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

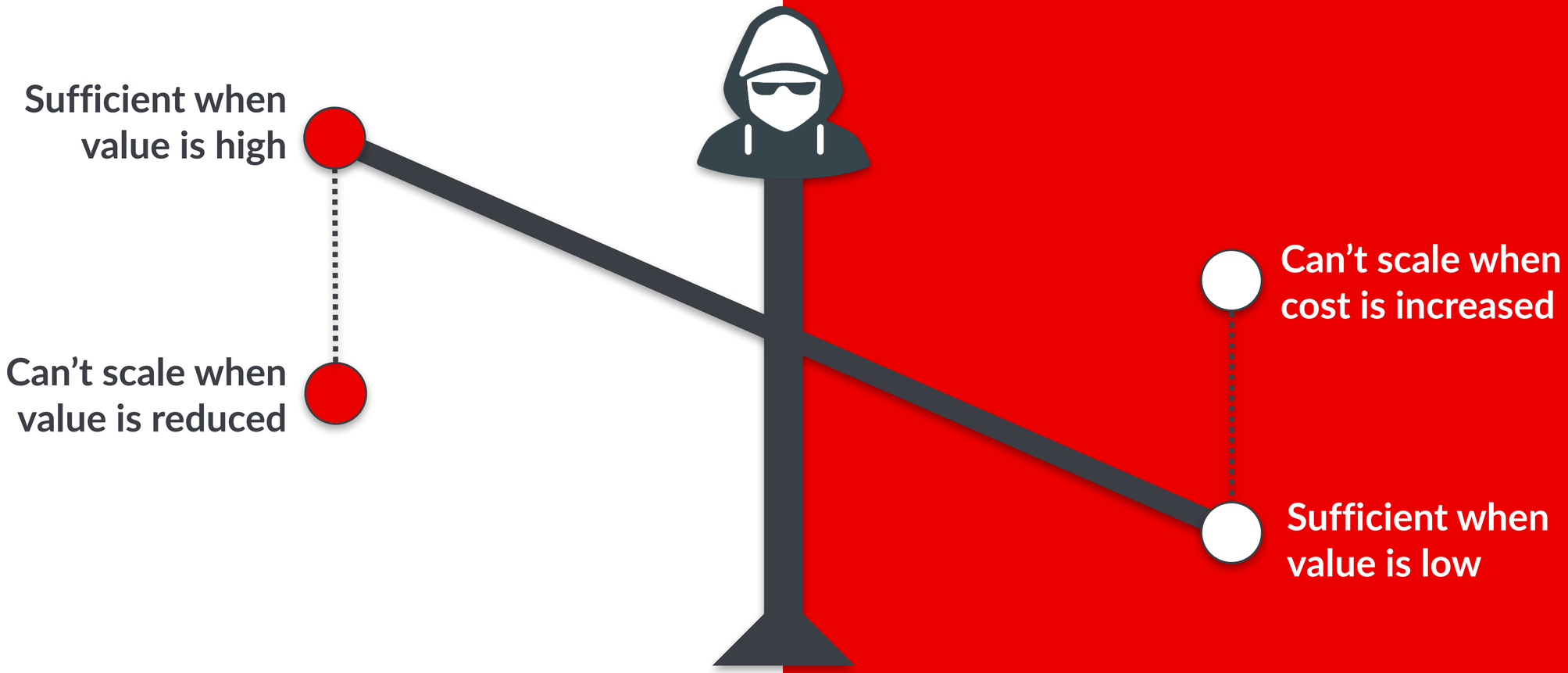
1. **The cost of an attack**
2. How attacks have evolved
3. Where fraud goes from here

MANUAL WORK

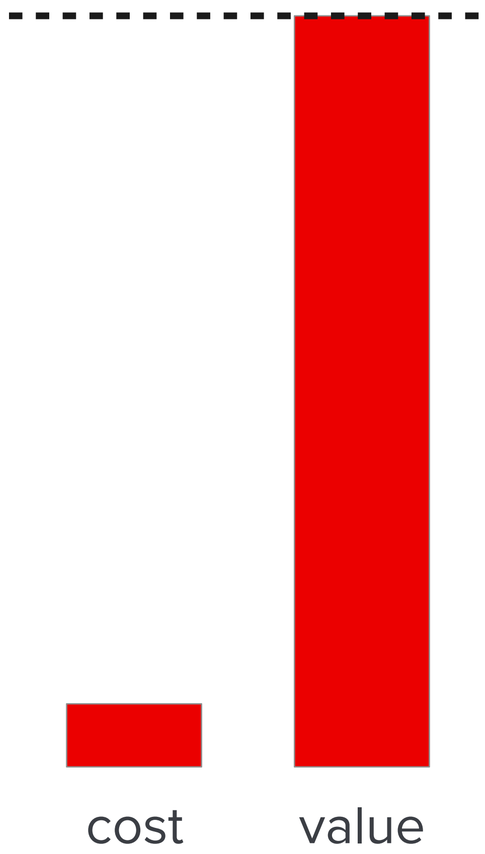
AUTOMATION

MANUAL WORK

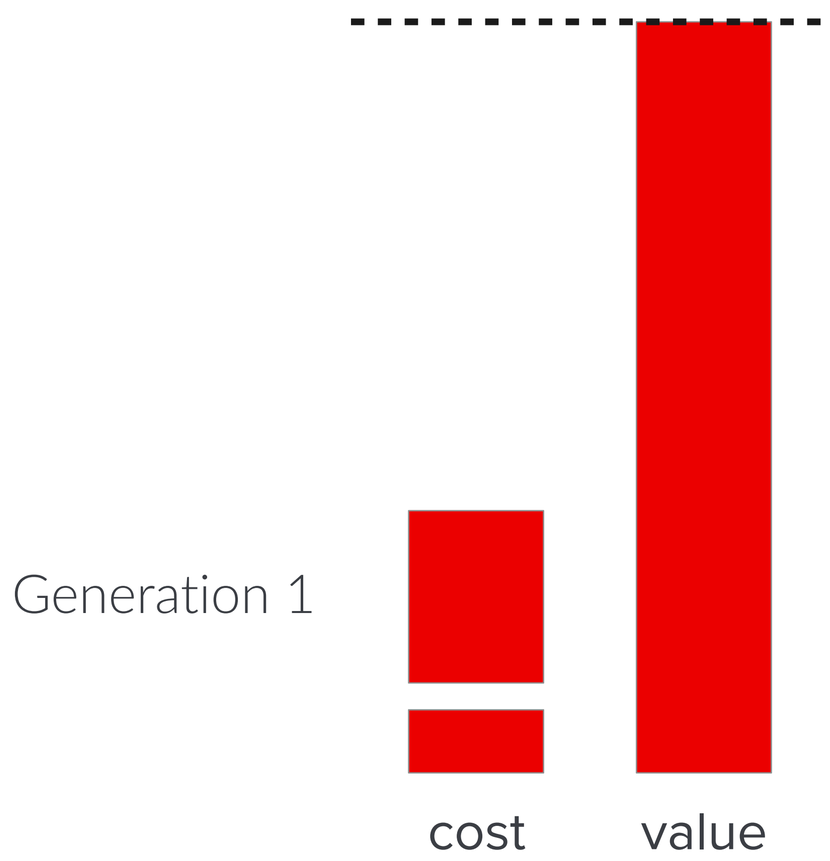
AUTOMATION



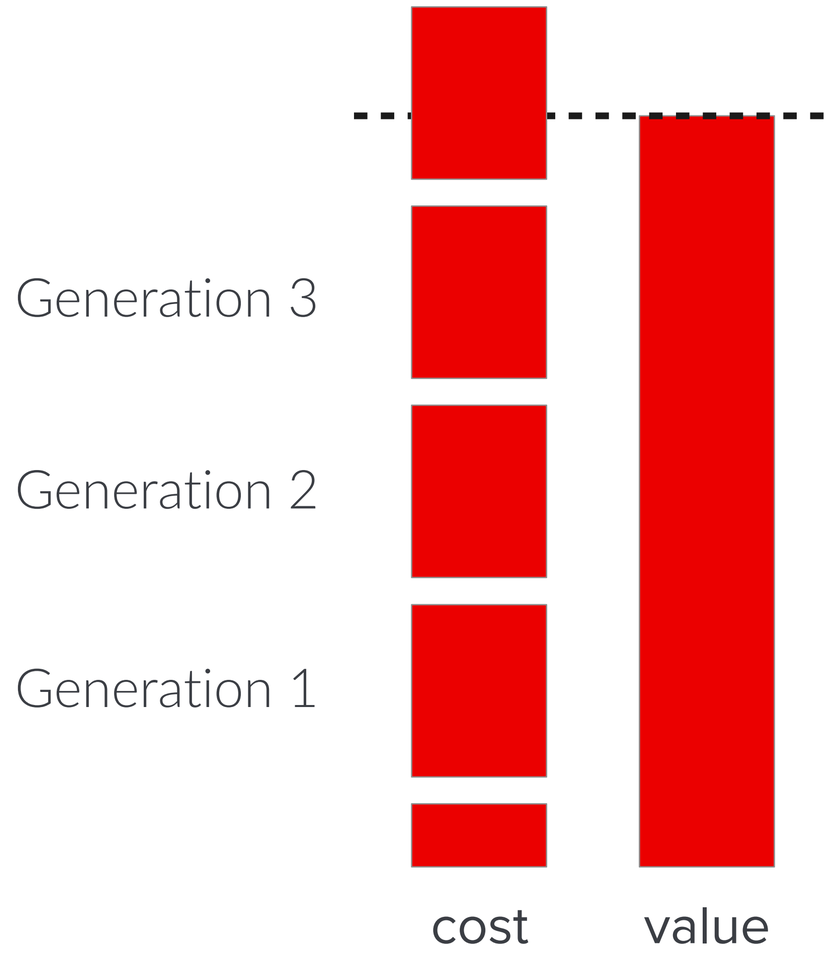
If there are no defenses in place, the cost is nearly zero.



Any defense increases the cost by forcing a generational shift.

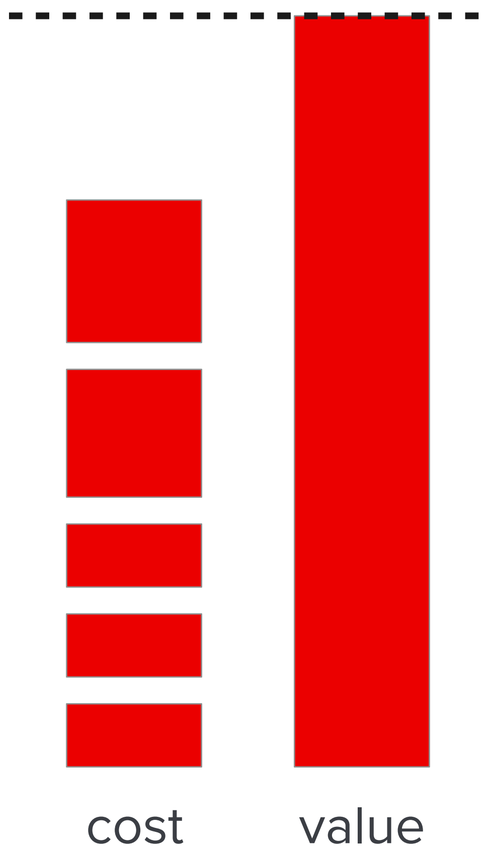


Enough defenses tip cost vs value in your favor

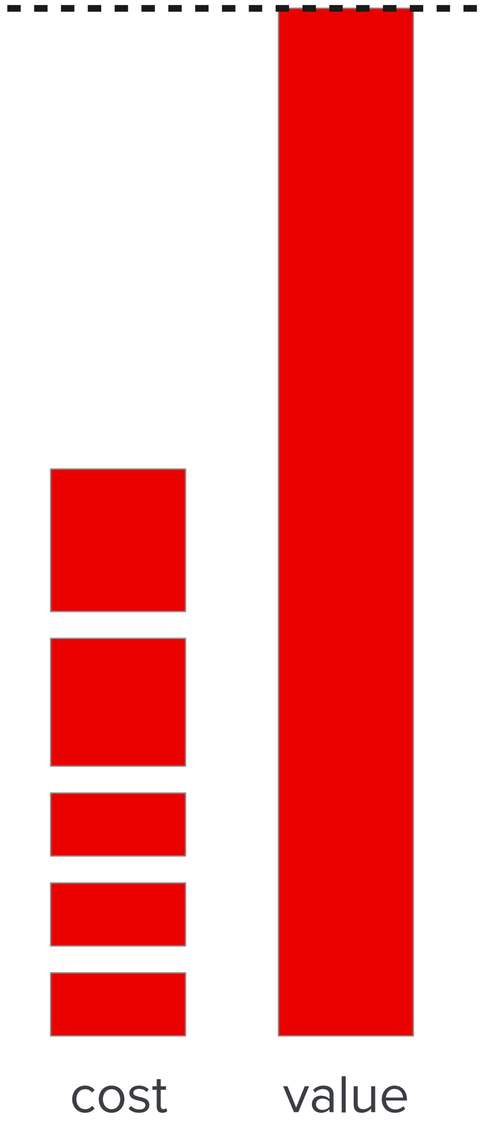


The cost of entry for each generation decreases over time.

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
/krəˈden(t)SHəl ˈstəfiNG/

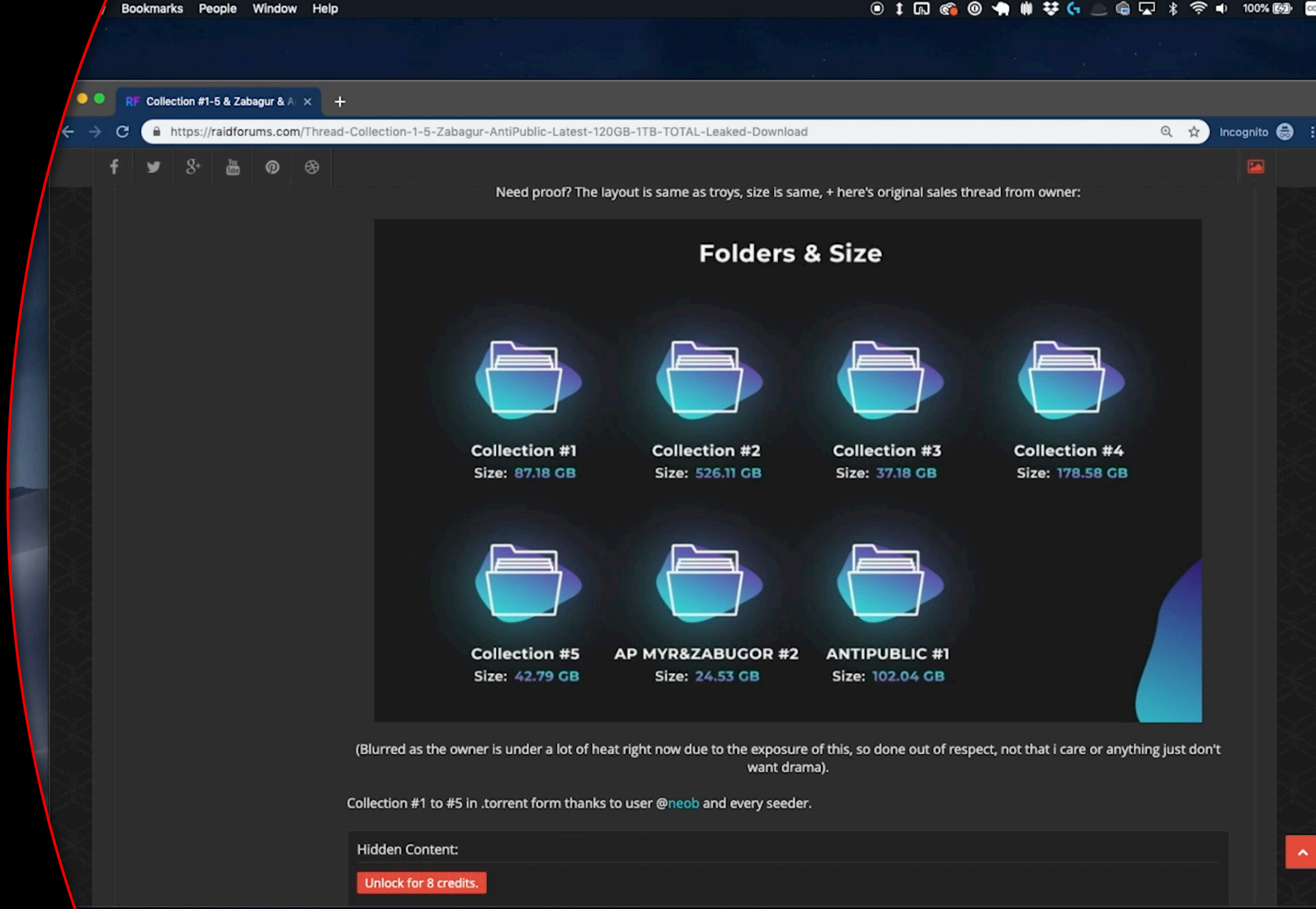
The replay of breached username/password pairs across sites to find accounts where passwords have been reused.

STEP BY STEP GUIDE

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

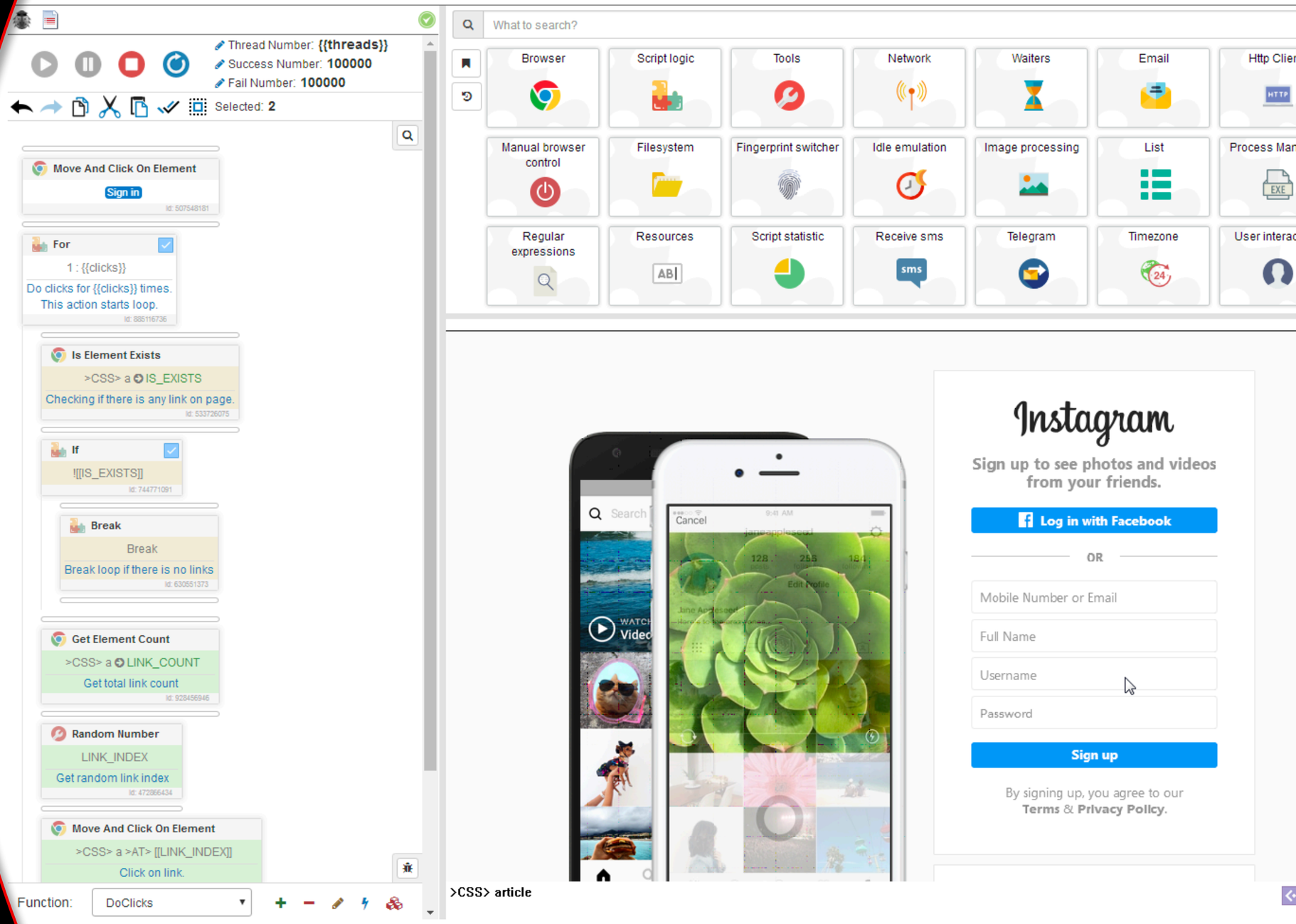
CREDENTIAL STUFFING

1. Get Credentials



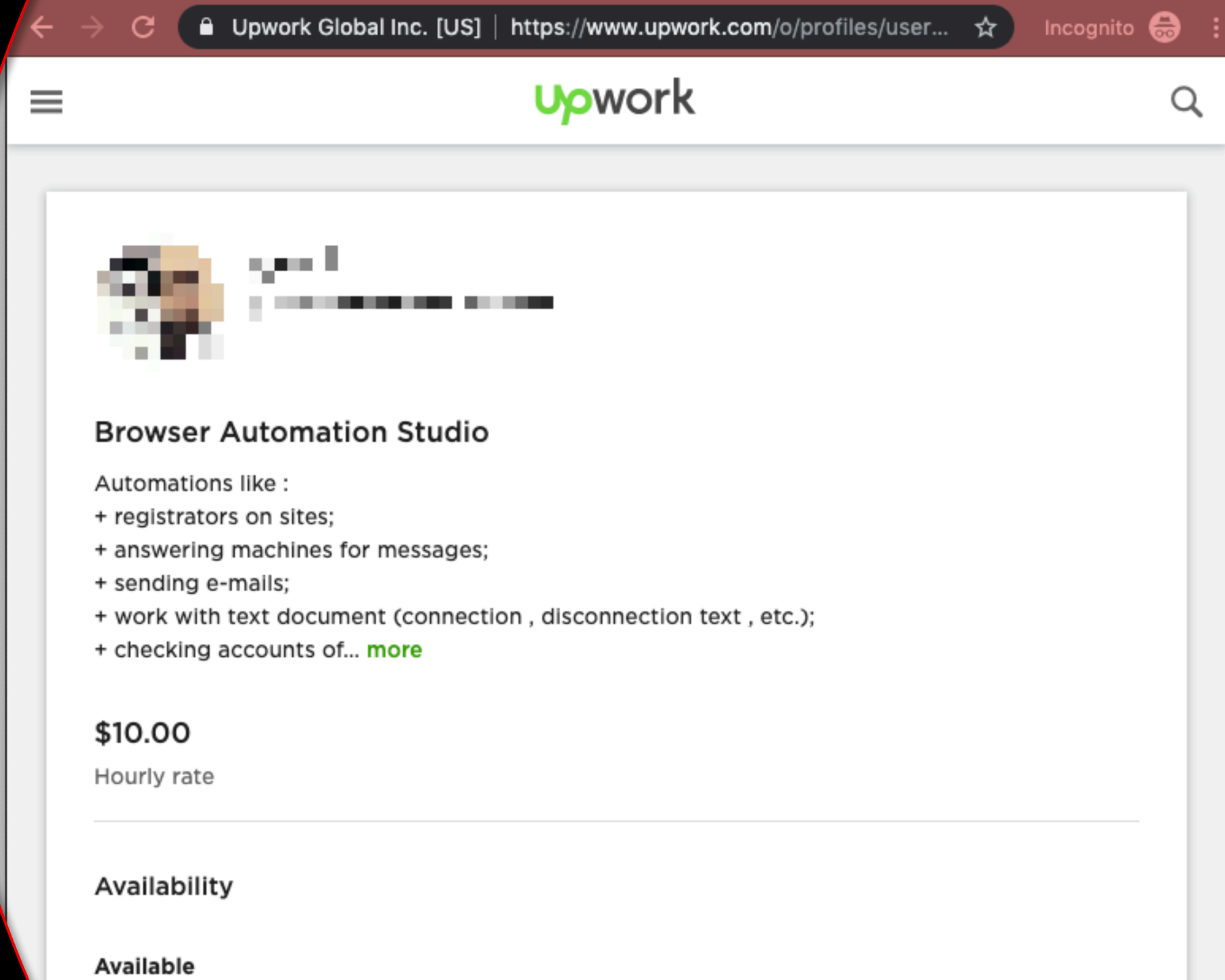
CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login



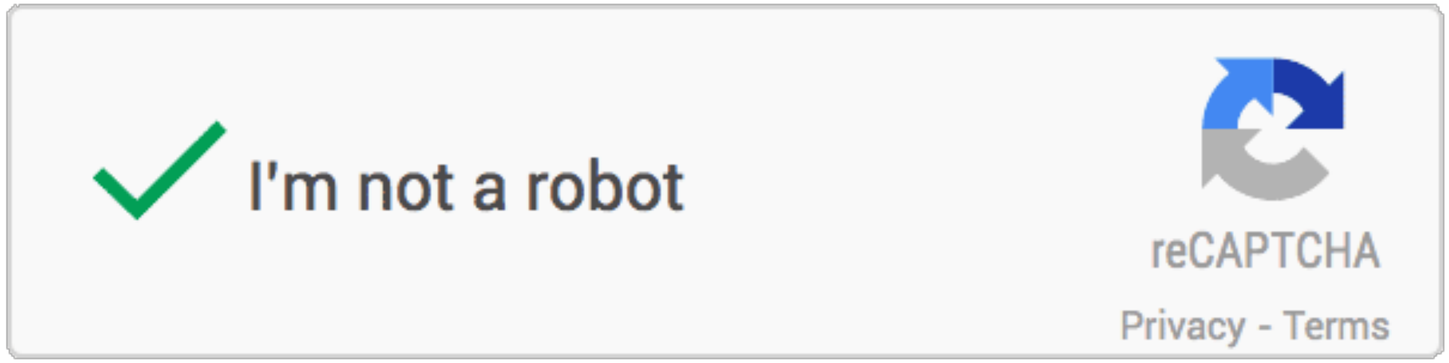
CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login



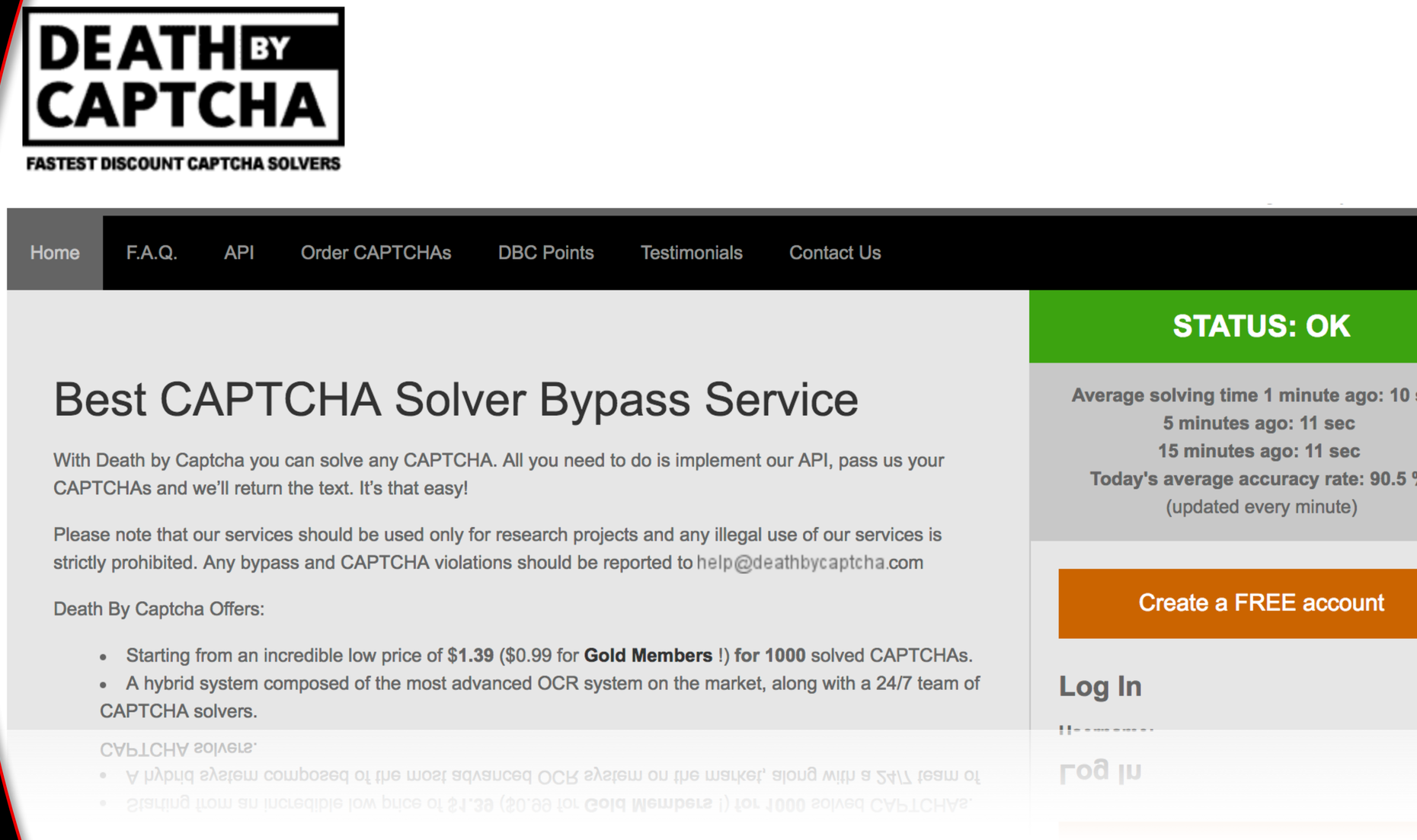
CREDENTIAL STUFFING

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

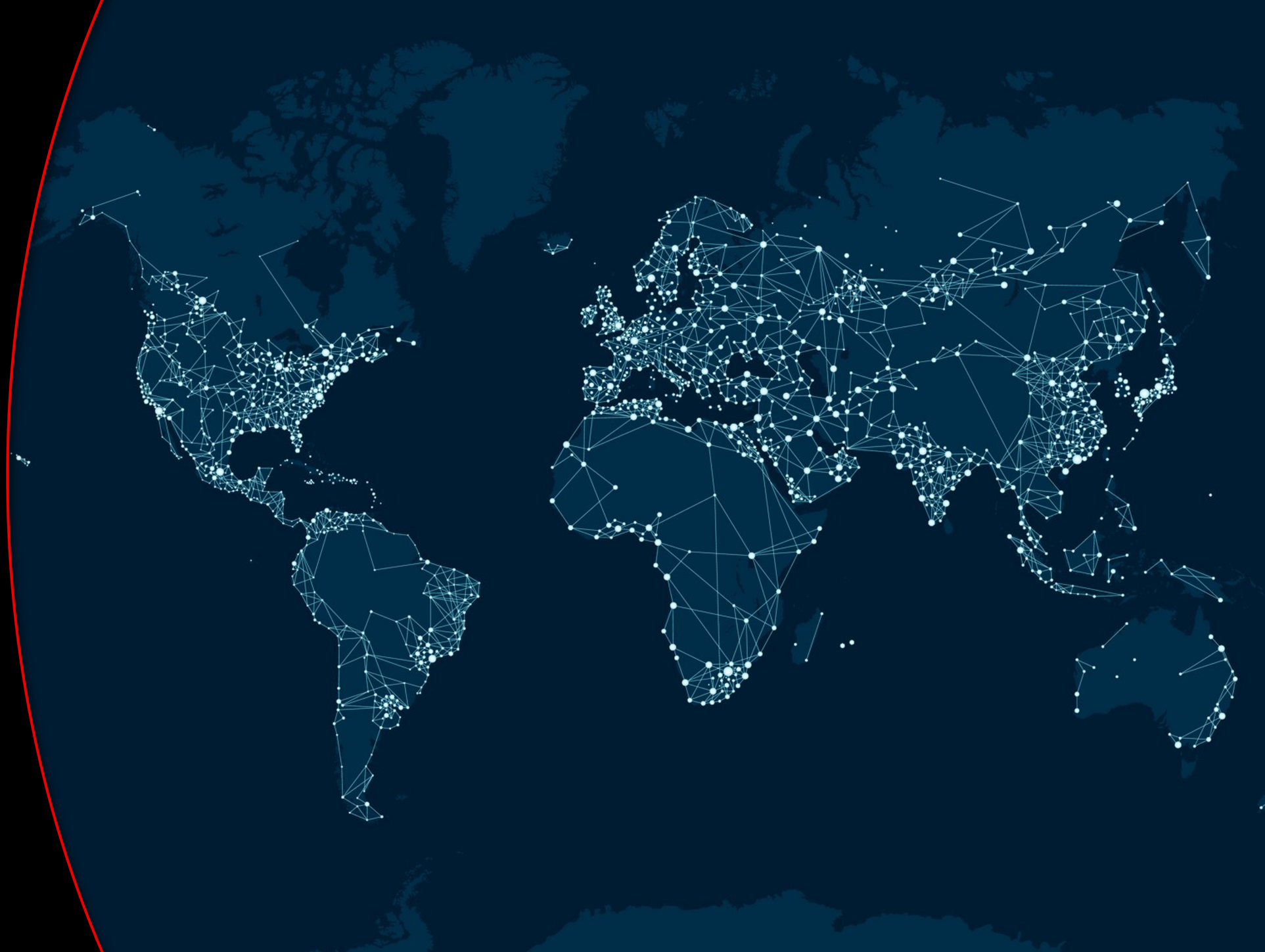


CREDENTIAL STUFFING

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



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

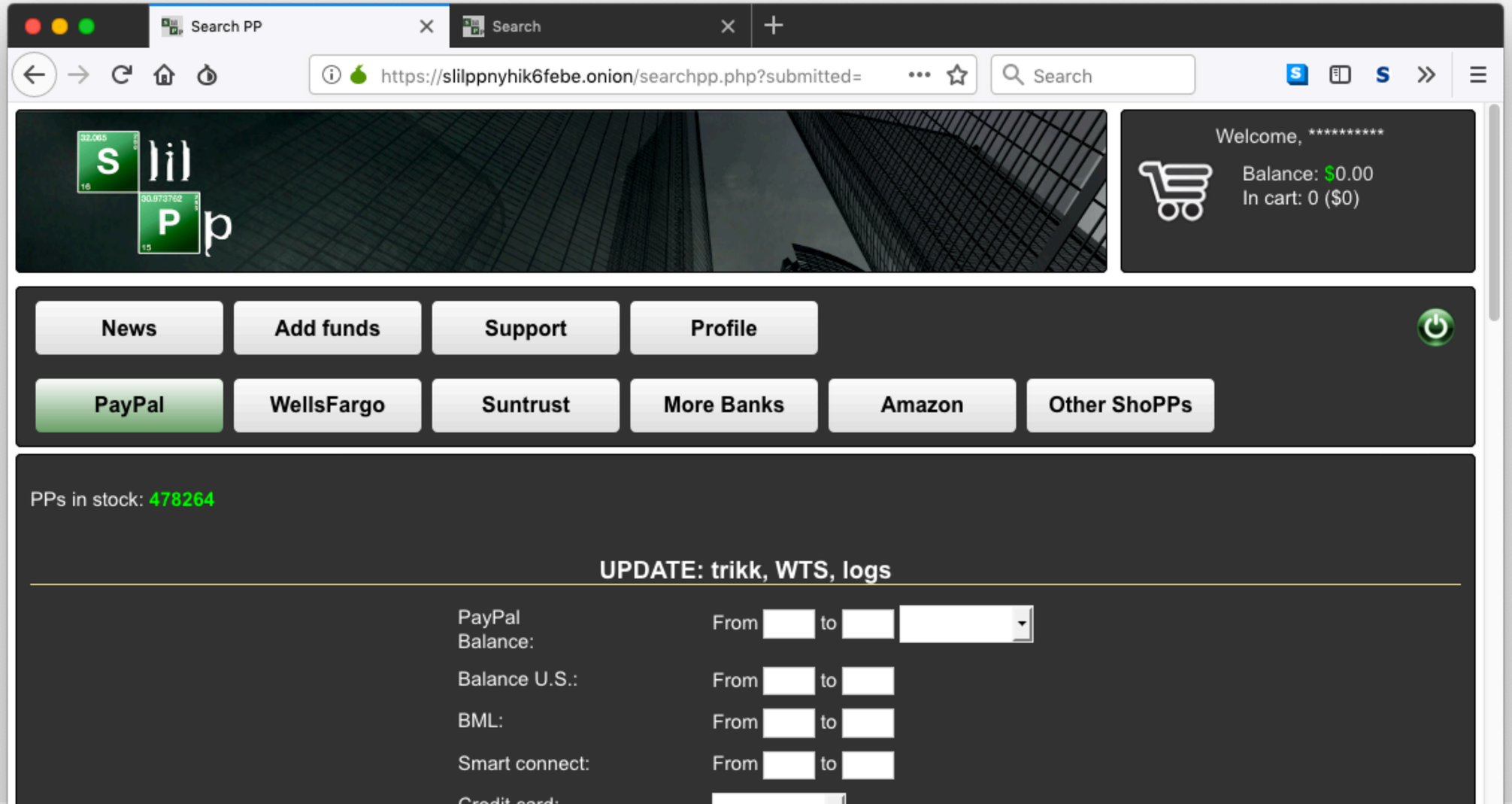
$0-10

For 1,000 global IPs

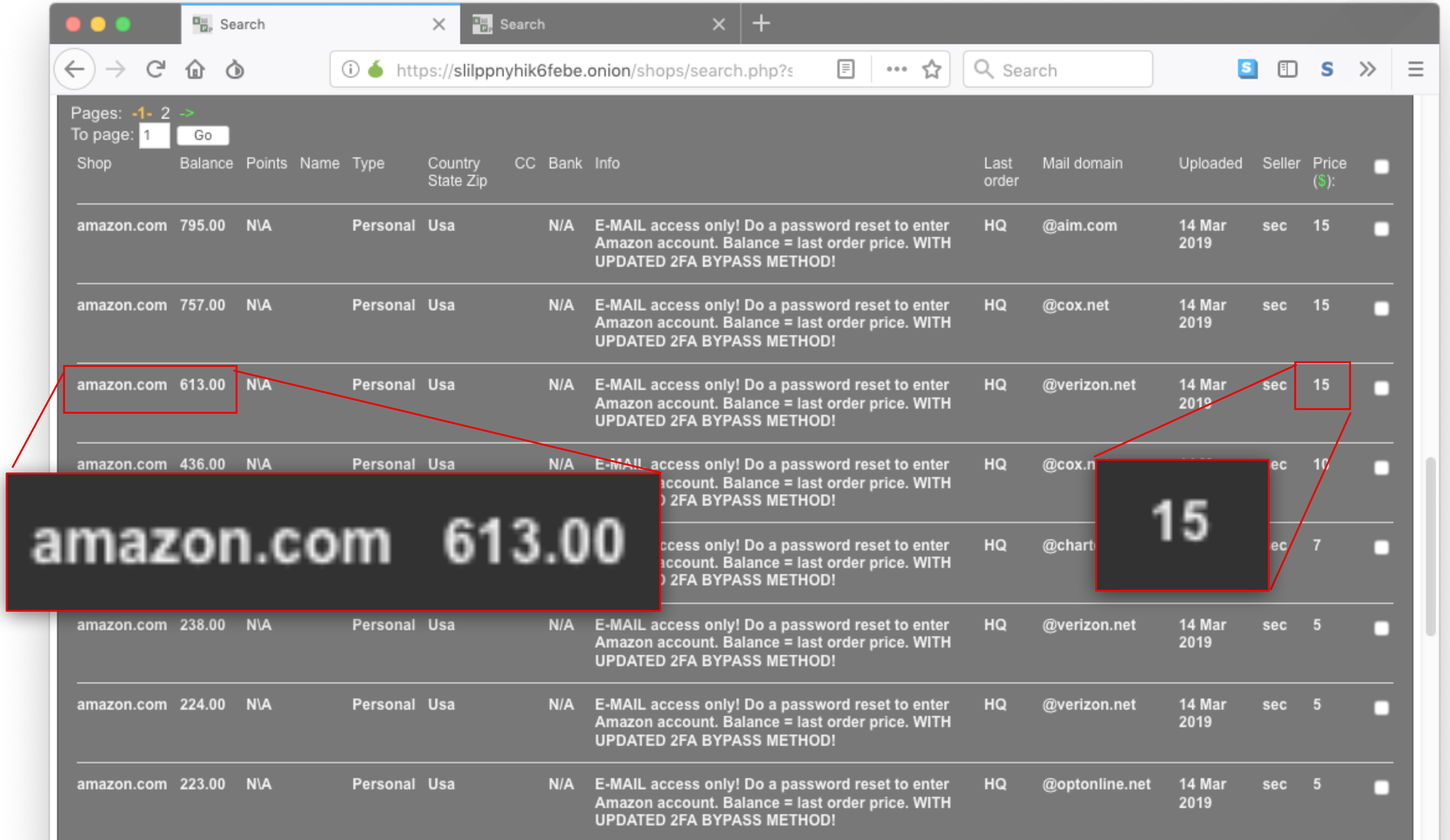
<$0.002

per ATO attempt.

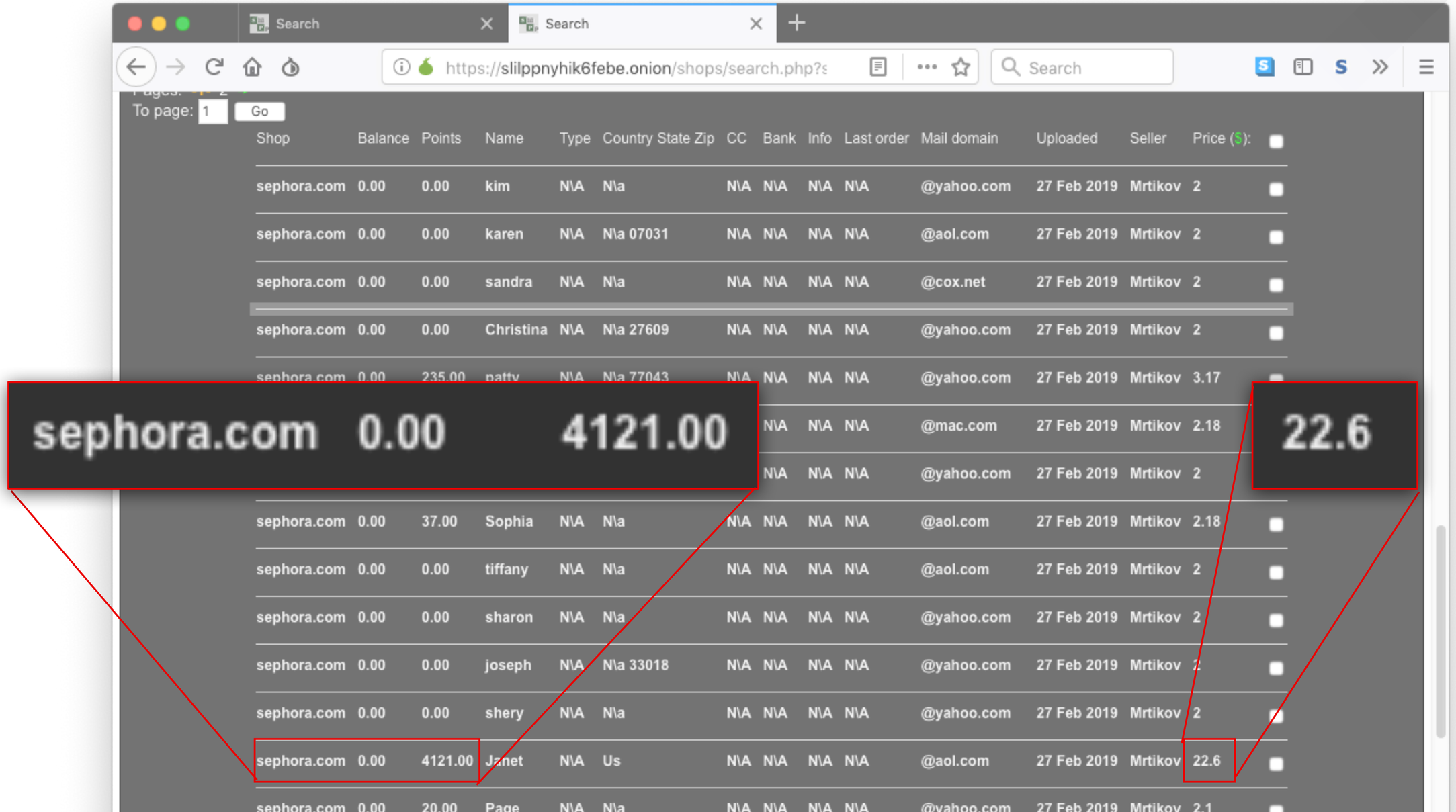
The value of accounts is variable, from pennies to hundreds.



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



Sephora accounts with 4,121 points sell for $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
							N\A	N\A	N\A	@mac.com	27 Feb 2019	Mrtikov	2.18
							N\A	N\A	N\A	@yahoo.com	27 Feb 2019	Mrtikov	2
sephora.com	0.00	37.00	Sophia	N\A	N\a	N\A	N\A	N\A	N\A	@aol.com	27 Feb 2019	Mrtikov	2.18
sephora.com	0.00	0.00	tiffany	N\A	N\a	N\A	N\A	N\A	N\A	@aol.com	27 Feb 2019	Mrtikov	2
sephora.com	0.00	0.00	sharon	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	joseph	N\A	N\a 33018	N\A	N\A	N\A	N\A	@yahoo.com	27 Feb 2019	Mrtikov	2
sephora.com	0.00	0.00	shery	N\A	N\a	N\A	N\A	N\A	N\A	@yahoo.com	27 Feb 2019	Mrtikov	2
sephora.com	0.00	4121.00	Janet	N\A	Us	N\A	N\A	N\A	N\A	@aol.com	27 Feb 2019	Mrtikov	22.6
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

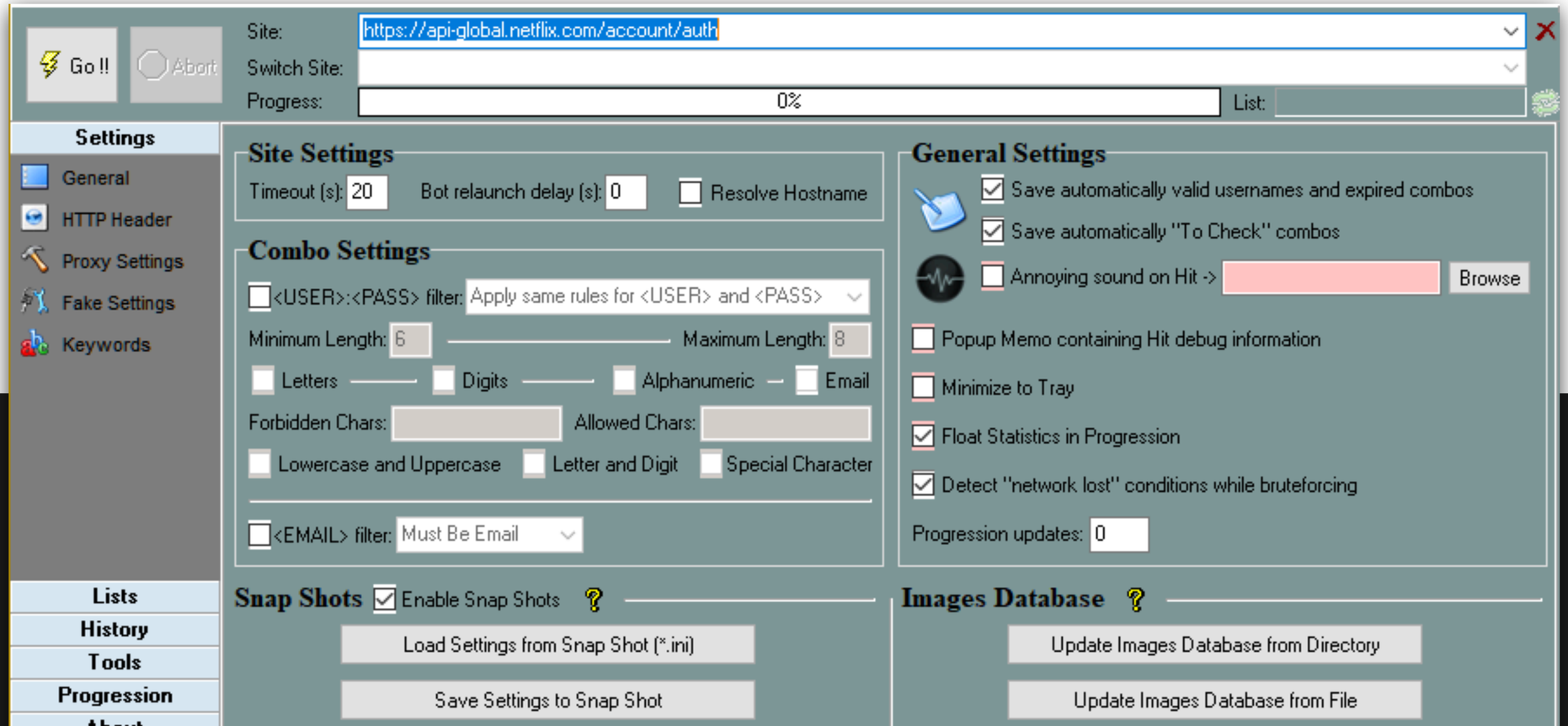
1. The cost of an attack
2. **How attacks have evolved**
3. Where fraud goes from here

Generation 0: Basic HTTP requests with common tools

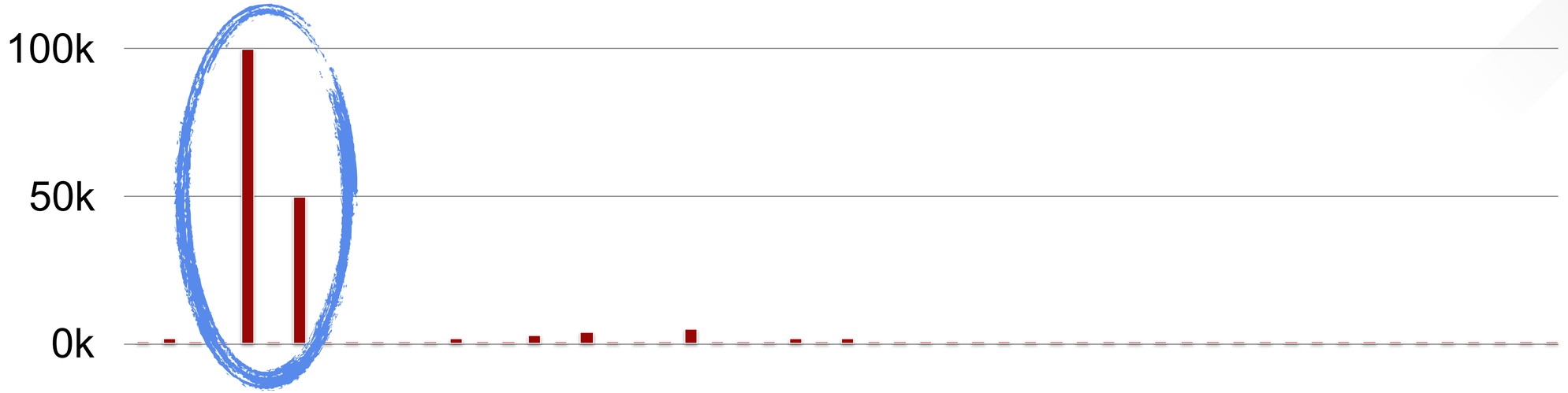
```
$
```

SentryMBA

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



Early defense: IP Rate limiting.



Free Proxy List

FREE PROXY | WEB PROXY | SOCKS PROXY | BUY PROXY | COMPANY

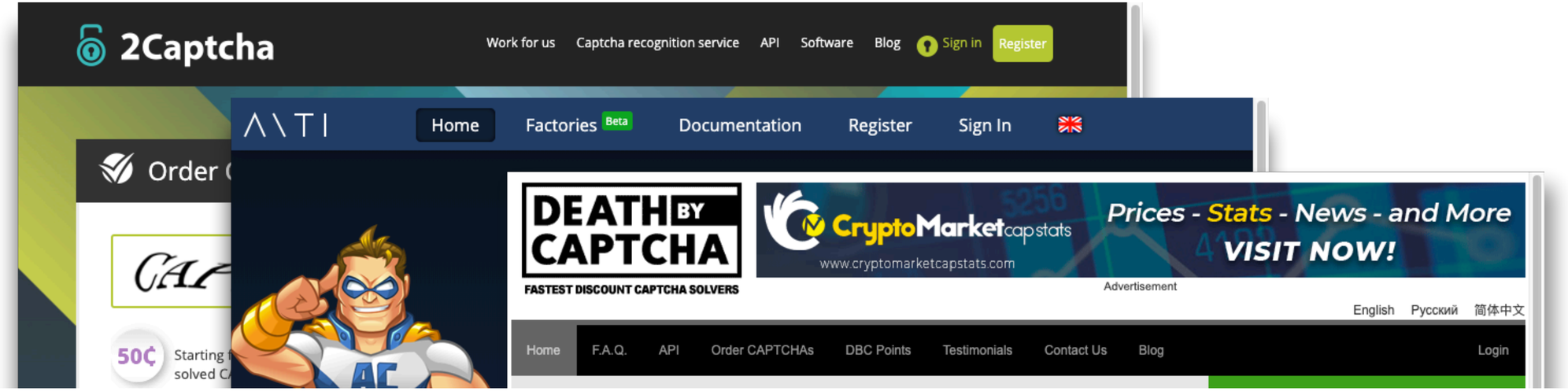
Show 20 entries

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

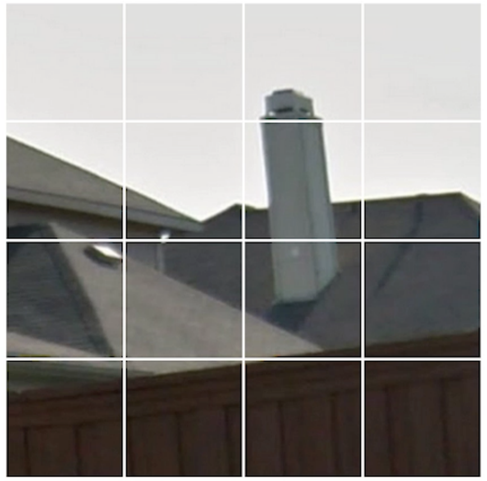
Iteration 1 : Rotate through proxies

Defense: Text-based CAPTCHAs



Iteration 2: Attacks using CAPTCHA Solvers.

Defense: Dynamic sites and JavaScript heavy defenses.



PhantomJS

Full web stack
No browser required

trifleJS

Headless automation for Internet Explorer

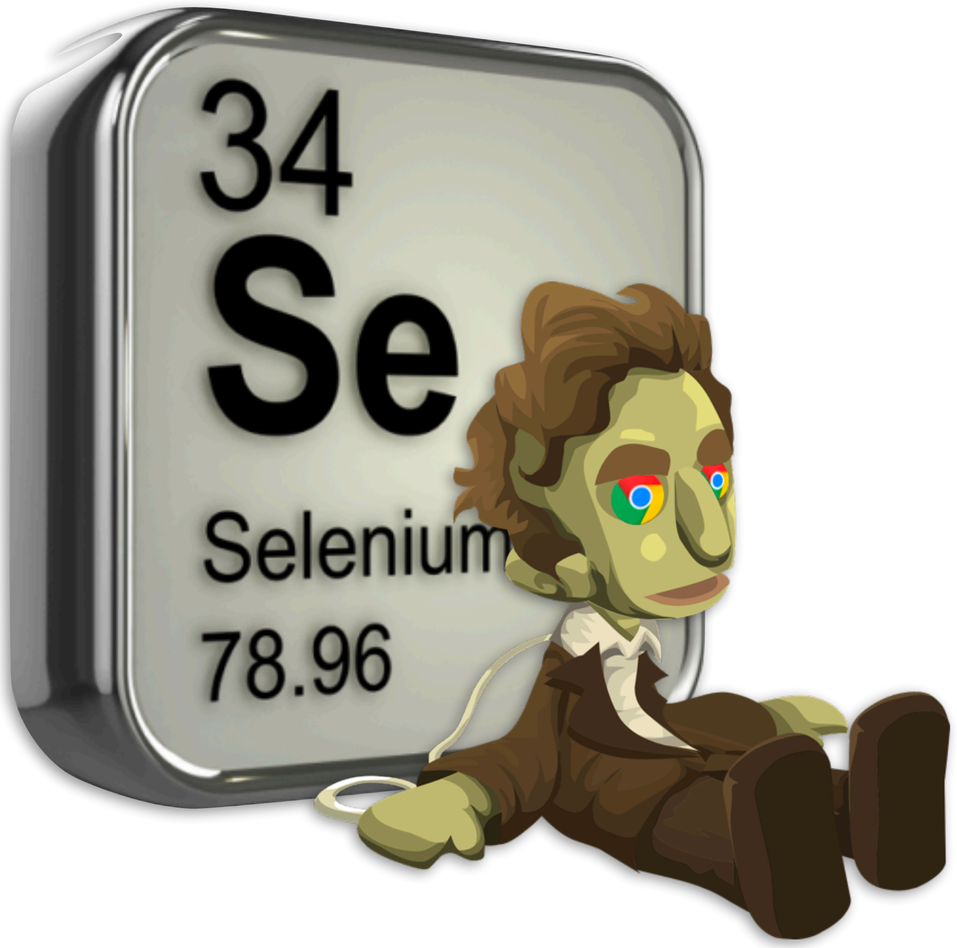
Iteration 3: Scriptable WebViews

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.
(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 (KHT
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.

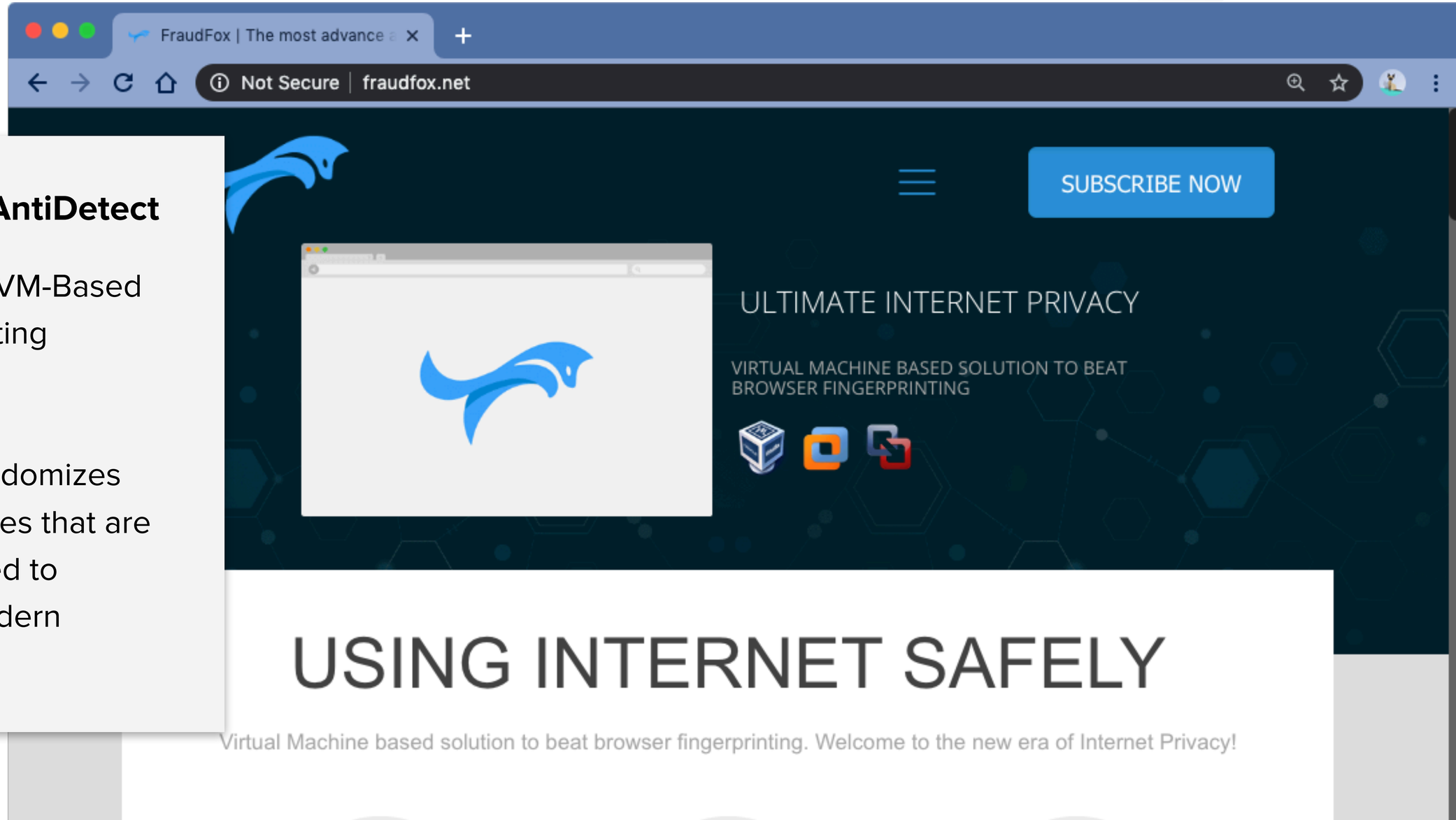
This identifies the source of traffic even when tunneling through proxies.

Iteration 5: Randomizing Fingerprint Data Sources

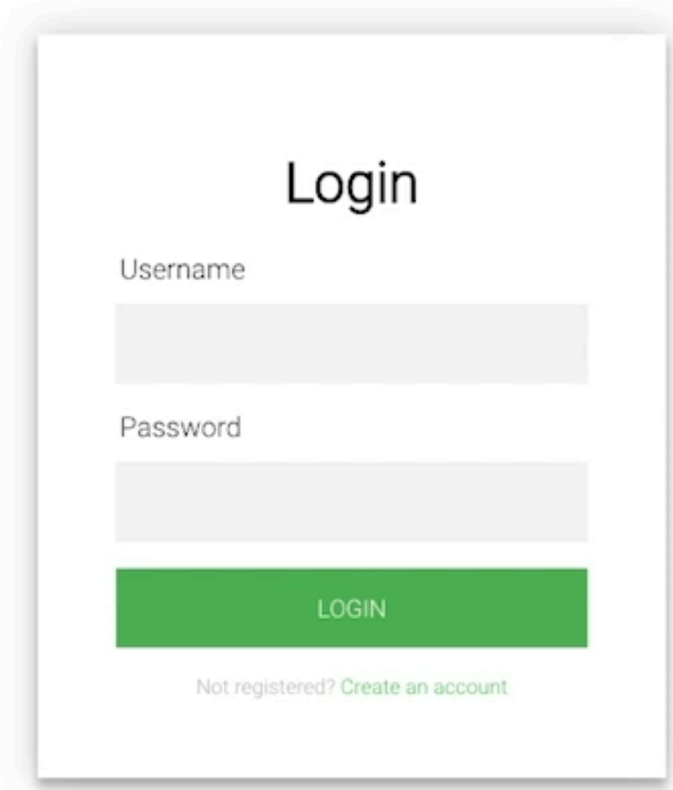
FraudFox & AntiDetect

FraudFox is a VM-Based anti-fingerprinting solution.

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



Defense: Behavior Analysis for Negative Traits



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.

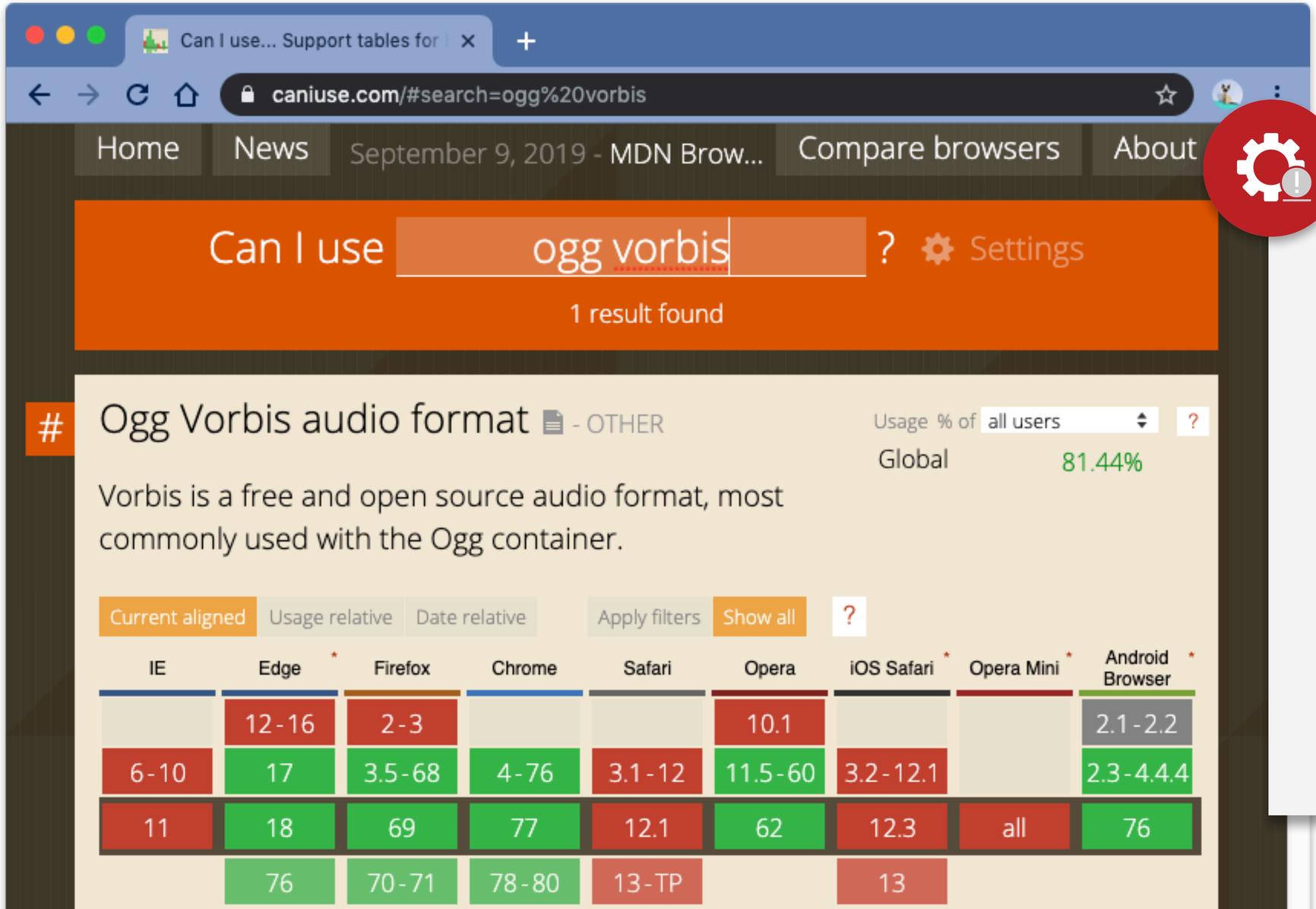
Iteration 6: Behavior Emulation

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



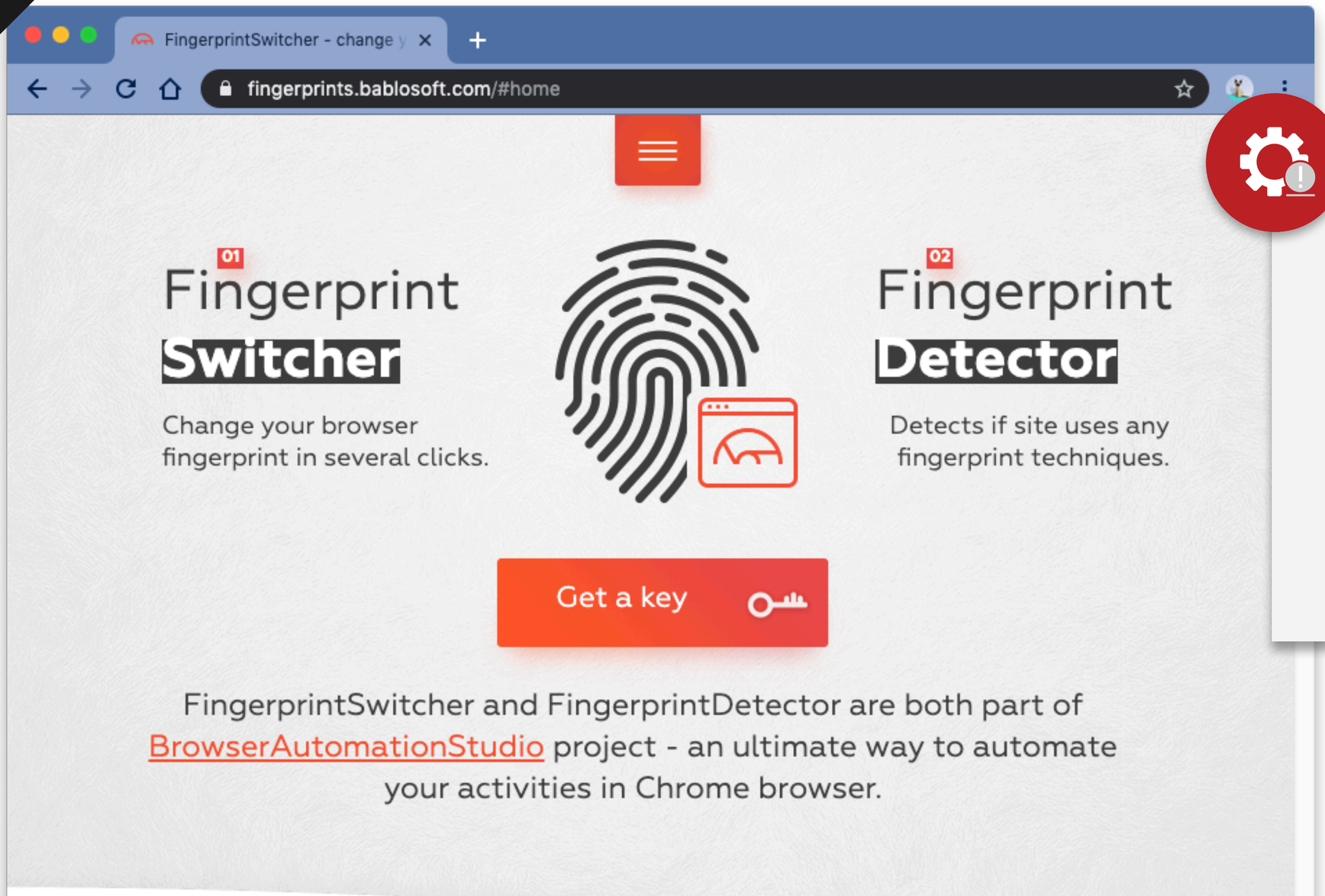
Validating Fingerprint Data

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



Using Real Fingerprints

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

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.

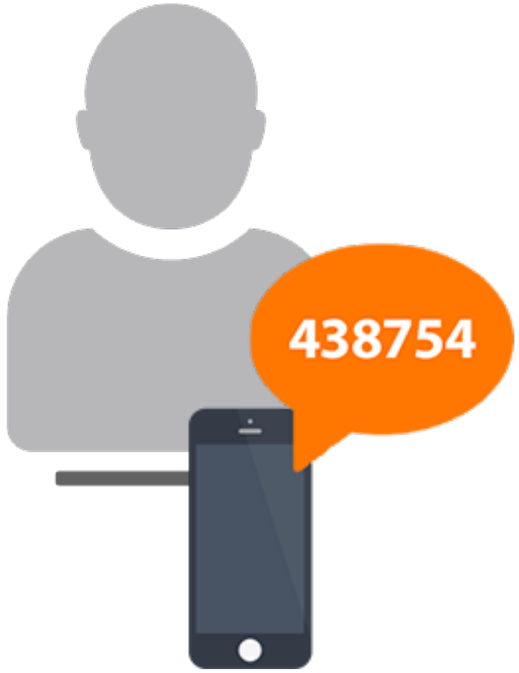
2FA stops automated account takeovers.

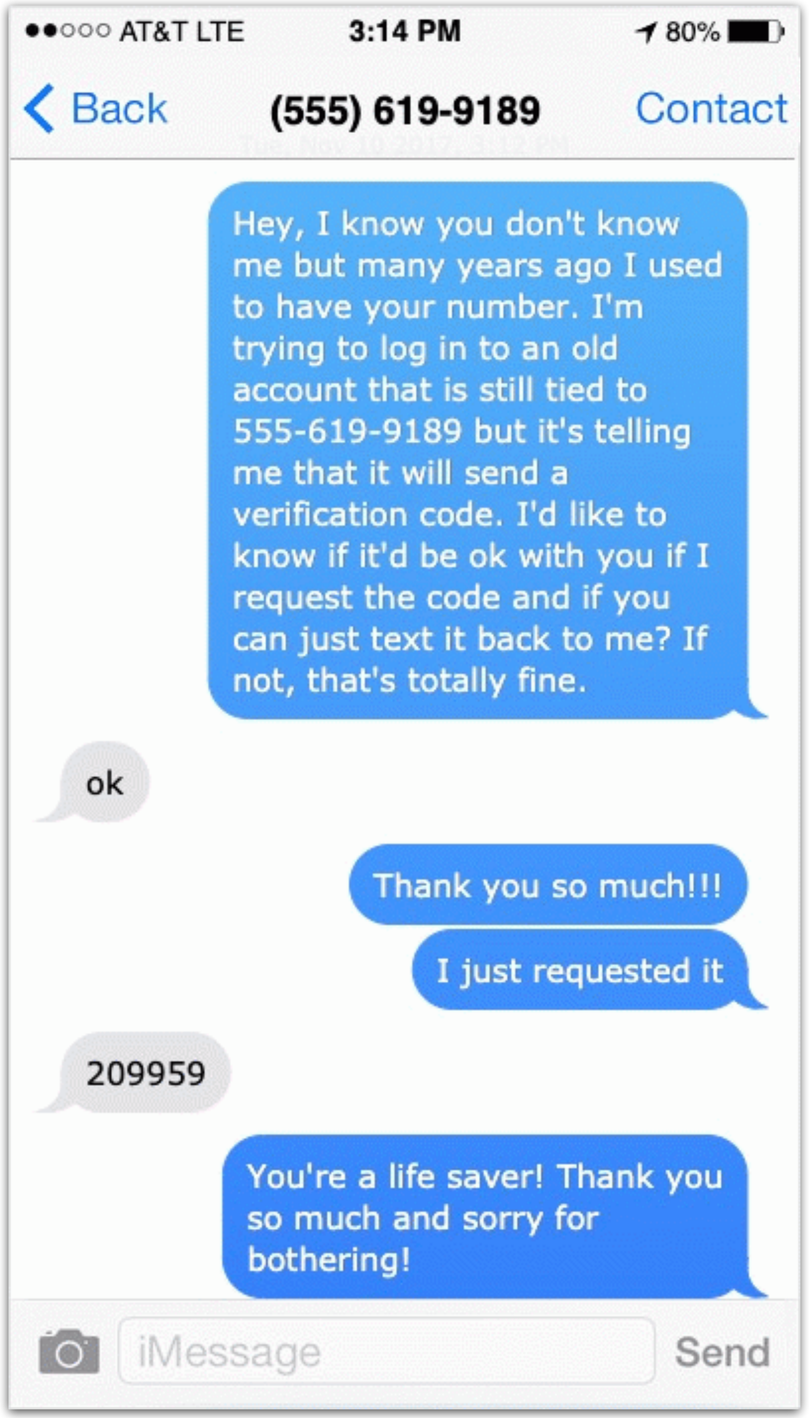
The goal of credential stuffing is to find valid accounts.

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.

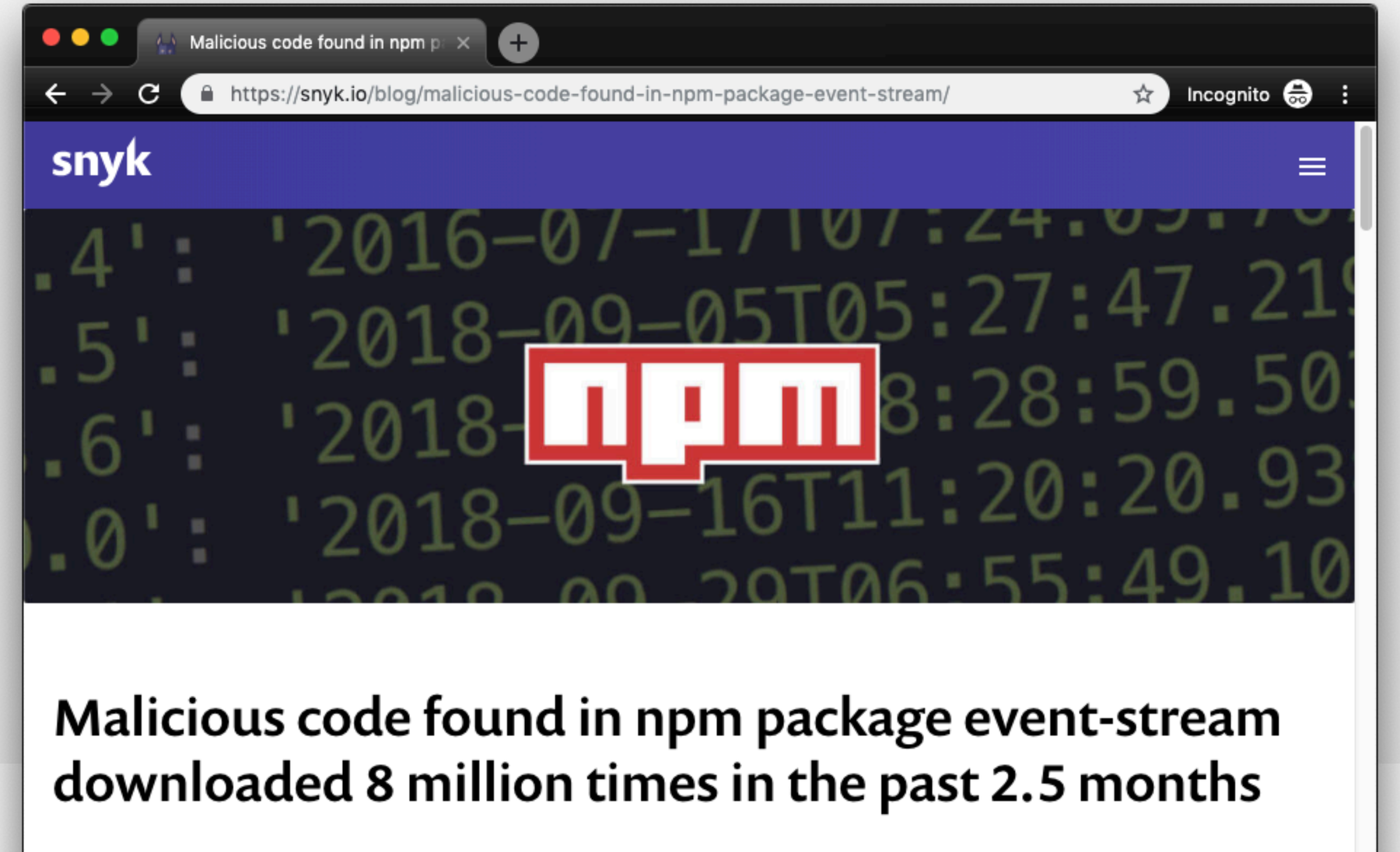




A valid account changes the game.
Manual social engineering is an option.

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

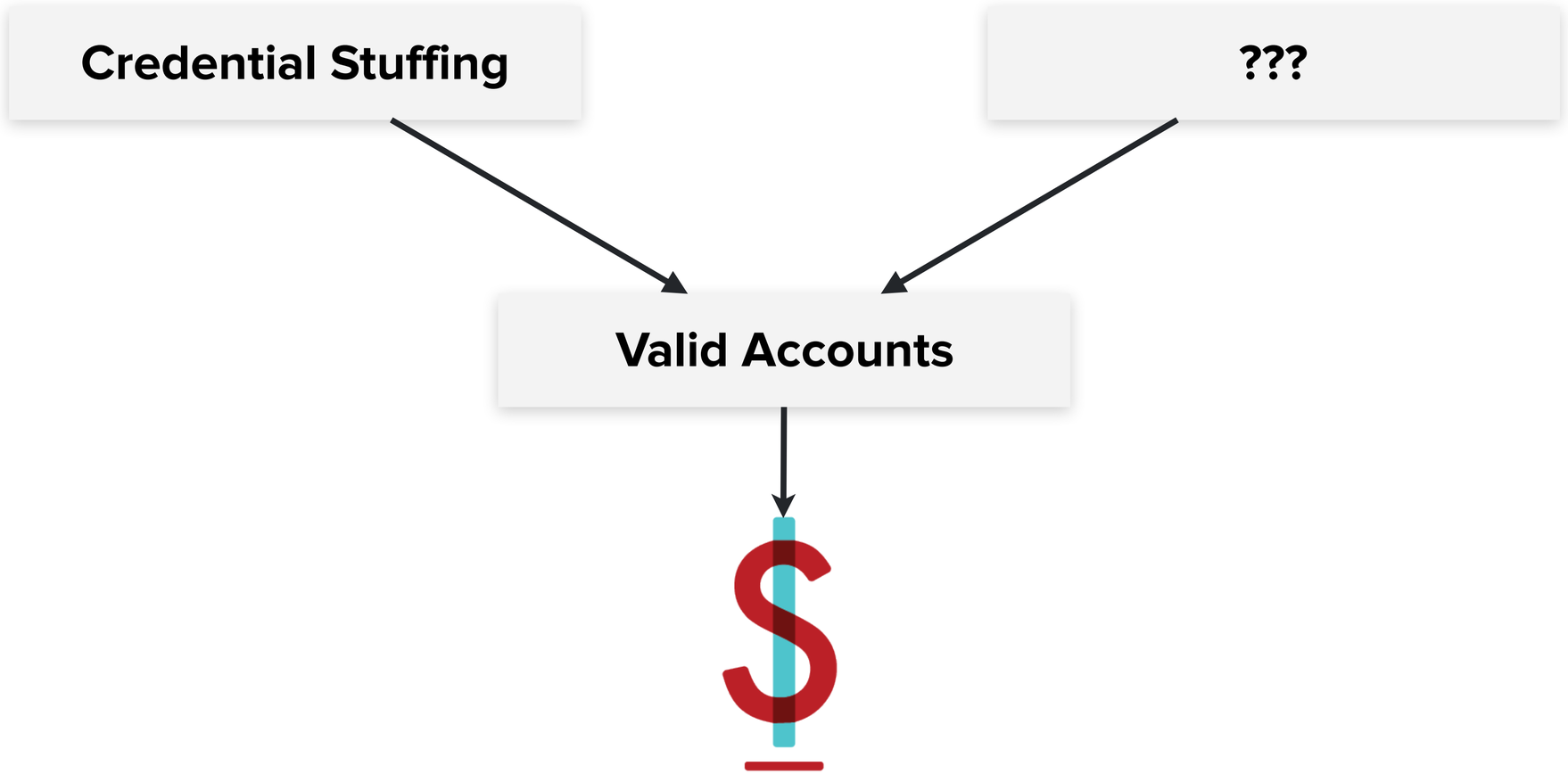
Open source supply chain attacks inject malware directly into your applications.



What's next?

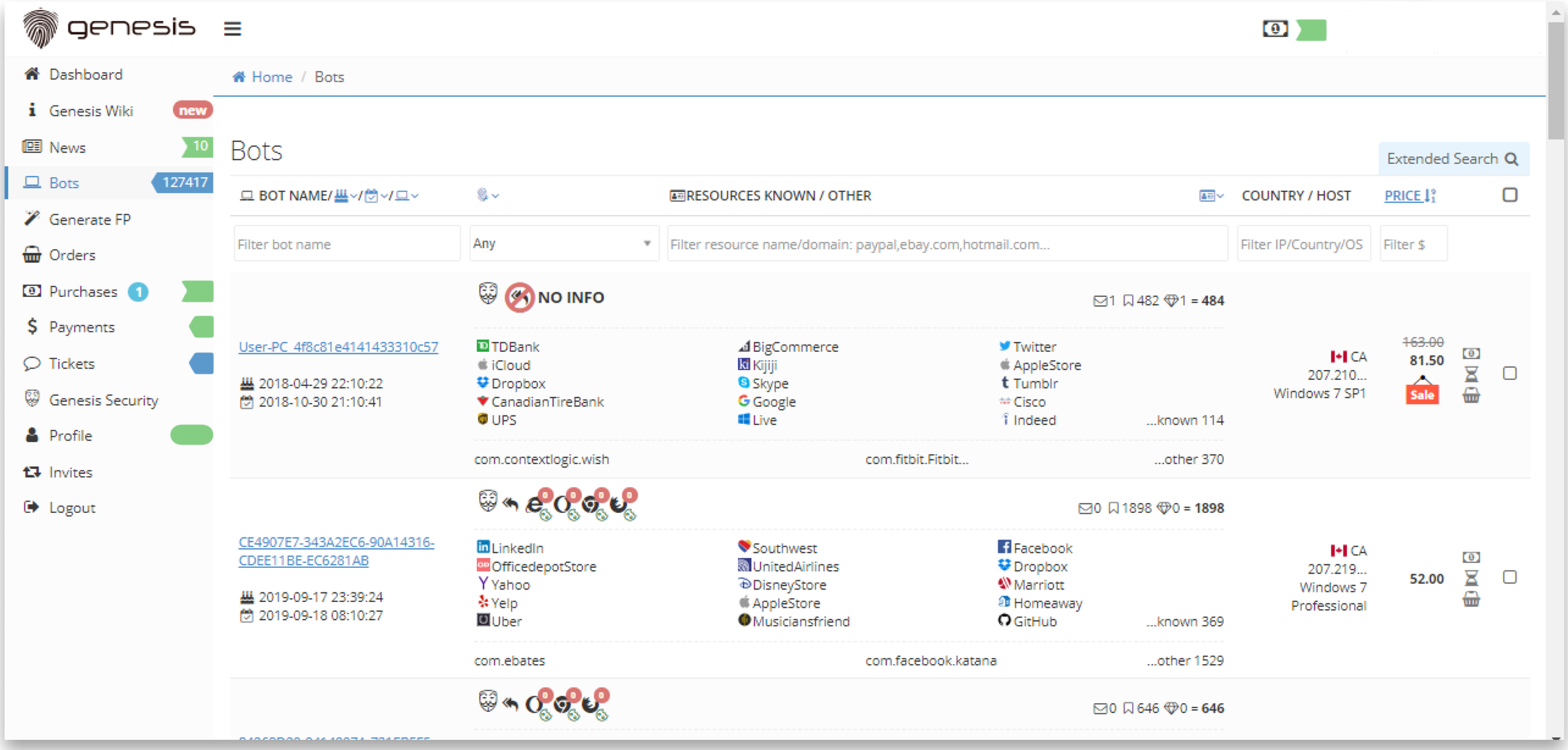
The value in our accounts is not going away.

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

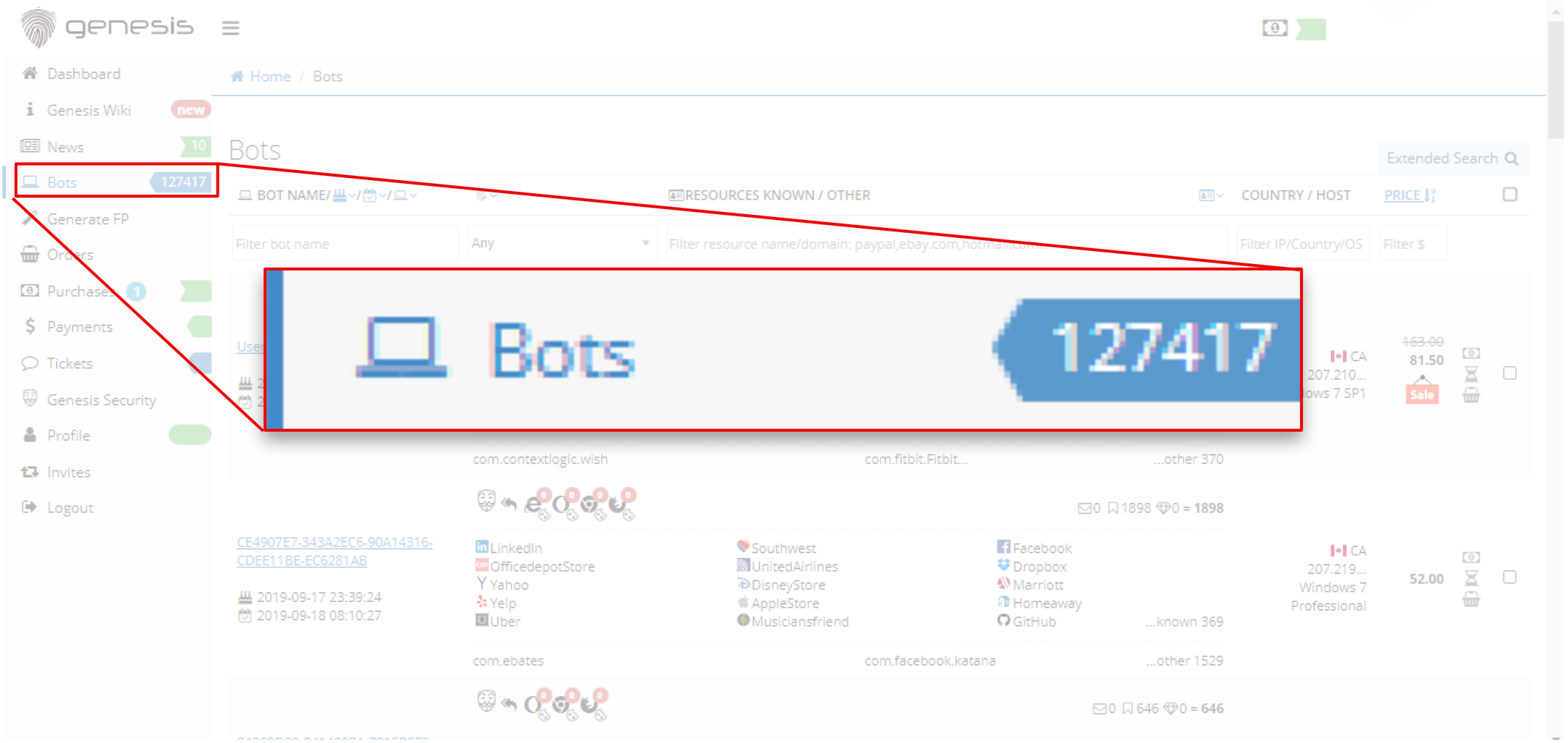


Genesis is an early example of the next generation.

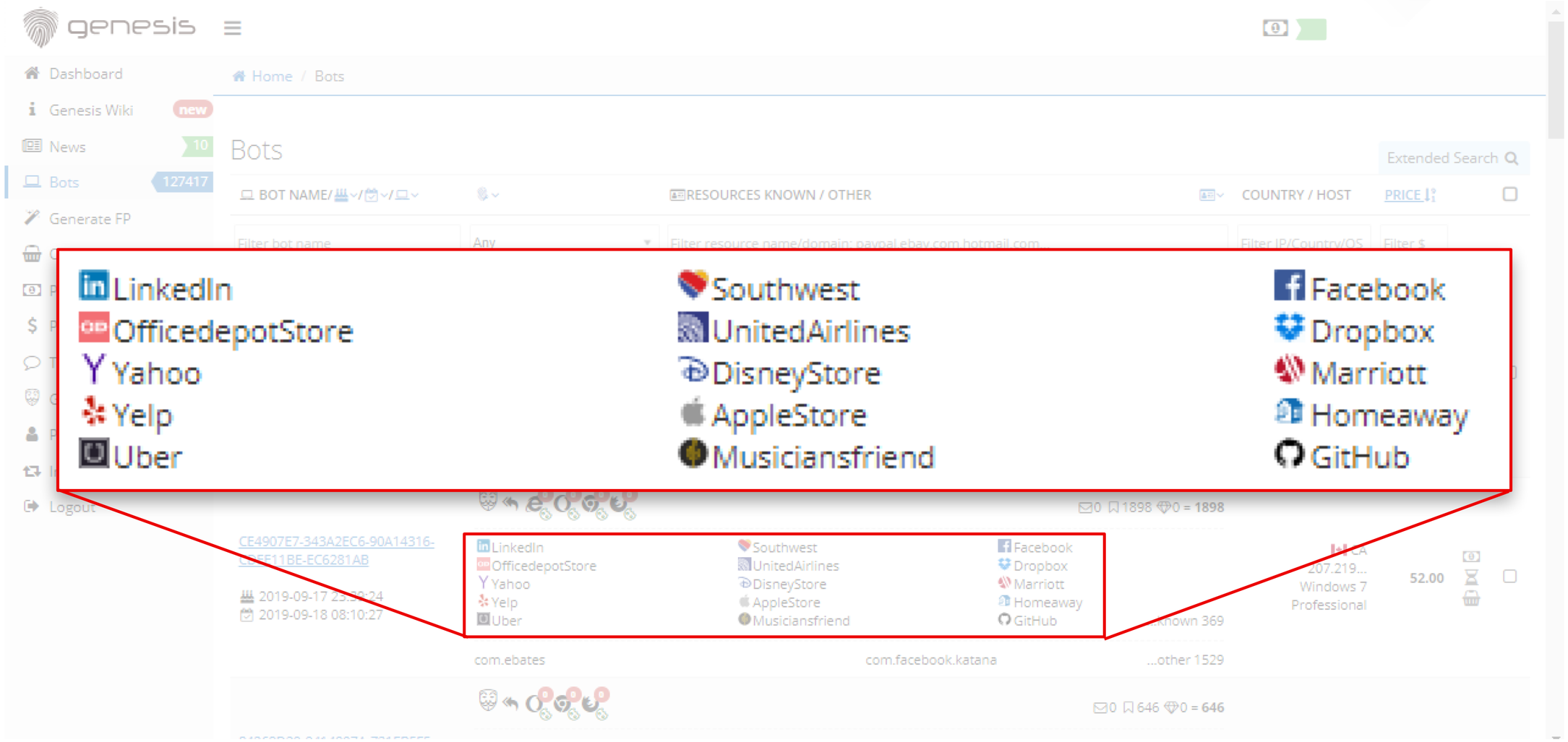
Malware that resides at the host to scrape account and environment details.



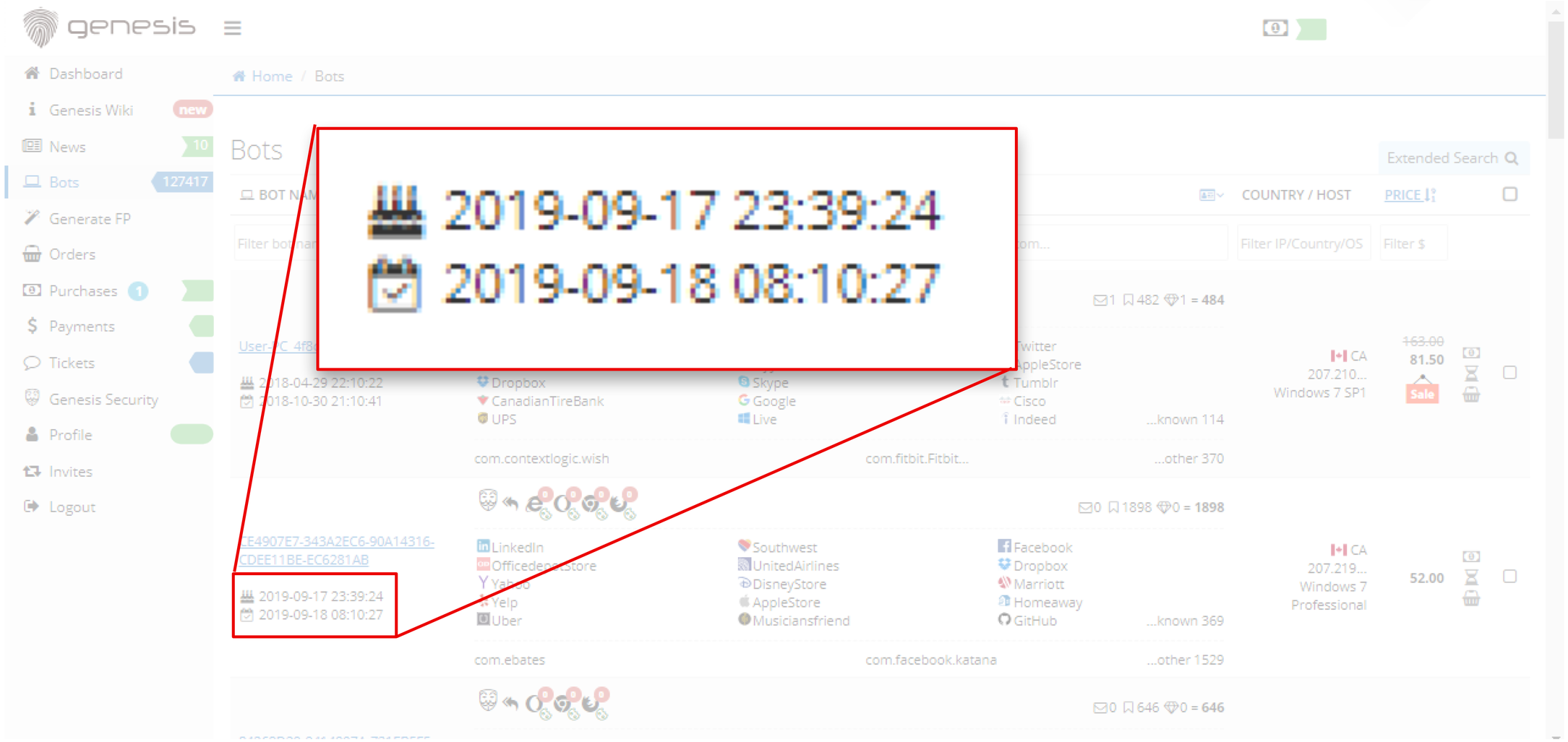
Thousands of infections and growing.



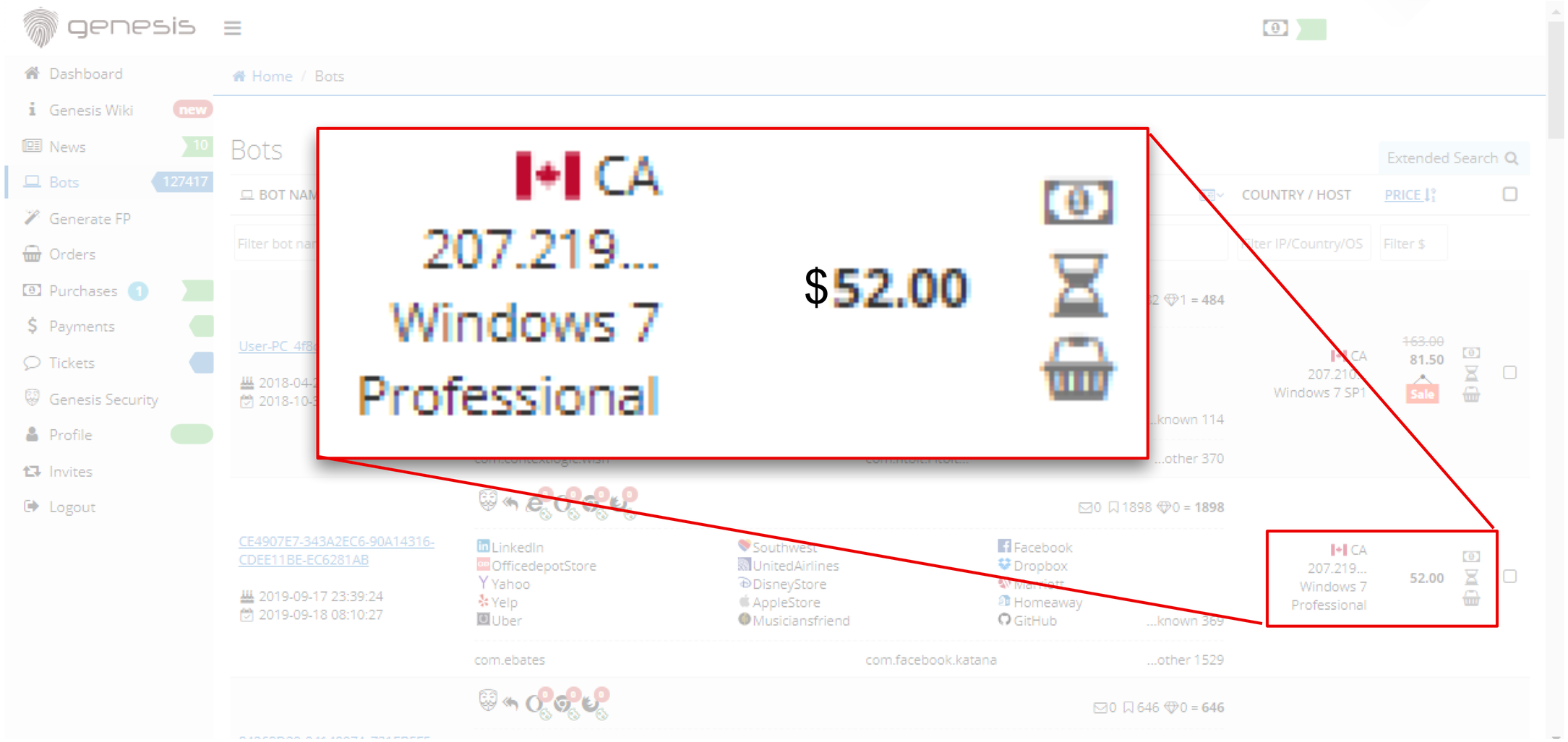
Advertises the high profile accounts the bot has already scraped.



Regularly updates its records with newly acquired accounts.

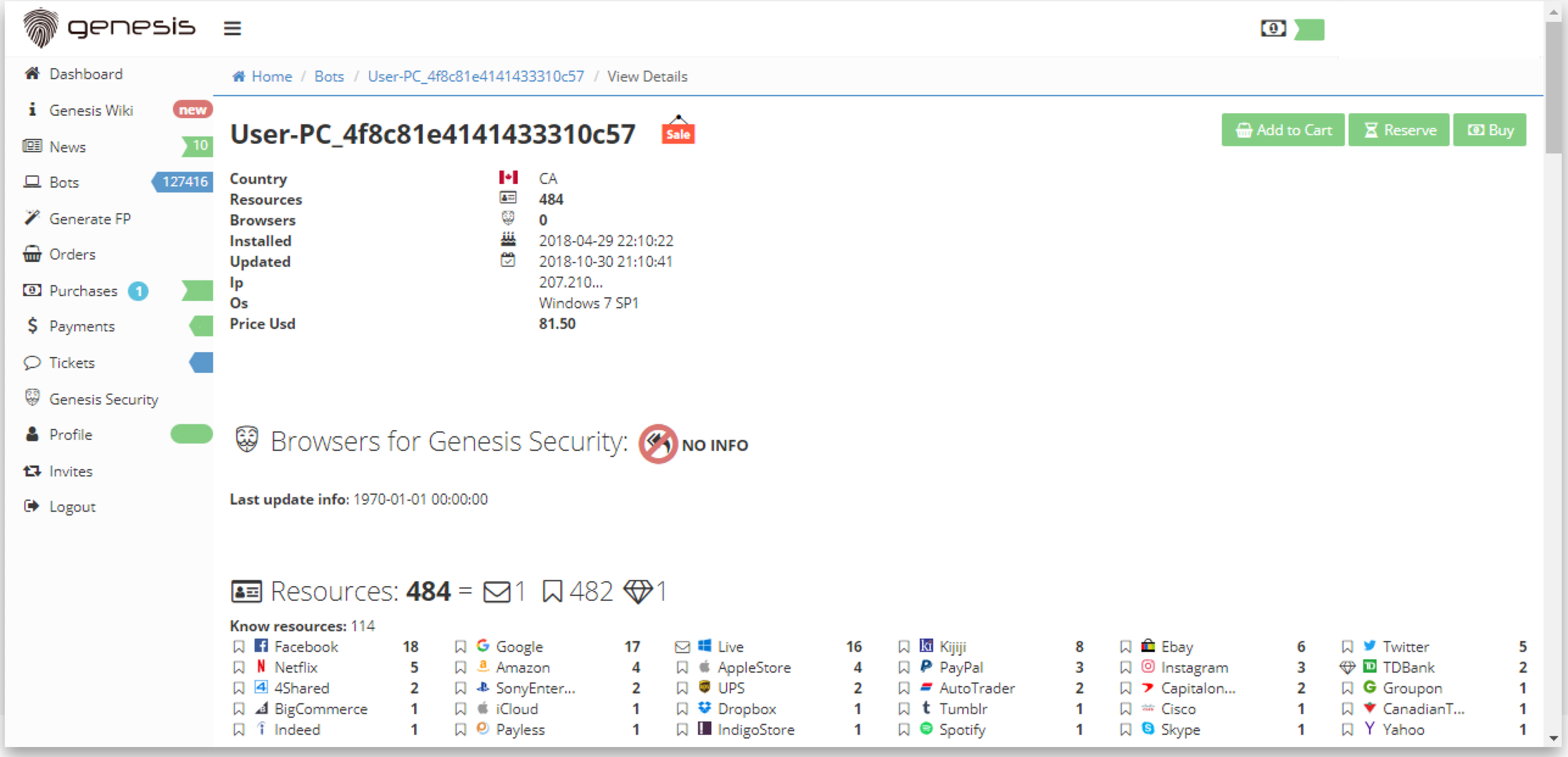


Each infected computer and its data is sold as one unit



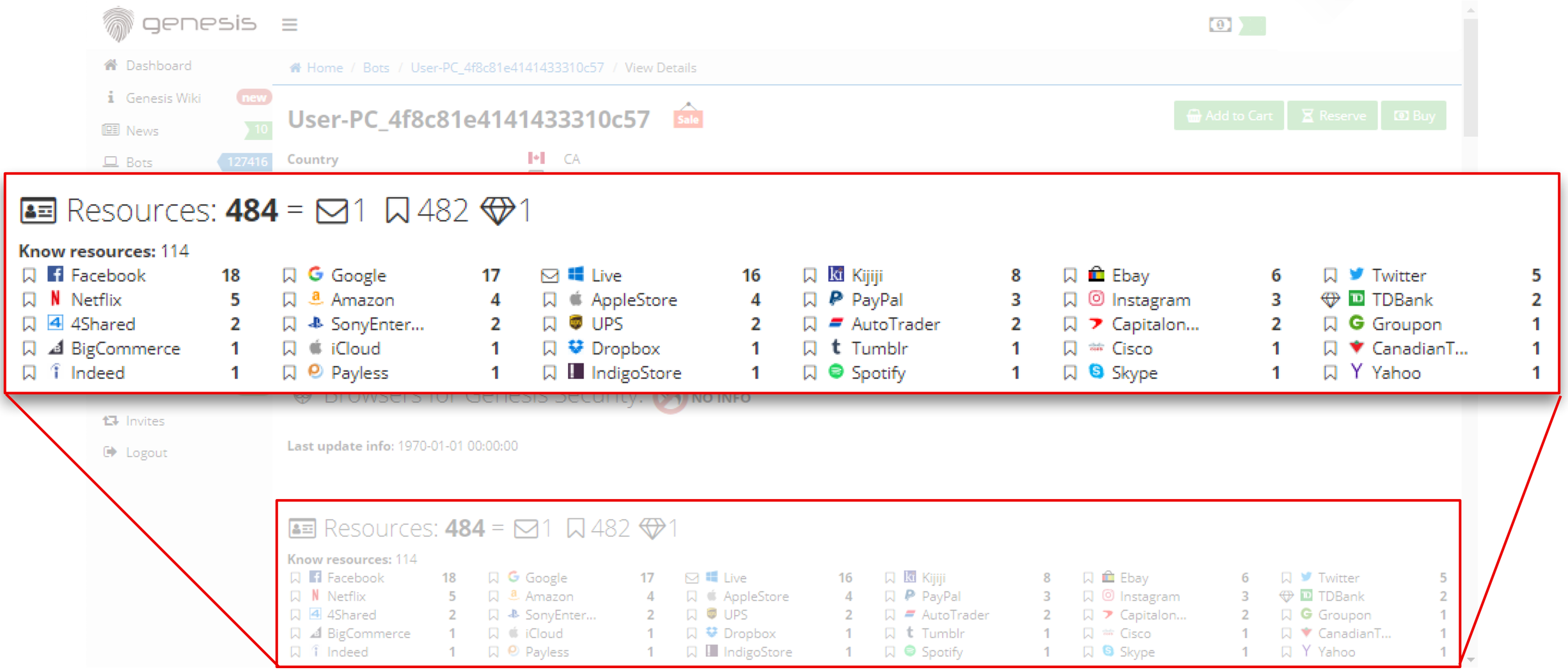
Each bot gives the purchaser exclusive access to its data.

One buyer per bot.



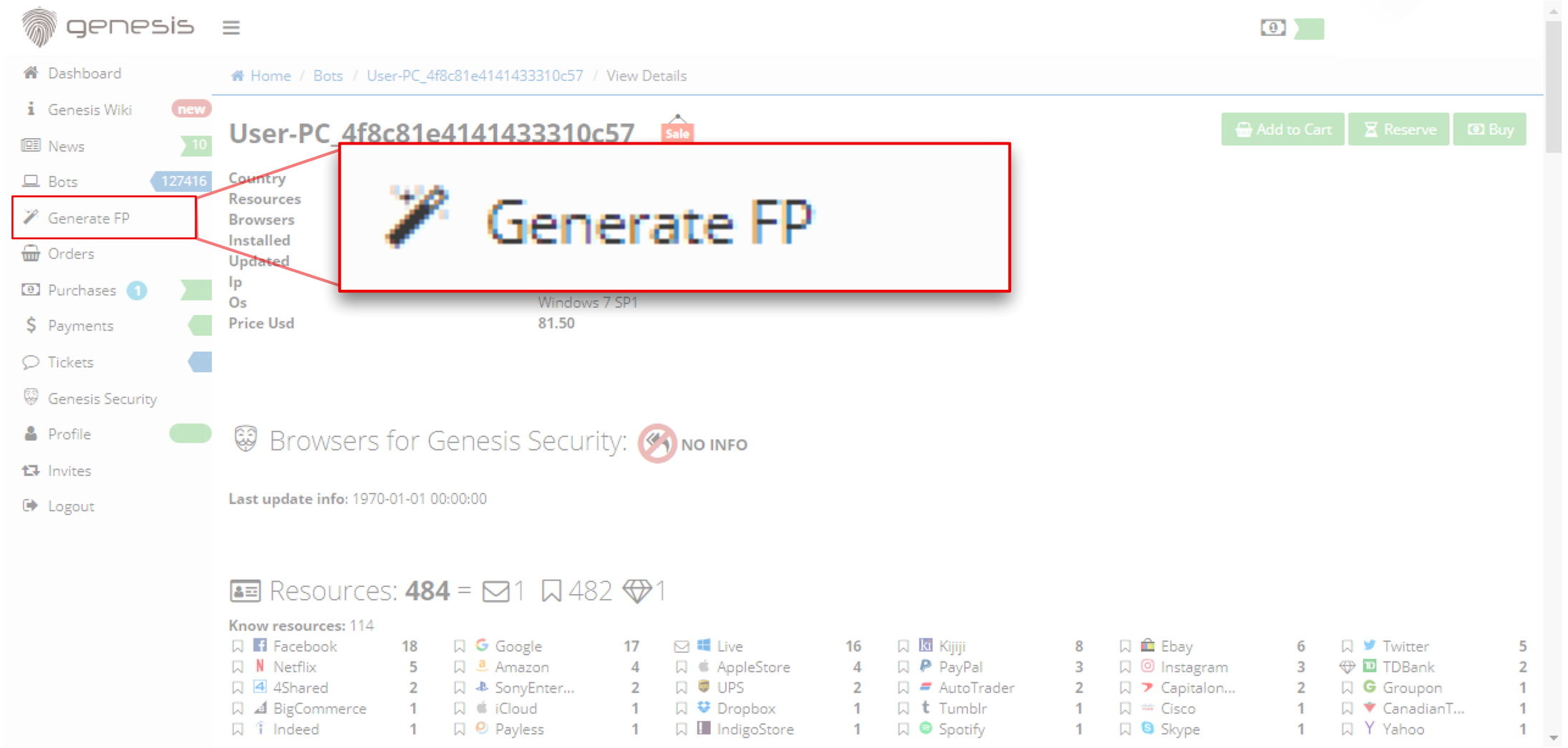
Bots can have hundreds of scraped resources and accounts.

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



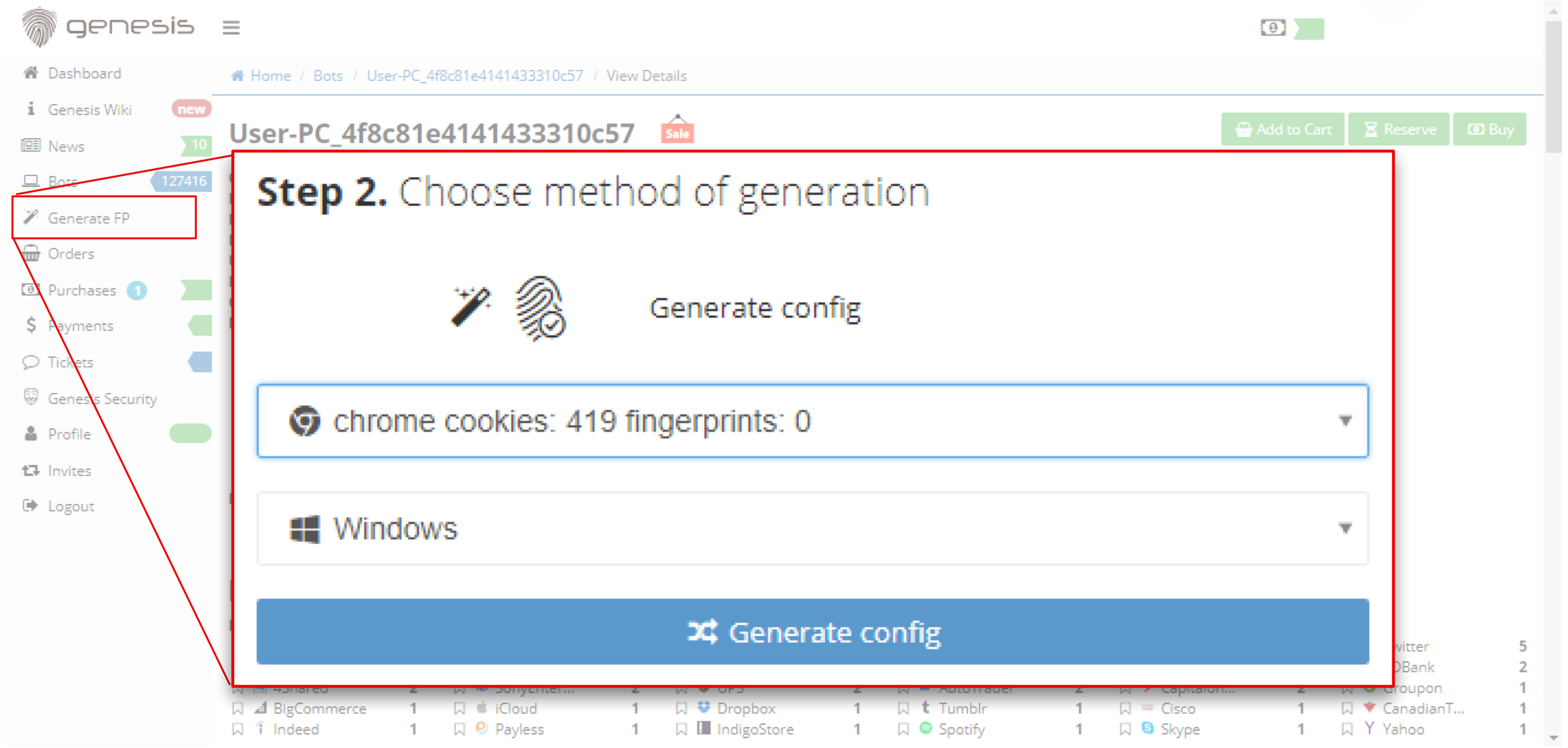
Genesis can generate the fingerprints of your exact target.

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



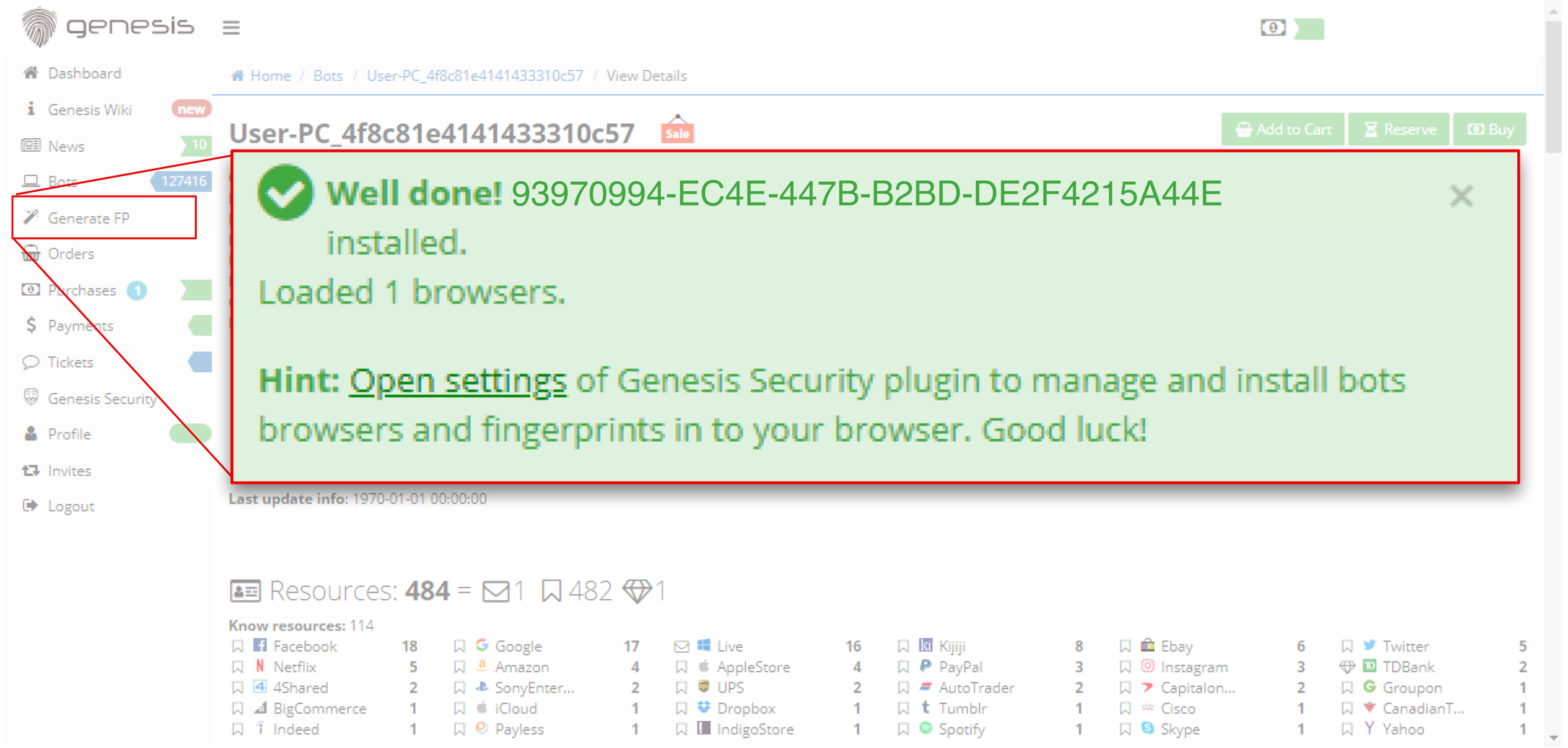
Select the fingerprint you are looking for

Configure which parts you want to emulate



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

Voila! Now you are your target.



It follows the rules of shady actors in the CIS.

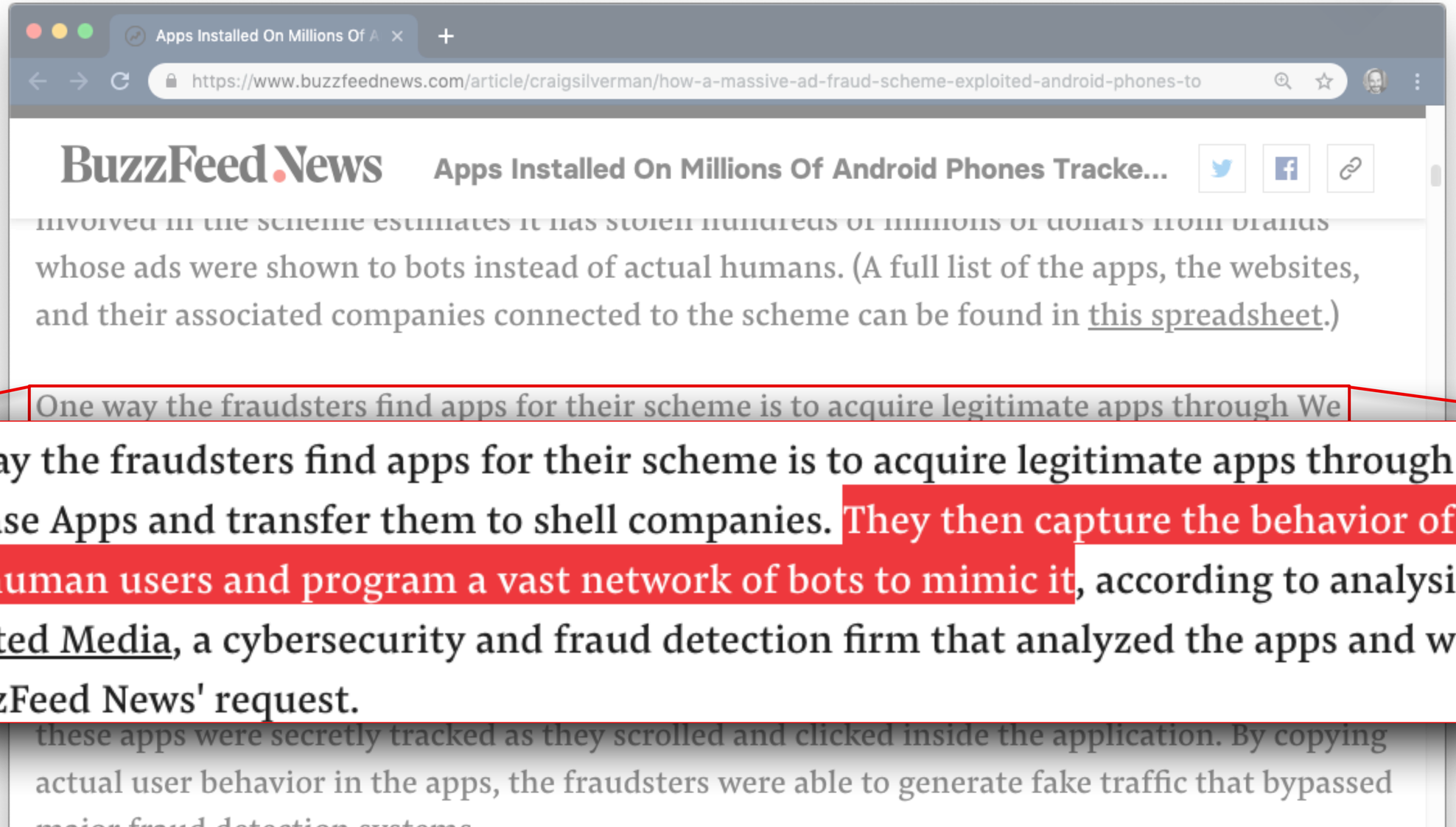
Genesis Store & Genesis Security Terms of Service

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.



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.

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.**

THANK YOU

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

Jarrod Overson

@jsoverson on twitter, medium, and github.