



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.

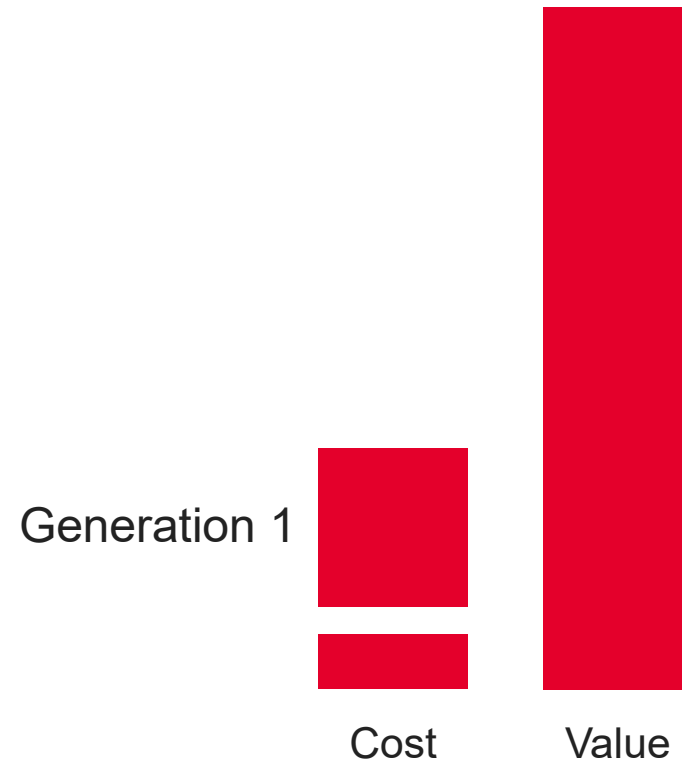
12:01 AM · Sep 14, 2014 · Twitter for iPhone

Cost vs Value

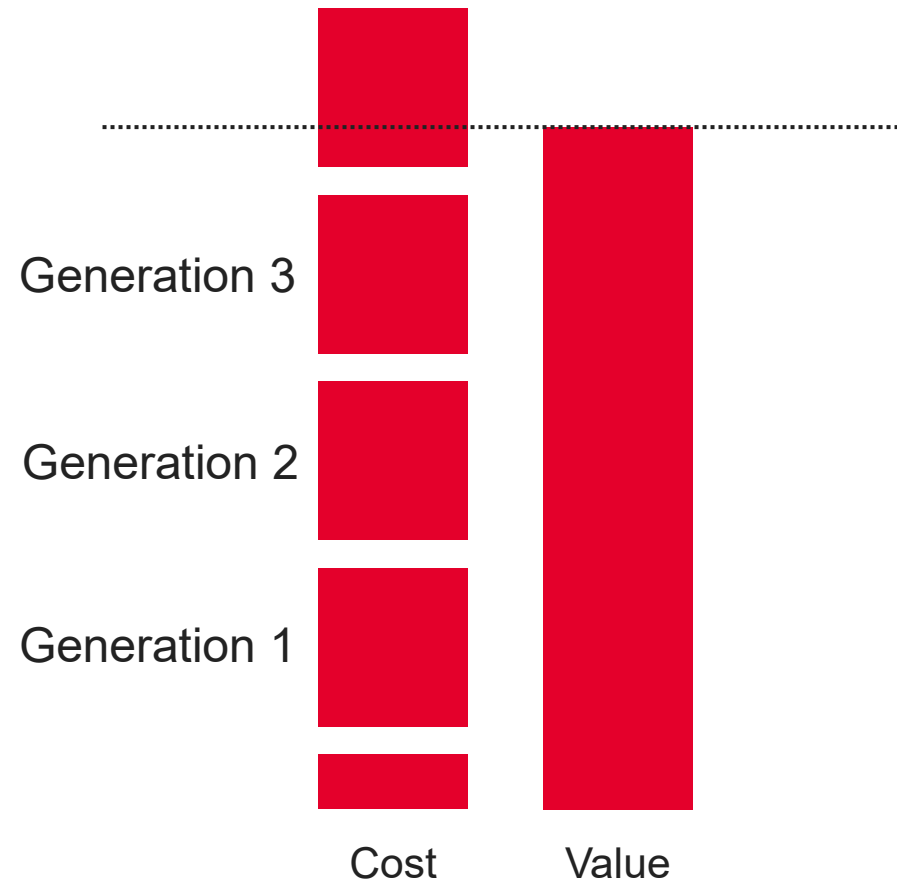
...with no defenses in place, it costs nothing to attack.



Adding a defense increases cost by forcing evolution.

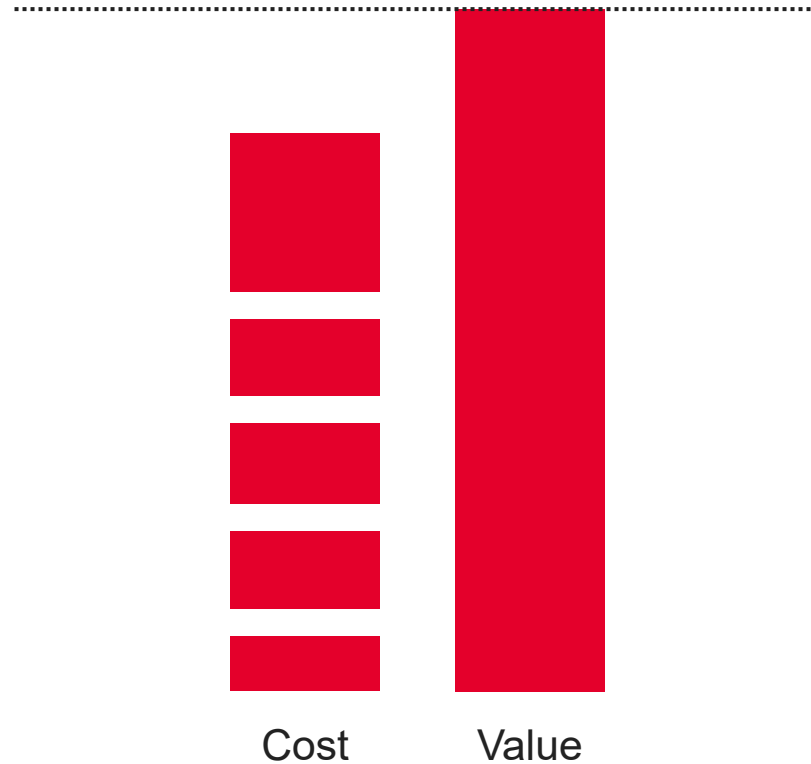


Enough defenses will tip the cost/value ratio in your favor.

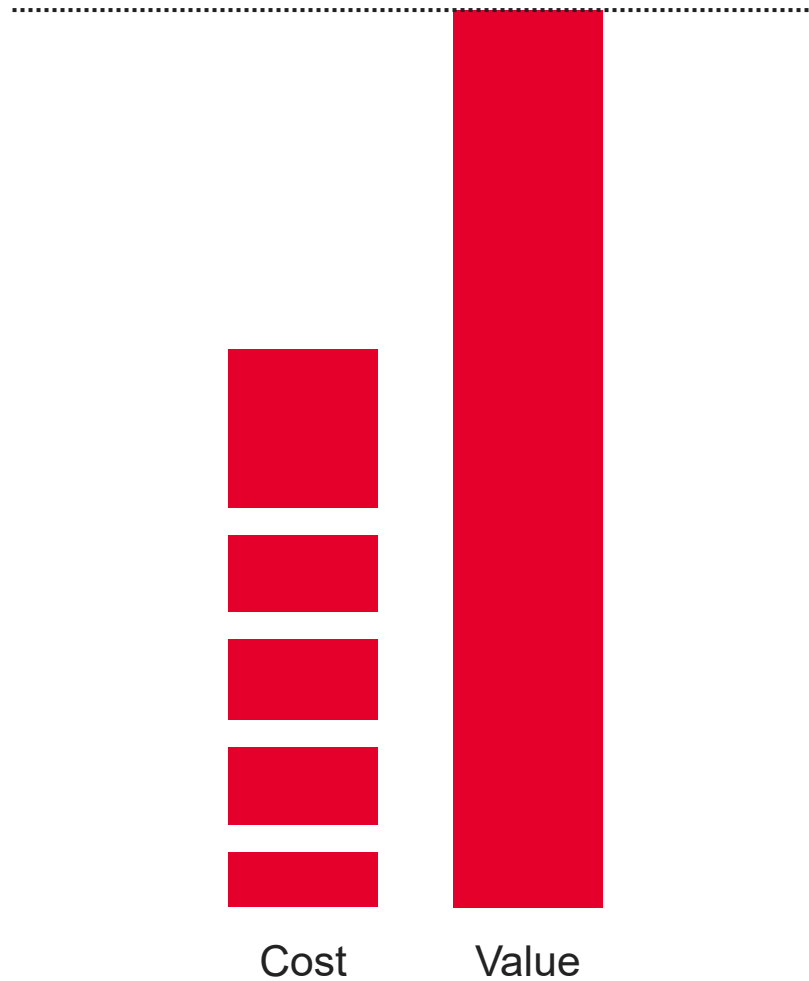


As with all technology, the cost of entry decreases over time.

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

The screenshot displays a web browser window with the Upwork profile of 'Igor L. - Browser Automation Studio'. The browser's address bar shows the URL 'https://www.upwork.com/o/profiles/user...'. The profile page includes a placeholder for a profile picture, the name 'Browser Automation Studio', and a list of services: 'Automations like : + registrators on sites; + answering machines for messages; + sending e-mails; + work with text document (connection , disconnection text , etc.); + checking accounts of... more'. The hourly rate is listed as '\$10.00'. To the right of the browser window, a sidebar contains a search bar and a grid of automation tools: Network, Waiters, Email, Http Client, Idle emulation, Image processing, List, Process Manager, Receive sms, Telegram, Timezone, and User interaction. Below the browser window, a portion of an Instagram sign-up page is visible, featuring the Instagram logo and the text 'Sign up to see photos and videos from your friends.' with a 'Log in with Facebook' button.

Thread Number: {{threads}}
Success Number: 100000

What to search?

Browser Script logic Tools

Network Waiters Email Http Client

Idle emulation Image processing List Process Manager

Receive sms Telegram Timezone User interaction

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

Instagram

Sign up to see photos and videos from your friends.

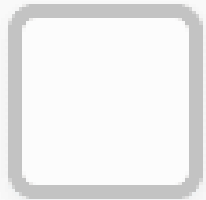
[Log in with Facebook](#)

OR

Mobile Number or Email

Full Name

3. Defeat defenses



I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)

3. Defeat defenses

Best Captcha Solving Service | x +

deathbycaptcha.com

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

i

72M+ Residential Proxy IPs

7-Day Free Trial!

Advertisement

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.
- DeCaptcha** 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

14 ©2023 F5

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



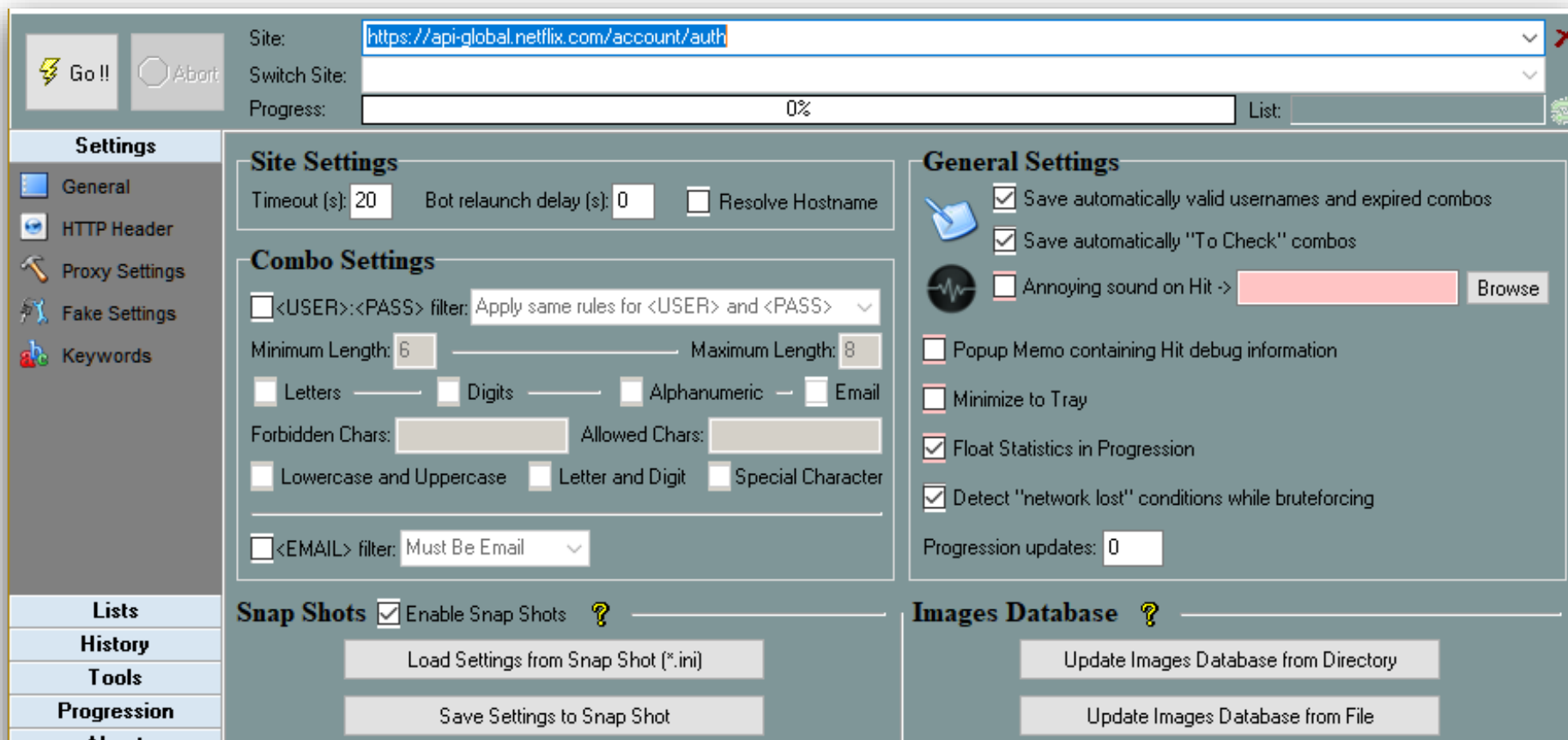
Generation 0: Basic HTTP requests with common tools



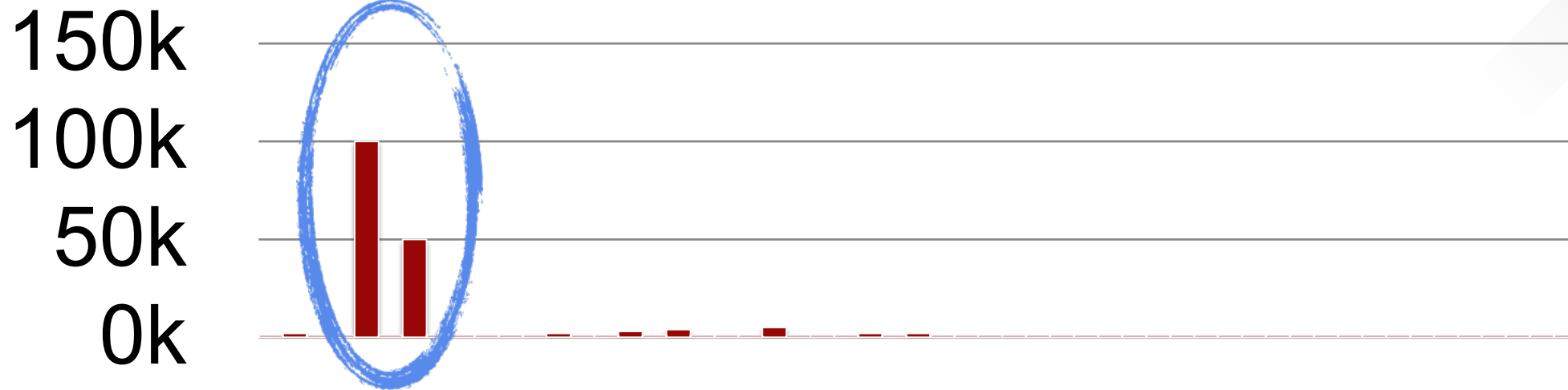


SentryMBA

- 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

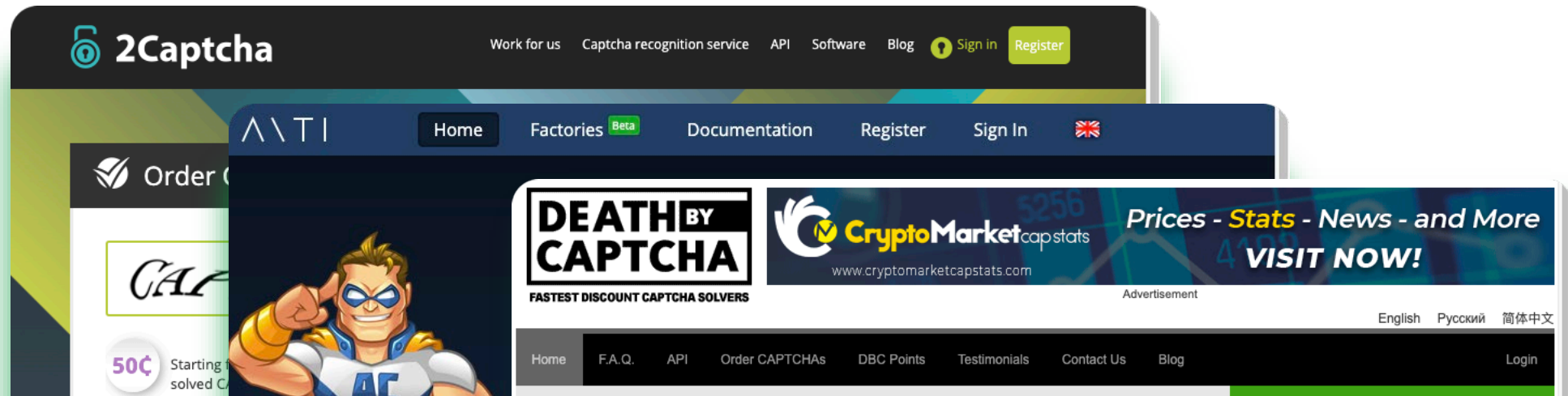
Search all columns:

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



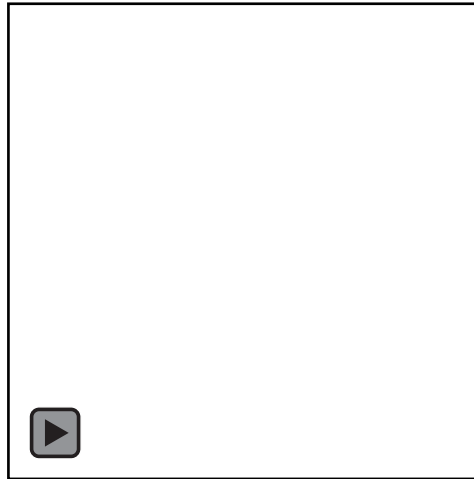
Defense: Text-based CAPTCHAs



Iteration 2: Use CAPTCHA Solvers.



Defense: Dynamic sites and JavaScript heavy defenses.



**Full web stack
No browser required**



trifleJS

Headless automation for Internet Explorer

Iteration 3: Scriptable WebViews



Defense: Header Fingerprinting & Environment Checks



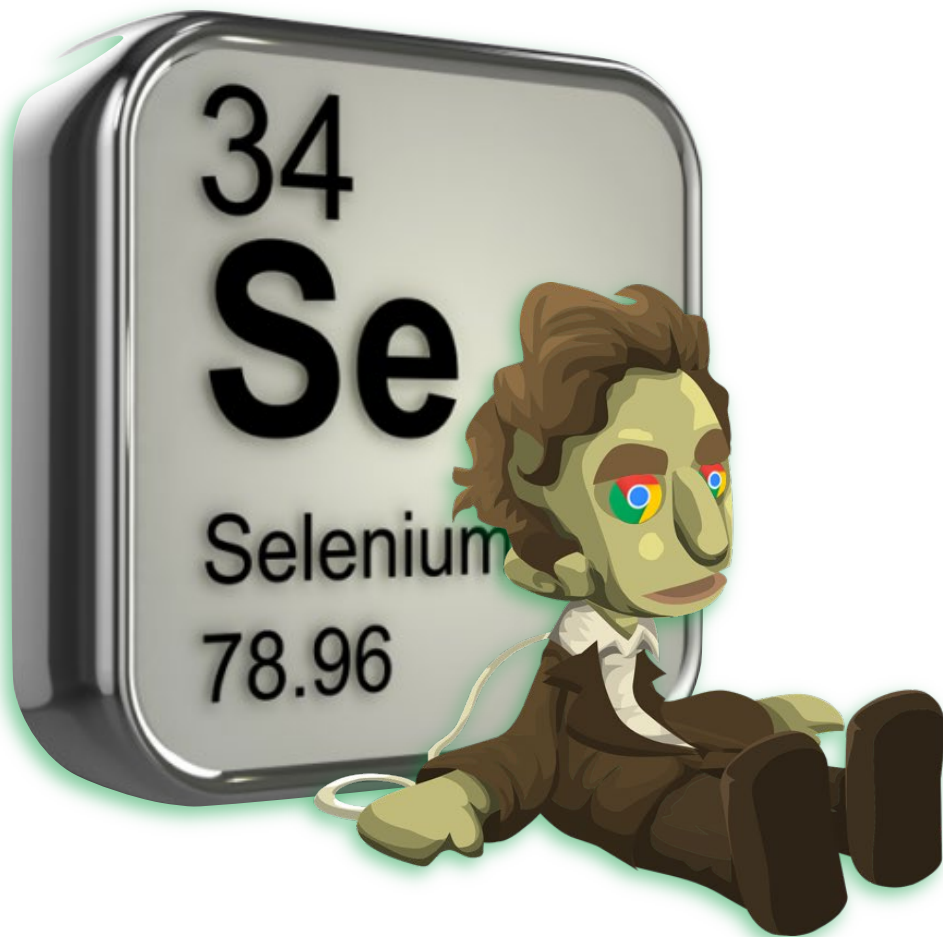
```
GET / HTTP/1.1
Host: localhost:1337
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko)
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ru;q=0.6
```



```
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
```



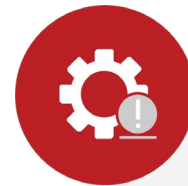
Iteration 4: Scriptable Consumer Browsers



Started with developer libraries like Puppeteer and Selenium.

Now attack tools drive the browsers directly.

Defense: Browser Fingerprinting

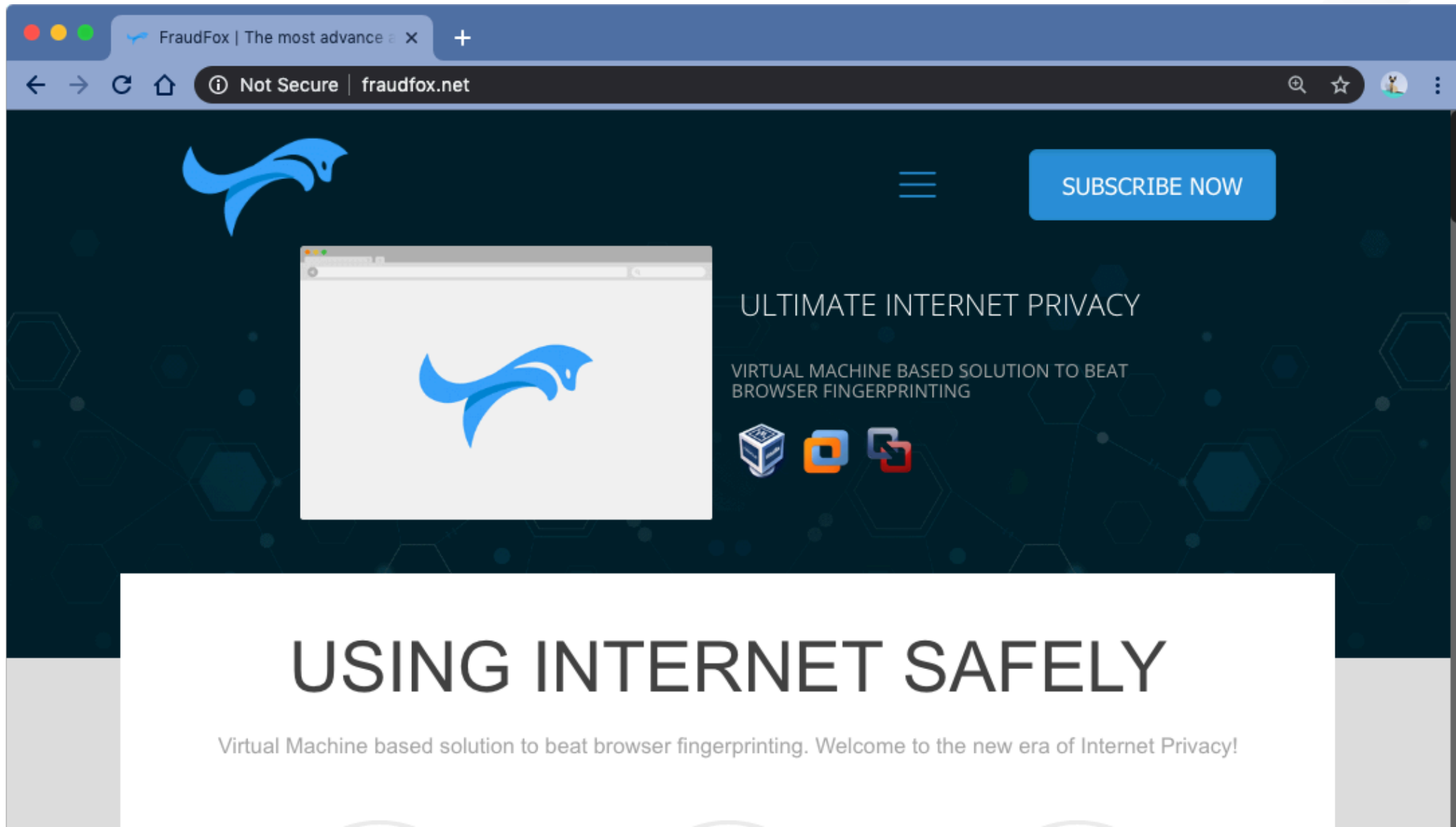


Browser Fingerprinting

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 y x +

fingerprints.bablossoft.com/#capabilities

CAPABILITIES

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

<input checked="" type="checkbox"/> Canvas data	<input checked="" type="checkbox"/> Webgl data	<input checked="" type="checkbox"/> Video card properties
<input checked="" type="checkbox"/> Audio data	<input checked="" type="checkbox"/> Audio settings	<input checked="" type="checkbox"/> Font list
<input checked="" type="checkbox"/> WebRTC IP	<input checked="" type="checkbox"/> Browser language	<input checked="" type="checkbox"/> Timezone
<input checked="" type="checkbox"/> Plugin list	<input checked="" type="checkbox"/> Screen properties	<input checked="" type="checkbox"/> User agent
<input checked="" type="checkbox"/> Platform ID	<input checked="" type="checkbox"/> Touch support	<input checked="" type="checkbox"/> Battery capacity
<input checked="" type="checkbox"/> Do not track	<input checked="" type="checkbox"/> Gamepad	<input checked="" type="checkbox"/> Geolocation
<input checked="" type="checkbox"/> Connection	<input checked="" type="checkbox"/> USB devices	<input checked="" type="checkbox"/> SVG reading



Iteration 7: Use real device data

genesis

Dashboard Home / Bots

Genesis Wiki new

News 10

Bots 127417

Generate FP

Orders

Purchases 1

Payments

Tickets

Genesis Security

Profile

Invites

Logout

Bots

Extended Search

BOT NAME / Filter bot name Any Filter resource name/domain: paypal,ebay.com,hotmail.com... COUNTRY / HOST PRICE

Filter IP/Country/OS Filter \$

NO INFO 1 482 1 = 484

User-PC_4f8c81e4141433310c57

2018-04-29 22:10:22

2018-10-30 21:10:41

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

0 1898 0 = 1898

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

0 646 0 = 646

8186828-216-18371-73158555

163.00

81.50

207.210...

Windows 7 SP1

Sale



52.00

207.219...


Windows 7 Professional





Iteration 7: Use real device data


 genesis 


[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


 CA


 484


 0


 2018-04-29 22:10:22


 2018-10-30 21:10:41


 207.210...



 Windows 7 SP1

 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

 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

genesis

Dashboard Home / Bots / User-PC_4f8c81e4141433310c57 / View Details

Genesis Wiki 10 new

News 127416

Bots

Generate FP

Orders

Purchases 1

Payments

Tickets

Genesis Security

Profile

Invites

Logout

User-PC_4f8c81e4141433310c57

Country Resources Browsers Installed Updated Ip Os Price Used

Windows 7 SP1 81.50

Add to Cart Reserve Buy

Generate FP

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

genesis

Dashboard Home / Bots / User-PC_4f8c81e4141433310c57 / View Details

Genesis Wiki 127416

News 10

Bots 127416

Generate FP

Orders

Purchases 1

Payments

Tickets

Genesis Security

Profile



Invites


Logout


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

BigCommerce	1	iCloud	1	Dropbox	1	Tumblr	1	Cisco	1	CanadianT...	1
Indeed	1	Payless	1	IndigoStore	1	Spotify	1	Skype	1	Yahoo	1

Twitter 5
Bank 2
Coupon 1
1
1
1



Iteration 7: Use real device data

genesis

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

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!

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

Dashboard

Genesis Market

New

Buy

Genesis Market

Order

Product

Payment

Ticket

Genesis Market

Profile

Invite

Logout

THIS WEBSITE HAS BEEN SEIZED



OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit:
haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov















Indeet

Payless

IndigoStore

Spotify

Skype

Yahoo

Buy

5

2

1

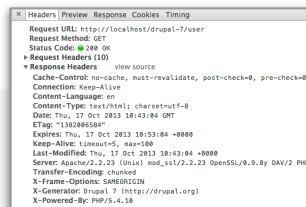
1

1

Modern Bot Defense

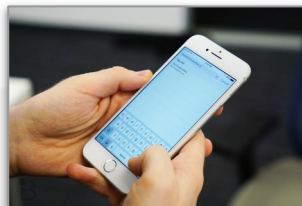
Client Interaction Signals

F5 analyzes three categories of signals to identify illegitimate traffic



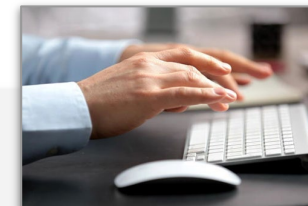
Network

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

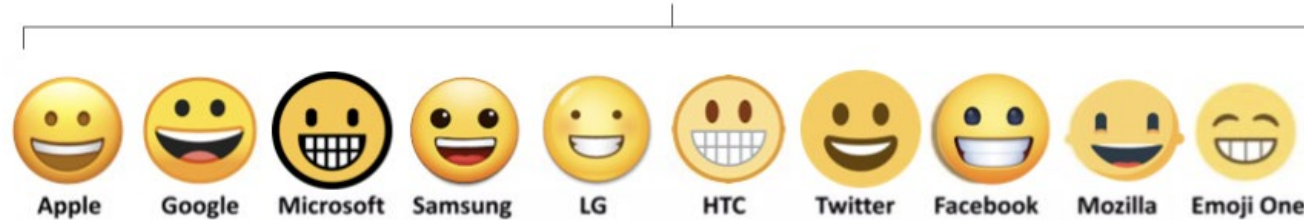


Behaviour

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

0xFFFFFFFFFFFFFFFFBFF

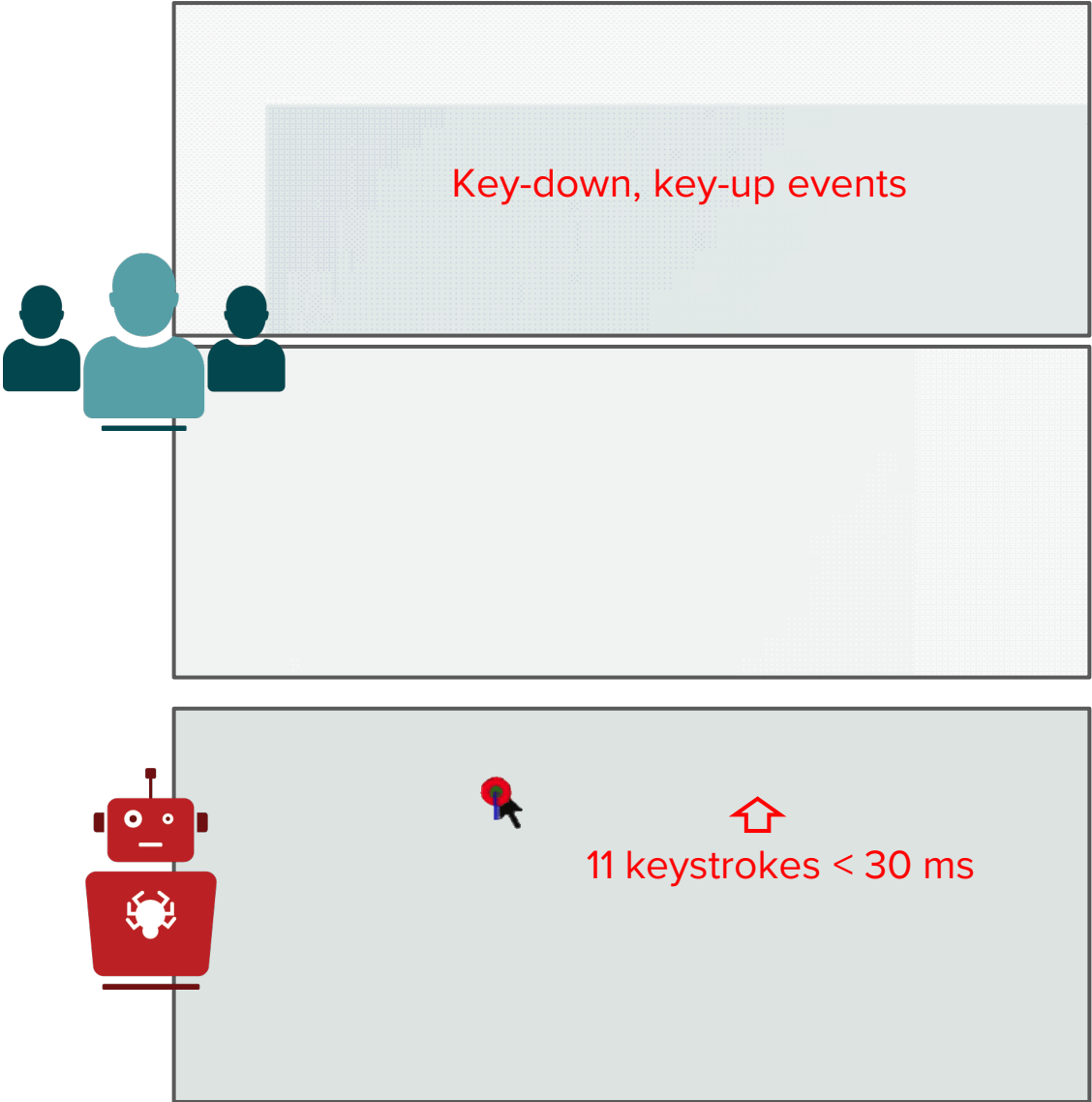
= 18,446,744,073,709,552,000
18,446,744,073,709,550,000
18,446,744,073,709,550,591

Really big numbers convert differently on different platforms

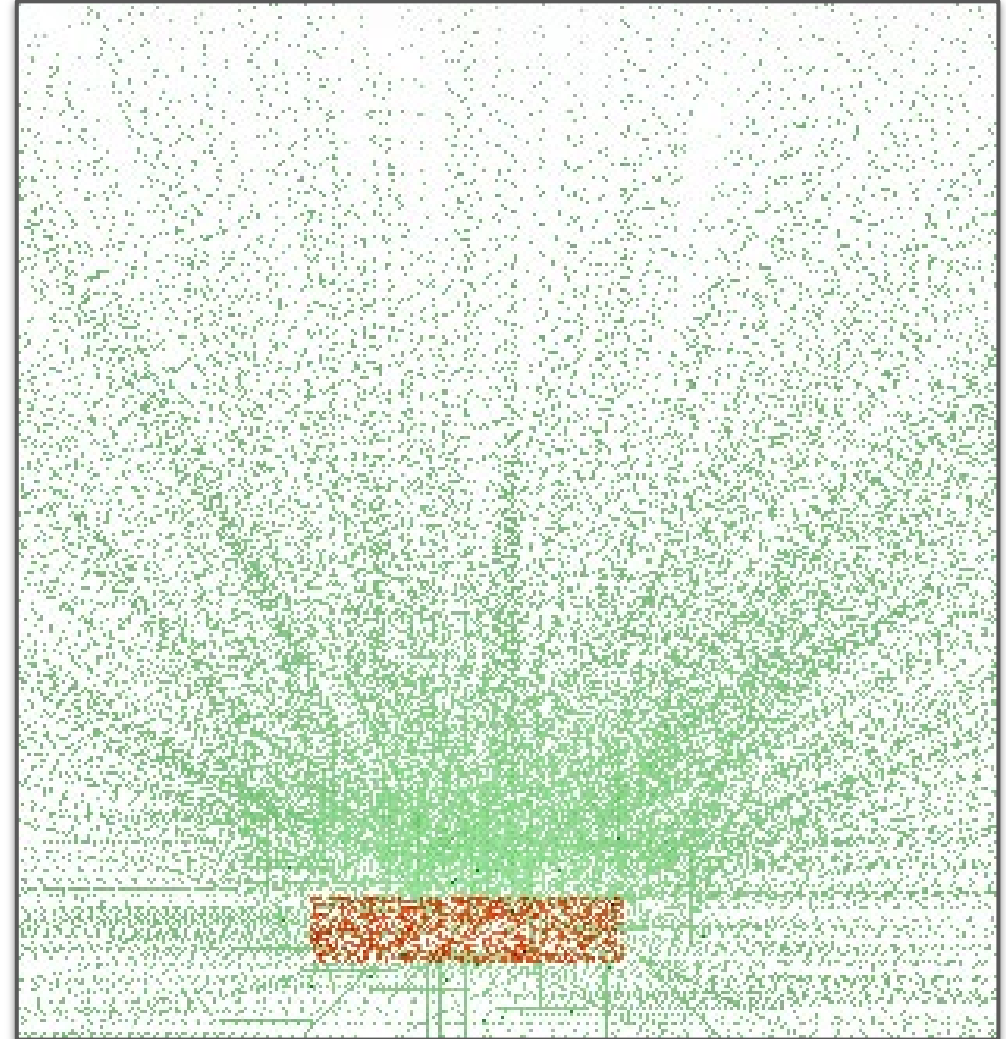
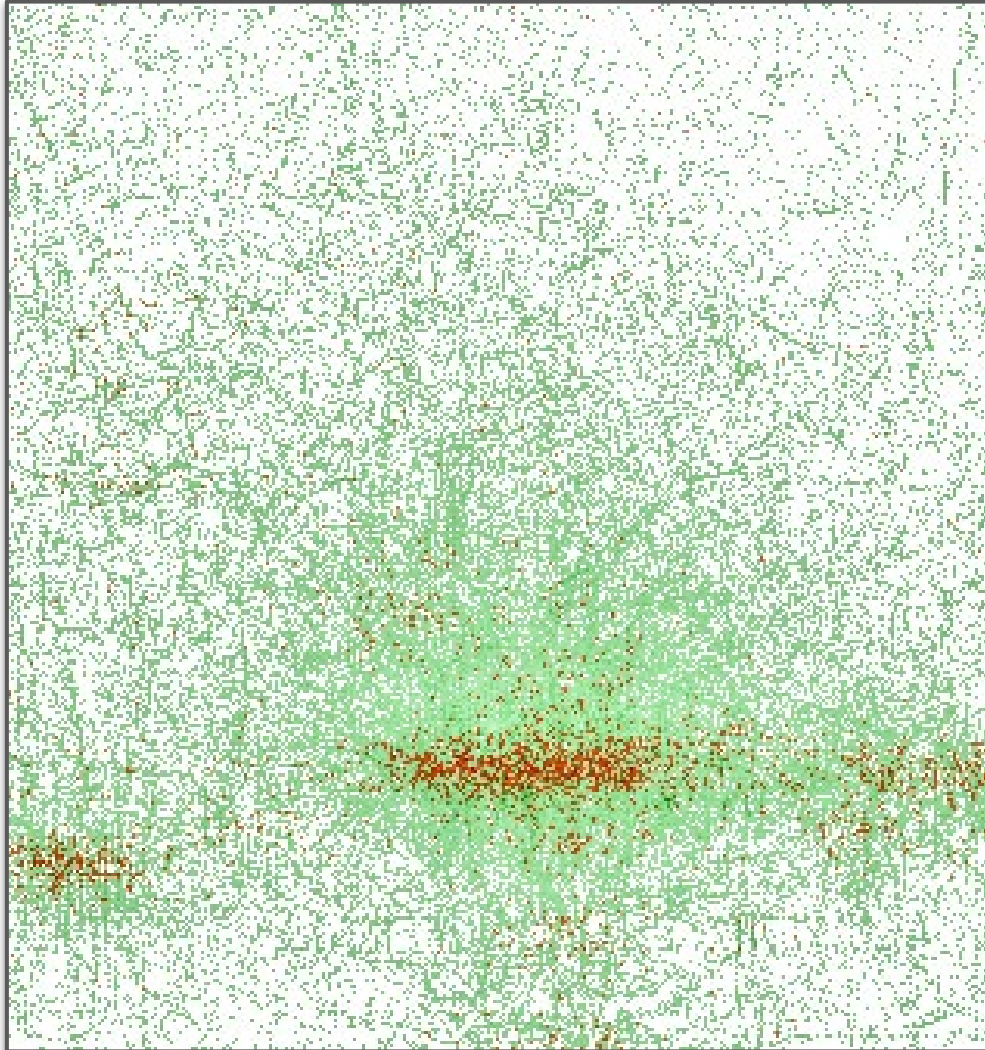
Behavior Signals

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.

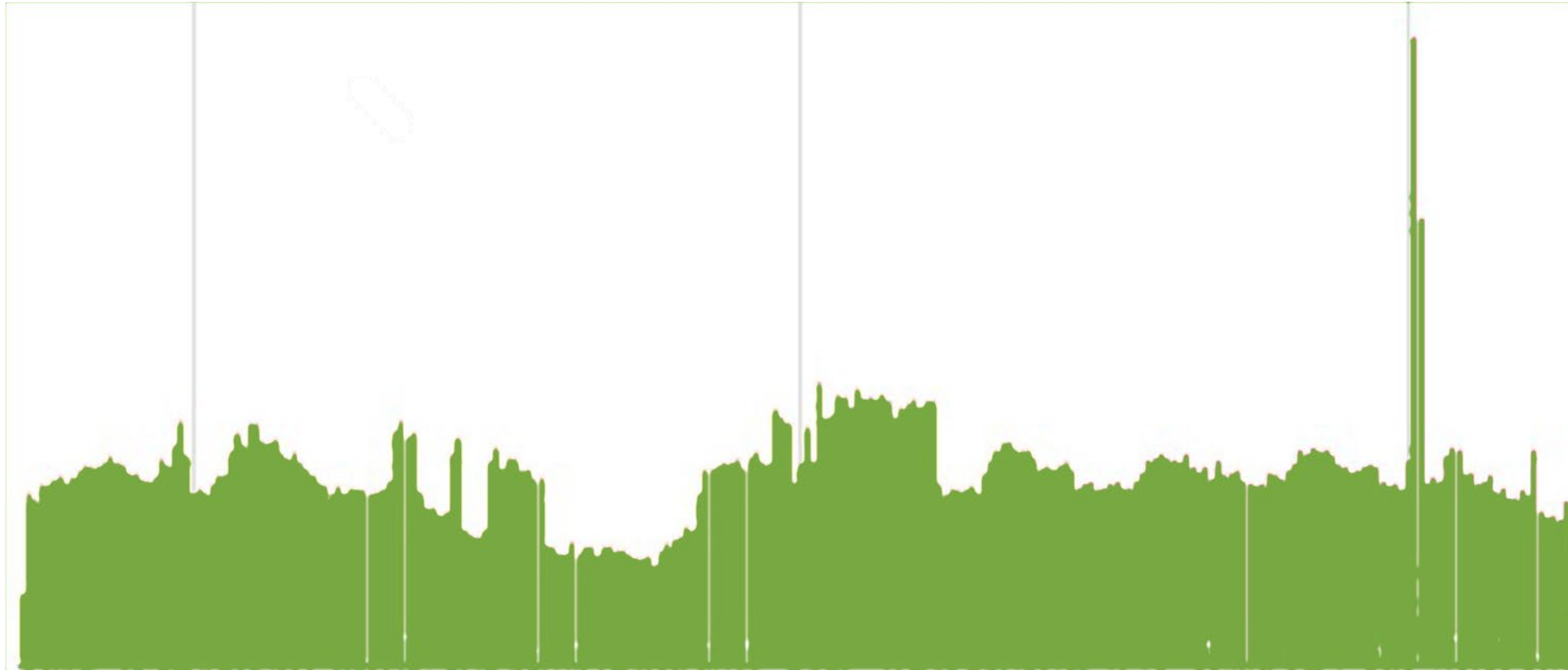


Can you tell which is automated?



Are you human or bot?

Typical customer traffic



Typical customer traffic after F5 deployment

