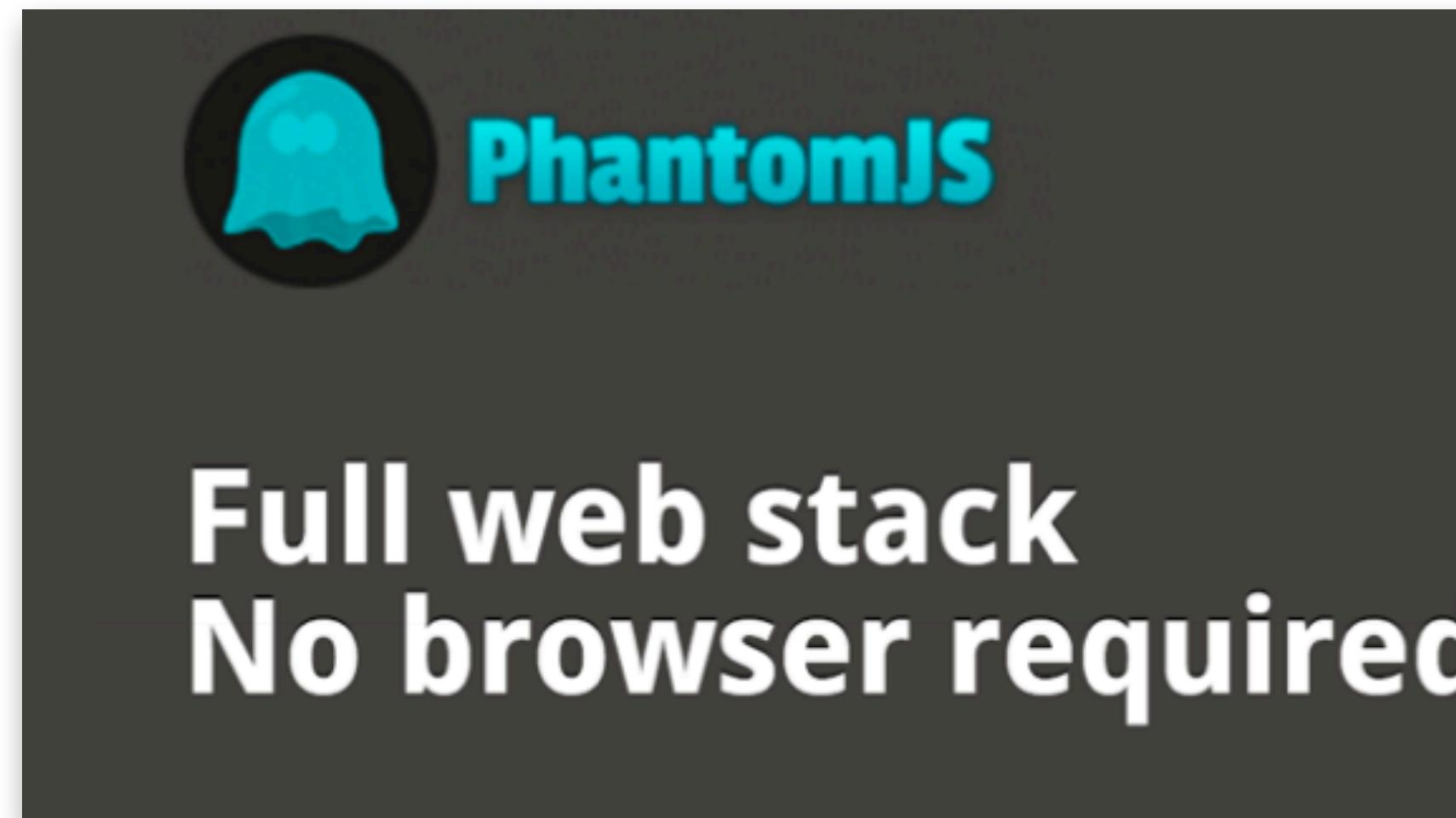
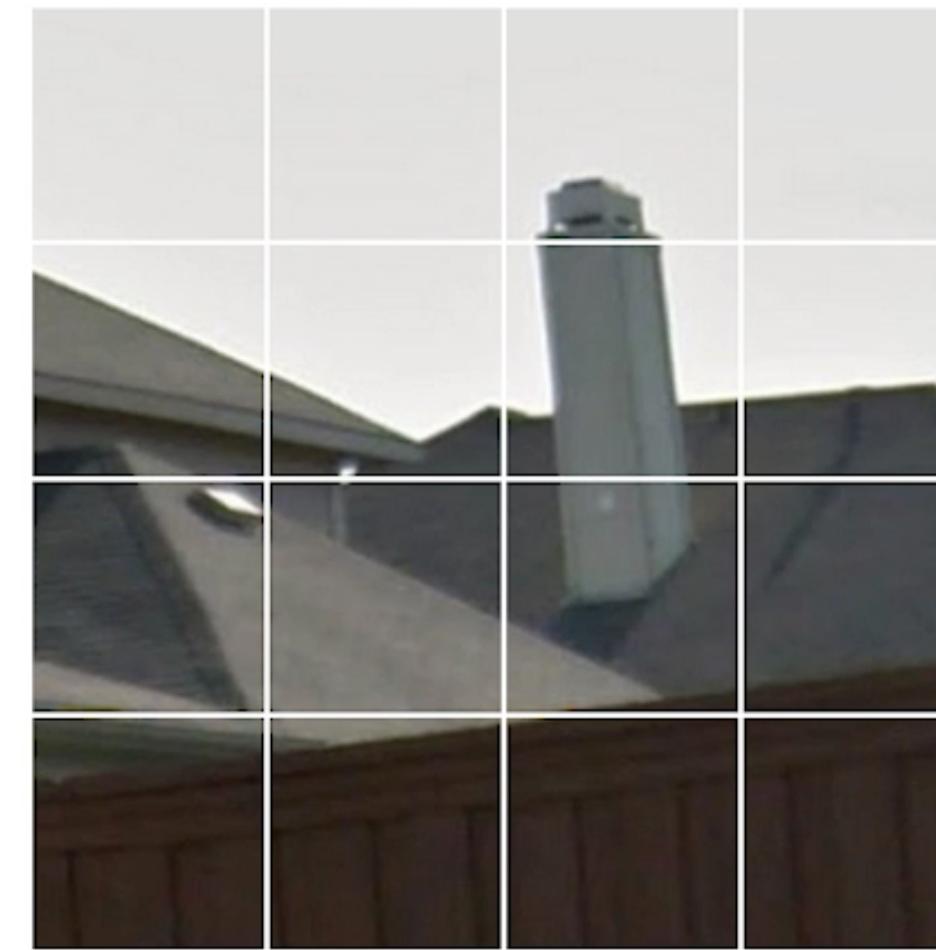
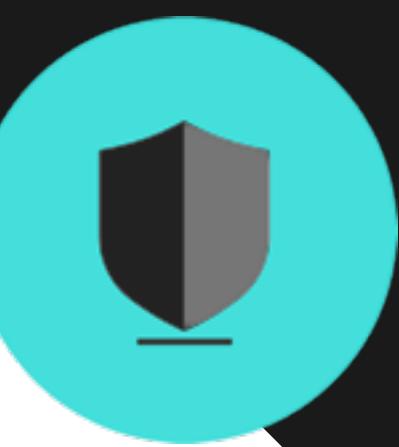
# Defense: Text-based CAPTCHAs



**Iteration 2: Use CAPTCHA Solvers.**



# Defense: Dynamic sites and JavaScript heavy defenses.



Iteration 3: Scriptable WebViews





# Defense: Header Fingerprinting & Environment Checks



```
GET / HTTP/1.1
Host: localhost:1337
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
```

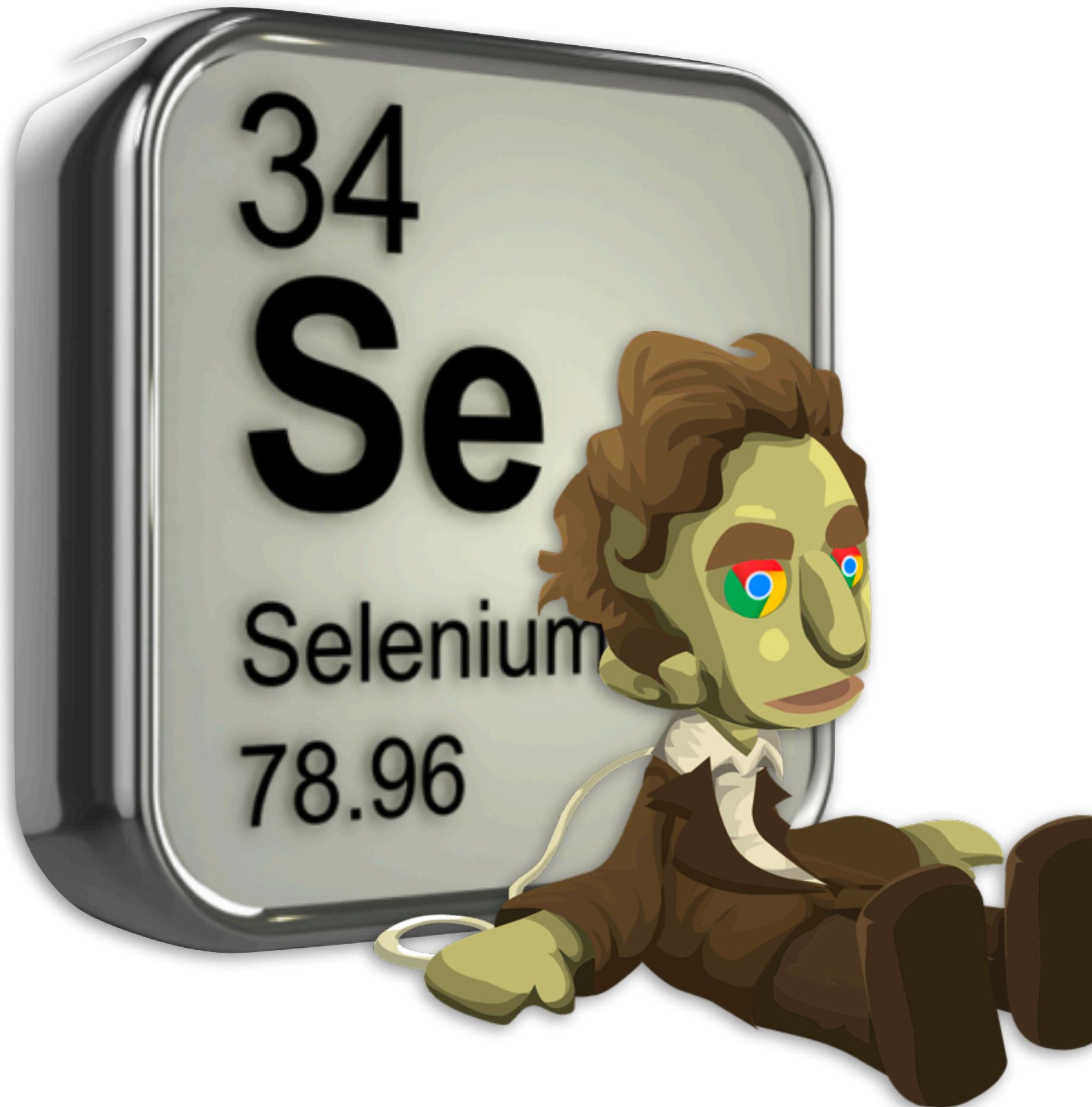


```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.8 Safari/534.34
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US, *
Host: localhost:1337
```

# **Modern Era**



# Iteration 4: Scriptable Consumer Browsers



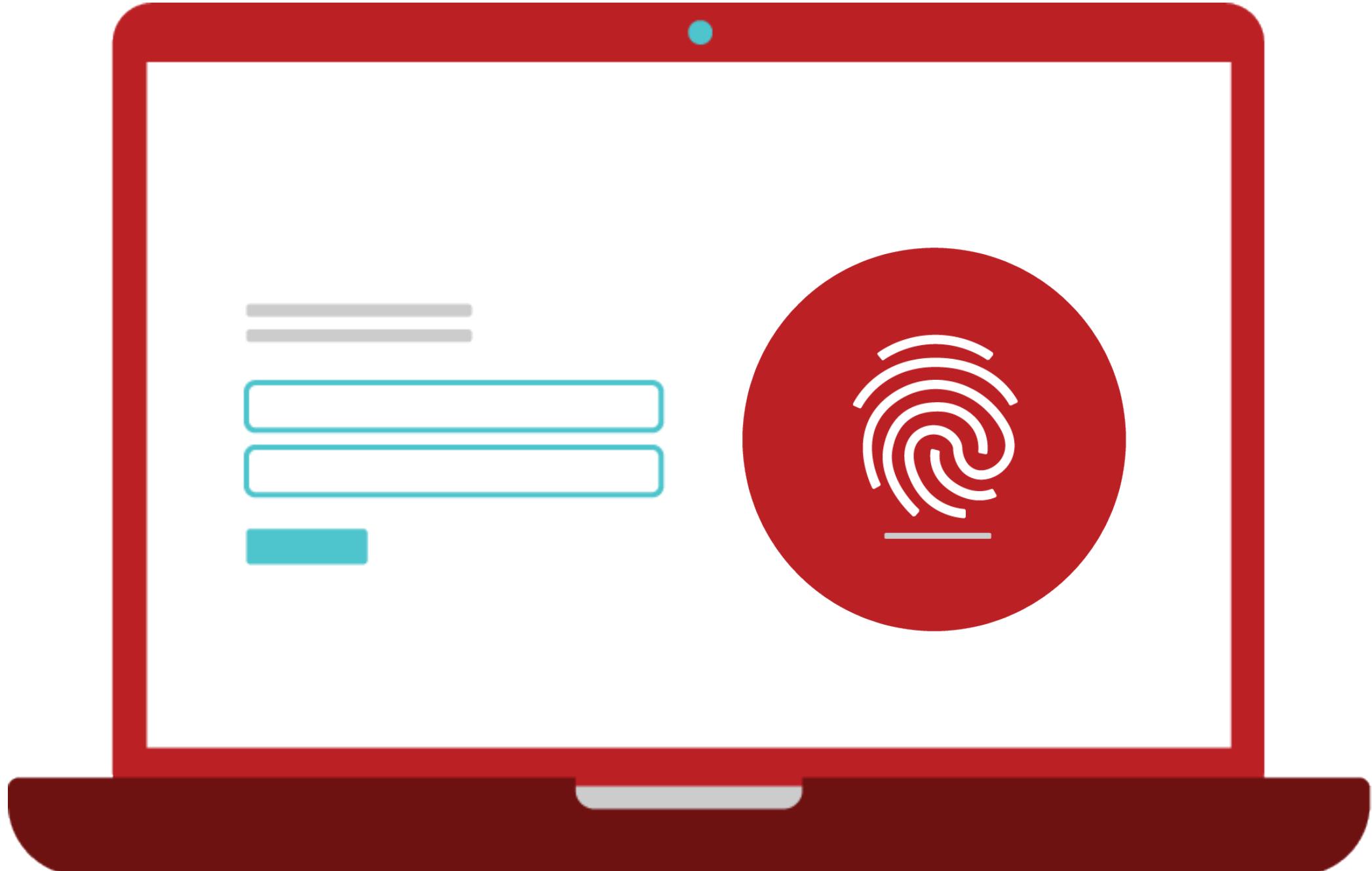
## Selenium & Puppeteer

---

Selenium is a free, open source testing tool that scripts popular browsers.

Puppeteer is a Google project that automates Firefox and Chromium based browsers.

# Defense: Browser Fingerprinting



## Browser Fingerprinting

High-entropy data points are collected to produce an acceptably unique fingerprint.

Data points like screen size, fonts, plugins, hardware profiles, et al.

This identifies the source of traffic even when tunneling through proxies.



# Iteration 5: Randomizing Fingerprint Data Sources



## FraudFox & AntiDetect

FraudFox is a VM-Based anti-fingerprinting solution.

AntiDetect randomizes the data sources that are commonly used to fingerprint modern browsers.

The screenshot shows the homepage of the FraudFox website. The header includes a browser window icon and the text "FraudFox | The most advance a...". The address bar says "Not Secure | fraudfox.net". Below the header is a large blue banner with the FraudFox logo (a blue fox head) and the text "SUBSCRIBE NOW". To the right of the banner is a menu icon (three horizontal lines) and the text "ULTIMATE INTERNET PRIVACY" and "VIRTUAL MACHINE BASED SOLUTION TO BEAT BROWSER FINGERPRINTING". At the bottom of the page, there is a large call-to-action button with the text "USING INTERNET SAFELY". A footer at the very bottom reads "Virtual Machine based solution to beat browser fingerprinting. Welcome to the new era of Internet Privacy!".

# Defense: Behavior Analysis for Negative Traits



Login

Username

Password

**LOGIN**

Not registered? [Create an account](#)



## Behavior Analysis

Naive bots give themselves away by ignoring normal human behavior.

Humans don't always click in the upper left hand corner and don't type out words all at once.

Capturing basic behavior can make naive automation easy to knock down.



# Iteration 6: Human Behavior Emulation

About Store



Gmail Images

Sign in



## Browser Automation Studio

BAS is an automation tool that combines CAPTCHA solving, proxy rotation, and emulated human behavior.



# Defense: Browser Consistency Checks



The screenshot shows a browser window displaying the Can I use... website at [caniuse.com/#search=ogg%20vorbis](https://caniuse.com/#search=ogg%20vorbis). The search bar contains "ogg vorbis". The results page for "Ogg Vorbis audio format" shows a global usage of 81.44%. A red circle with a gear and exclamation mark icon is overlaid on the top right of the page.

# Ogg Vorbis audio format - OTHER

Vorbis is a free and open source audio format, most commonly used with the Ogg container.

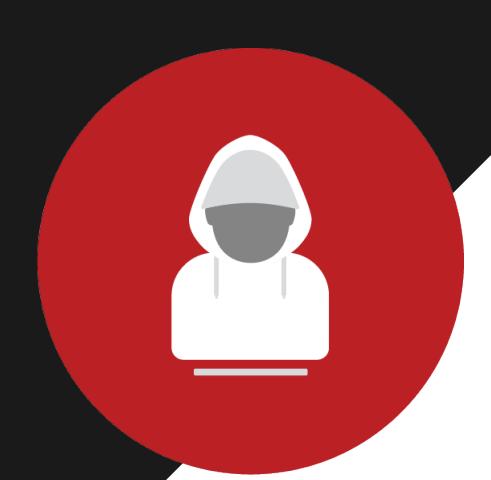
IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser
12-16	2-3	3.5-68	4-76	3.1-12	10.1	11.5-60	3.2-12.1	2.1-2.2
6-10	17	4-76	12.1	62	12.3	all	2.3-4.4.4	
11	18	69	77				76	
	76	70-71	78-80	13-TP		13		

## Validating Fingerprint Data

Good Users don't lie much.

Attackers lie a lot. They use a handful of clients but need to look like they are coming from thousands.

Those lies add up.



# Iteration 7: Use real device data

The screenshot shows a browser window titled "FingerprintSwitcher - change y" with the URL "fingerprints.bablossoft.com/#capabilities". The main content is a dark-themed list titled "CAPABILITIES" with a gear icon. It lists various browser properties with checkboxes:

Property	Value
Canvas data	✓
Webgl data	✓
Video card properties	✓
Audio data	✓
Audio settings	✓
Font list	✓
Webrtc ip	✓
Browser language	✓
Timezone	✓
Plugin list	✓
Screen properties	✓
User agent	✓
Platform id	✓
Touch support	✓
Battery capacity	✓
Do not track	✓
Gamepad	✓
Geolocation	✓
Connection	✓
USB devices	✓
SVG reading	✓



## Using Real Values

Bablossoft's Fingerprint Switcher allows a user to cycle through a real browser's fingerprintable data points, reducing the number of lies present in the data.

# **This keeps going but the direction is clear.**

The end goal is perfect emulation of humans and their environments.

# **We're calling these Imitation Attacks**

Imitation attacks indicate sophisticated fraud from dedicated adversaries.

The aim is to blend in and bypass risk & automation defenses.

Not all automation is an imitation attack, not all imitation attacks are automated.

1

Why credential stuffing is evolving

2

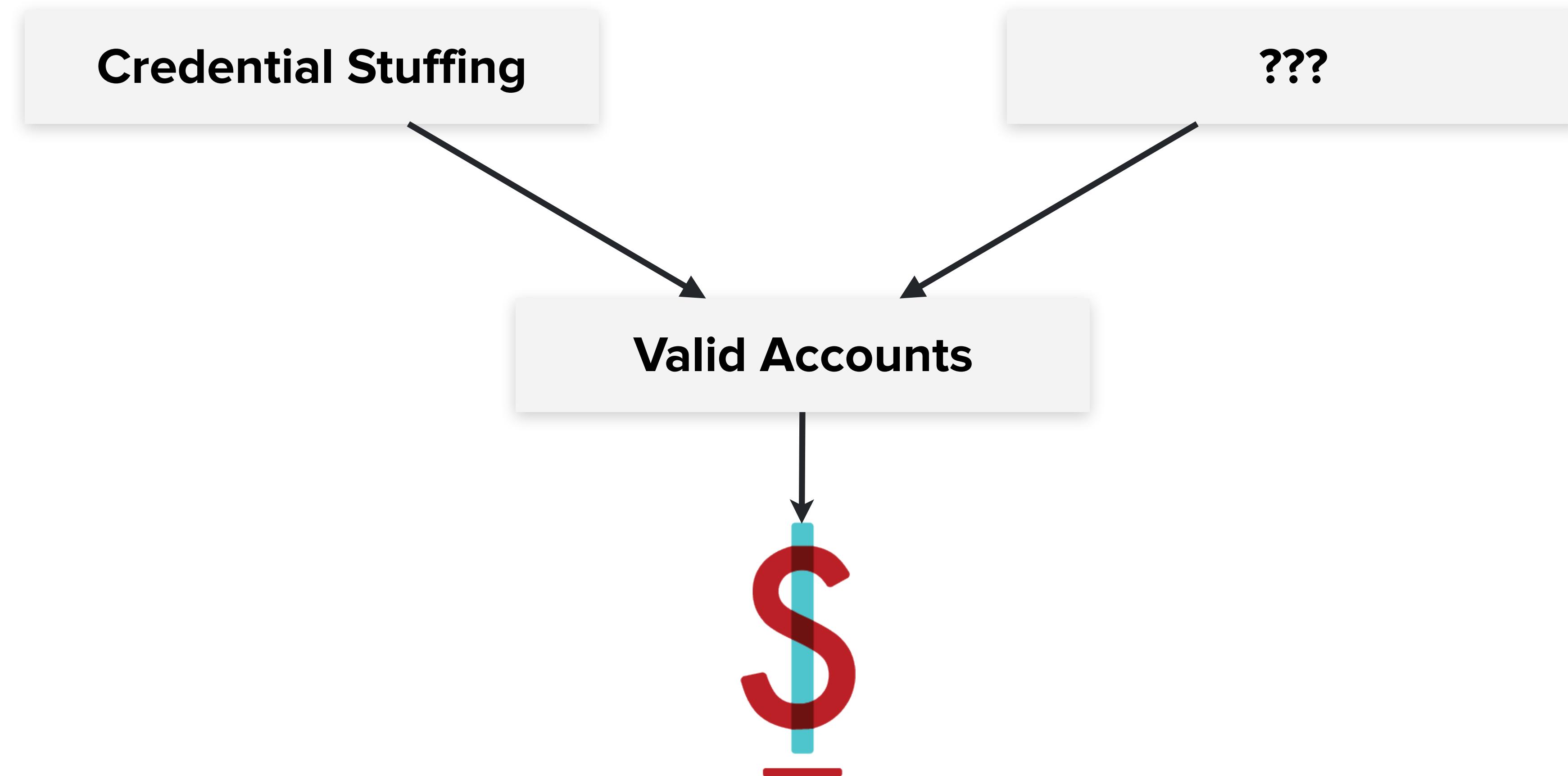
How credential stuffing has evolved

3

**Where do we go from here?**

# The value in our accounts is not going away.

As we raise the cost of credential stuffing there is greater incentive to diversify attacks.



# Genesis is an early example of what's next.

Malware that resides on the victim to scrape account and environment details.

The screenshot shows the Genesis malware interface, specifically the 'Bots' section. The left sidebar includes links for Dashboard, Genesis Wiki, News, Bots (127417), Generate FP, Orders, Purchases (1), Payments, Tickets, Genesis Security, Profile, Invites, and Logout. The main area displays harvested data in three sections:

- User-PC\_4f8c81e4141433310c57**: Bot name is 'User-PC\_4f8c81e4141433310c57'. It was active on 2018-04-29 22:10:22 and 2018-10-30 21:10:41. Resources known/other include TDBank, iCloud, Dropbox, CanadianTireBank, UPS, BigCommerce, Kijiji, Skype, Google, Live, Twitter, AppleStore, Tumblr, Cisco, and Indeed. The bot is located in CA, running on Windows 7 SP1, with a price of 81.50 CAD. A 'Sale' button is present.
- CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB**: Bot name is 'CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB'. It was active on 2019-09-17 23:39:24 and 2019-09-18 08:10:27. Resources known/other include LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber, Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend, Facebook, Dropbox, Marriott, Homeaway, and GitHub. The bot is located in CA, running on Windows 7 Professional, with a price of 52.00 CAD.
- com.ebates**: Bot name is 'com.ebates'. Resources known/other include com.contextlogic.wish, com.fitbit.Fitbit..., and ...other 370.
- com.facebook.katana**: Bot name is 'com.facebook.katana'. Resources known/other include ...known 114 and ...other 1529.
- com.ebates**: Bot name is 'com.ebates'. Resources known/other include ...known 369 and ...other 1529.

At the bottom, there is a footer with the text '© 2018-2020 34449234 73458555'.

# Thousands of infections and growing

 genesis

Dashboard Home / Bots Genesis Wiki new

News 10 Bots

Bots 127417

Generate FP Orders Purchases 1 Payments Tickets Genesis Security Profile Invites Logout

Extended Search

BOT NAME / RESOURCES KNOWN / OTHER COUNTRY / HOST PRICE ↑

Filter bot name: Any Filter resource name/domain: paypal,ebay.com,hotmail.com... Filter IP/Country/OS Filter \$

 **Bots**

**127417**

163.00 CA 81.50 207.219... Windows 7 SP1 Sale

com.contextlogic.wish com.fitbit.Fitbit... ...other 370

CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB LinkedIn Southwest Facebook CA 207.219... Windows 7 Professional 52.00

2019-09-17 23:39:24 OfficedepotStore UnitedAirlines Dropbox

2019-09-18 08:10:27 Yahoo DisneyStore Marriott

LinkedIn Uber AppleStore Homeaway

OfficedepotStore Musiciansfriend GitHub

Yahoo

DisneyStore

AppleStore

Homeaway

Musiciansfriend

GitHub

com.ebates com.facebook.katana ...other 1529

com.ebates

com.facebook.katana

...other 1529

646

# Advertises the high profile accounts the bot has already scraped.

The screenshot shows the genesis web interface with a sidebar on the left and a main content area. The sidebar includes links for Dashboard, Genesis Wiki, News, Bots (127417), Generate FP, and Logout. The main content area is titled 'Bots' and shows a list of resources known/other. A red box highlights several entries: LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber, Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend, Facebook, Dropbox, Marriott, Homeaway, and GitHub. Below this, there are sections for com.ebates, com.facebook.katana, and ...other 1529, each with a red box around its respective list of scraped accounts. At the bottom, there is a footer section with a red box around the '...other 1529' link.

genesis

Dashboard Home / Bots

Genesis Wiki new

News 10 Bots 127417

Generate FP

Logout

CE4907E7-343A2EC6-90A14316-  
C0FF11BE-EC6281AB

2019-09-17 23:22:24  
2019-09-18 08:10:27

LinkedIn OfficedepotStore Yahoo Yelp Uber Southwest UnitedAirlines DisneyStore AppleStore Musiciansfriend Facebook Dropbox Marriott Homeaway GitHub

com.ebates com.facebook.katana ...other 1529

...other 369

0 1898 0 = 1898

LA 207.219... Windows 7 Professional 52.00

0 646 0 = 646

# Regularly updates its records with newly acquired accounts.

genesis

Dashboard Home / Bots

Bots (10) 127417 new

Filter bot name

Extended Search

COUNTRY / HOST PRICE

Filter IP/Country/OS Filter \$

2019-09-17 23:39:24

2019-09-18 08:10:27

User-C 4f8... 2018-04-29 22:10:22 2018-10-30 21:10:41

Dropbox CanadianTireBank UPS Skype Google Live Twitter AppleStore Tumblr Cisco Indeed ...known 114

com.contextlogic.wish com.fitbit.Fitbit... ...other 370

CE4907E7-343A2EC6-90A14316- CDEE11BE-EC6281AB 2019-09-17 23:39:24 2019-09-18 08:10:27

LinkedIn Officedepotstore Yahoo Yelp Uber Southwest UnitedAirlines DisneyStore AppleStore Musiciansfriend Facebook Dropbox Marriott Homeaway GitHub ...known 369

com.ebates com.facebook.katana ...other 1529

0 1898 0 = 1898

207.219... Windows 7 Professional 52.00

163.00 81.50 Sale

Logout

CE4907E7-343A2EC6-90A14316- CDEE11BE-EC6281AB 2019-09-17 23:39:24 2019-09-18 08:10:27

0 646 0 = 646

0 1482 0 = 1484

207.210... Windows 7 SP1

# Each bot and its data is sold as one unit

The screenshot shows the genesis platform interface. On the left is a sidebar with various menu items: Dashboard, Genesis Wiki, News (10), Bots (127417, highlighted), Generate FP, Orders, Purchases (1), Payments, Tickets, Genesis Security, Profile, Invites, and Logout. The main area is titled "Home / Bots" and shows a list of bots. One bot is highlighted with a red box and a large red arrow pointing to a detailed view of its data. The detailed view shows the following information:

**Bot Details:**

- IP: CA  
Country: CA  
Public IP: 207.219...  
OS: Windows 7 Professional
- Price: \$52.00
- Icons: Computer monitor, hourglass, shopping basket.

**Bot Statistics:**

- Known: 114
- Other: 370

**Associated Data:**

- CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB  
Last Seen: 2019-09-17 23:39:24  
Last Activity: 2019-09-18 08:10:27
- LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber, Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend, Facebook, Dropbox, Marriott, Homeaway, GitHub
- com.ebates, com.facebook.katana, ...other 1529
- ...known 369

**Bottom Navigation:**

- Logout

# Bot detail page

genesis ≡

0 Green

[Dashboard](#) [Home / Bots / User-PC\\_4f8c81e4141433310c57 / View Details](#)

[Genesis Wiki](#) new

[News](#) 10

[Bots](#) 127416

[Generate FP](#)

[Orders](#)

[Purchases](#) 1

[Payments](#)

[Tickets](#)

[Genesis Security](#)

[Profile](#)

[Invites](#)

[Logout](#)

**User-PC\_4f8c81e4141433310c57** Sale

Country: CA  
Resources: 484  
Browsers: 0  
Installed: 2018-04-29 22:10:22  
Updated: 2018-10-30 21:10:41  
Ip: 207.210...  
Os: Windows 7 SP1  
Price Usd: 81.50

Add to Cart Reserve Buy

Browsers for Genesis Security: No Info

Last update info: 1970-01-01 00:00:00

Resources: 484 = 1 482 ⚡ 1

Know resources: 114

<a href="#">Facebook</a>	18	<a href="#">Google</a>	17	<a href="#">Live</a>	16	<a href="#">Kijiji</a>	8	<a href="#">Ebay</a>	6	<a href="#">Twitter</a>	5
<a href="#">Netflix</a>	5	<a href="#">Amazon</a>	4	<a href="#">AppleStore</a>	4	<a href="#">PayPal</a>	3	<a href="#">Instagram</a>	3	<a href="#">TDBank</a>	2
<a href="#">4Shared</a>	2	<a href="#">SonyEnter...</a>	2	<a href="#">UPS</a>	2	<a href="#">AutoTrader</a>	2	<a href="#">Capitalon...</a>	2	<a href="#">Groupon</a>	1
<a href="#">BigCommerce</a>	1	<a href="#">iCloud</a>	1	<a href="#">Dropbox</a>	1	<a href="#">Tumblr</a>	1	<a href="#">Cisco</a>	1	<a href="#">CanadianT...</a>	1
<a href="#">Indeed</a>	1	<a href="#">Payless</a>	1	<a href="#">IndigoStore</a>	1	<a href="#">Spotify</a>	1	<a href="#">Skype</a>	1	<a href="#">Yahoo</a>	1

# Bots have hundreds of scraped resources and accounts.

The screenshot shows a web-based interface for managing scraped resources. At the top, there's a navigation bar with links for Dashboard, Genesis Wiki, News, and Bots. The Bots section is active, showing a list of bots with their names and status. One bot, "User-PC\_4f8c81e4141433310c57", is highlighted and shown in more detail. This detailed view includes a summary of resources (484 total, broken down by type like email, files, diamonds, and gold), a list of known resources (Facebook, Google, Live, etc.), and a list of browsers used for scraping. A red box highlights the resource summary and the list of known resources. A red arrow points from the bottom-left towards this highlighted area.

genesis

Dashboard Genesis Wiki News Bots 127416

Home / Bots / User-PC\_4f8c81e4141433310c57 / View Details

User-PC\_4f8c81e4141433310c57 Sale

Add to Cart Reserve Buy

Country CA

Resources: 484 = 1 482 1

Know resources: 114

Facebook	18	Google	17	Live	16	Kijiji	8	Ebay	6	Twitter	5
Netflix	5	Amazon	4	AppleStore	4	PayPal	3	Instagram	3	TDBank	2
4Shared	2	SonyEnter...	2	UPS	2	AutoTrader	2	Capitalon...	2	Groupon	1
BigCommerce	1	iCloud	1	Dropbox	1	Tumblr	1	Cisco	1	CanadianT...	1
Indeed	1	Payless	1	IndigoStore	1	Spotify	1	Skype	1	Yahoo	1

Invites Logout

Last update info: 1970-01-01 00:00:00

Resources: 484 = 1 482 1

Know resources: 114

Facebook	18	Google	17	Live	16	Kijiji	8	Ebay	6	Twitter	5
Netflix	5	Amazon	4	AppleStore	4	PayPal	3	Instagram	3	TDBank	2
4Shared	2	SonyEnter...	2	UPS	2	AutoTrader	2	Capitalon...	2	Groupon	1
BigCommerce	1	iCloud	1	Dropbox	1	Tumblr	1	Cisco	1	CanadianT...	1
Indeed	1	Payless	1	IndigoStore	1	Spotify	1	Skype	1	Yahoo	1

# Genesis can generate the fingerprints of your exact target.

This bypasses many risk-scoring mechanisms that look for activity from new devices.

 genesis ≡

\$ 0 0

[Dashboard](#) [Home / Bots / User-PC\\_4f8c81e4141433310c57 / View Details](#)

[Genesis Wiki](#) new

[News](#) 10

[Bots](#) 127416

[Generate FP](#)

[Orders](#)

[Purchases](#) 1

[Payments](#)

[Tickets](#)

[Genesis Security](#)

[Profile](#)

[Invites](#)

[Logout](#)

Last update info: 1970-01-01 00:00:00

**User-PC\_4f8c81e4141433310c57** Sale

 **Generate FP**

Windows 7 SP1  
81.50

[Country](#)  
[Resources](#)  
[Browsers](#)  
[Installed](#)  
[Updated](#)  
[Ip](#)  
[Os](#)  
[Price Usd](#)

Add to Cart Reserve Buy

**Browsers for Genesis Security:**  **NO INFO**

**Resources: 484 =**  1  482  1

Know resources: 114

  Facebook	18	 Google	17	 Live	16	 Kijiji	8	 Ebay	6	 Twitter	5
 Netflix	5	 Amazon	4	 AppleStore	4	 PayPal	3	 Instagram	3	 TDBank	2
 4Shared	2	 SonyEnter...	2	 UPS	2	 AutoTrader	2	 Capitalon...	2	 Groupon	1
 BigCommerce	1	 iCloud	1	 Dropbox	1	 Tumblr	1	 Cisco	1	 CanadianT...	1
 Indeed	1	 Payless	1	 IndigoStore	1	 Spotify	1	 Skype	1	 Yahoo	1

# Select the fingerprint you are looking for

The screenshot shows the genesis web interface. On the left, a sidebar menu is visible with various options like Dashboard, Genesis Wiki, News, Bots (127416), Orders, Purchases (1), Payments, Tickets, Genesis Security, Profile, Invites, and Logout. The 'Bots' option is highlighted with a red box and has a sub-menu item 'Generate FP' also highlighted with a red box. The main content area is titled 'User-PC\_4f8c81e4141433310c57' and includes a 'Sale' badge. It displays the message 'Step 2. Choose method of generation'. Below this, there are two dropdown menus: one for 'chrome cookies: 419 fingerprints: 0' and another for 'Windows'. At the bottom, a large blue button labeled 'Generate config' is shown. The entire main content area is enclosed in a red box.

genesis

Dashboard

Genesis Wiki

News

Bots 127416

Generate FP

Orders

Purchases 1

Payments

Tickets

Genesis Security

Profile

Invites

Logout

Home / Bots / User-PC\_4f8c81e4141433310c57 / View Details

User-PC\_4f8c81e4141433310c57 Sale

Add to Cart Reserve Buy

Step 2. Choose method of generation

Generate config

chrome cookies: 419 fingerprints: 0

Windows

Generate config

Twitter	5	
DBank	2	
Groupon	1	
LinkedIn	1	
IndigoStore	1	
Spotify	1	
Cisco	1	
CanadianTire	1	
Skype	1	
Yahoo	1	

# And load it into the Genesis Security Plugin

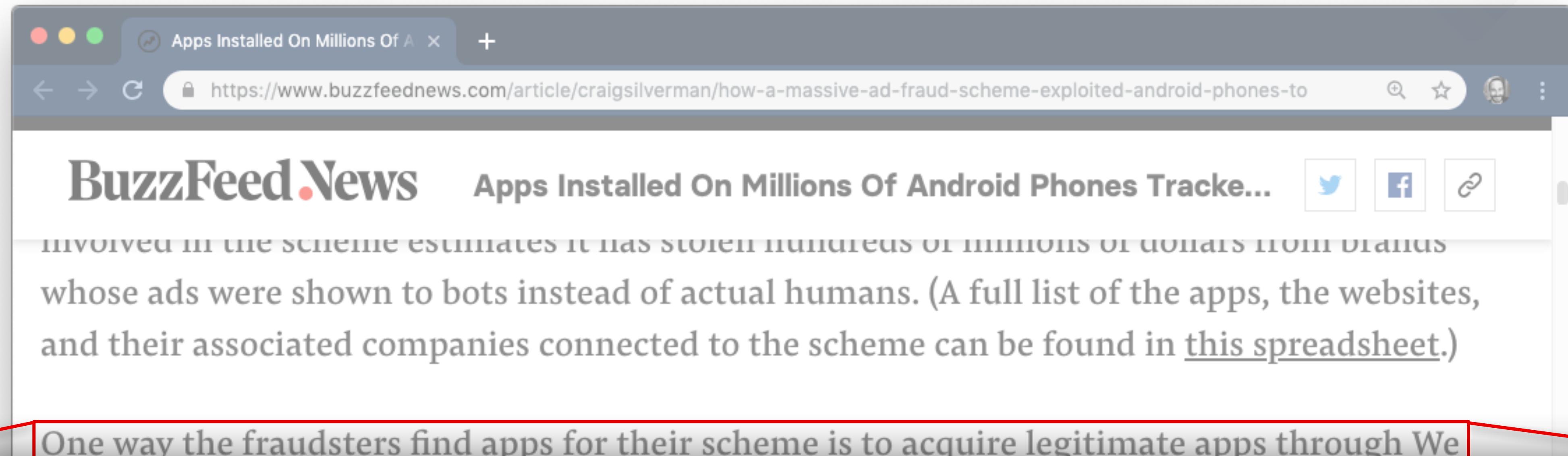
Voila! You are now your target.

The screenshot shows the genesis web interface. On the left is a sidebar with various links: Dashboard, Genesis Wiki (new), News (10), Bots (127416), Generate FP (highlighted with a red box), Orders, Purchases (1), Payments, Tickets, Genesis Security, Profile, Invites, and Logout. The main content area shows a breadcrumb path: Home / Bots / User-PC\_4f8c81e4141433310c57 / View Details. The title is "User-PC\_4f8c81e4141433310c57" with a "Sale" badge. A large green box contains the message: "Well done! 93970994-EC4E-447B-B2BD-DE2F4215A44E installed. Loaded 1 browsers. Hint: Open settings of Genesis Security plugin to manage and install bots browsers and fingerprints in to your browser. Good luck!" Below this box is a note: "Last update info: 1970-01-01 00:00:00". At the bottom, there's a summary: "Resources: 484 = 1 482 ⚳". A table titled "Know resources: 114" lists various websites and services with their counts:

Resource Type	Resource Name	Count
Facebook	Facebook	18
Netflix	Netflix	5
4Shared	4Shared	2
BigCommerce	BigCommerce	1
Indeed	Indeed	1
Google	Google	17
Amazon	Amazon	4
SonyEnter...	SonyEnter...	2
iCloud	iCloud	1
Payless	Payless	1
Live	Live	16
AppleStore	AppleStore	4
UPS	UPS	2
Dropbox	Dropbox	1
IndigoStore	IndigoStore	1
Kijiji	Kijiji	8
PayPal	PayPal	3
AutoTrader	AutoTrader	2
Tumblr	Tumblr	1
Spotify	Spotify	1
Ebay	Ebay	6
Instagram	Instagram	3
Capitalon...	Capitalon...	2
Cisco	Cisco	1
Skype	Skype	1
Twitter	Twitter	5
TDBank	TDBank	2
Groupon	Groupon	1
CanadianT...	CanadianT...	1
Yahoo	Yahoo	1

# Malware that scrapes, learns, imitates, and proxies through its victim is next

We've started seeing the signs in ad fraud.

A screenshot of a web browser window. The title bar says "Apps Installed On Millions Of A X". The address bar shows the URL "https://www.buzzfeednews.com/article/craigsilverman/how-a-massive-ad-fraud-scheme-exploited-android-phones-to". The main content area displays the BuzzFeed News logo and the headline "Apps Installed On Millions Of Android Phones Track...". Below the headline, there is a snippet of text: "INVOLVED IN THE SCHEME ESTIMATES IT HAS STOLEN HUNDREDS OF MILLIONS OF DOLLARS FROM VARIOUS whose ads were shown to bots instead of actual humans. (A full list of the apps, the websites, and their associated companies connected to the scheme can be found in [this spreadsheet](#).)".

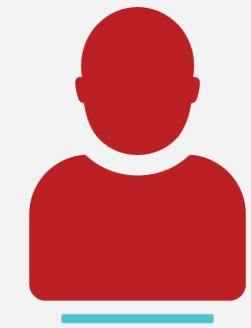
One way the fraudsters find apps for their scheme is to acquire legitimate apps through We

One way the fraudsters find apps for their scheme is to acquire legitimate apps through We Purchase Apps and transfer them to shell companies. They then capture the behavior of the app's human users and program a vast network of bots to mimic it, according to analysis from Protected Media, a cybersecurity and fraud detection firm that analyzed the apps and websites at BuzzFeed News' request.

these apps were secretly tracked as they scrolled and clicked inside the application. By copying actual user behavior in the apps, the fraudsters were able to generate fake traffic that bypassed major fraud detection systems.

# This is a human problem, not a technical problem.

There are no silver bullet solutions against humans. (Except literal silver bullets, but...)



Advanced credential stuffing is sophisticated fraud. It is more than simple automation. **Fraud teams aren't staffed for this, they need help.**



Imitation attacks are designed to blend in. **Look deeply even if you think you don't have a problem.**



Attackers are economically driven. We need to attack the economics. **Every defense will fail if the value is still there.**

# THANK YOU

Jarrod Overson

@jsoverson on twitter, medium, and github.