The Games Shape Plays

Mitigate Bots and other Automated Attacks with F5

Luboš Klokner | F5 | Senior Solution Engineer

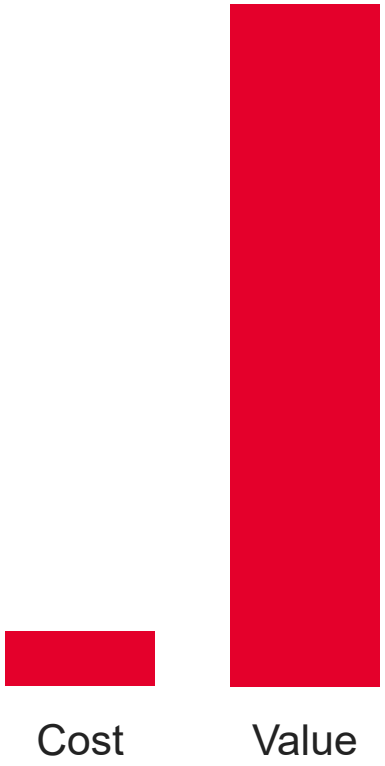
Phil Venables
@philvenables

Attackers have bosses and budgets too.

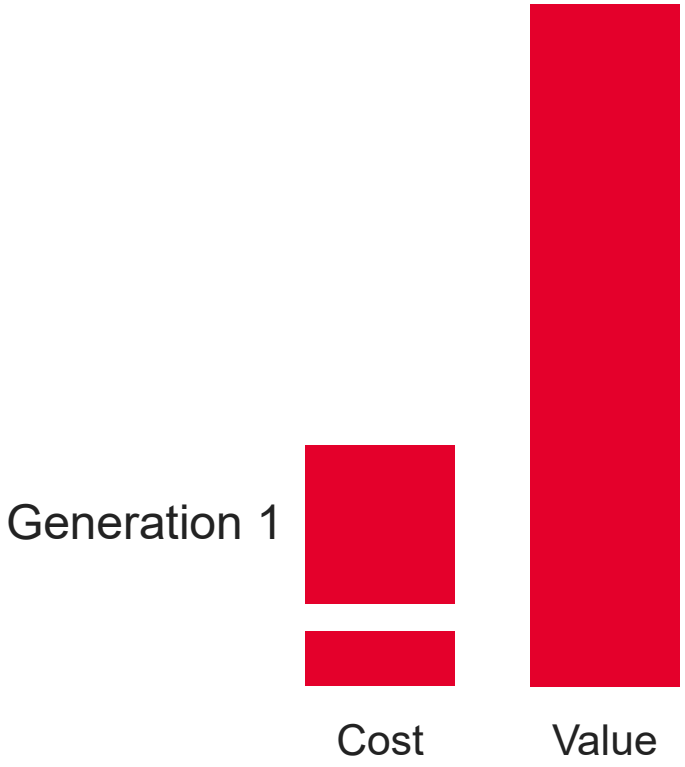
12:01 AM · Sep 14, 2014 · Twitter for iPhone

Cost vs Value

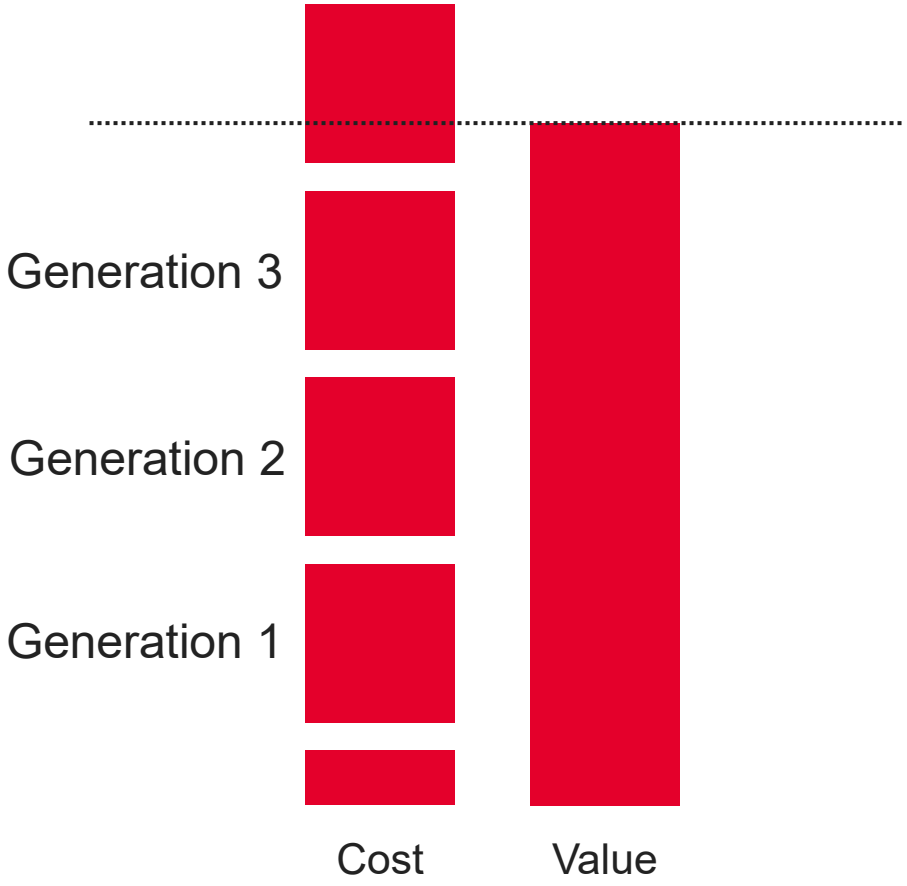
…with no defenses in place, it costs nothing to attack.



Adding a defense increases cost by forcing evolution.

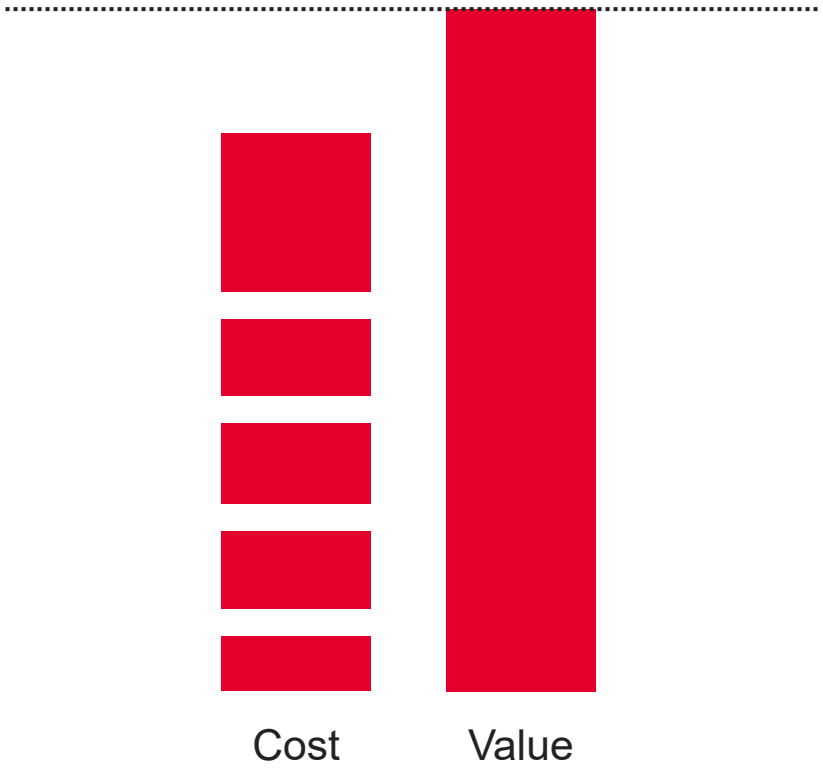


Enough defenses will tip the cost/value ratio in your favor.

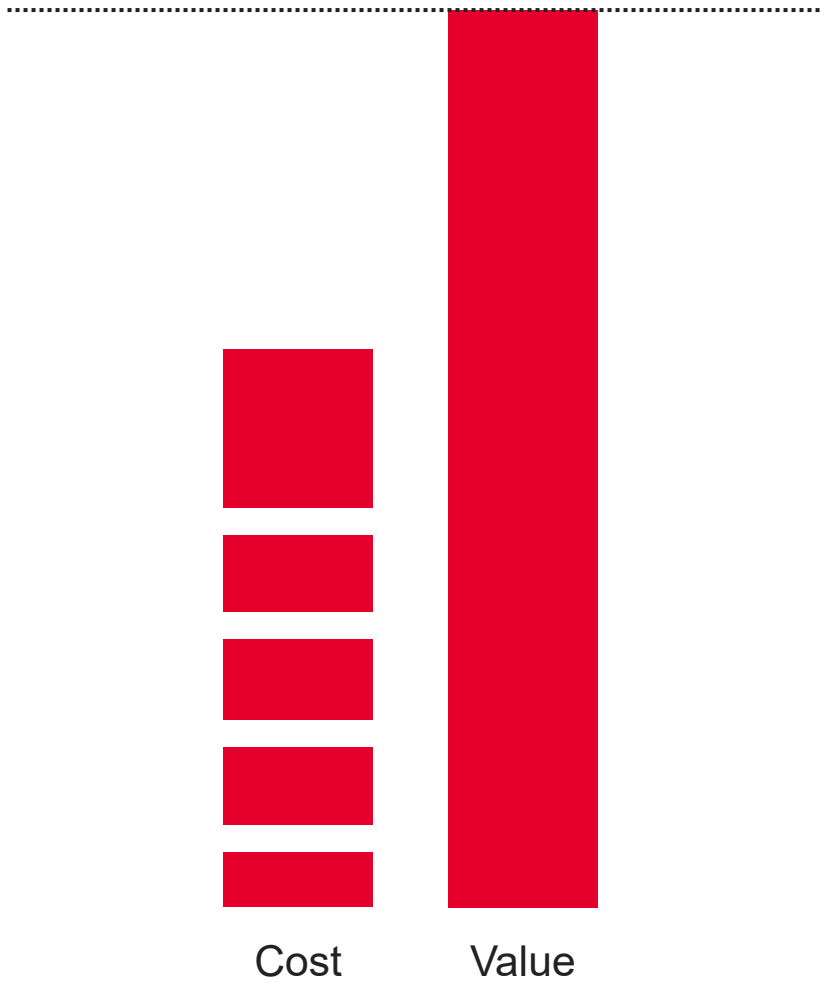


As with all technology, the cost of entry decreases over time.

TECHNOLOGY BECOMES CHEAPER THE MORE IT BECOMES GENERALIZED AND UNDERSTOOD



While the value of successful attacks only goes up.



What’s the cost?

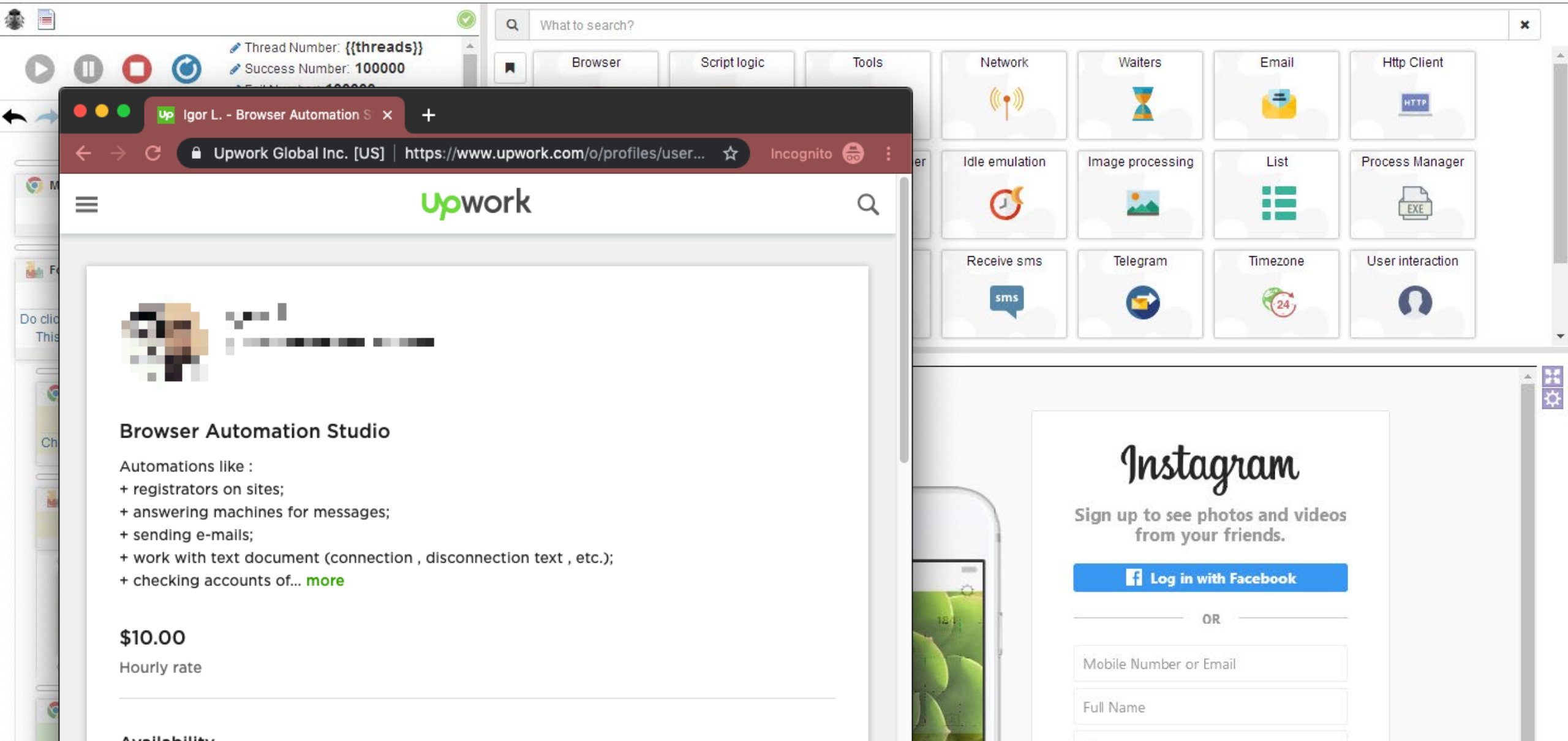
What's the cost?

BREAK OUT THE COMPONENTS.

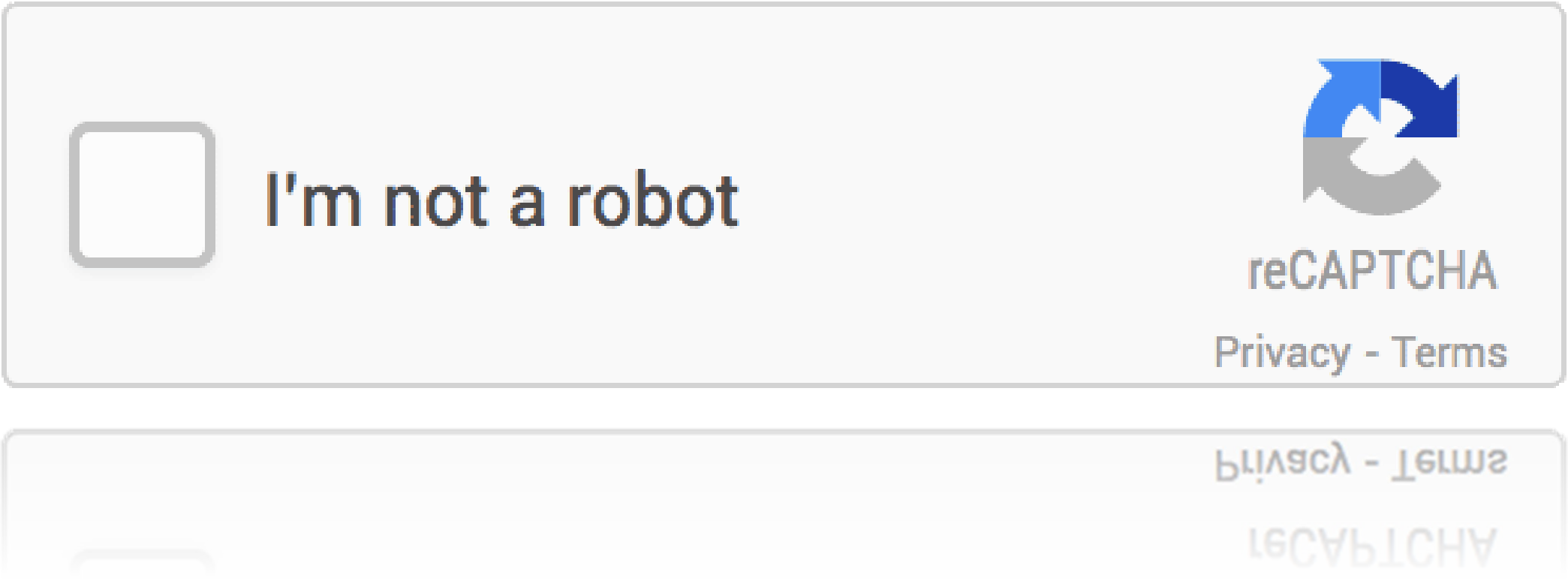
1. Gather a dataset (e.g. credentials)
2. Automate your actions (e.g. login)
3. Defeat Existing Defenses (e.g. CAPTCHA)
4. Scale up

1. Gather your dataset

2. Automate your actions



3. Defeat defenses



3. Defeat defenses

Best Captcha Solving Service |

deathbycaptcha.com

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

ENGLISH

Home F.A.Q. API Order CAPTCHAs DBC Points Testimonials Contact Us Blog LOGIN SIGN-UP

Best CAPTCHA Solver Bypass Service

With DeathByCaptcha 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 incredibly 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.
- An ***average response time of 9 seconds*** for normal text CAPTCHAs, with an ***average accuracy rate of 90% or more***. And you always pay for correctly solved CAPTCHA only!
- Easy-to-use ***API*** available for most popular programming languages.
- ***DeCaptcher*** and ***Antigate (Anti-Captcha)*** API support to make migration to ***Death By Captcha*** as easy as possible.

STATUS: OK

Average Solving Time
16 seconds (1 minute ago)
20 seconds (5 minutes ago)
20 seconds (15 minutes ago)

Updates

Apr 24: 20% OFF , as free credit, on all the 100K CAPTCHA packages ordered via our Avangate/2Checkout payment processor - Order Now!! Valid until June 30. Contact us with your username and payment details to add the freebies and/or if you have any

4. Scale up

A campaign of 100,000 ATO attempts runs around $200

$0

For 2.3 billion credentials

$0 - 40

For an automation tool

$0 - 140

To solve 100,000 CAPTCHAs

$0 - 10

For 1,000 IPs

< $0.002

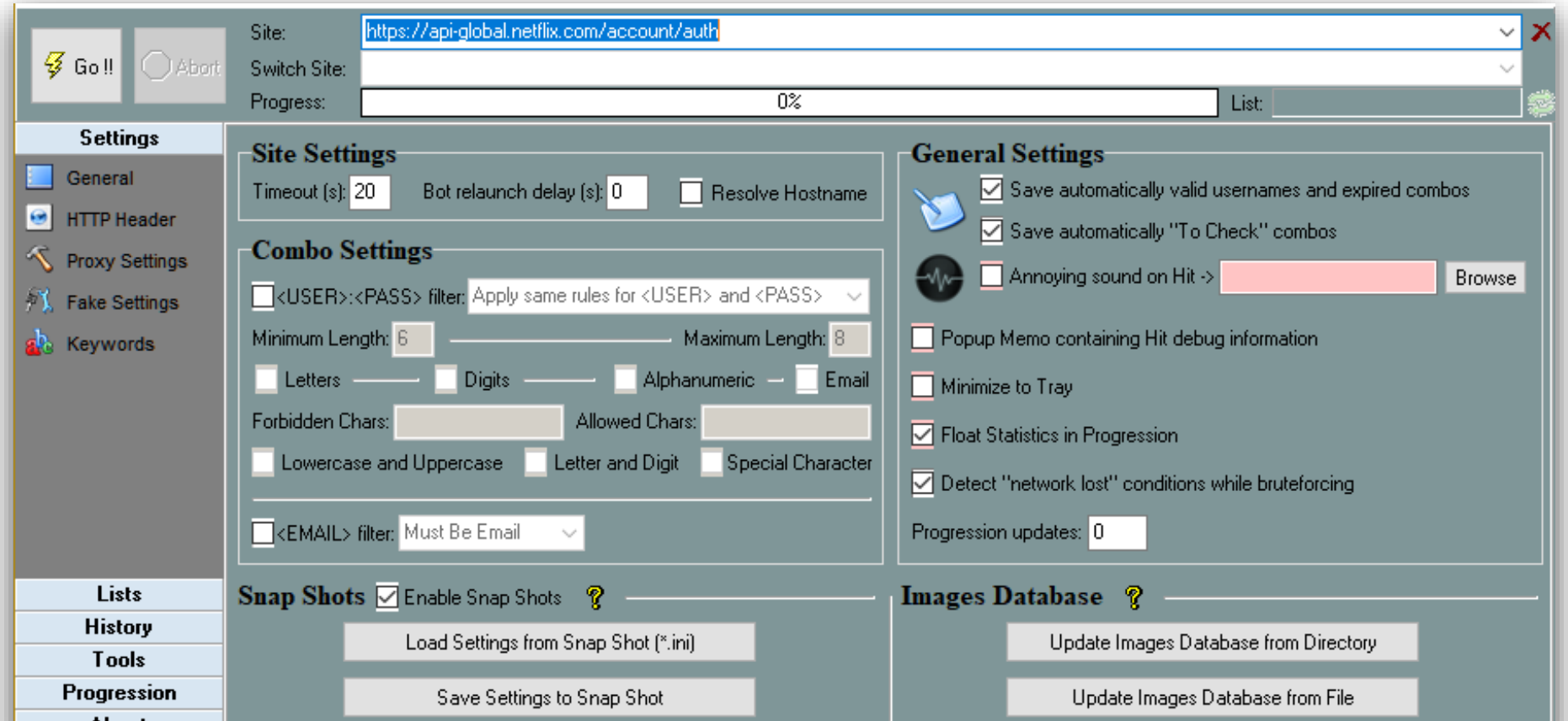
Two tenths of one penny per ATO attempt.

Evolution of the tools

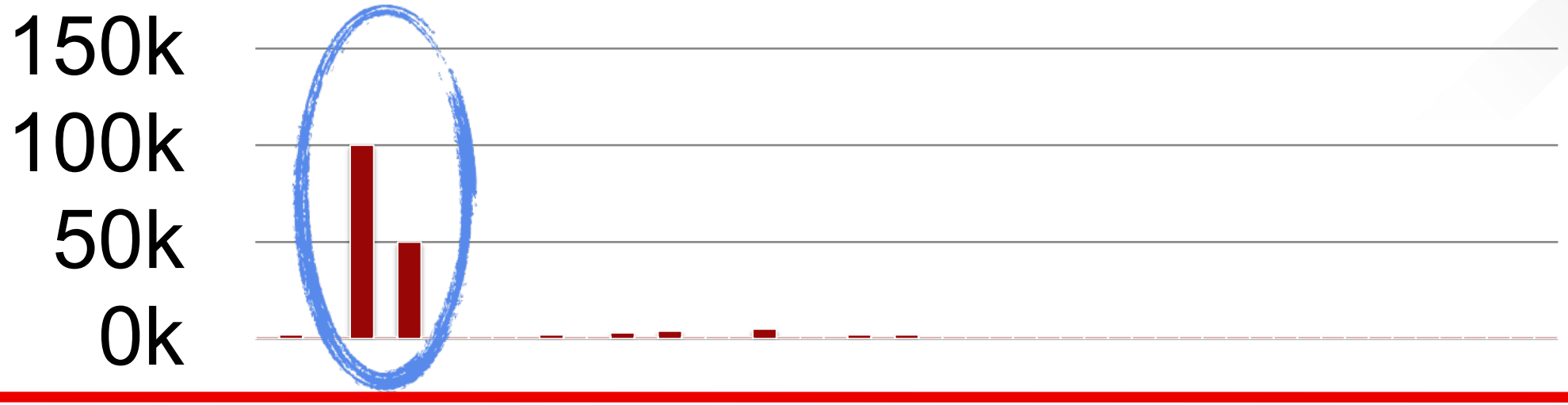
Generation 0: Basic HTTP requests with common tools

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

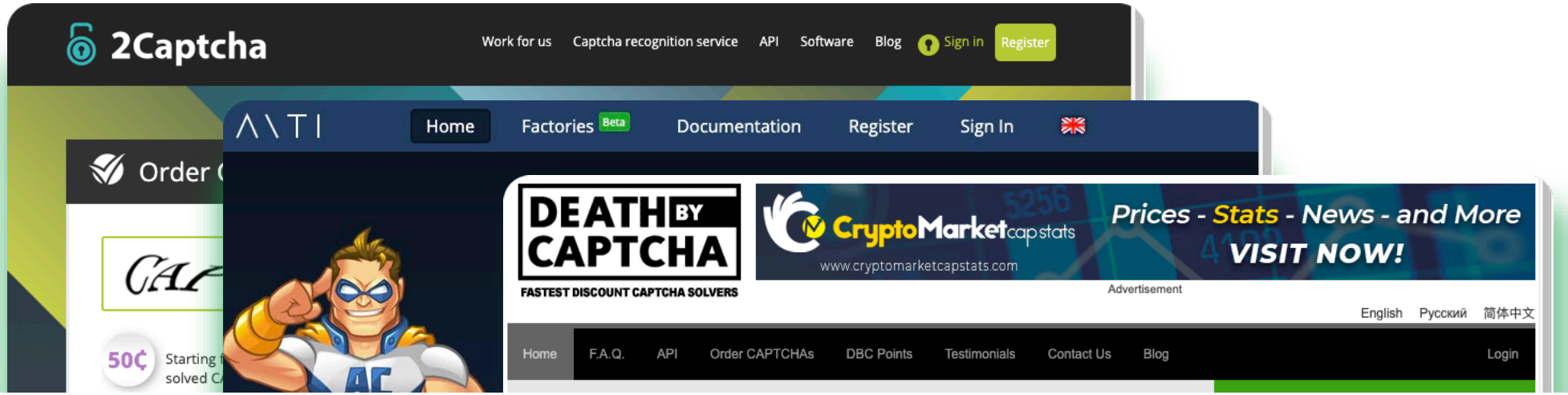
Show 20 entries

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

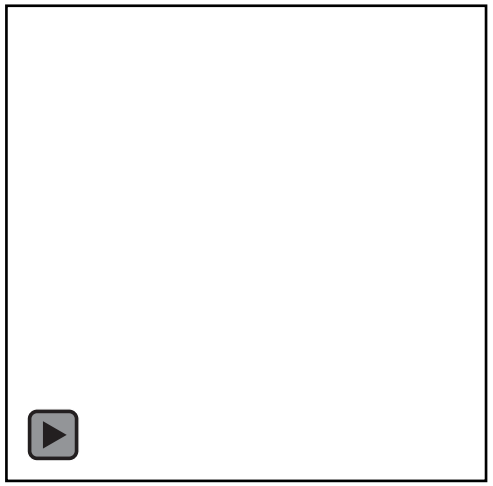
Iteration 1 : Rotate through proxies

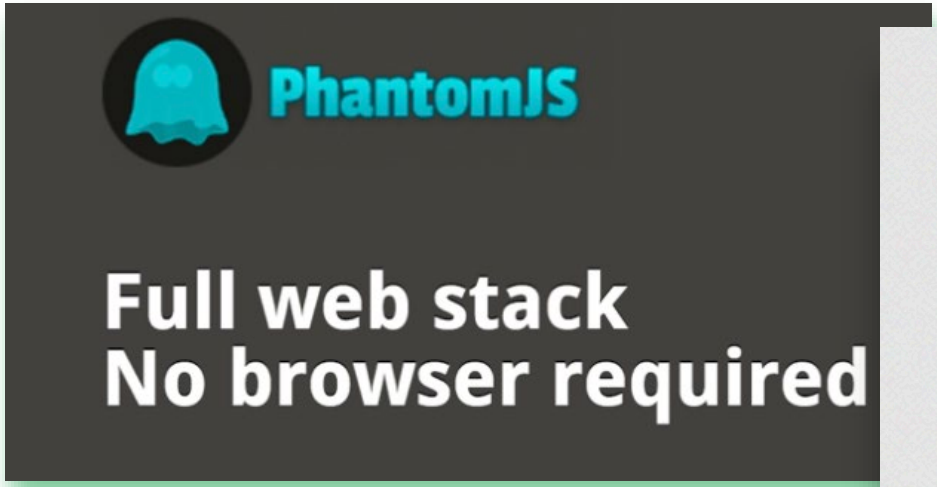
Defense: Text-based CAPTCHAs



Iteration 2: 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 Gec
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ru;q=0.6
```

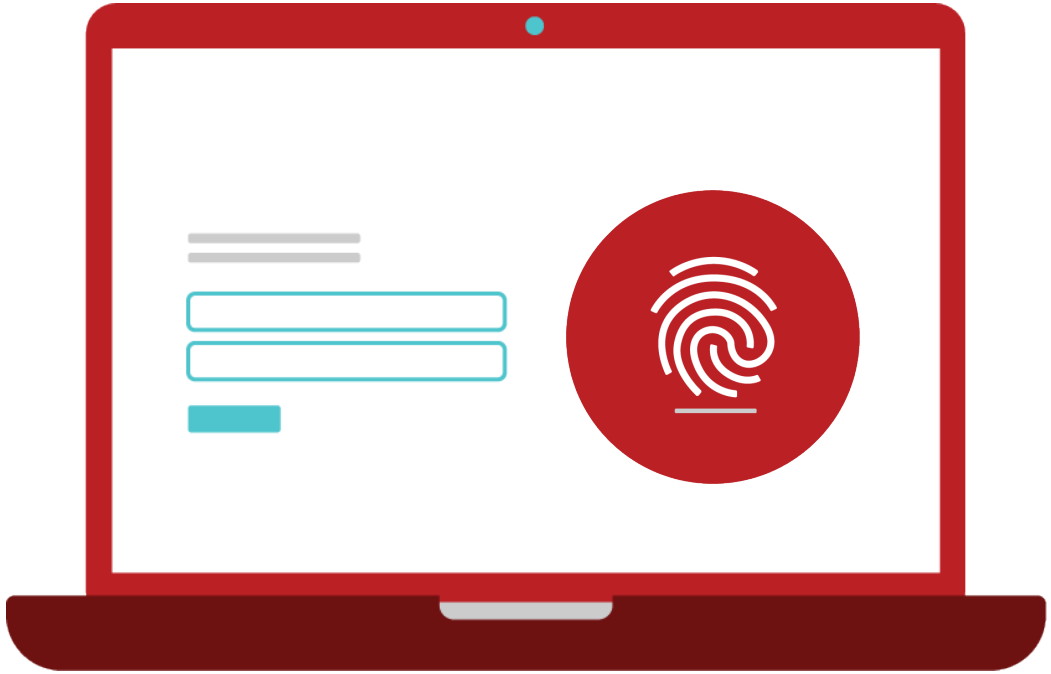
```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: localhost:1337
```

Iteration 4: Scriptable Consumer Browsers

Started with developer libraries like Puppeteer and Selenium.

Now attack tools drive the browsers directly.

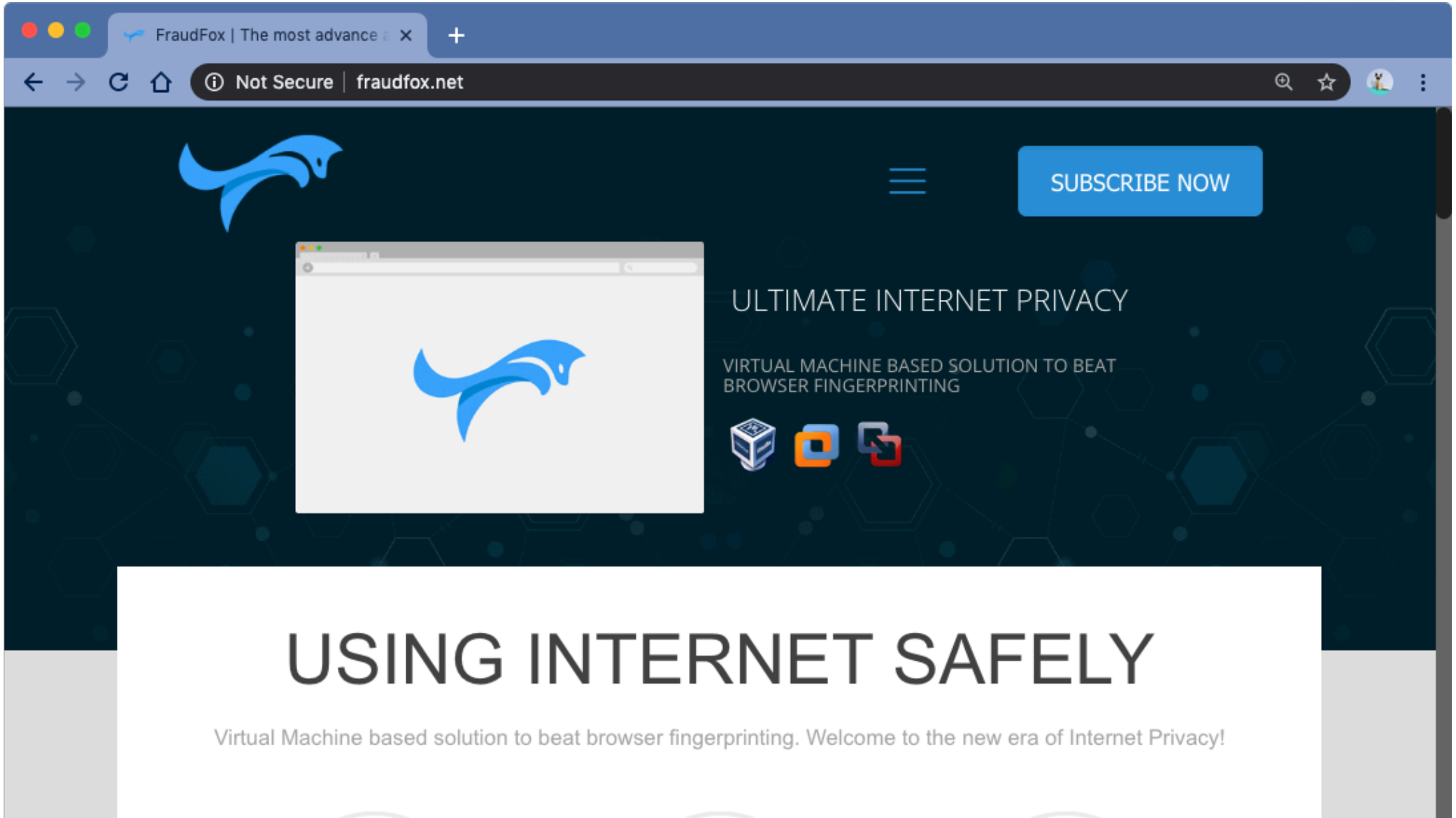
Defense: Browser Fingerprinting



Browser Fingerprinting

Data like screen size, fonts, plugins, & hardware combine to produce a unique value.

Iteration 5: Randomizing Fingerprint Data Sources



Defense: Behavior Analysis for Negative Traits

Iteration 6: Human Behavior Emulation

Where we go from here?

Iteration 7: Use real device data

FingerprintSwitcher - change

fingerprints.bablosoft.com/#capabilities

CAPABILITIES

Here is a list of properties involved in browser fingeprinting. They can be changed with FingerprintSwitcher service:

- 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

Iteration 7: Use real device data

genesis

Dashboard
Genesis Wiki new
News 10
Bots 127417
Generate FP
Orders
Purchases 1
Payments
Tickets
Genesis Security
Profile
Invites
Logout

Home / Bots

Bots

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 $
User-PC_4f8c81e4141433310c57 2018-04-29 22:10:22 2018-10-30 21:10:41	NO INFO 1 482 1 = 484 TDBank, iCloud, Dropbox, CanadianTireBank, UPS BigCommerce, Kijiji, Skype, Google, Live Twitter, AppleStore, Tumblr, Cisco, Indeed ...known 114 com.contextlogic.wish com.fitbit.Fitbit... ...other 370		CA 207.210... Windows 7 SP1	~~163.00~~ 81.50 Sale
CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB 2019-09-17 23:39:24 2019-09-18 08:10:27	0 1898 0 = 1898 LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend Facebook, Dropbox, Marriott, Homeaway, GitHub ...known 369 com.ebates com.facebook.katana ...other 1529		CA 207.219... Windows 7 Professional	52.00
	0 646 0 = 646			

Iteration 7: Use real device data

genesis

- Dashboard
- Genesis Wiki new
- 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

Add to Cart | Reserve | Buy

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

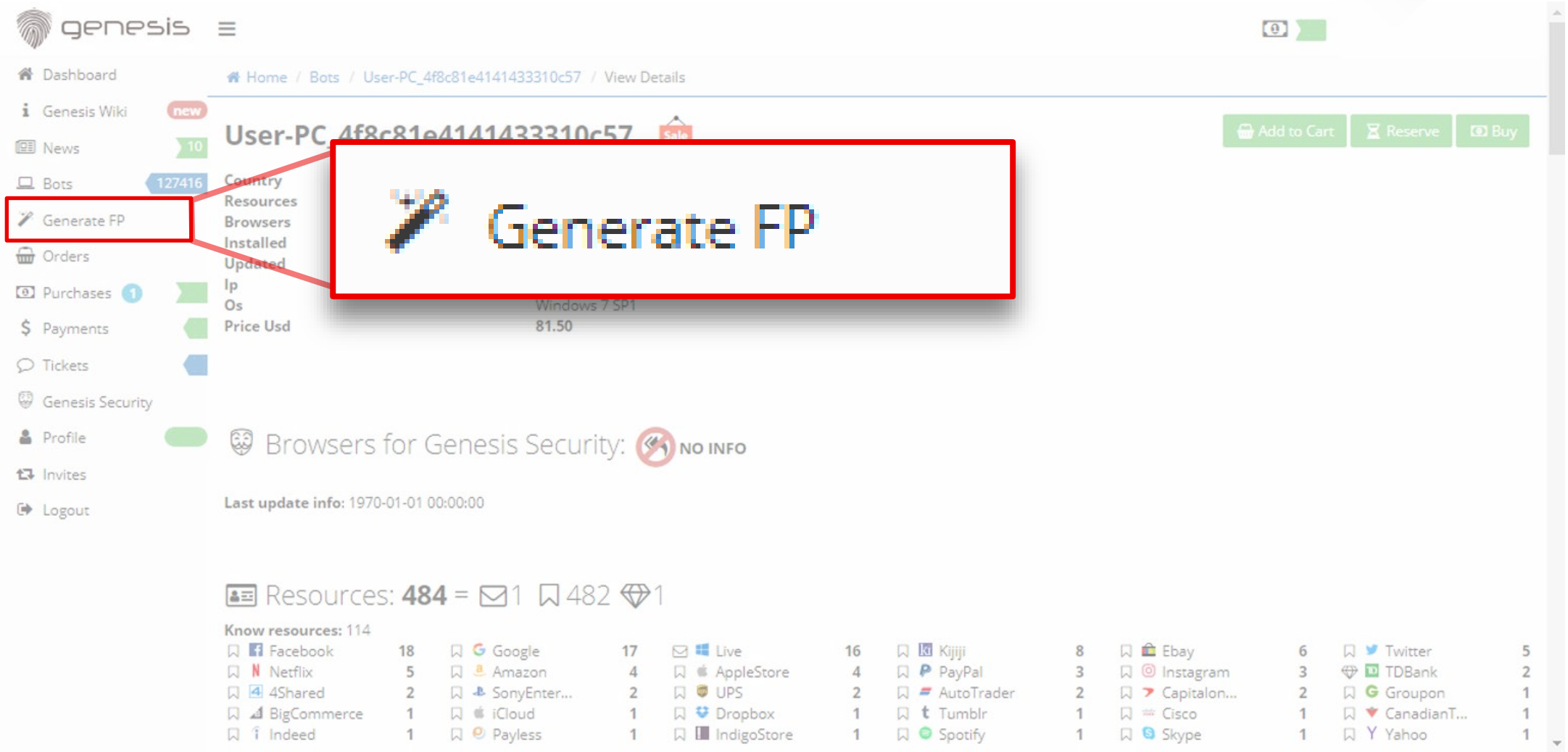
Last update info: 1970-01-01 00:00:00

Resources: 484 = 1 482 1

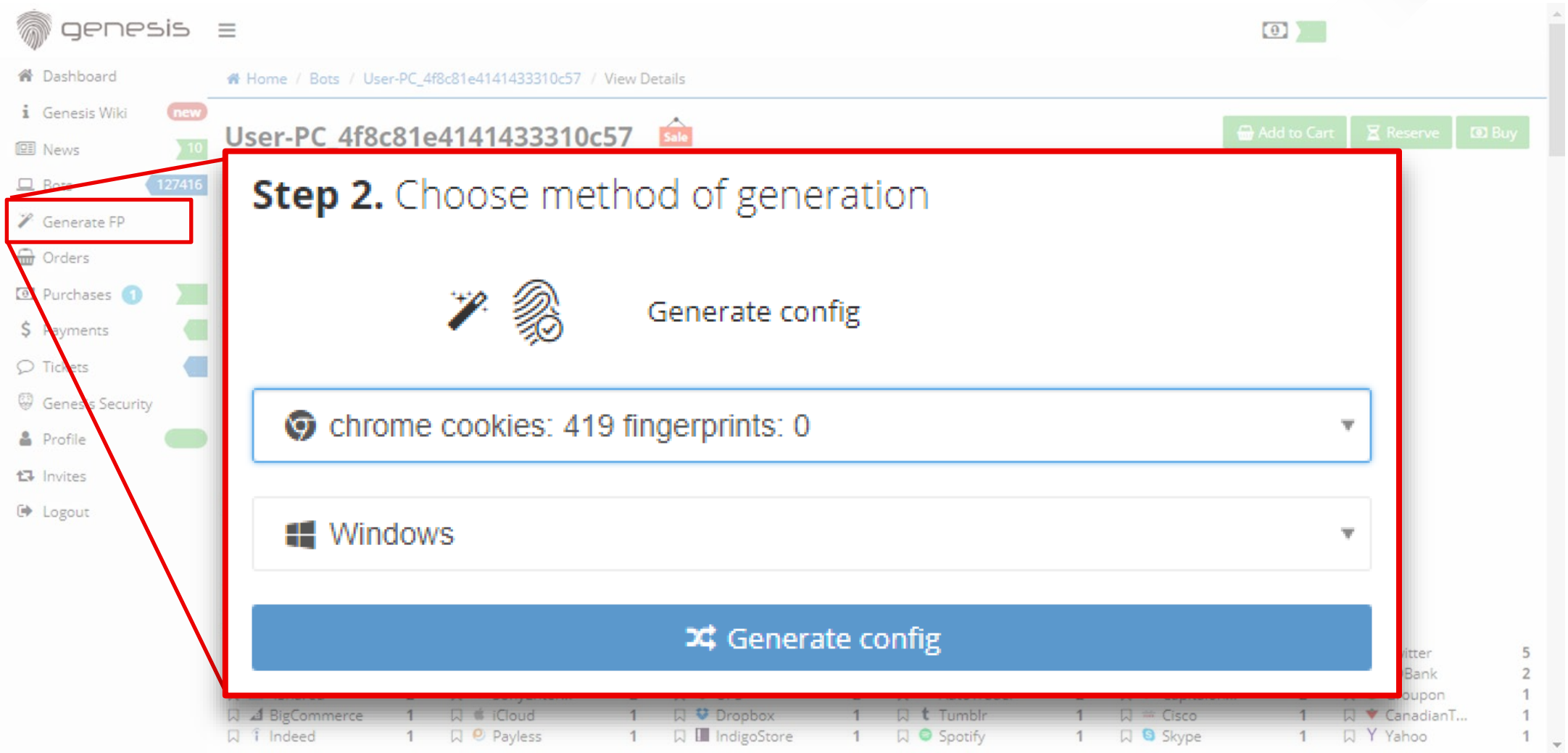
Know resources: 114

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

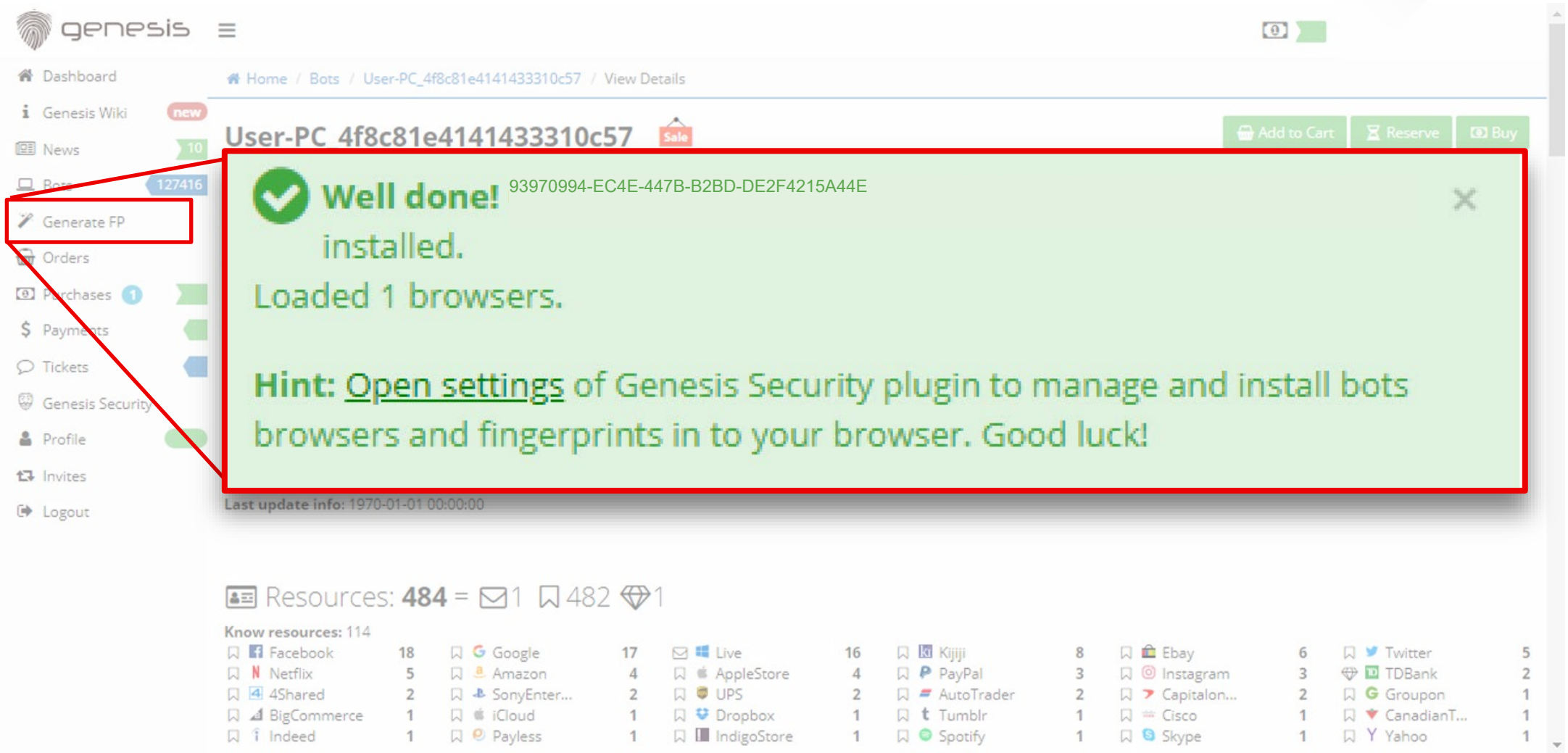
Iteration 7: Use real device data



Iteration 7: Use real device data



Iteration 7: Use real device data

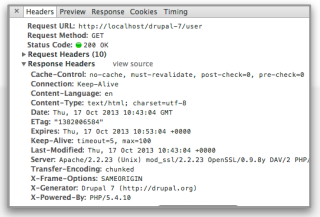


Iteration 7: Use real device data

Modern Bot Defense

Client Interaction Signals

F5 analyzes three categories of signals to identify illegitimate traffic



Network

Normalized list of safe HTTP headers. A finite data source useful for basic patterns and attacks.

Environment

Browser and device signals that reveal both immediate signs of spoofing, alongside emergent patterns

Behaviour

User interaction signals that reveal signs of invalid interactions, scaled interactions or pseudo-randomness

Browser Environment Signals

:D

Emojis render differently on different platforms/apps

0xFFFFFFFFFFFFFBFF

=

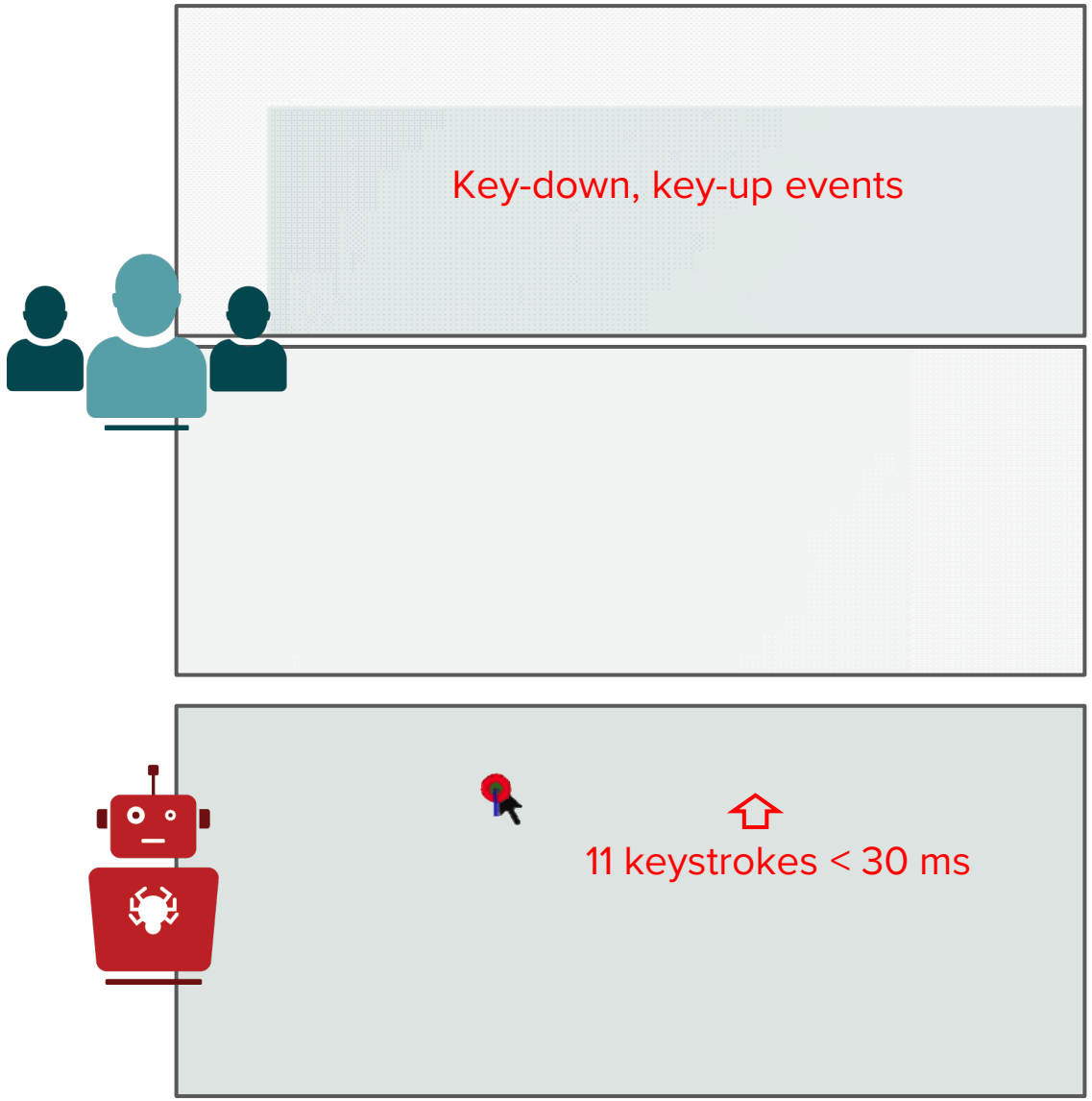
18,446,744,073,709,552,000
18,446,744,073,709,550,000
18,446,744,073,709,550,591

Really big numbers convert differently on different platforms

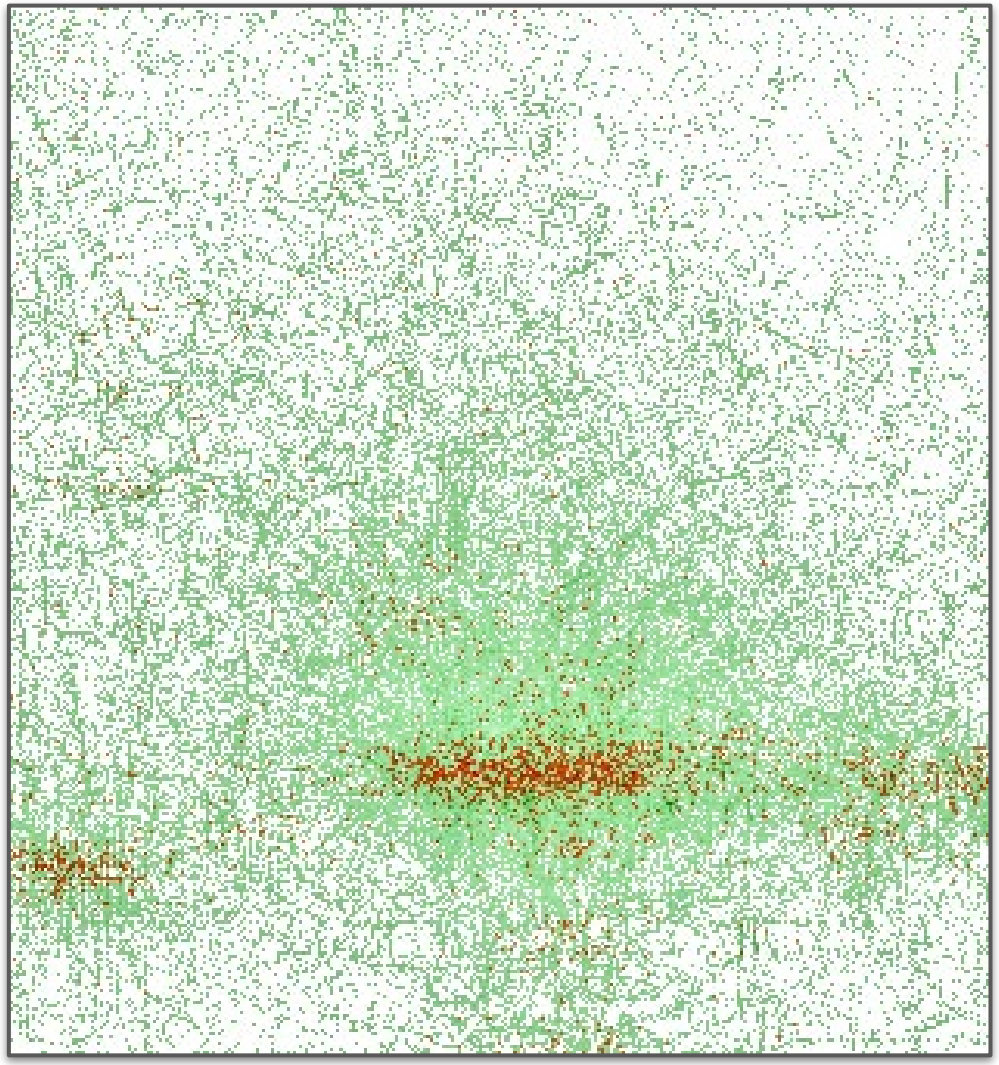
Behavior Signals

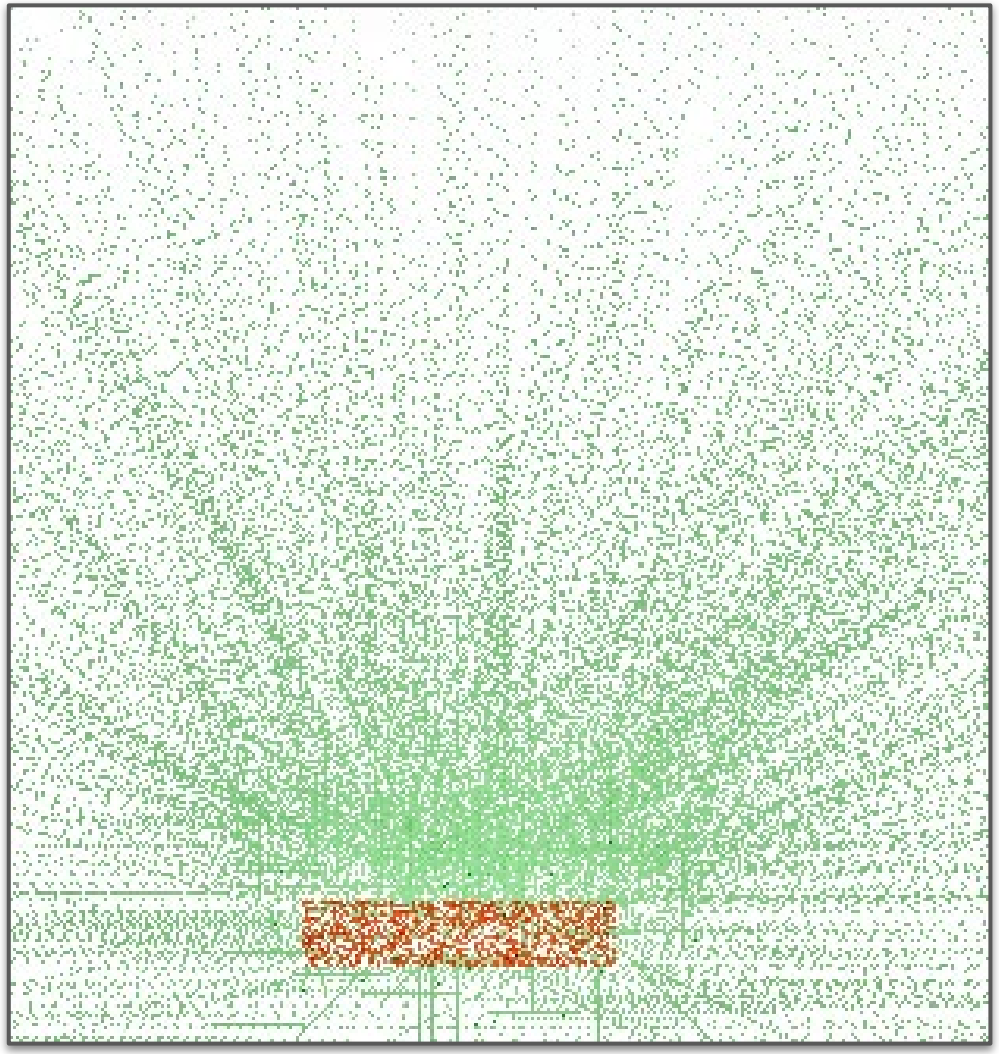
Immediate and Long Term Patterns Emerge from Advanced Automation

Blue Bar	Key-down.
Orange Bar	Key-up.
Red Circle	Mouse-click.
Green Tick	Captured mouse event.
Dashed Line	High speed movement between two points.
Brown Square	Long pause.
Grey Line	Transition from non-mouse event to mouse event.



Can you tell which is automated?

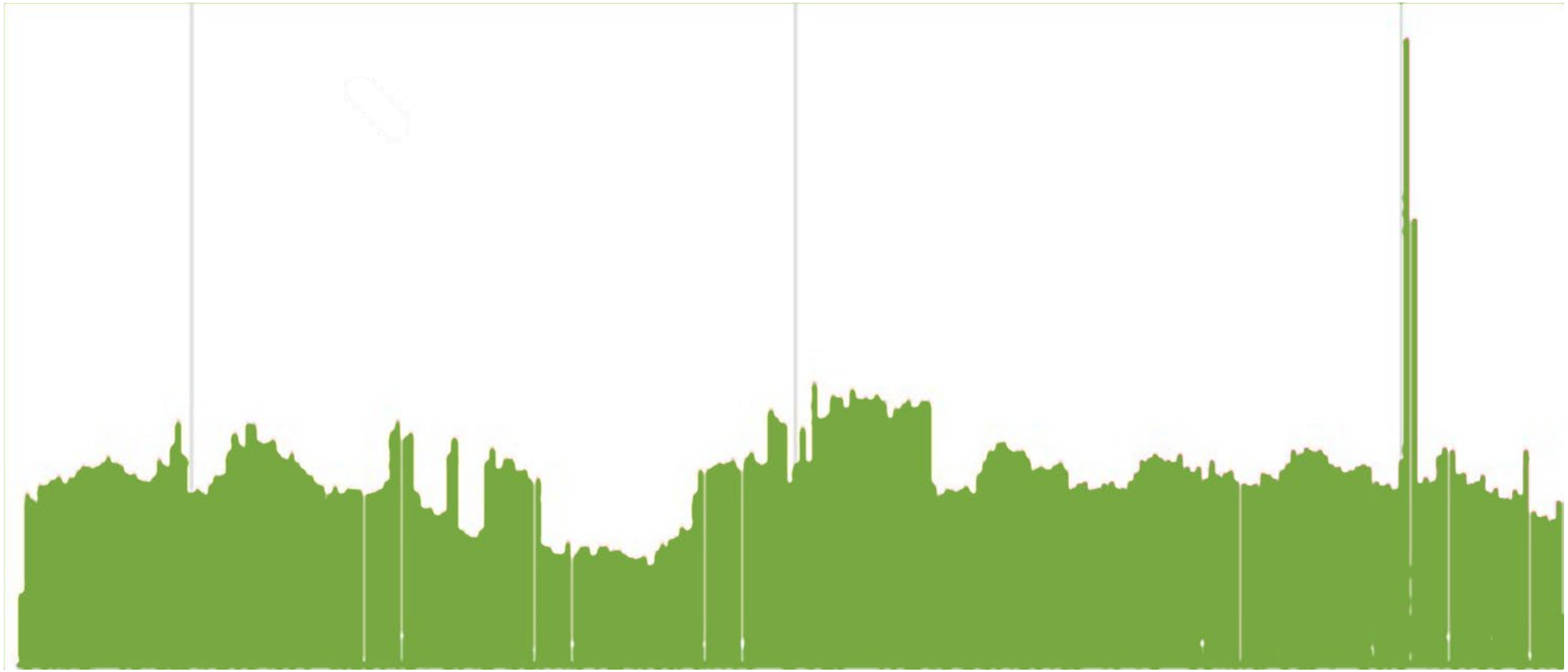




Mouse Move Mouse Click

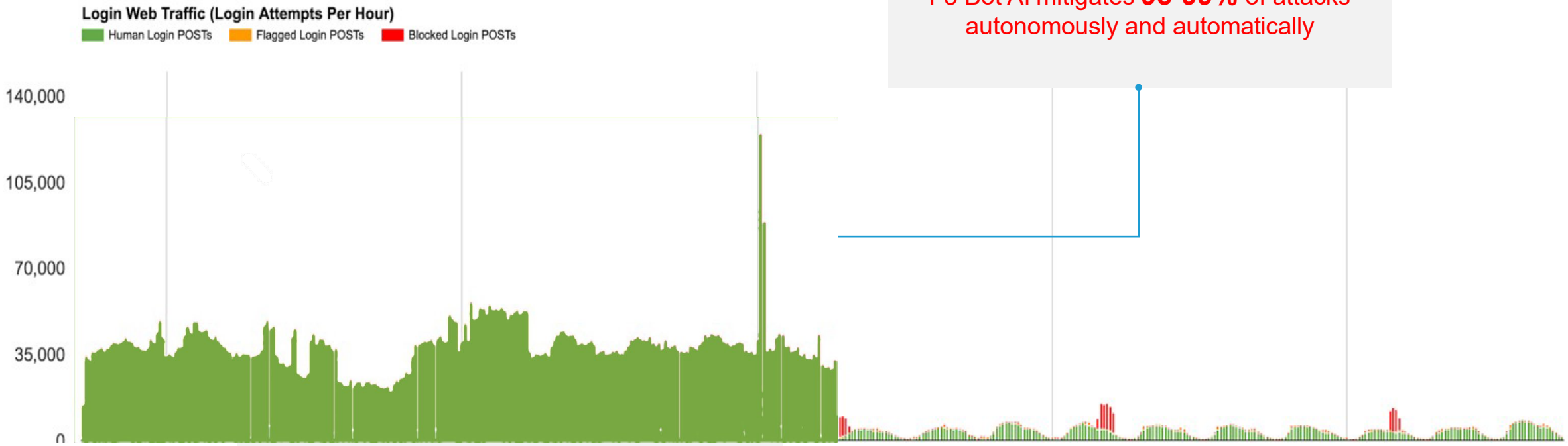
Are you human or bot?

Typical customer traffic



Typical customer traffic after F5 deployment

F5 Bot AI mitigates **95-99%** of attacks autonomously and automatically



- 30k credential stuffing attacks *per hour*
- 0.1-2% attack success rate
- $50 lost *per ATO*