



FRAUD PREVENTION IS MORE THAN Bot MITIGATION

Jarrod Overson
Director of Engineering

Credential Stuffing by the numbers

A problem that has exploded.

1 Billion

New credentials spilled in 2018.

2 Billion

The record number of attacks
Shape has blocked in one day.

3 Billion

The largest recorded attack
campaign against one URL for
one company in one week.

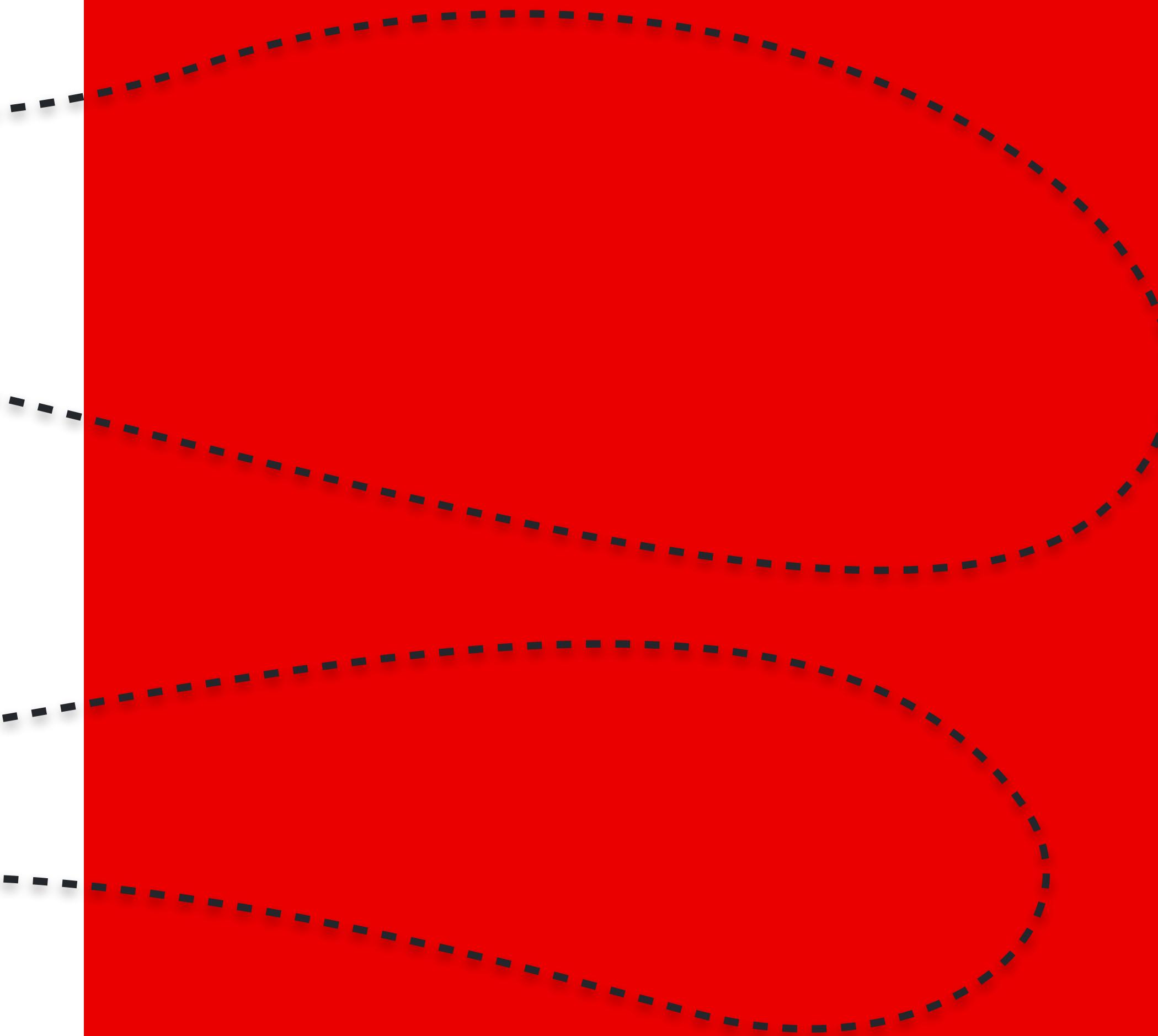
Agenda

- 1 The cost of an attack
- 2 How attacks have evolved
- 3 Where fraud goes from here

MANUAL WORK

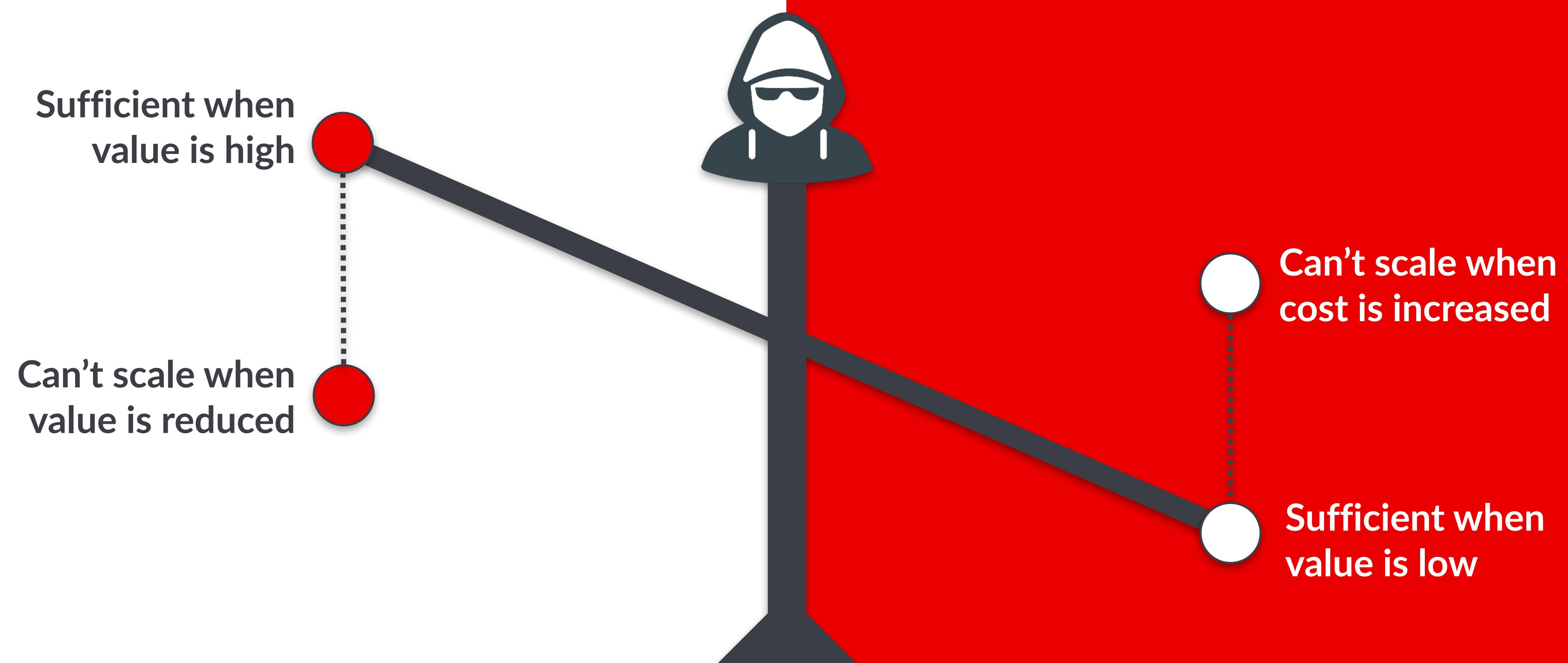


AUTOMATION



MANUAL WORK

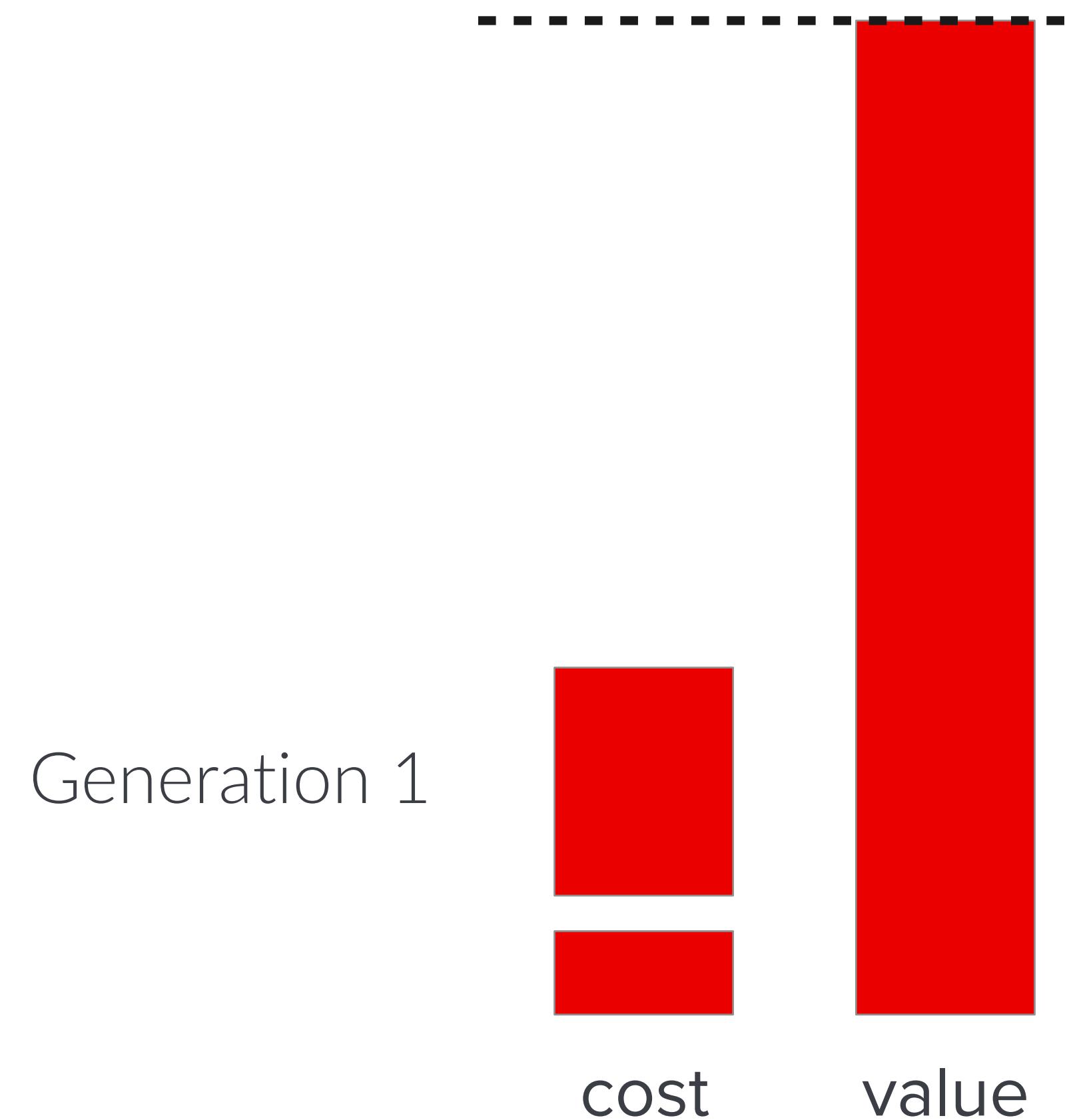
AUTOMATION



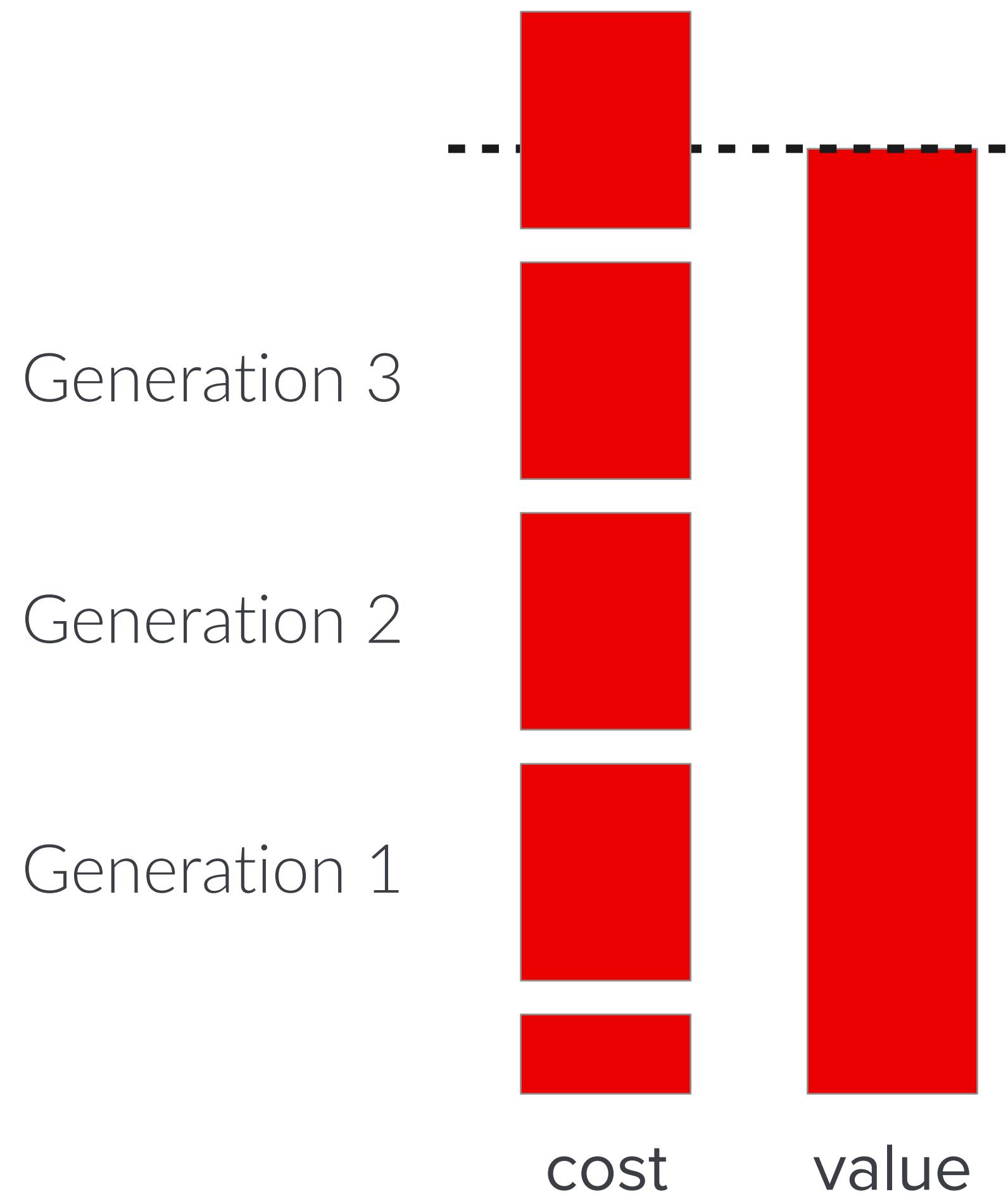
If there are no defenses in place, the cost is nearly zero.



Any defense increases the cost by forcing a generational shift.

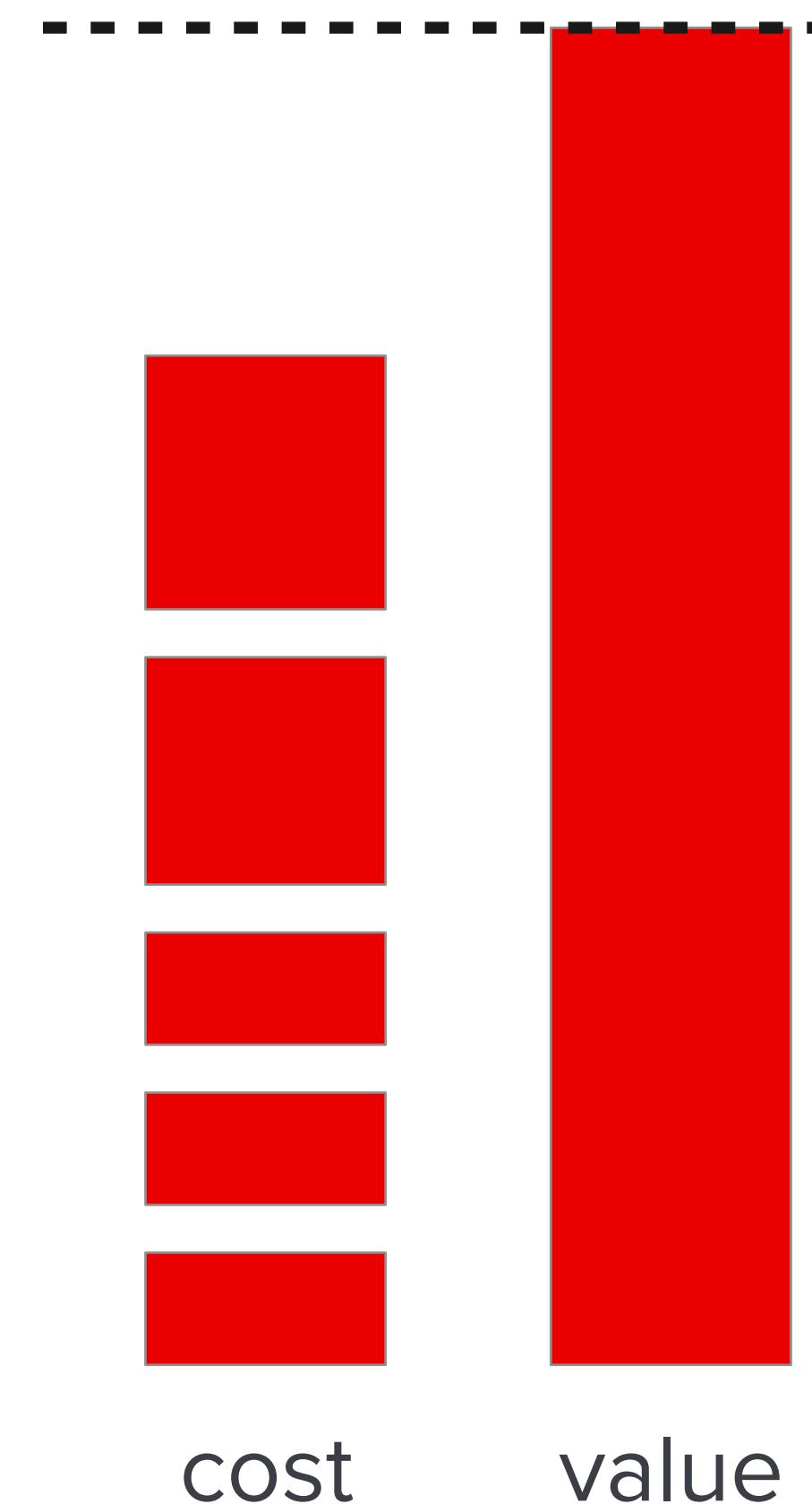


Enough defenses tip cost vs value in your favor

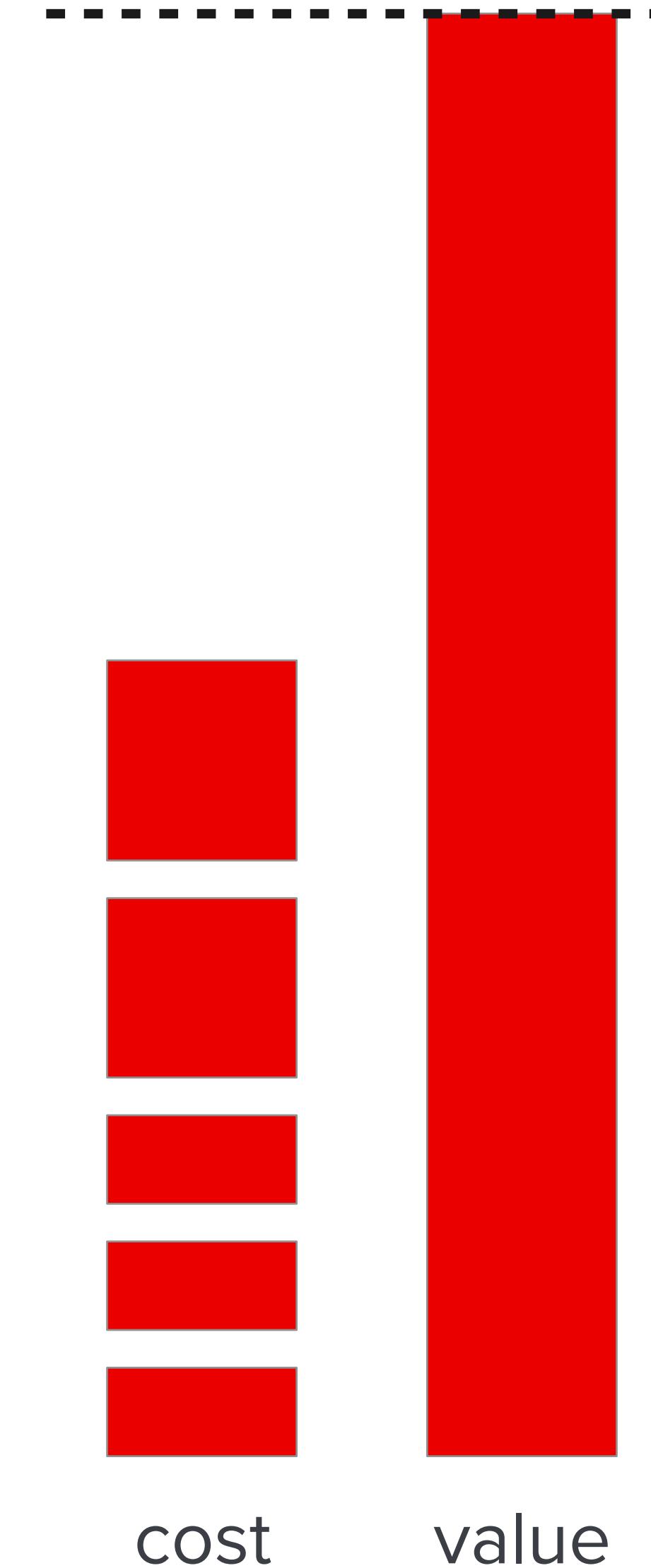


The cost of entry for each generation decreases over time.

All technology gets cheaper as it becomes better understood.



While the value of successful attacks only goes up.



CREDENTIAL STUFFING

cre·den·tial stuff·ing

/krə'den(t)SHəl 'stəfiNG/

The replay of breached username/password pairs across sites to find accounts where passwords have been reused.

STEP BY STEP GUIDE

- 1 Get Credentials
- 2 Automate Login
- 3 Defeat Automation 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 shows a complex user interface for credential stuffing. On the left, a screenshot of a software interface displays a flowchart of automation steps:

- Thread Number: {{threads}}
- Success Number: 100000
- Fail Number: 100000
- Selected: 2
- Move And Click On Element (Sign in)
- For 1 : {{clicks}}
Do clicks for {{clicks}} times.
This action starts loop.
- Is Element Exists (>CSS> a IS_EXISTS)
Checking if there is any link on page.
- If ![[IS_EXISTS]]
Break
Break loop if there is no links
- Get Element Count (>CSS> a LINK_COUNT)
Get total link count
- Random Number
LINK_INDEX
Get random link index
- Move And Click On Element (>CSS> a >AT> [[LINK_INDEX]])
Click on link.

On the right, there is a screenshot of an Instagram sign-up screen and a mobile phone displaying a succulent image.

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

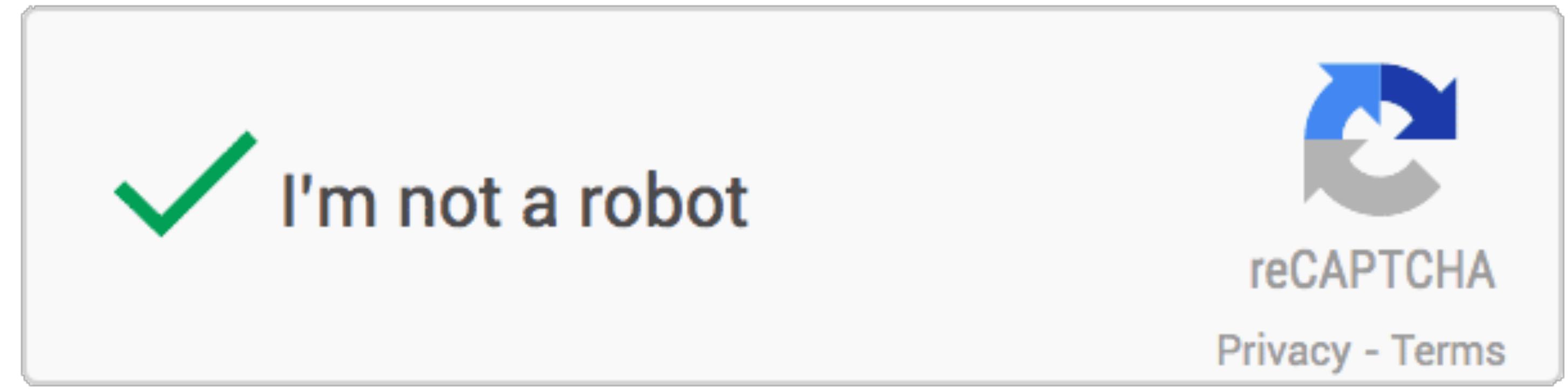
Hourly rate

Availability

Available

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

Death By Captcha Offers:

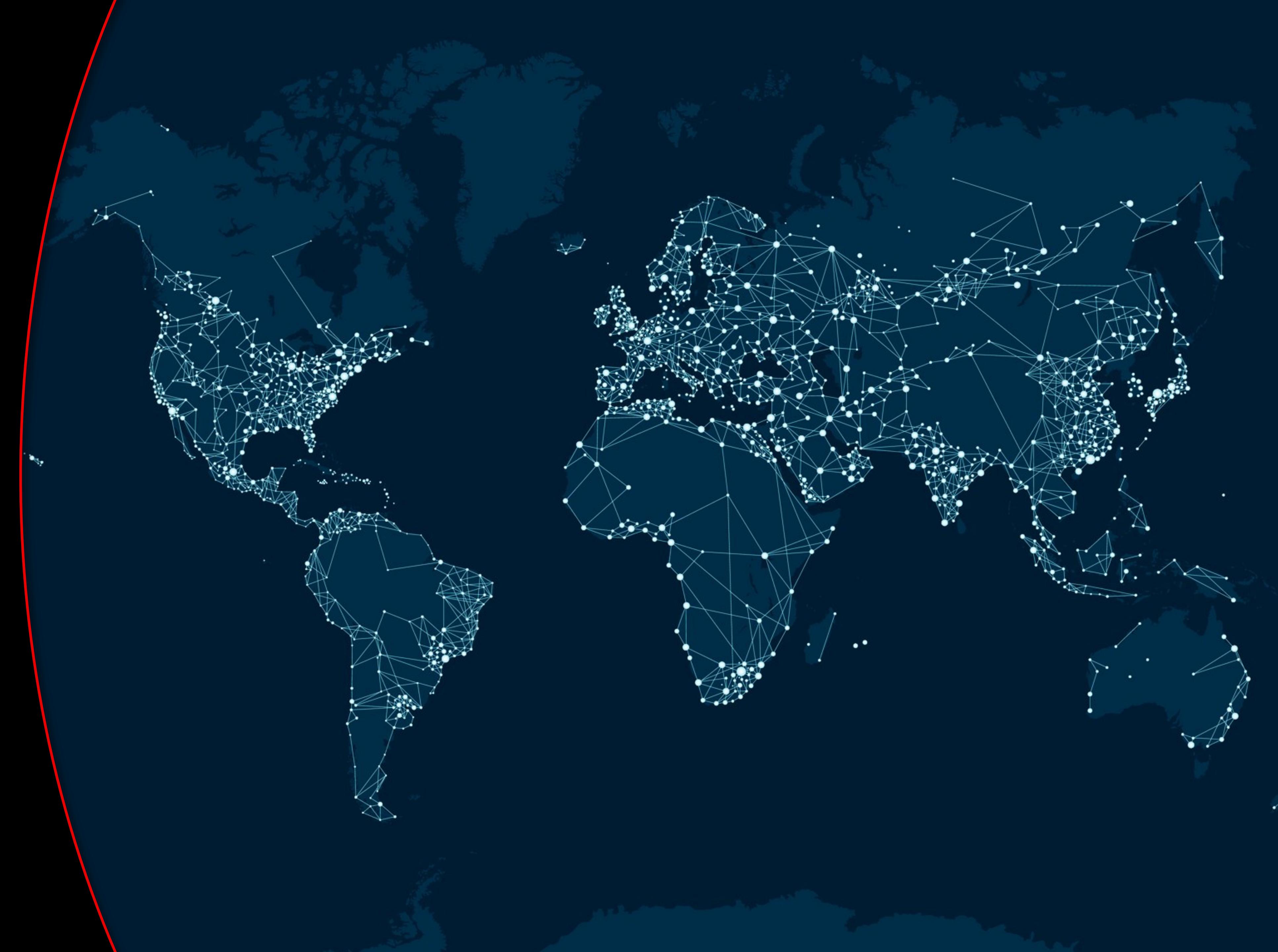
- Starting from an incredible low price of **\$1.39 (\$0.99 for Gold Members !)** for **1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.

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 value of accounts is variable, from pennies to hundreds.

A screenshot of a web browser window displaying a dark-themed application interface. The browser's title bar shows two tabs: "Search PP" and "Search". The address bar indicates the URL is <https://slilppnyhik6febe.onion/searchpp.php?submitted=1>. The main content area features a header with a green and black design featuring the letters "S", "P", and "PP". To the right, a welcome message reads "Welcome, *****" and displays a balance of "\$0.00" and items in cart totaling "0 (\$0)". Below the header is a navigation bar with buttons for "News", "Add funds", "Support", "Profile", "PayPal" (highlighted in green), "WellsFargo", "Suntrust", "More Banks", "Amazon", and "Other ShoPPs". A sidebar on the left shows "PPs in stock: 478264". At the bottom, there is a section titled "UPDATE: trikk, WTS, logs" with various input fields for managing account balances across different platforms like PayPal, BML, and Smart connect.

PPs in stock: 478264

UPDATE: trikk, WTS, logs

| | |
|--------------------|--|
| PayPal Balance: | From <input type="text"/> to <input type="text"/> <input type="button" value="▼"/> |
| Balance U.S.: | From <input type="text"/> to <input type="text"/> |
| BML: | From <input type="text"/> to <input type="text"/> |
| Smart connect: | From <input type="text"/> to <input type="text"/> |
| Credit card: | <input type="text"/> |

Amazon accounts with a last purchase price of \$613 sell for \$15

| Shop | Balance | Points | Name | Type | Country State Zip | CC | Bank | Info | Last order | Mail domain | Uploaded | Seller | Price (\$): |
|------------|---------|--------|------|----------|----------------------|-----|------|--|---------------|----------------|-------------|--------|----------------|
| amazon.com | 795.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @aim.com | 14 Mar 2019 | sec | 15 |
| amazon.com | 757.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @cox.net | 14 Mar 2019 | sec | 15 |
| amazon.com | 613.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @verizon.net | 14 Mar 2019 | sec | 15 |
| amazon.com | 436.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @cox.net | sec | 10 | |
| amazon.com | 238.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @verizon.net | 14 Mar 2019 | sec | 5 |
| amazon.com | 224.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @verizon.net | 14 Mar 2019 | sec | 5 |
| amazon.com | 223.00 | N/A | | Personal | Usa | N/A | | E-MAIL access only! Do a password reset to enter Amazon account. Balance = last order price. WITH UPDATED 2FA BYPASS METHOD! | HQ | @optonline.net | 14 Mar 2019 | sec | 5 |

Sephora accounts with 4,121 points sell for \$22.60

The screenshot shows a search results page for "sephora.com" accounts. The results are listed in a table with columns for Shop, Balance, Points, Name, Type, Country, State, Zip, CC, Bank, Info, Last order, Mail domain, Uploaded, Seller, and Price (\$). The first result, which is highlighted with a red box, shows a balance of 0.00, 4121 points, and a price of 22.60.

| Shop | Balance | Points | Name | Type | Country | State | Zip | CC | Bank | Info | Last order | Mail domain | Uploaded | Seller | Price (\$) |
|--------------------------------|---------|--------|-----------|---------|---------|-------|-----|-------------|------|------|------------|-------------|-------------|---------|------------|
| sephora.com | 0.00 | 0.00 | kim | N/A | N/A | | | N/A | N/A | N/A | N/A | @yahoo.com | 27 Feb 2019 | Mrtikov | 2 |
| sephora.com | 0.00 | 0.00 | karen | N/A | N/A | 07031 | | N/A | N/A | N/A | N/A | @aol.com | 27 Feb 2019 | Mrtikov | 2 |
| sephora.com | 0.00 | 0.00 | sandra | N/A | N/A | | | N/A | N/A | N/A | N/A | @cox.net | 27 Feb 2019 | Mrtikov | 2 |
| sephora.com | 0.00 | 0.00 | Christina | N/A | N/A | 27609 | | N/A | N/A | N/A | N/A | @yahoo.com | 27 Feb 2019 | Mrtikov | 2 |
| sephora.com | 0.00 | 235.00 | patty | N/A | N/A | 77043 | | N/A | N/A | N/A | N/A | @yahoo.com | 27 Feb 2019 | Mrtikov | 3.17 |
| sephora.com 0.00 4121.00 | | | | 4121.00 | | | | N/A N/A N/A | | | | @mac.com | 27 Feb 2019 | Mrtikov | 2.18 |
| sephora.com 0.00 4121.00 Janet | | | | N/A Us | | | | N/A N/A N/A | | | | @aol.com | 27 Feb 2019 | Mrtikov | 22.60 |
| sephora.com | 0.00 | 20.00 | Page | N/A | N/A | | | N/A | N/A | N/A | N/A | @yahoo.com | 27 Feb 2019 | Mrtikov | 2.1 |

Calculating our rate of return

\$0.002

Cost per individual attempt.

0.2% - 2%

Success rate of a typical credential stuffing attack.

\$2 - \$150+

Typical range of account values.

The rate of return on a credential stuffing attack is 100% on the low end and 150,000%+ on the high end.

Agenda

- 1 The cost of an attack
- 2 **How attacks have evolved**
- 3 Where fraud goes from here



Generation 0: Basic HTTP requests with common tools

\$ |



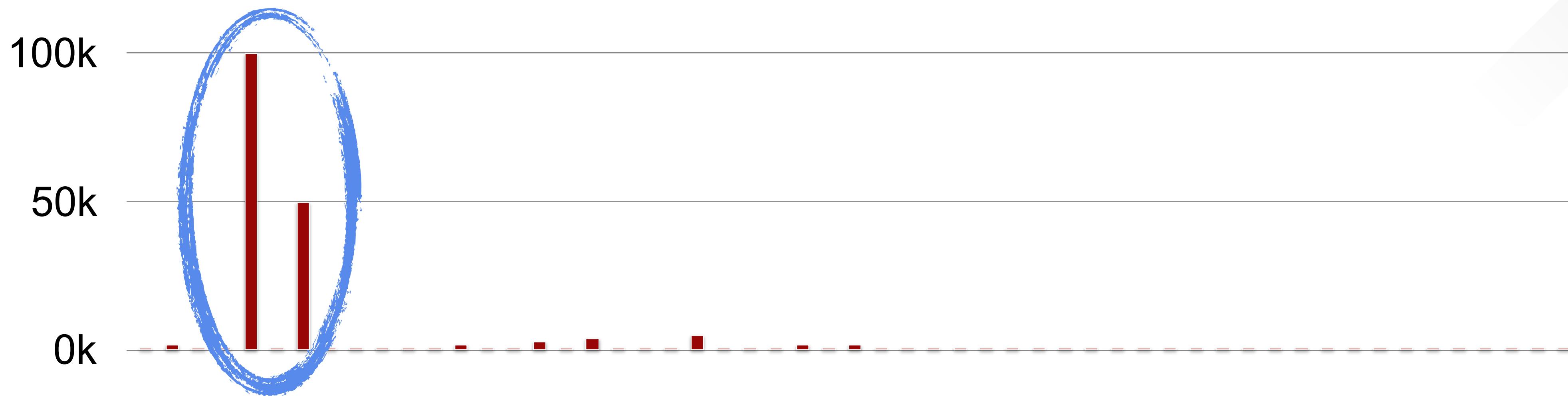
SentryMBA

- 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

Defense: Text-based CAPTCHAs

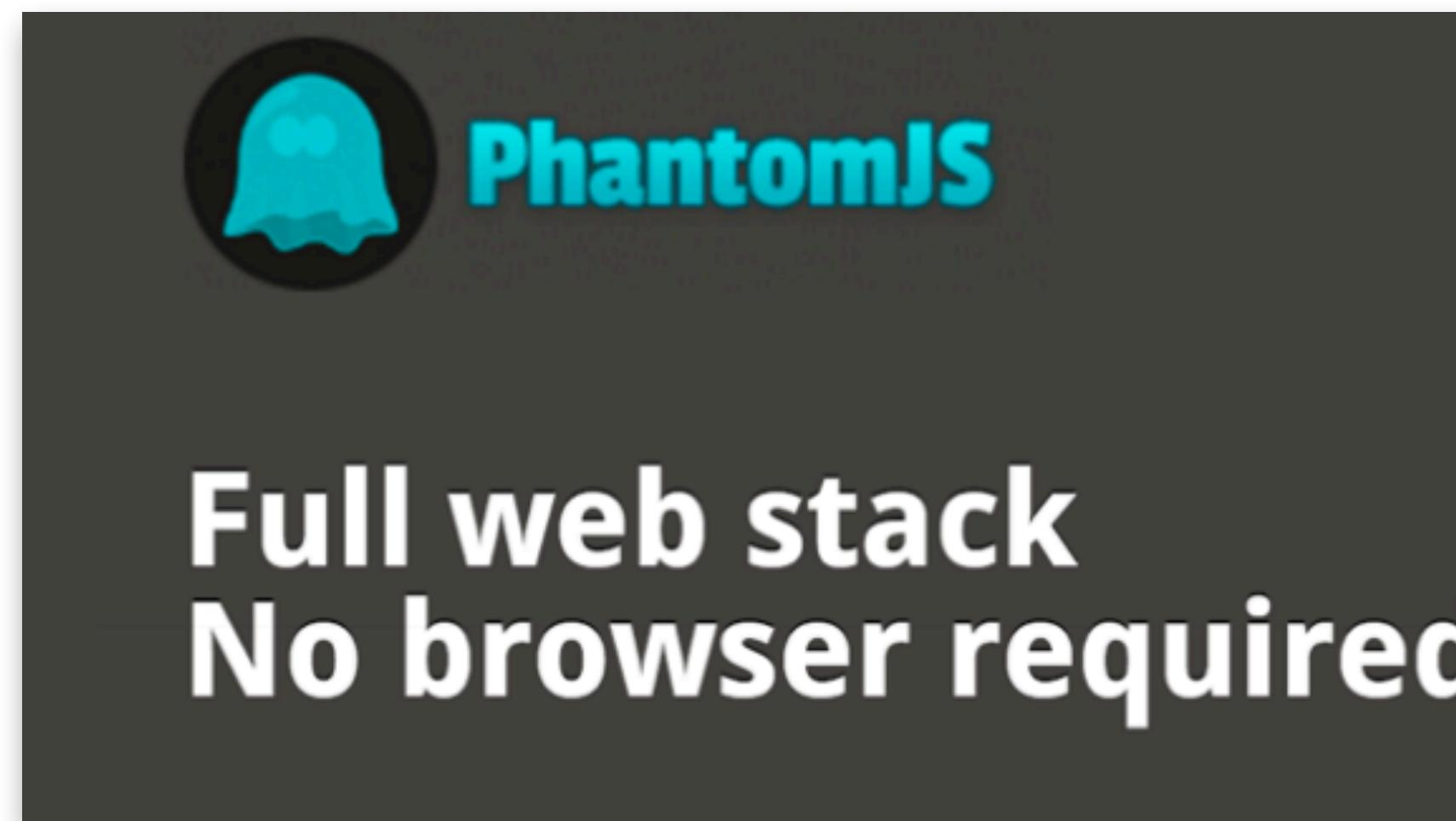
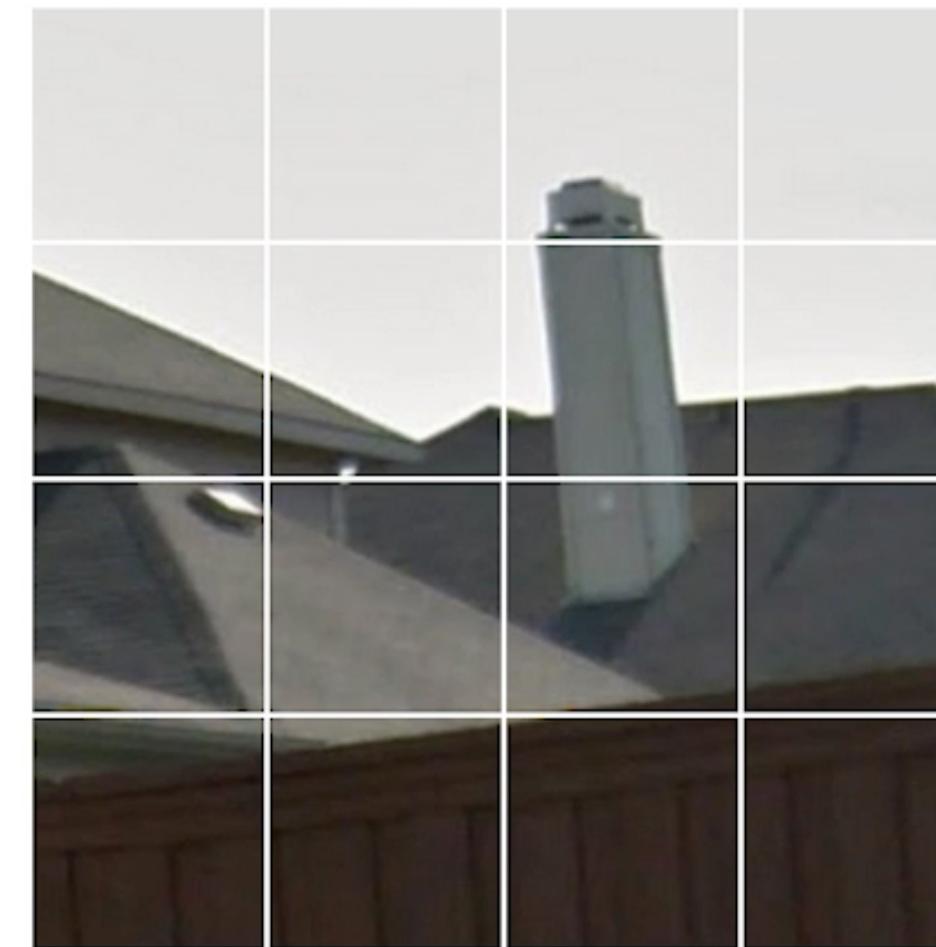
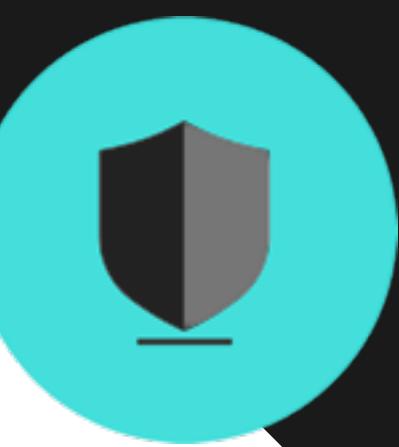


The screenshot shows the 2Captcha homepage. At the top, there's a navigation bar with links for "Work for us", "Captcha recognition service", "API", "Software", "Blog", "Sign in", and "Register". Below the navigation is a main menu with "Home", "Factories Beta", "Documentation", "Register", and "Sign In". A language selector shows "English" and "Русский". On the left, there's a sidebar with a "Order CAPTCHAs" section showing a "50¢" price and a "Starting from solved CAPTCHAs" note. The main content area features several advertisements: "DEATH BY CAPTCHA" (FASTEST DISCOUNT CAPTCHA SOLVERS), "CryptoMarket capstats" (www.cryptomarketcapstats.com), and "Prices - Stats - News - and More VISIT NOW!". At the bottom, there's a footer with links for "Home", "F.A.Q.", "API", "Order CAPTCHAs", "DBC Points", "Testimonials", "Contact Us", "Blog", "English", "Русский", "简体中文", and "Login".

Iteration 2: Attacks using CAPTCHA Solvers.



Defense: Dynamic sites and JavaScript heavy defenses.



Iteration 3: Scriptable WebViews





Defense: Header Fingerprinting & Environment Checks



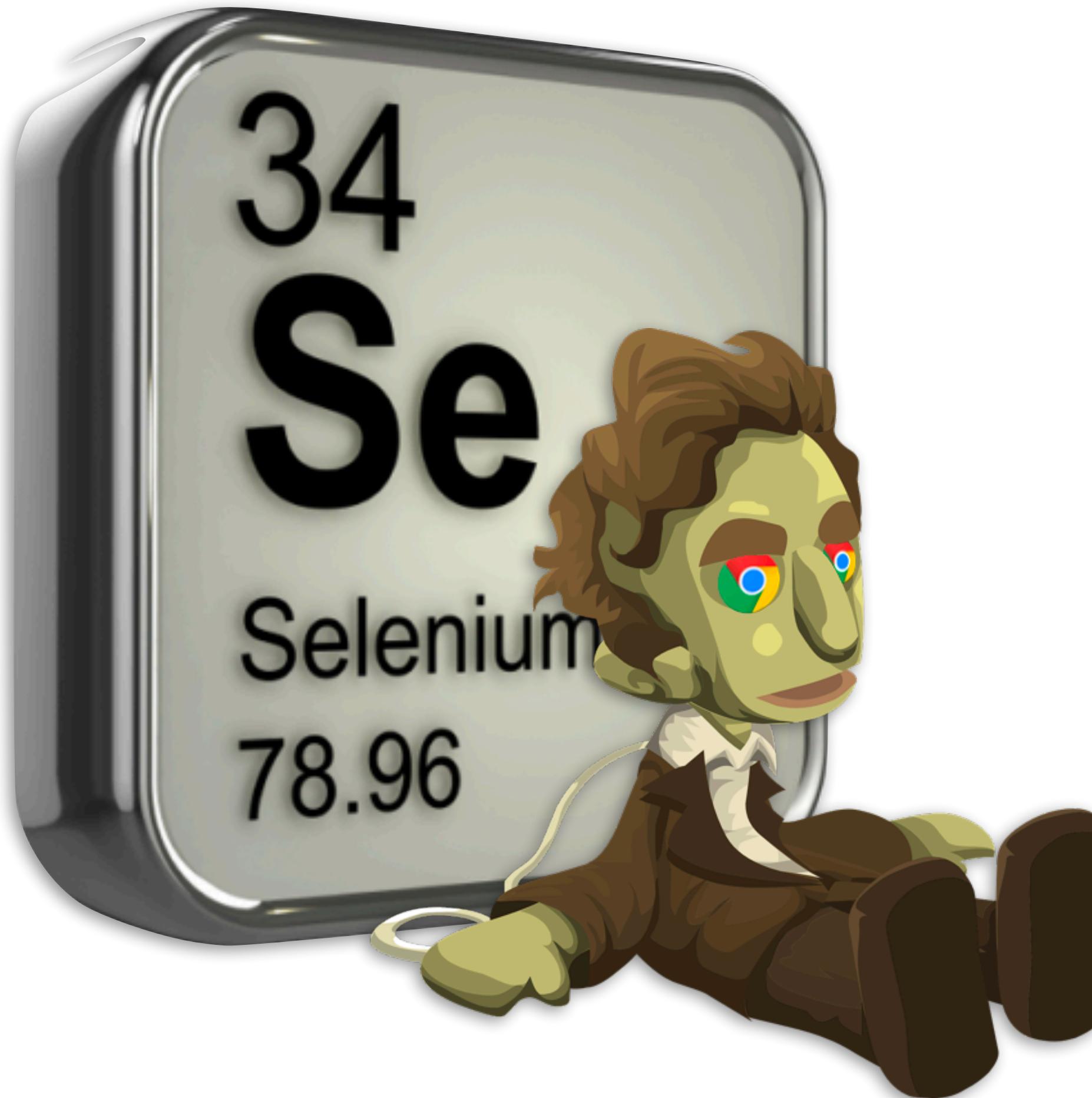
```
GET / HTTP/1.1
Host: localhost:1337
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Accept-Encoding: gzip,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



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



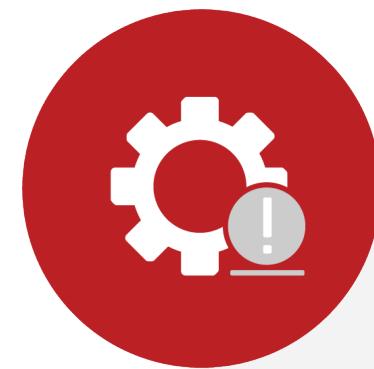
Login

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: 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



A screenshot of the Can I use... website. The search bar contains "ogg vorbis". The results page shows "1 result found" for "Ogg Vorbis audio format". The usage chart indicates "Global 81.44%". A red gear icon with an exclamation mark is overlaid on the top right of the screenshot.

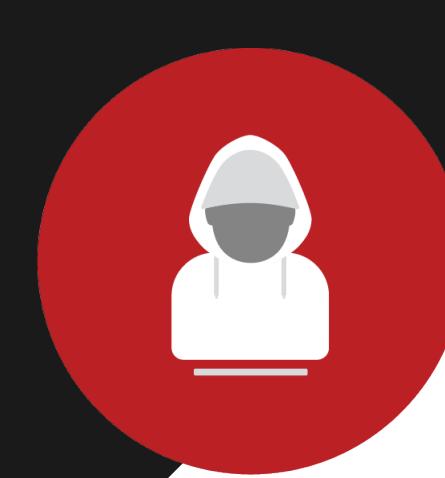
| Browser | Version Range |
|-----------------|---------------|
| IE | 12-16 |
| Edge | 17 |
| Firefox | 2-3 |
| Chrome | 4-76 |
| Safari | 3.1-12 |
| Opera | 10.1 |
| iOS Safari | 3.2-12.1 |
| Opera Mini | all |
| Android Browser | 2.1-2.2 |
| 6-10 | 3.5-68 |
| 11 | 77 |
| | 12.3 |
| | 76 |
| | 76 |
| | 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 fingerprints

The screenshot shows a web browser window with the title "FingerprintSwitcher - change your browser fingerprint". The URL in the address bar is "fingerprints.bablosoft.com/#home". The page content includes:

- 01 Fingerprint Switcher**: A large graphic of a fingerprint next to a small browser icon. Below it is the text "Change your browser fingerprint in several clicks." and a red button labeled "Get a key" with a key icon.
- 02 Fingerprint Detector**: A smaller graphic of a fingerprint next to a small browser icon. Below it is the text "Detects if site uses any fingerprint techniques."



Using Real Fingerprints

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

FingerprintSwitcher and FingerprintDetector are both part of [BrowserAutomationStudio](#) project - an ultimate way to automate your activities in Chrome browser.



The direction these attacks are moving in is clear.

Increasingly perfect emulation of humans and their environments.

We call these Imitation Attacks

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

Agenda

- 1 The cost of an attack
- 2 How attacks have evolved
- 3 Where fraud goes from here

Misconceptions about 2FA

2FA does not stop credential stuffing.

2FA stops automated account takeovers.

The goal of credential stuffing is to find valid accounts.

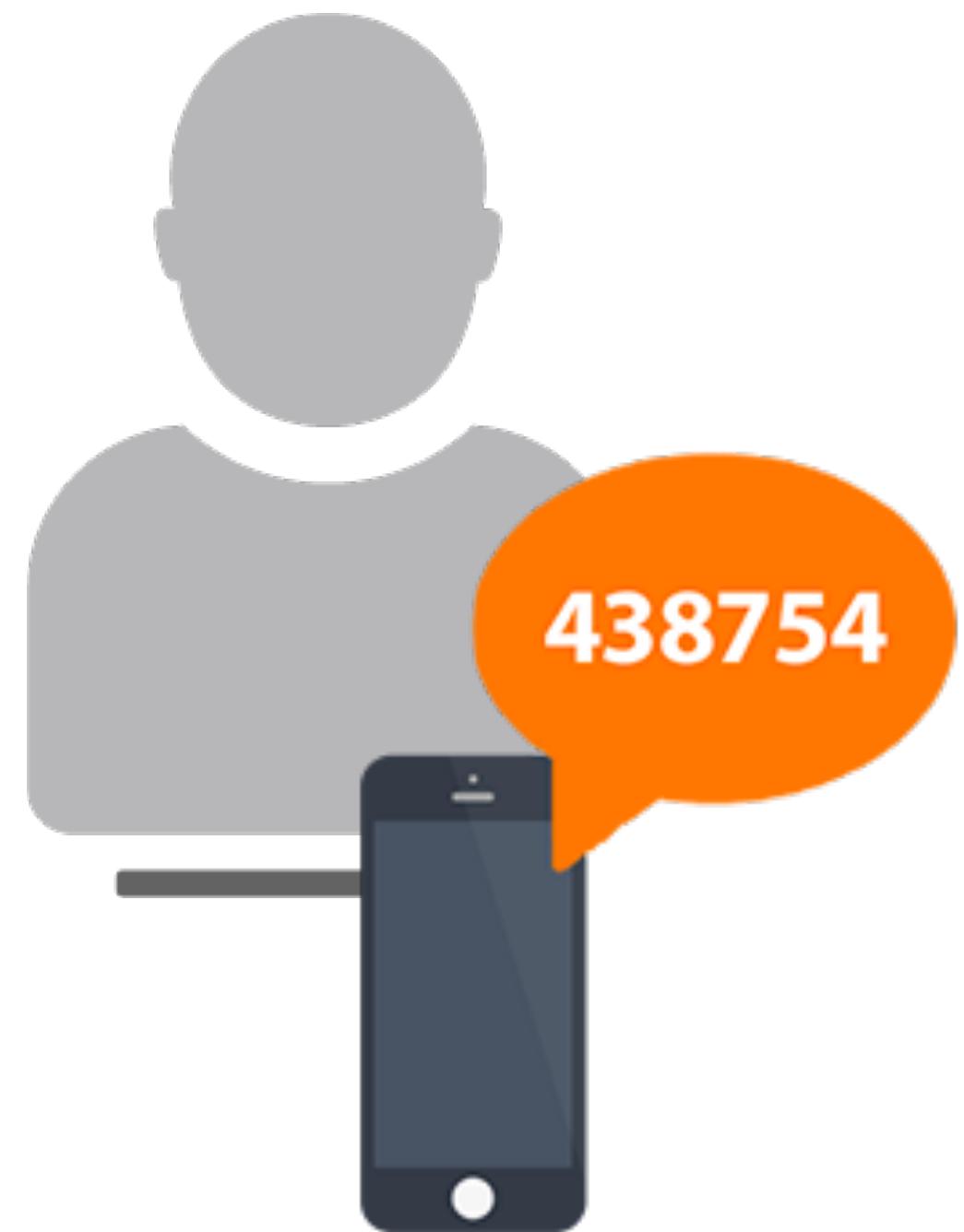
Credential stuffing, even with 2FA, still results in valid accounts.

How can an attacker bypass 2FA?

Don't overthink it. Easy attacks are cheap and get good results.



A screenshot of a login interface. It features a light gray background with rounded corners. Inside, there's a white rectangular area containing two input fields and a blue button. The first field is labeled "Username" and contains the text "victim@gmail.com". The second field is labeled "Password" and contains a series of asterisks ("*****"). Below these fields is a large blue button with the word "Submit" in white. A black cursor arrow is positioned over the "Submit" button, indicating it is being clicked. To the left of the form, there is a small, semi-transparent red illustration of a person wearing a hood and holding a telephone receiver to their ear.



[Back](#)

(555) 619-9189

[Contact](#)

Hey, I know you don't know me but many years ago I used to have your number. I'm trying to log in to an old account that is still tied to 555-619-9189 but it's telling me that it will send a verification code. I'd like to know if it'd be ok with you if I request the code and if you can just text it back to me? If not, that's totally fine.

ok

Thank you so much!!!

I just requested it

209959

You're a life saver! Thank you so much and sorry for bothering!



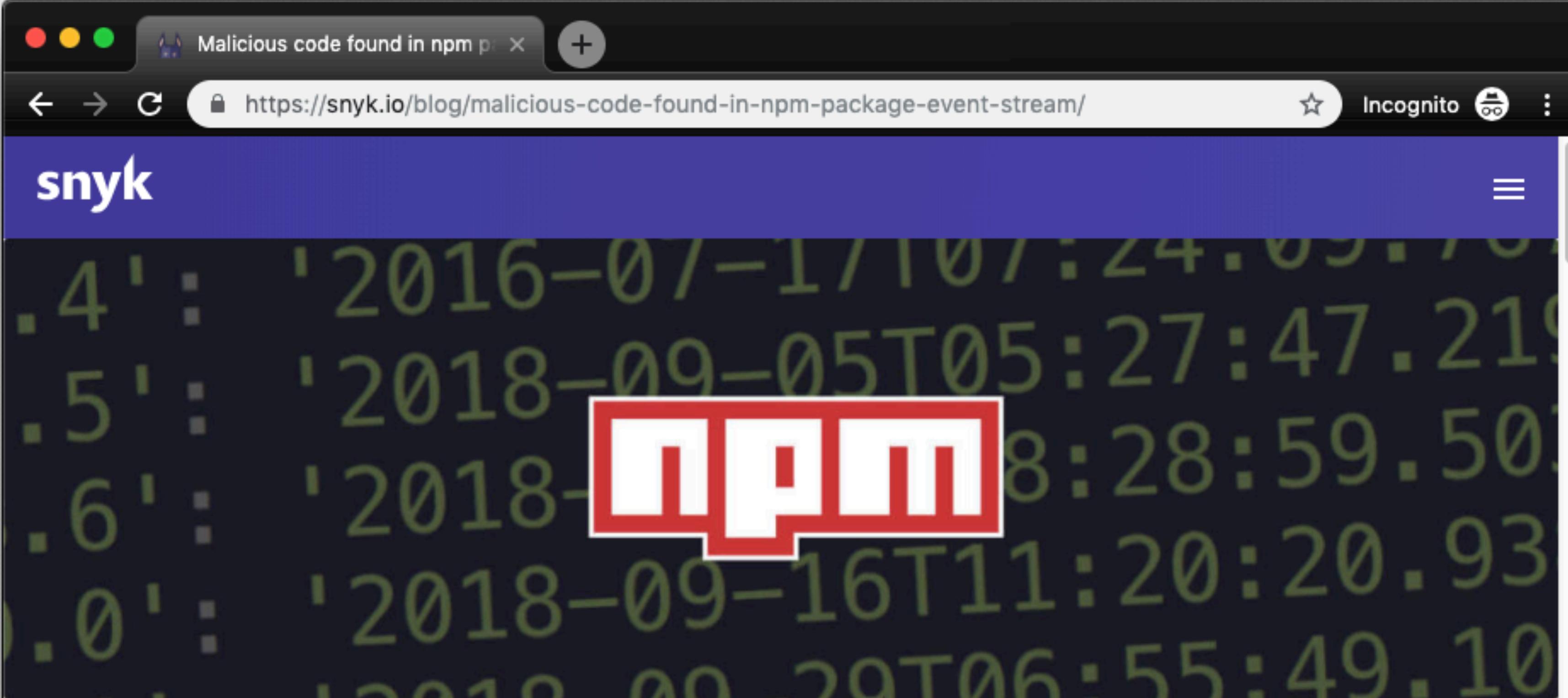
iMessage

Send

**A valid account changes the game.
Manual social engineering is an option.**

Not good enough? Build your malware directly into your target.

Open source supply chain attacks inject malware directly into your applications.



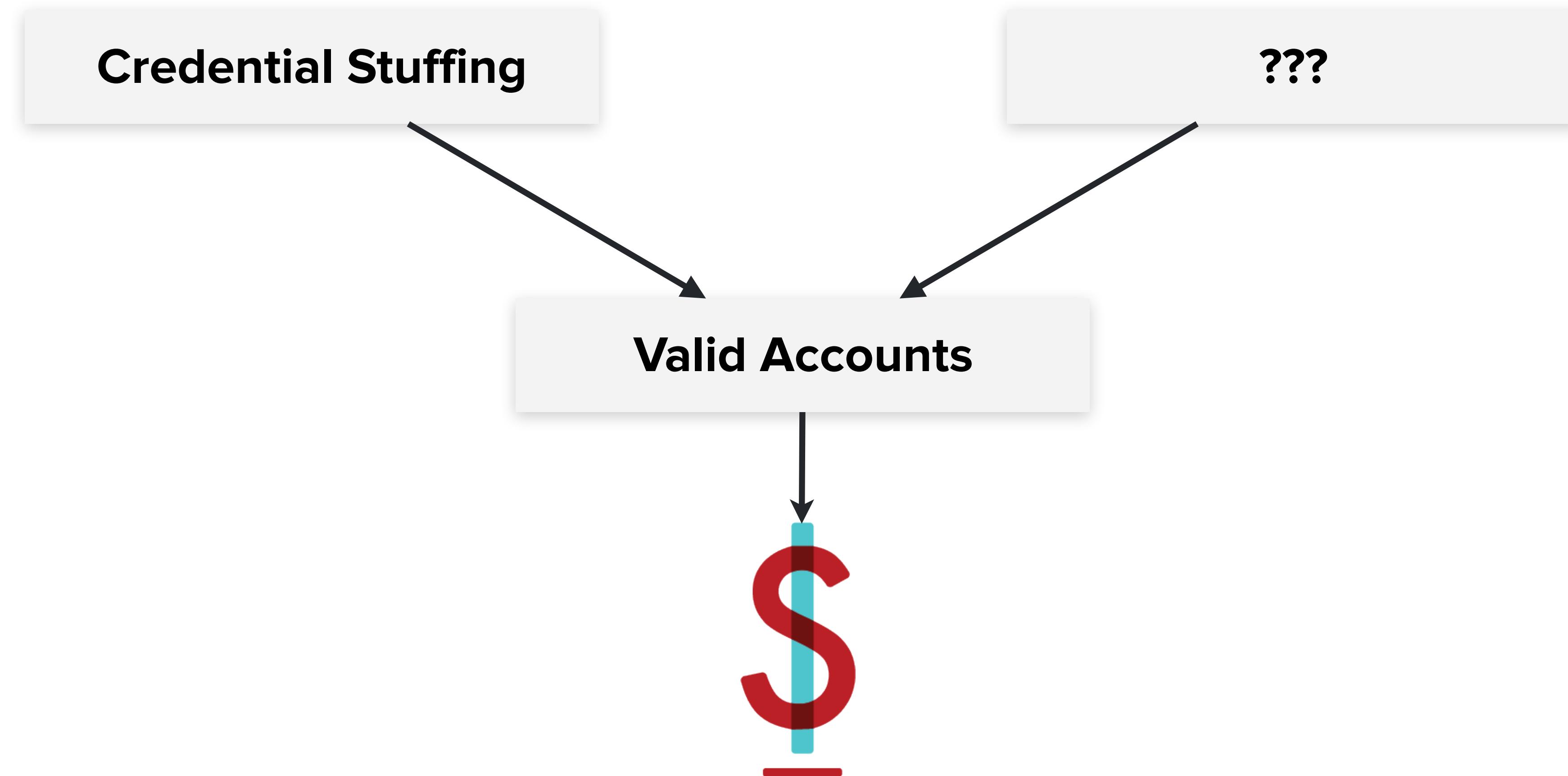
The screenshot shows a web browser window with the title "Malicious code found in npm package event-stream" and the URL "https://snyk.io/blog/malicious-code-found-in-npm-package-event-stream/". The page content is a blog post by Snyk, featuring a large red "npm" logo watermark over a list of package versions and their download dates. The text below the image reads:

Malicious code found in npm package event-stream downloaded 8 million times in the past 2.5 months

What's next?

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 the next generation.

Malware that resides at the host 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 rows:

| Bot Name | Resources Known / Other | Country / Host | Price |
|--|---|----------------------------|---------------------|
| User-PC_4f8c81e4141433310c57 | TDBank, iCloud, Dropbox, CanadianTireBank, UPS, BigCommerce, Kijiji, Skype, Google, Live, Twitter, AppleStore, Tumblr, Cisco, Indeed, com.contextlogic.wish, com.fitbit.Fitbit..., ...other 370 | CA, Windows 7 SP1 | 163.00, 81.50, Sale |
| CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB | LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber, Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend, Facebook, Dropbox, Marriott, Homeaway, GitHub, com.ebates, com.facebook.katana, ...other 1529 | CA, Windows 7 Professional | 52.00 |
| | | | |

Thousands of infections and growing

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

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

10

127417

114

369

1529

646

1898

81.50

52.00

163.00

207.219...

Windows 7 Professional

Sale

Profile

Logout

Invites

Genesis Security

Tickets

Payments

Purchases (1)

Orders

Generate FP

Bots (127417)

News

Genesis Wiki (new)

Dashboard

Home / Bots

Bots

Filter bot name

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

10

127417

114

369

1529

646

1898

81.50

52.00

163.00

207.219...

Windows 7 Professional

Sale

Each infected computer and its data is sold as one unit

The screenshot shows the genesis web interface. 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 a compromised computer for sale. A large red box highlights the main listing:

**CA
207.219...
Windows 7 Professional**

\$52.00

Icons for a monitor, hourglass, and trash can are shown. Below this, a smaller red box highlights another listing:

**CA
207.219...
Windows 7 Professional**

52.00

Icons for a monitor, hourglass, and trash can are shown. The background shows a grid of other compromised hosts with their IP addresses, countries, and prices.

Each bot gives the purchaser exclusive access to its data.

One buyer per bot.

genesis

≡

Dashboard Genesis Wiki News 10 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

| | |
|-----------|---------------------|
| 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 |

Browsers for Genesis Security: NO INFO

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 |

Bots can have hundreds of scraped resources and accounts.

The bots will collect everything it can, even if it isn't sure what it is yet.

The screenshot shows a web-based interface for managing accounts. 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 bot accounts. One account, "User-PC_4f8c81e4141433310c57", is selected and displayed in detail. The account has 127416 Bots and is located in CA. The main content area displays the following information:

Resources: 484 = 📧 1 🖥 482 💎 1

Known resources: 114

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

Below the table, there are links for "INVITES", "Logout", and "Last update info: 1970-01-01 00:00:00". A red box highlights the "Known resources" section and the first few items in the list. Another red box highlights the same section and list on a lower part of the page, connected by a red arrow pointing from the top highlighted area to the bottom one.

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

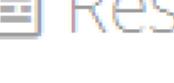
 **Generate FP**

Windows 7 SP1
81.50

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

Generate FP

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 |  TD Bank | 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

Configure which parts you want to emulate

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 (green bar), 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. On the right are buttons for Add to Cart, Reserve, and Buy. A large red box highlights the "Step 2. Choose method of generation" section. This section contains two dropdown menus: "chrome cookies: 419 fingerprints: 0" and "Windows". Below them is a large blue button labeled "Generate config". The bottom of the page shows a list of shared resources with counts: BigCommerce (1), Indeed (1), Copycenter... (1), Ops (1), Autorader (1), Capitalone... (1), Groupon (1), DBank (2), CanadianT... (1), Spotify (1), IndigoStore (1), Cisco (1), Skype (1), and Yahoo (1).

Step 2. Choose method of generation

chrome cookies: 419 fingerprints: 0

Windows

Generate config

| Resource | Count |
|---------------|-------|
| BigCommerce | 1 |
| Indeed | 1 |
| Copycenter... | 1 |
| Ops | 1 |
| Autorader | 1 |
| Capitalone... | 1 |
| Groupon | 1 |
| DBank | 2 |
| CanadianT... | 1 |
| Spotify | 1 |
| IndigoStore | 1 |
| Cisco | 1 |
| Skype | 1 |
| Yahoo | 1 |

And load it into your current session via the Genesis Security Plugin

Voila! Now you are 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 success message in a green box: "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 is a resources summary: "Resources: 484 = 1 482 ⚳". A table lists known resources: Facebook (18), Google (17), Live (16), Kijiji (8), Ebay (6), Twitter (5), Netflix (5), Amazon (4), AppleStore (4), PayPal (3), Instagram (3), TD Bank (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), and Skype (1).

genesis

Dashboard

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

Home / Bots / User-PC_4f8c81e4141433310c57 / View Details

User-PC_4f8c81e4141433310c57 Sale

Add to Cart Reserve Buy

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!

Resources: 484 = 1 482 ⚳

| Know resources: 114 | |
|---------------------|----|
| Facebook | 18 |
| Netflix | 5 |
| 4Shared | 2 |
| BigCommerce | 1 |
| Indeed | 1 |
| Google | 17 |
| Amazon | 4 |
| SonyEnter... | 2 |
| iCloud | 1 |
| Payless | 1 |
| Live | 16 |
| AppleStore | 4 |
| UPS | 2 |
| Dropbox | 1 |
| IndigoStore | 1 |
| Kijiji | 8 |
| PayPal | 3 |
| AutoTrader | 2 |
| Tumblr | 1 |
| Spotify | 1 |
| Ebay | 6 |
| Instagram | 3 |
| Capitalon... | 2 |
| Cisco | 1 |
| Skype | 1 |
| Twitter | 5 |
| TD Bank | 2 |
| Groupon | 1 |
| CanadianT... | 1 |
| Yahoo | 1 |

It follows the rules of shady actors in the CIS.

Genesis Store & Genesis Security Terms of Service

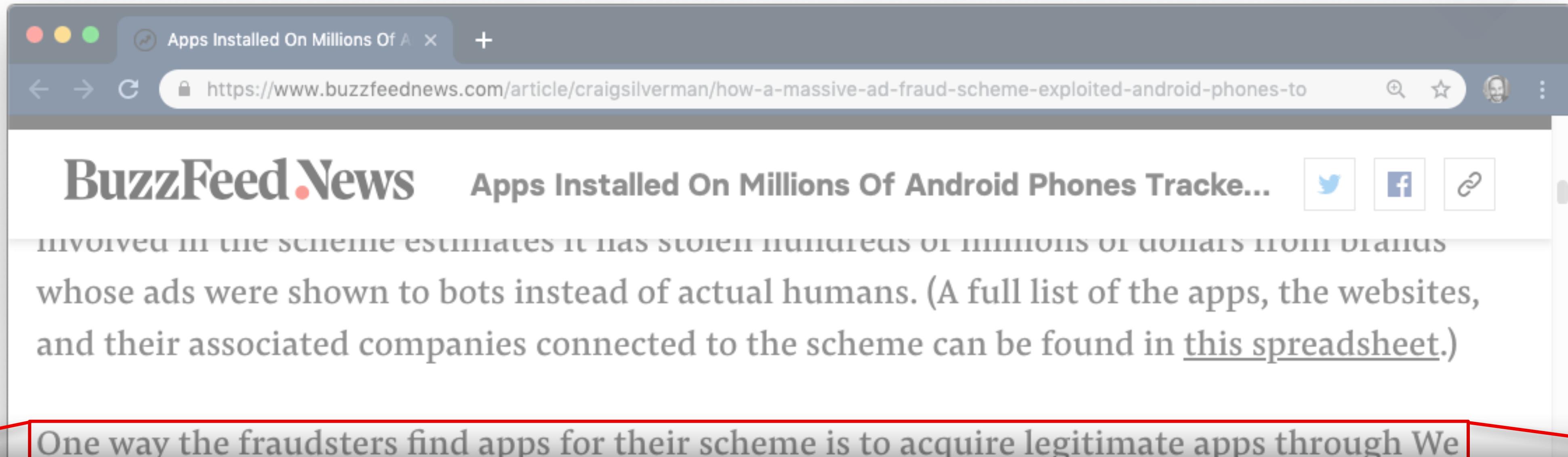
General rules:

1. All **payments** are made via the web-site **automatically**.
2. **Refund is not possible** in any way.
3. The Store has a right to **deny** a customer of service, **block** access to an account **without explanation**.
4. If a customer does not use the account for **more than 3 months** – the access is blocked, more than 6 months – account is deleted with no option to restore.
5. The contents of the site, such as text, graphics, images and other materials are **informational purposes only**.
6. The Store **does not use or sell** any products connected with **CIS**-countries' web-resources.
7. The Store **is not liable for** any moral or financial **damage** caused by using the acquired information.
8. By signing up with the Store, you **accept** these rules.



Malware that scrapes, learns, and imitates its host users is what's 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](#).)".

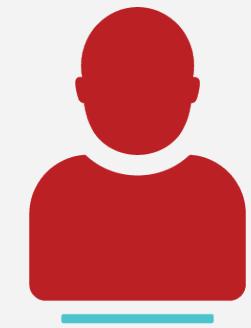
One way the fraudsters find apps for their scheme is to acquire legitimate apps through We

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.

Fraud is a human problem, not a technical problem.

There are no silver bullet solutions against humans.



Advanced credential stuffing is sophisticated fraud. Treat it as more than simple automation. **Talk to your fraud teams and work from the scams backward.**



Imitation attacks are designed to blend in. If you don't think you have a problem, **look deeper until you know you don't have a problem.**



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

SH-PE

THANK YOU

Visit us at booth #3 for more questions, information, and to
say hi!

Jarrod Overson
@jsoverson on twitter, medium, and github.