Cost vs Value

Understanding the economics that drive attacks

Jarrod Overson, Director @ShapeSecurity

How much does it cost to attack you?

Cost vs Value

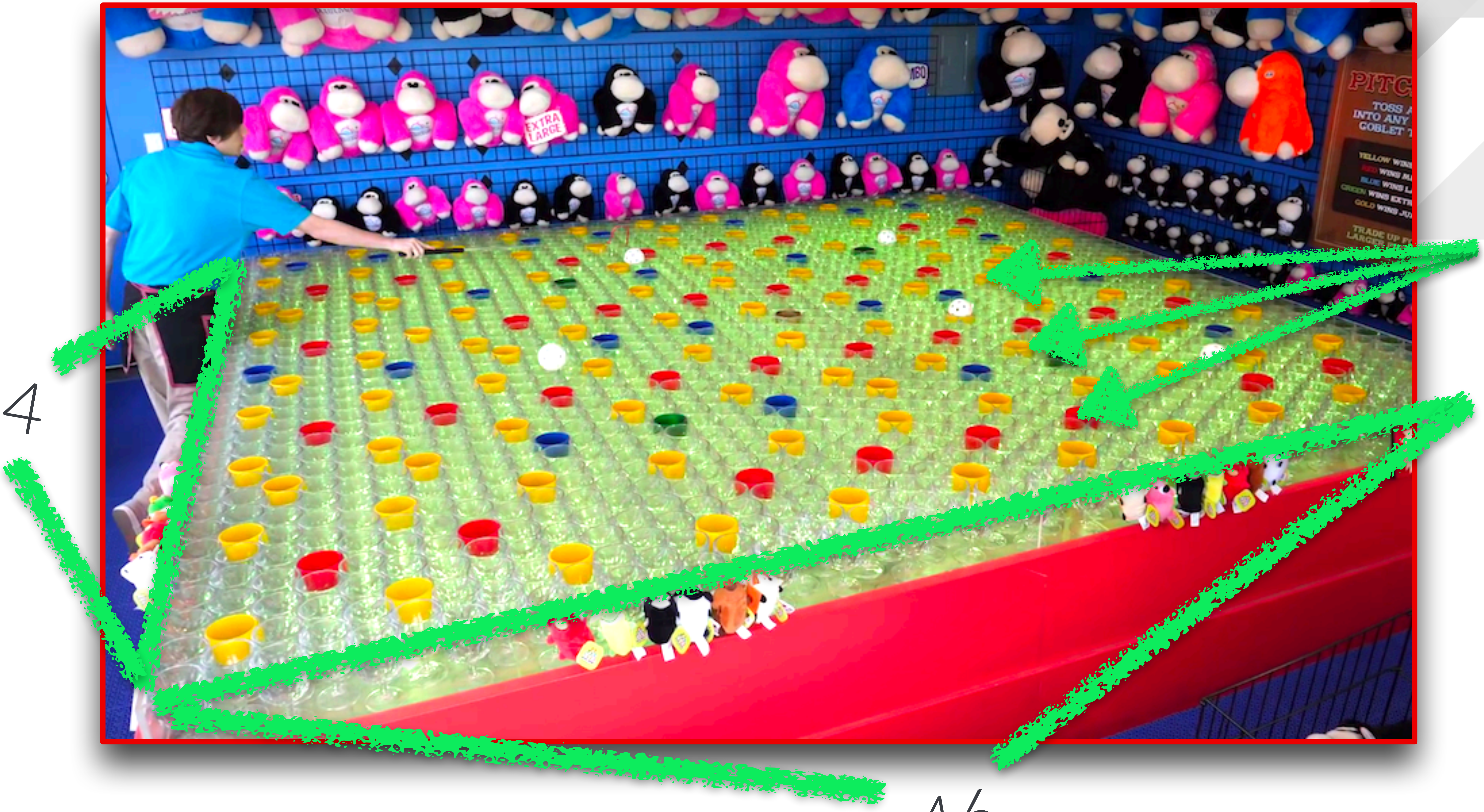
How much does it cost to play?

$1?

How much is this worth to you?

$10?

What are your chances of winning?



What are your chances of winning?

About 10%*

** not accounting for lack of walls and any carnival shenanigans.*
It's much lower in reality. Don't play these games.

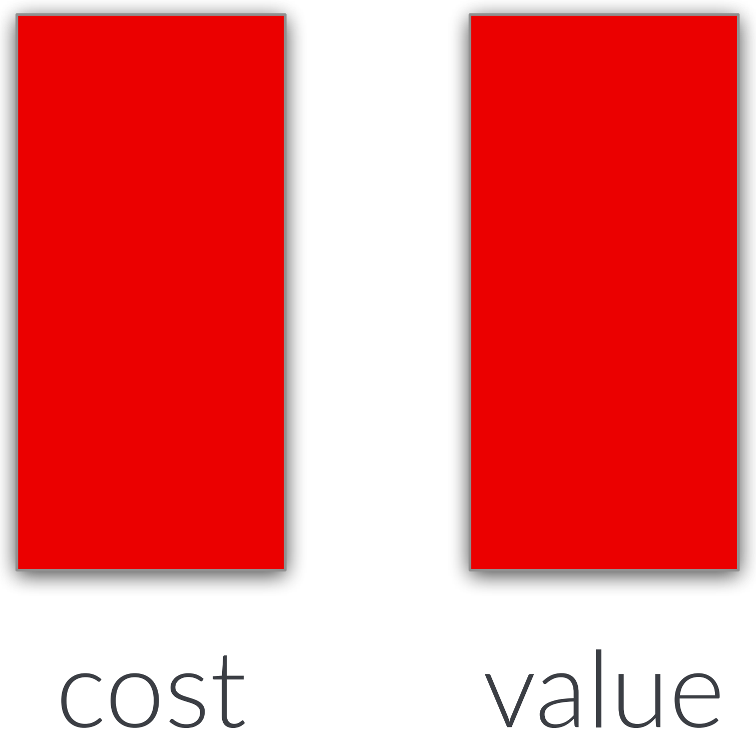
How to calculate our return.

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

Is it worth playing?

$$\frac{\$10 * 10\%}{\$1} - 100\% = 0\%$$

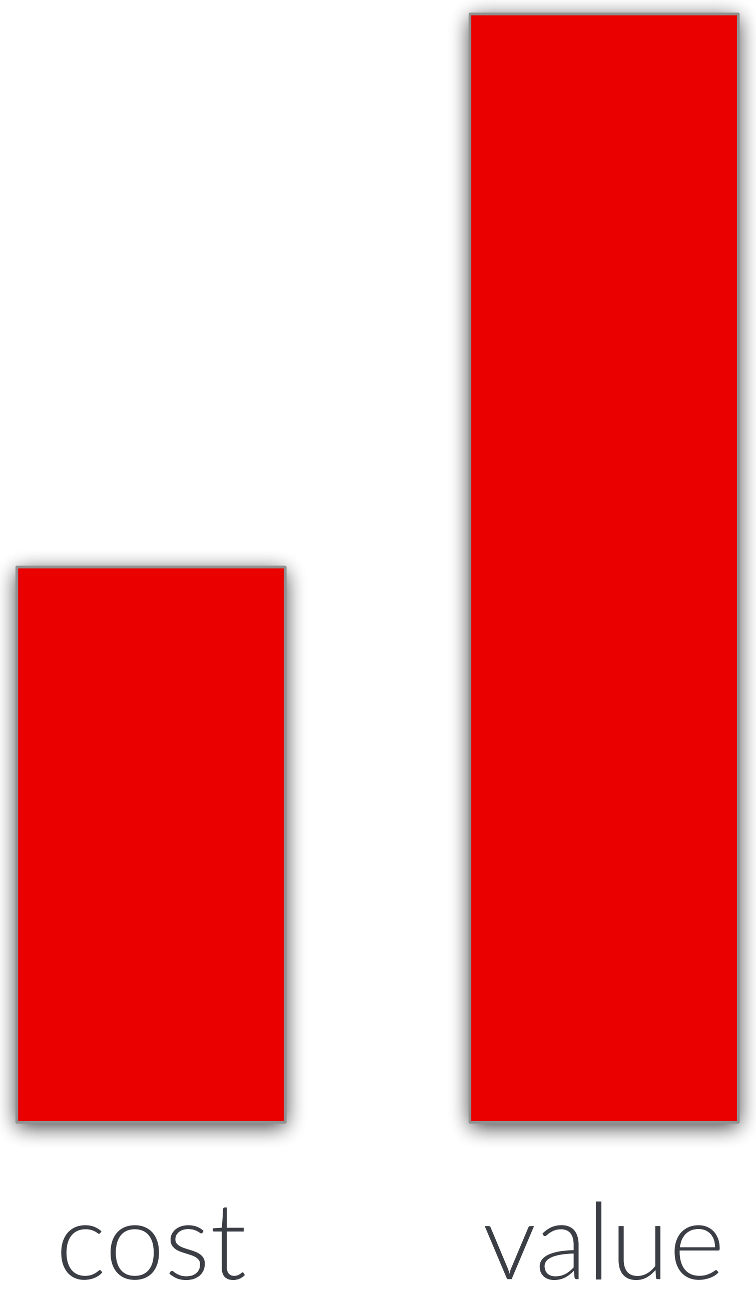
Eventually you will break even.



If value or chance improves, your return is higher.

$$\frac{\$20 * 10\%}{\$1} - 100\% = 100\%$$

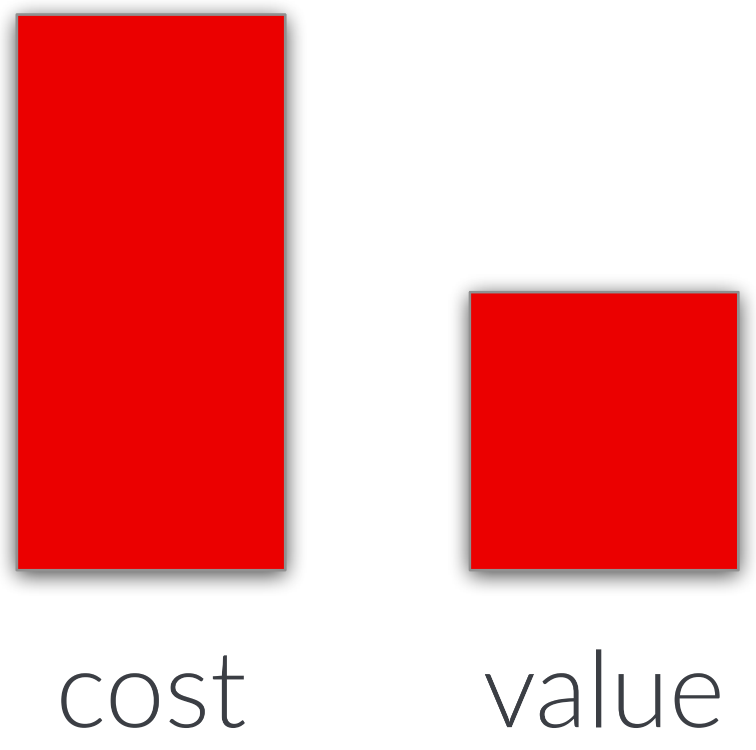
Over time you will come out ahead.



If value or chance decreases, your return is lower.

$$\frac{\$10 * 5\%}{\$1} - 100\% = -50\%$$

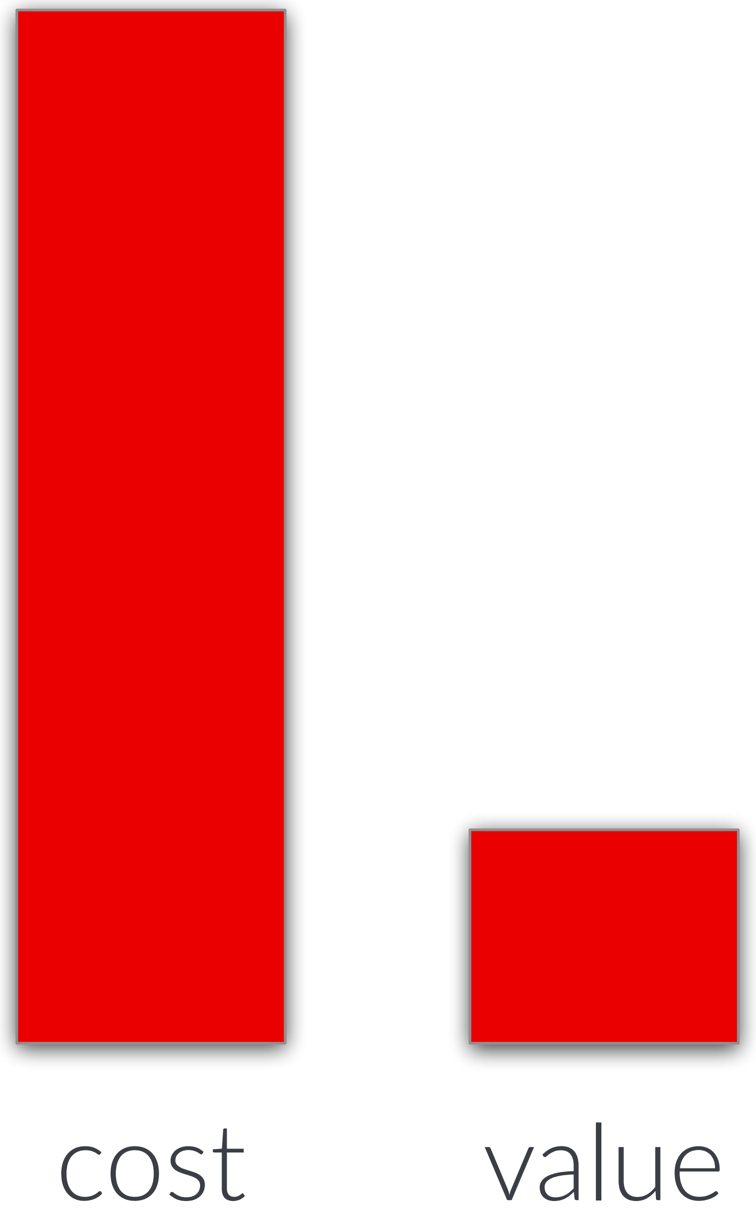
Over time you will go broke.



If cost increases it better still be less than the value.

$$\frac{\$10 * 5\%}{\$2} -100\% = -75\%$$

Otherwise you'll still go broke.



We make these calculations all day.

- When shopping
- While at work
- In relationships
- As a parent

Attackers do too.

This is why breaches and attacks are exploding.

Attacks are *dirt cheap* and the value is *astronomical*.

This is what I used to look like

Who am I?

- Web dork.
- Director at Shape Security & Google Dev Expert.
- Old-school video game hacker.
- @jsoverson most everywhere

SHaPe?

Ever heard of YKK?

YKK
YKK
YKK

You probably used Shape today.

We're the reason you log in a lot less and see fewer CAPTCHAs.

Agenda

1 **Cost vs value in security**

2 Attack in detail

3 How to affect cost

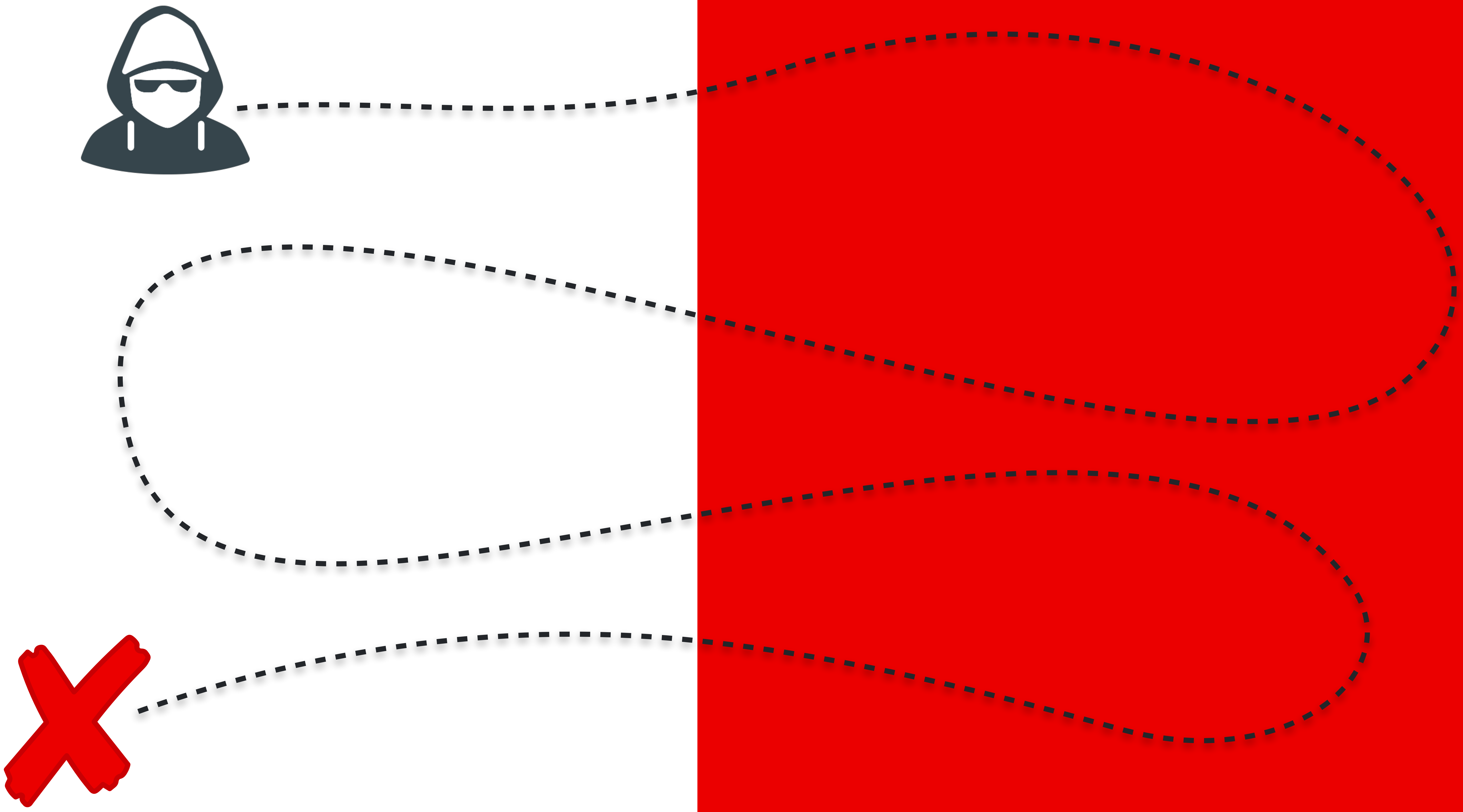
4 Real world example

MANUAL WORK

AUTOMATION

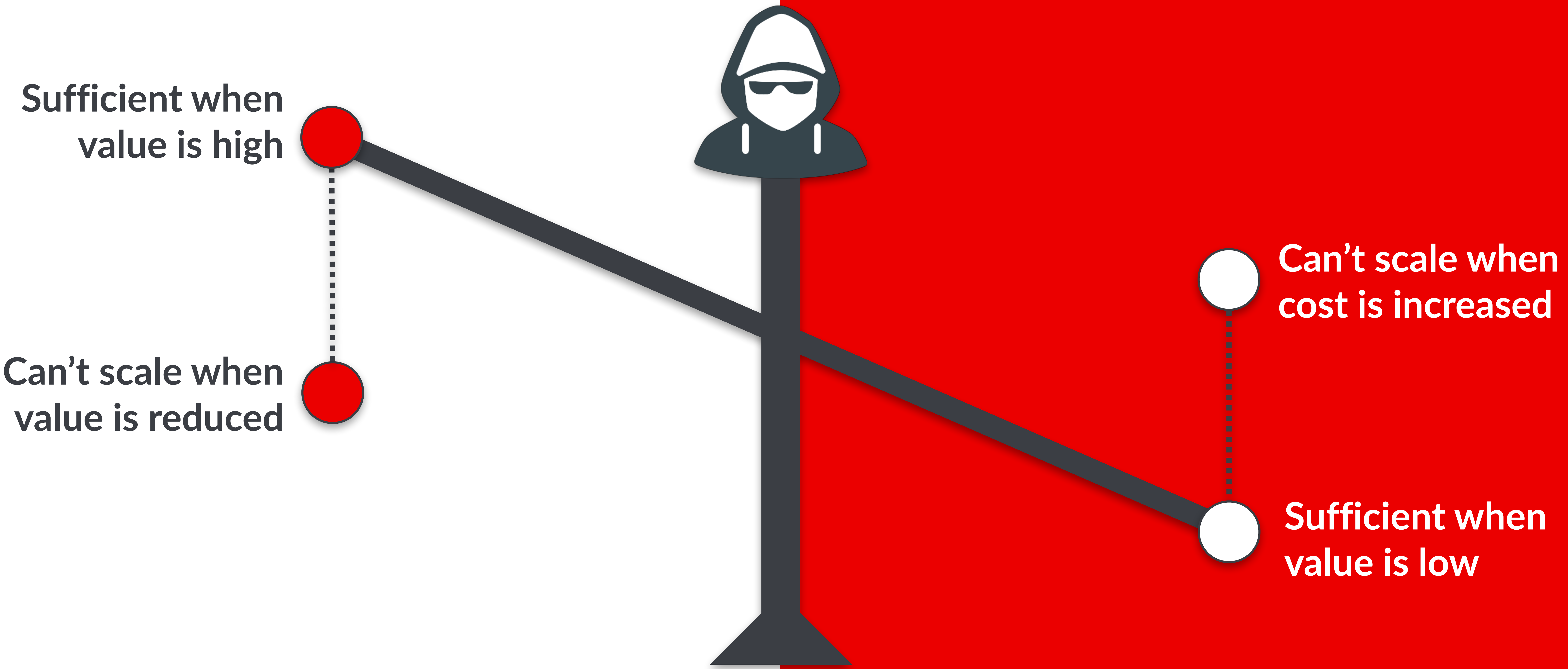
MANUAL WORK

AUTOMATION



MANUAL WORK

AUTOMATION



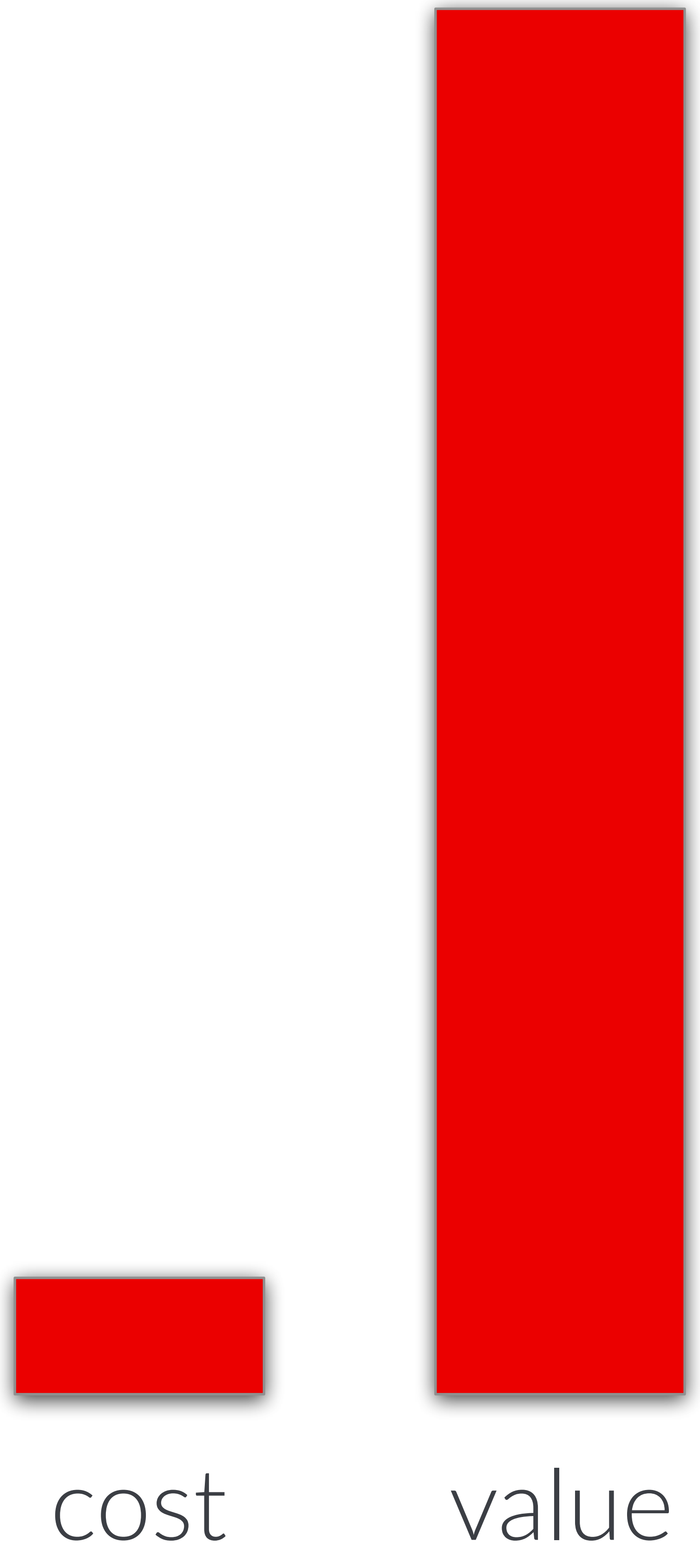
Sufficient when value is high

Can’t scale when value is reduced

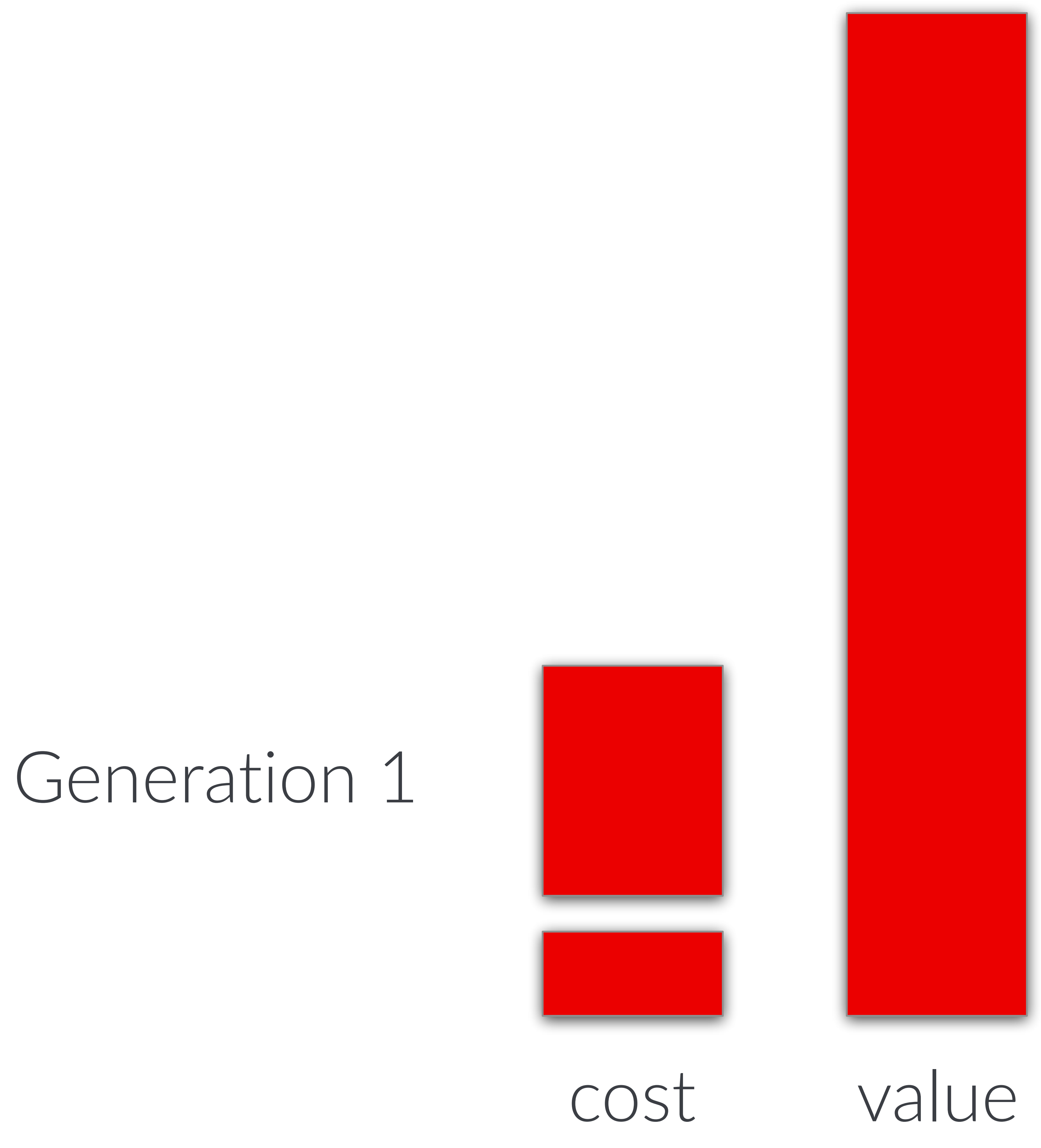
Can’t scale when cost is increased

Sufficient when value is low

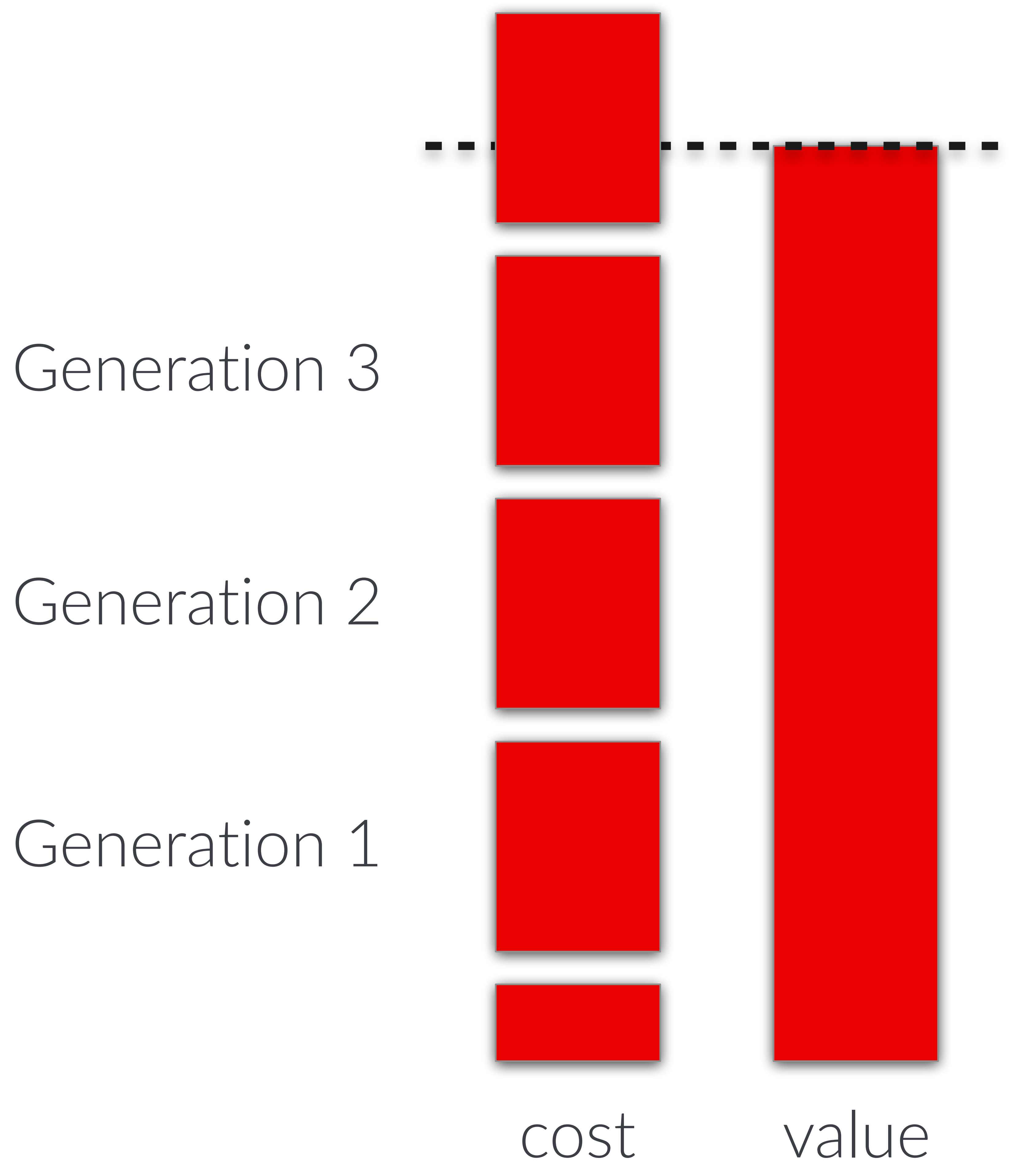
If there are no defenses in place, costs are negligible.



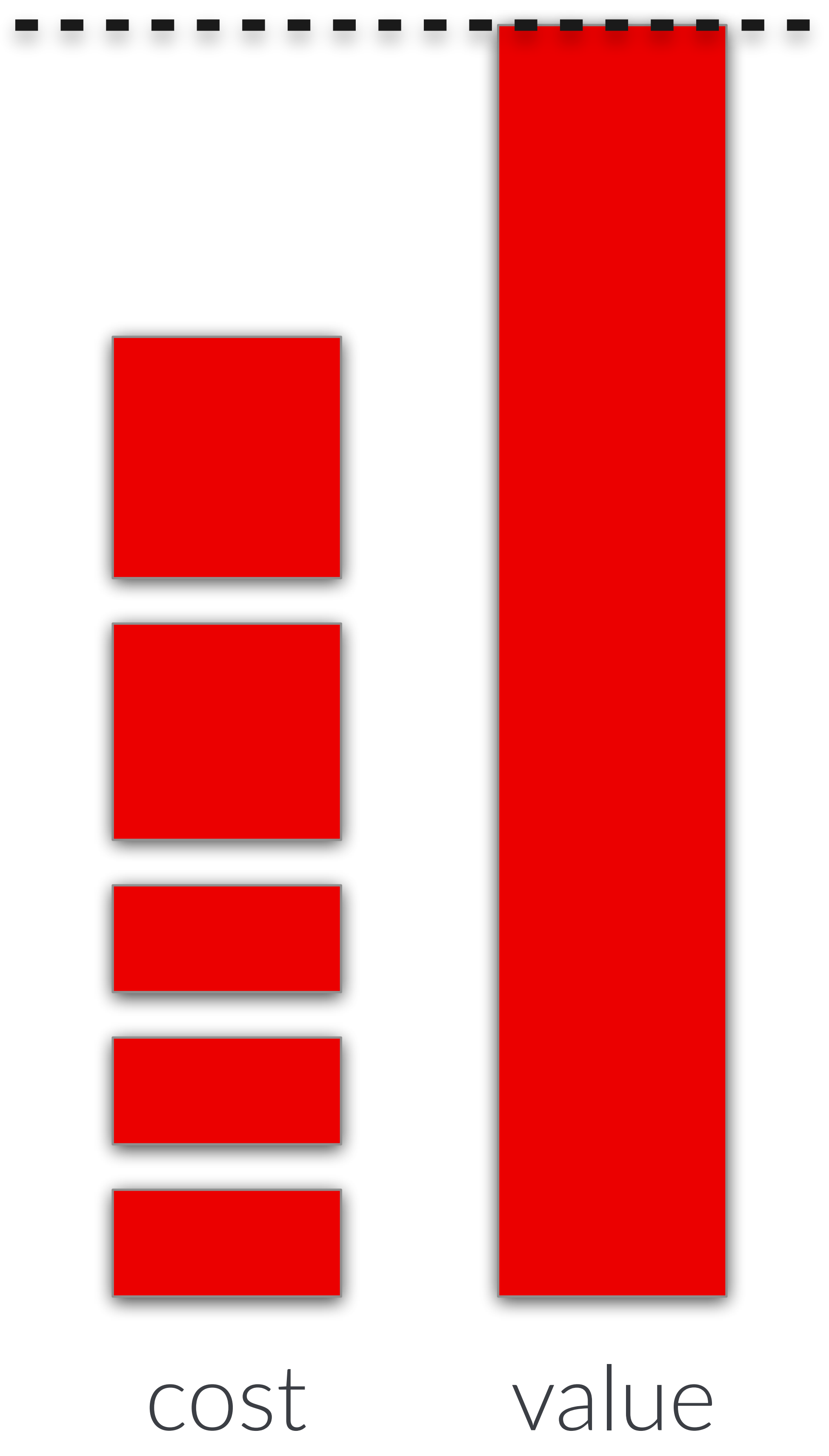
Any defense increases the cost by forcing a generational shift.



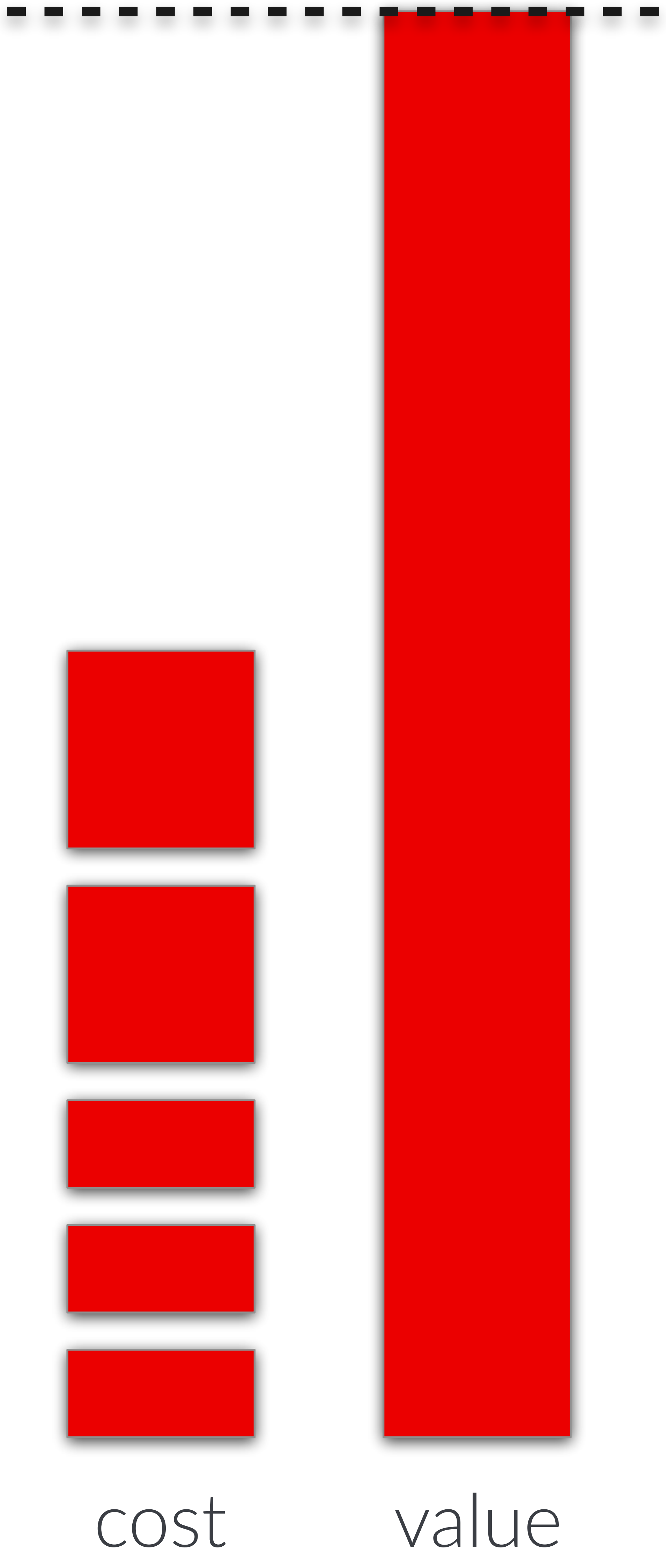
With enough defense cost vs value tips in your favor



The cost of entry for each generation decreases over time.

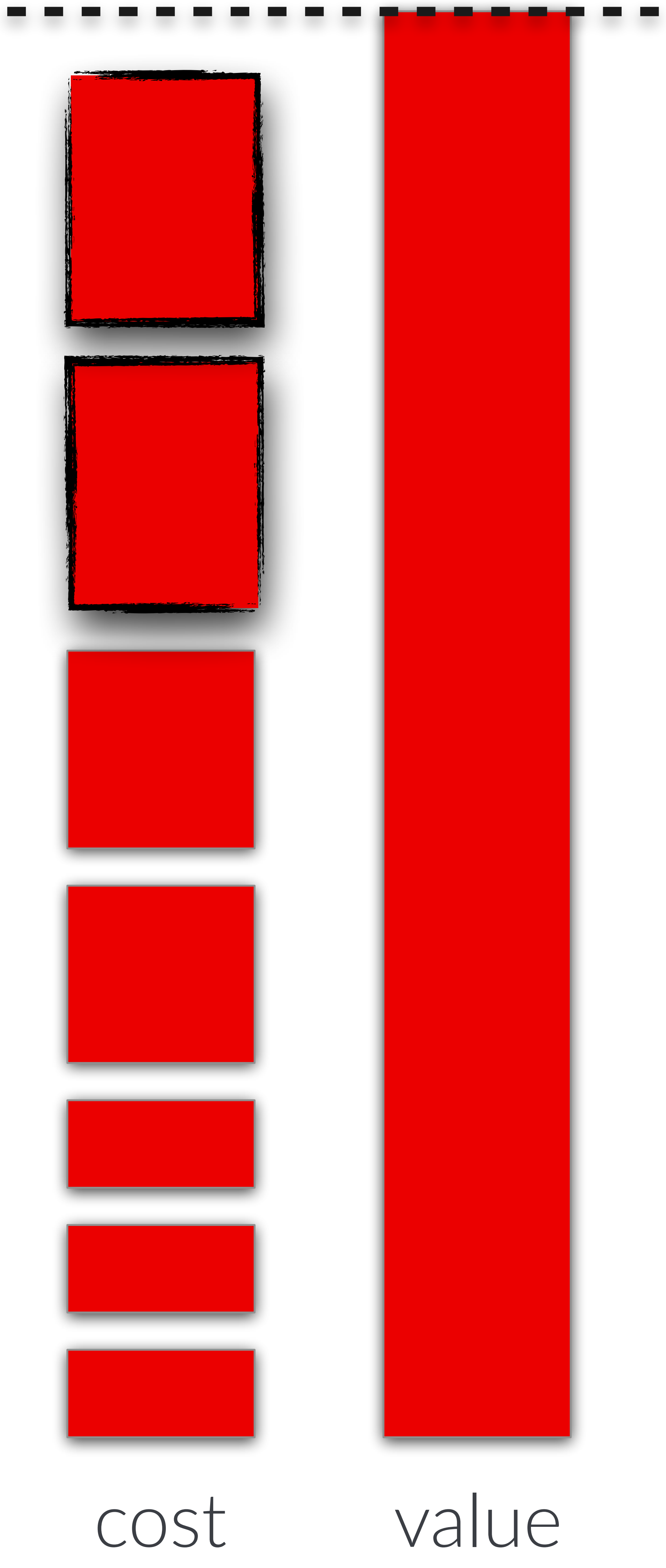


While the value of successful attacks only goes up.



And every generation necessitates new defenses.

which means sophistication is growing **rapidly**

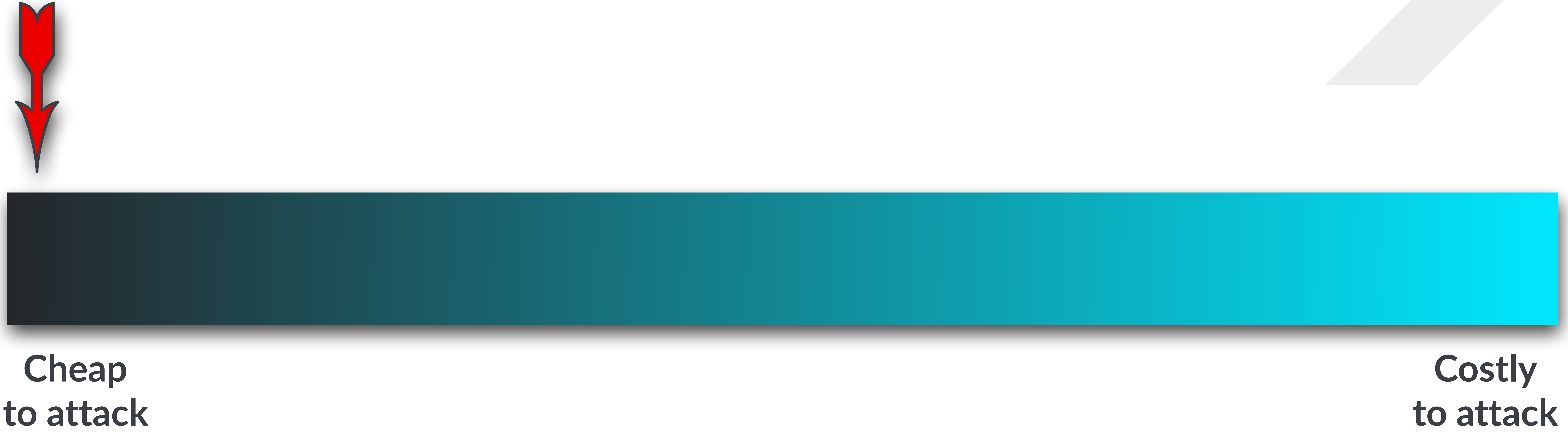


Security is a gradient of friction (attack cost)

Cheap
to attack

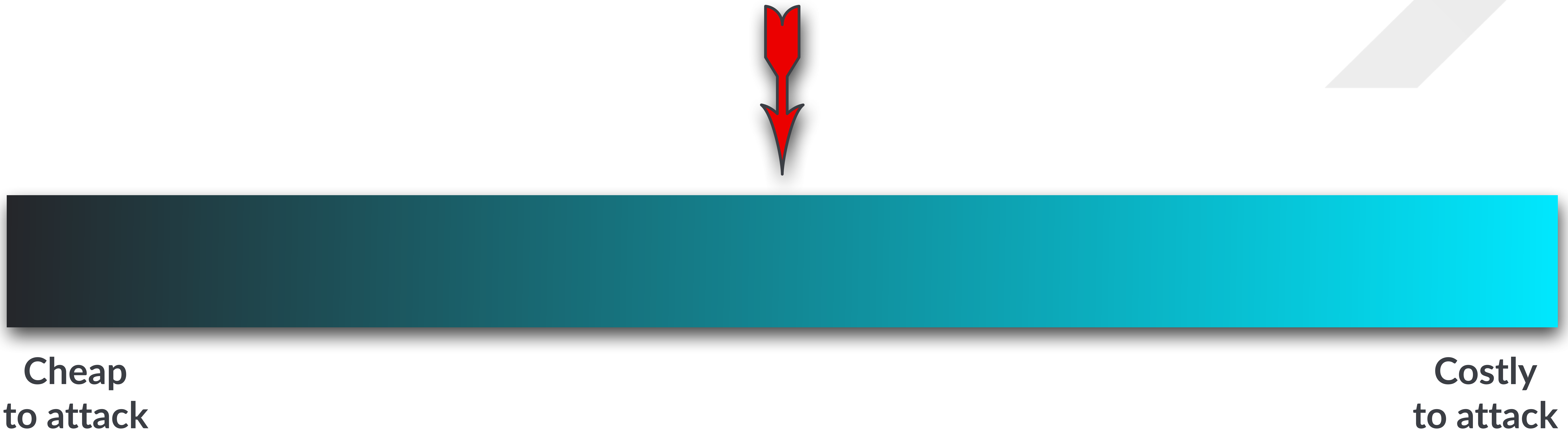
Costly
to attack

Don't patch anything ever?



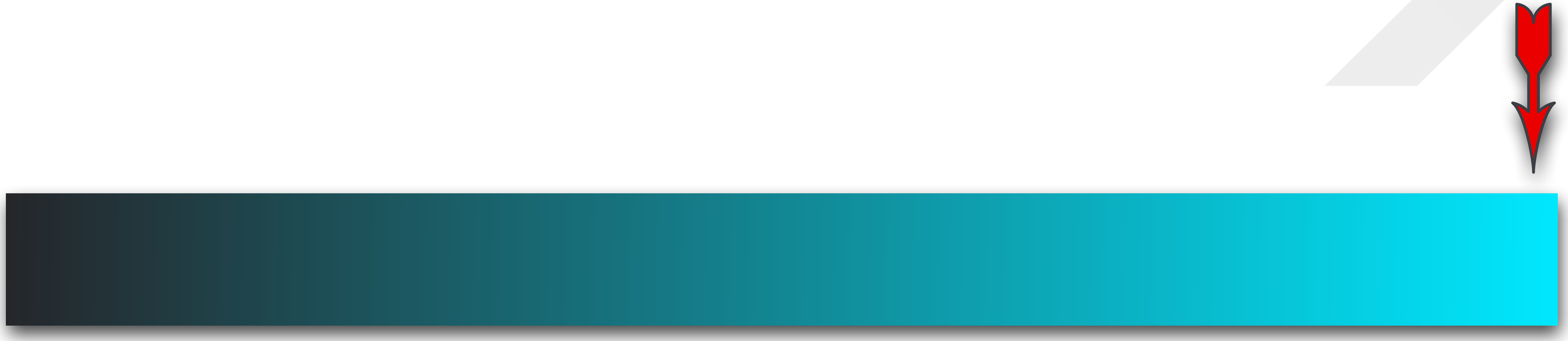
You're making it easy for script kiddies to attack you.

Patch within 3 months?



Then you're only vulnerable to the latest threat
for a 3 month window.

Patch on day 0?



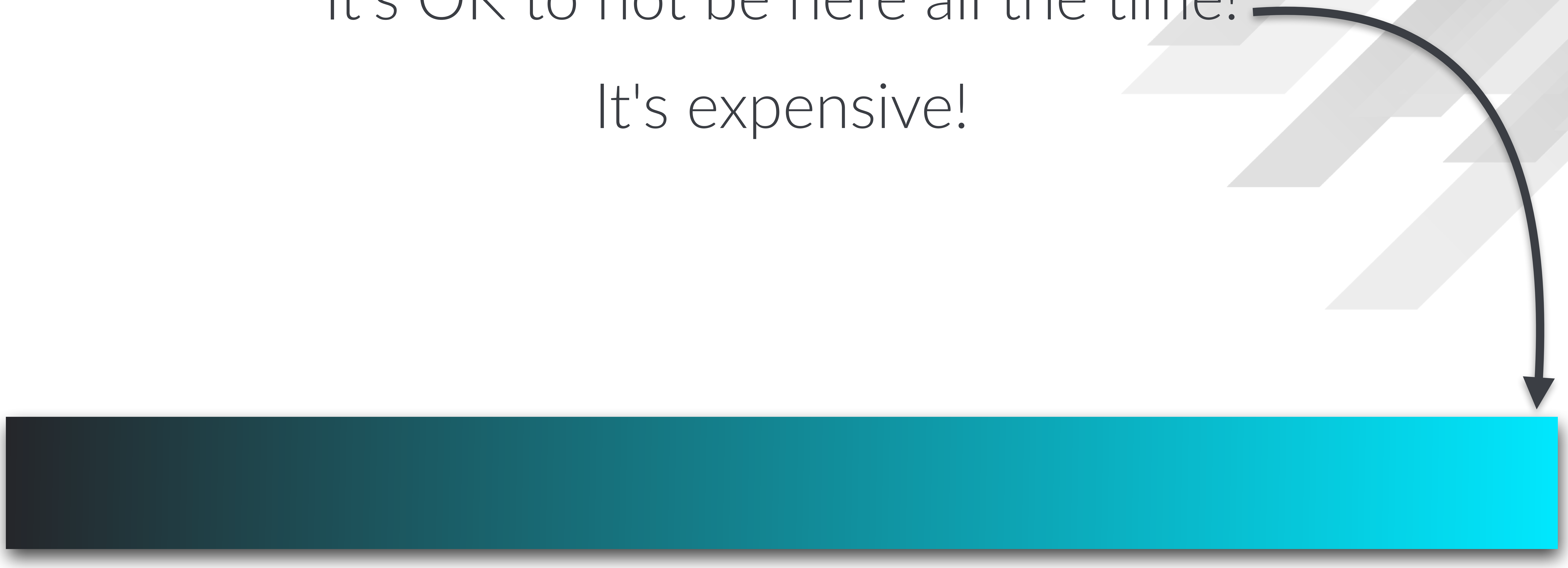
Cheap to attack

Costly to attack

You drive attackers to find their own vulnerabilities.

It's OK to not be here all the time!

It's expensive!



But you need to know the tradeoffs.

Some threats can't be patched away.

The OWASP Automated Threats are attacks that abuse inherent functionality.

OWASP Automated Threats

- OAT-020 Account Aggregation
- OAT-019 Account Creation
- OAT-003 Ad Fraud
- OAT-009 CAPTCHA Defeat
- OAT-010 Card Cracking
- OAT-001 Carding
- OAT-012 Cashing Out
- OAT-007 Credential Cracking
- OAT-008 Credential Stuffing
- OAT-021 Denial of Inventory
- OAT-015 Denial of Service
- OAT-006 Expediting
- OAT-004 Fingerprinting
- OAT-018 Footprinting
- OAT-005 Scalping
- OAT-011 Scraping
- OAT-016 Skewing
- OAT-013 Sniping
- OAT-017 Spamming
- OAT-002 Token Cracking
- OAT-014 Vulnerability Scanning

Agenda

1 Cost vs value in security

2 **Attack in detail**

3 How to affect cost

4 Real world example

CREDENTIAL STUFFING

cre·den·tial stuff·ing

/krəˈden(t)SHəl ˈstəfiNG/

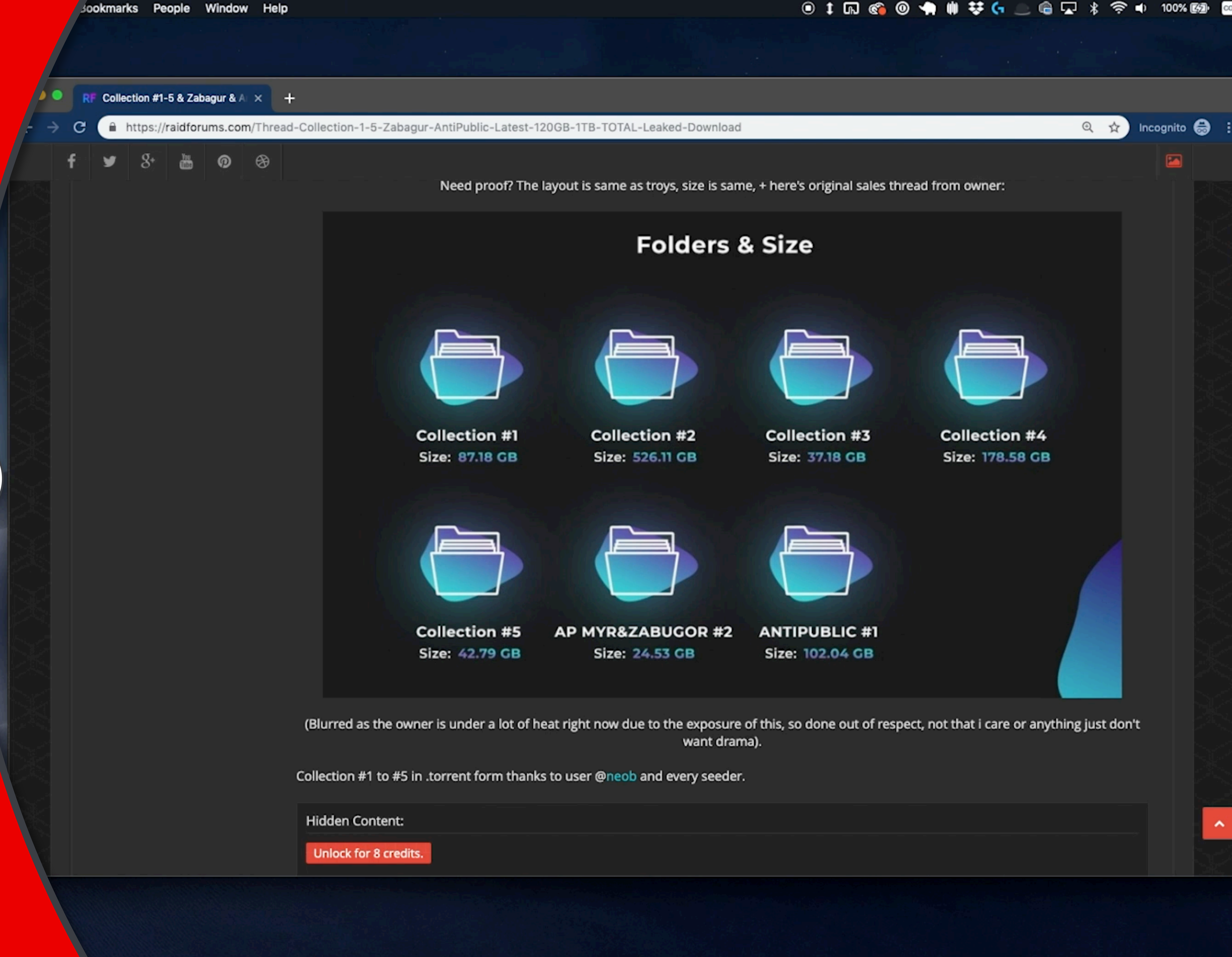
The replay of breached username/password pairs across sites to find accounts where passwords have been reused.

A STEP BY STEP GUIDE

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

CREDENTIAL STUFFING

1


Bookmarks
People
Window
Help
Collection #1-5 & Zabagur & A
https://raidforums.com/Thread-Collection-1-5-Zabagur-AntiPublic-Latest-120GB-1TB-TOTAL-Leaked-Download
Incognito

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

Folders & Size

Collection #1
Size: 87.18 GB

Collection #2
Size: 526.11 GB

Collection #3
Size: 37.18 GB

Collection #4
Size: 178.58 GB

Collection #5
Size: 42.79 GB

AP MYR&ZABUGOR #2
Size: 24.53 GB

ANTIPUBLIC #1
Size: 102.04 GB

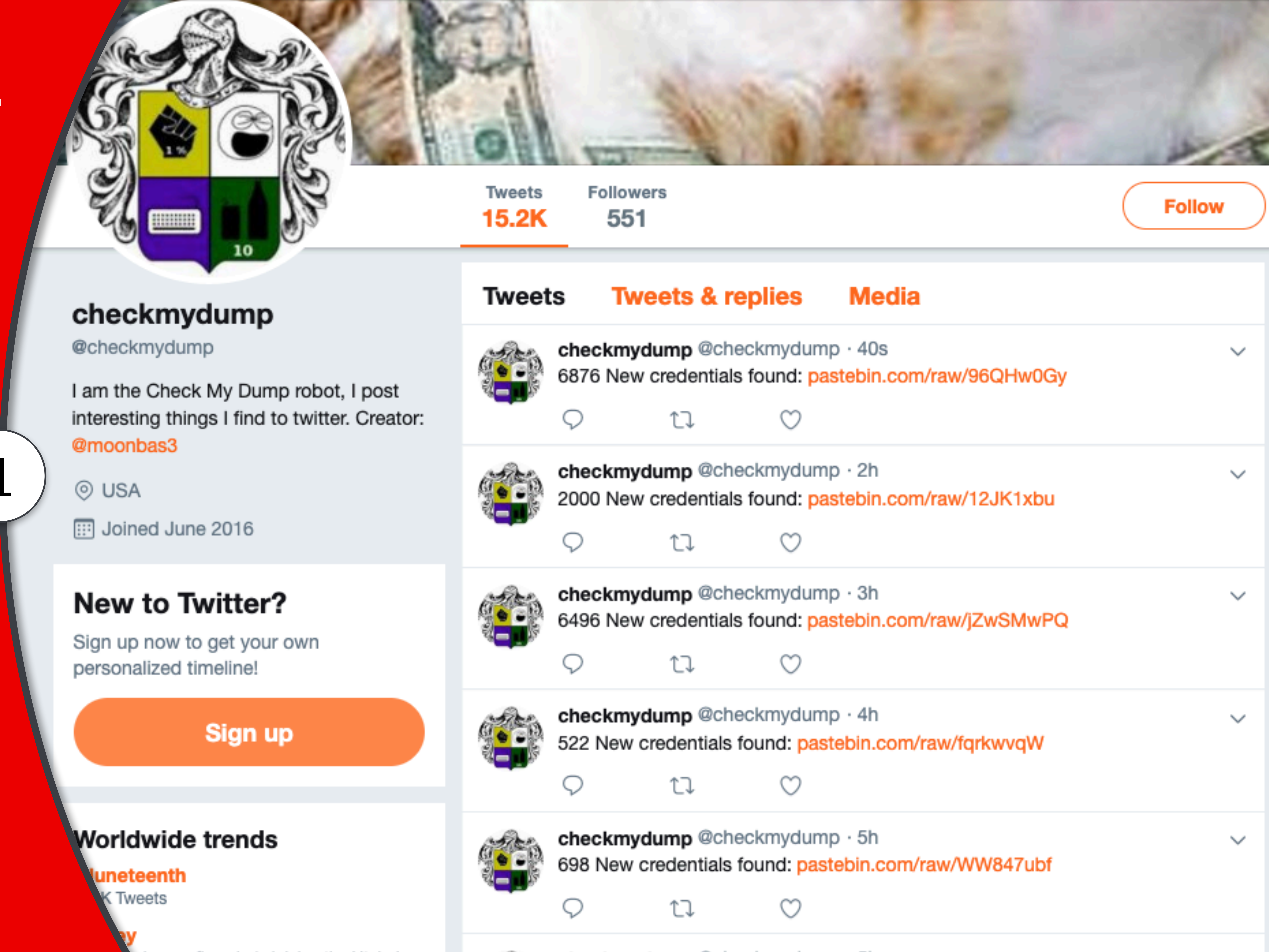
(Blurred as the owner is under a lot of heat right now due to the exposure of this, so done out of respect, not that i care or anything just don't want drama).

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

Hidden Content:

1. Get Credentials

CREDENTIAL STUFFING



1

Tweets 15.2K

Followers 551

Follow

checkmydump
@checkmydump

I am the Check My Dump robot, I post interesting things I find to twitter. Creator: @moonbas3

USA

Joined June 2016

New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

Worldwide trends

uneteenth
K Tweets

ey

Tweets | Tweets & replies | Media

checkmydump @checkmydump · 40s
6876 New credentials found: pastebin.com/raw/96QHw0Gy

checkmydump @checkmydump · 2h
2000 New credentials found: pastebin.com/raw/12JK1xbu

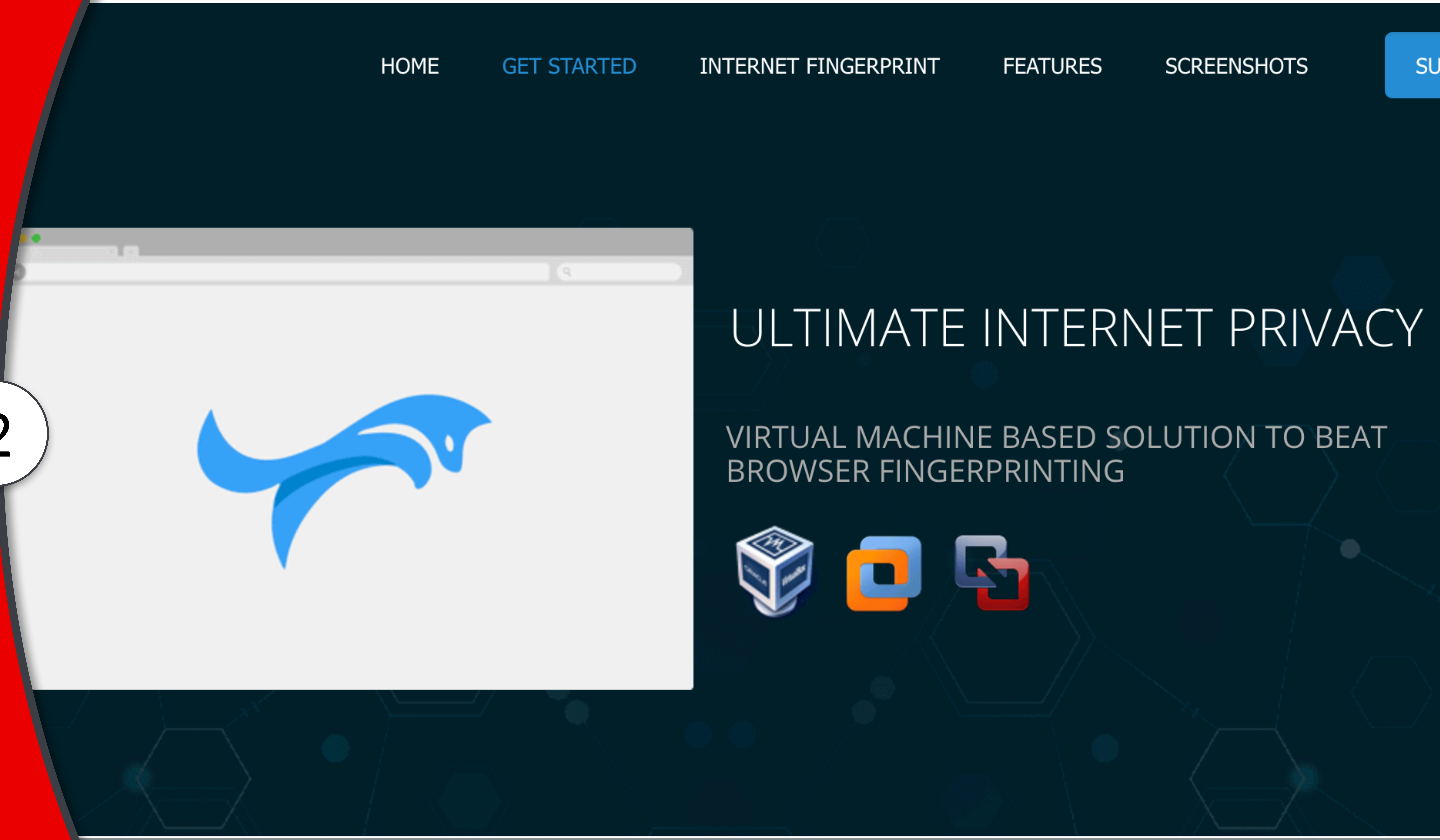
checkmydump @checkmydump · 3h
6496 New credentials found: pastebin.com/raw/jZwSMwPQ

checkmydump @checkmydump · 4h
522 New credentials found: pastebin.com/raw/fqrkwvqW

checkmydump @checkmydump · 5h
698 New credentials found: pastebin.com/raw/WW847ubf

1. Get Credentials

CREDENTIAL STUFFING



HOME GET STARTED INTERNET FINGERPRINT FEATURES SCREENSHOTS SU

ULTIMATE INTERNET PRIVACY

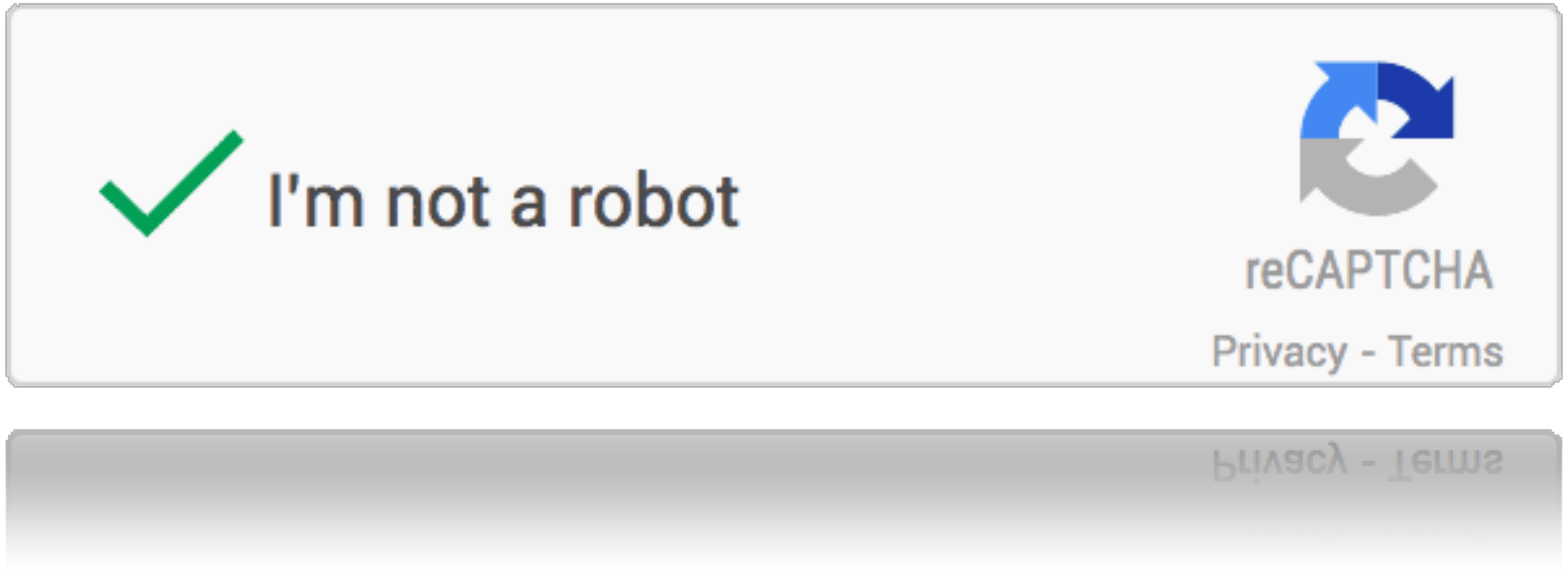
VIRTUAL MACHINE BASED SOLUTION TO BEAT BROWSER FINGERPRINTING

2

1. Get Credentials
2. Automate Login

CREDENTIAL STUFFING

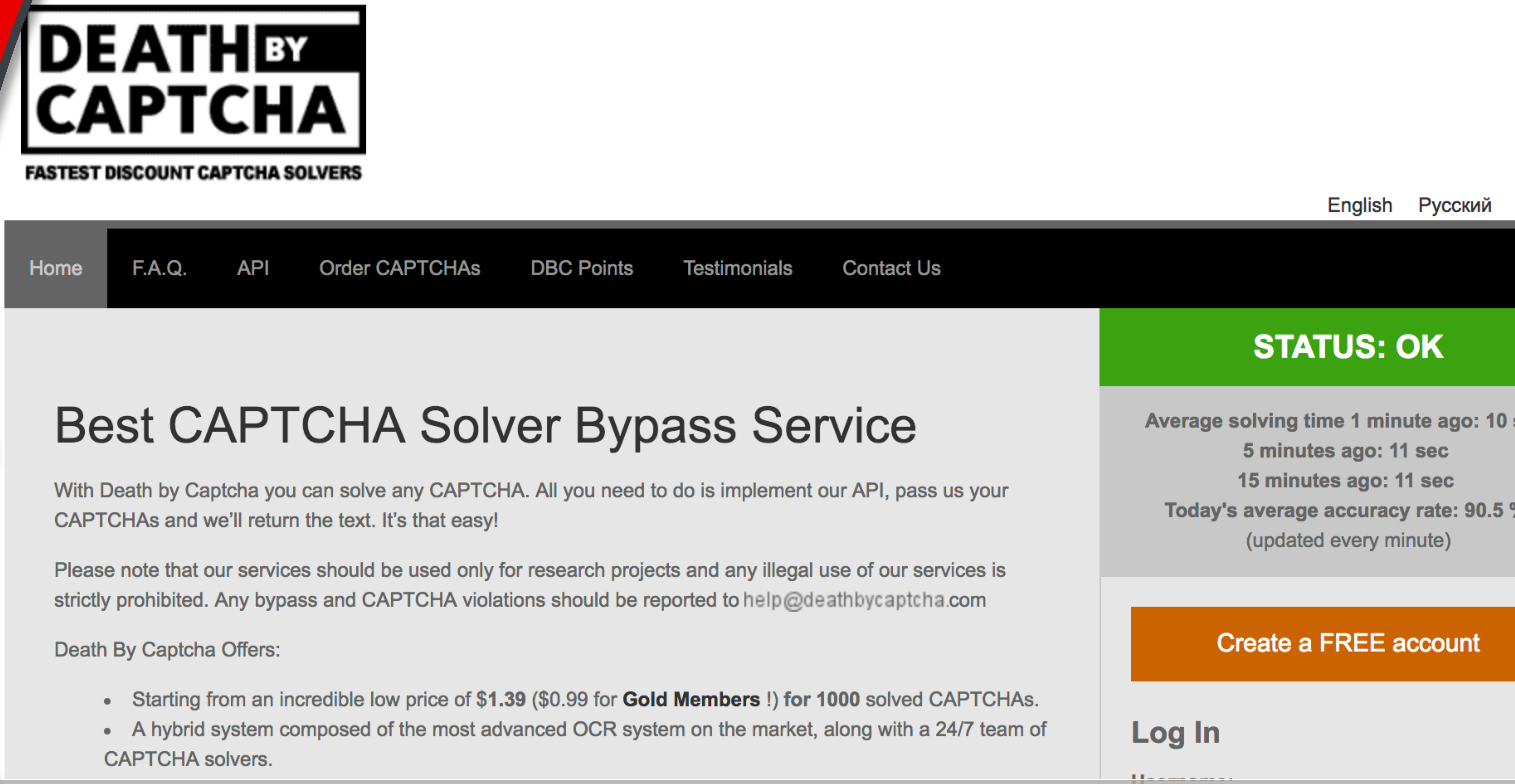
3



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

CREDENTIAL STUFFING

3



DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

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.

STATUS: OK

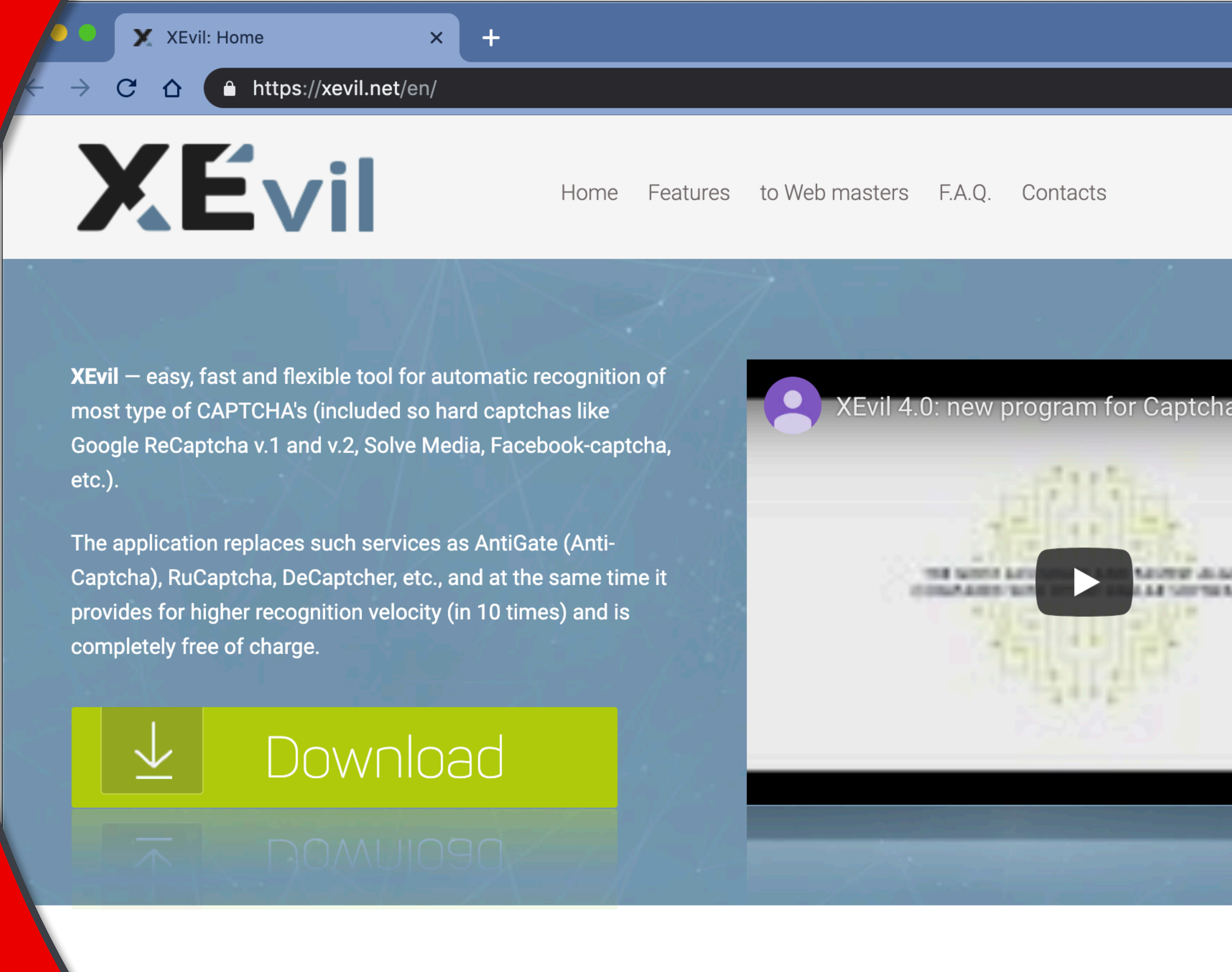
Average solving time 1 minute ago: 10
5 minutes ago: 11 sec
15 minutes ago: 11 sec
Today's average accuracy rate: 90.5
(updated every minute)

Log In

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

CREDENTIAL STUFFING

3



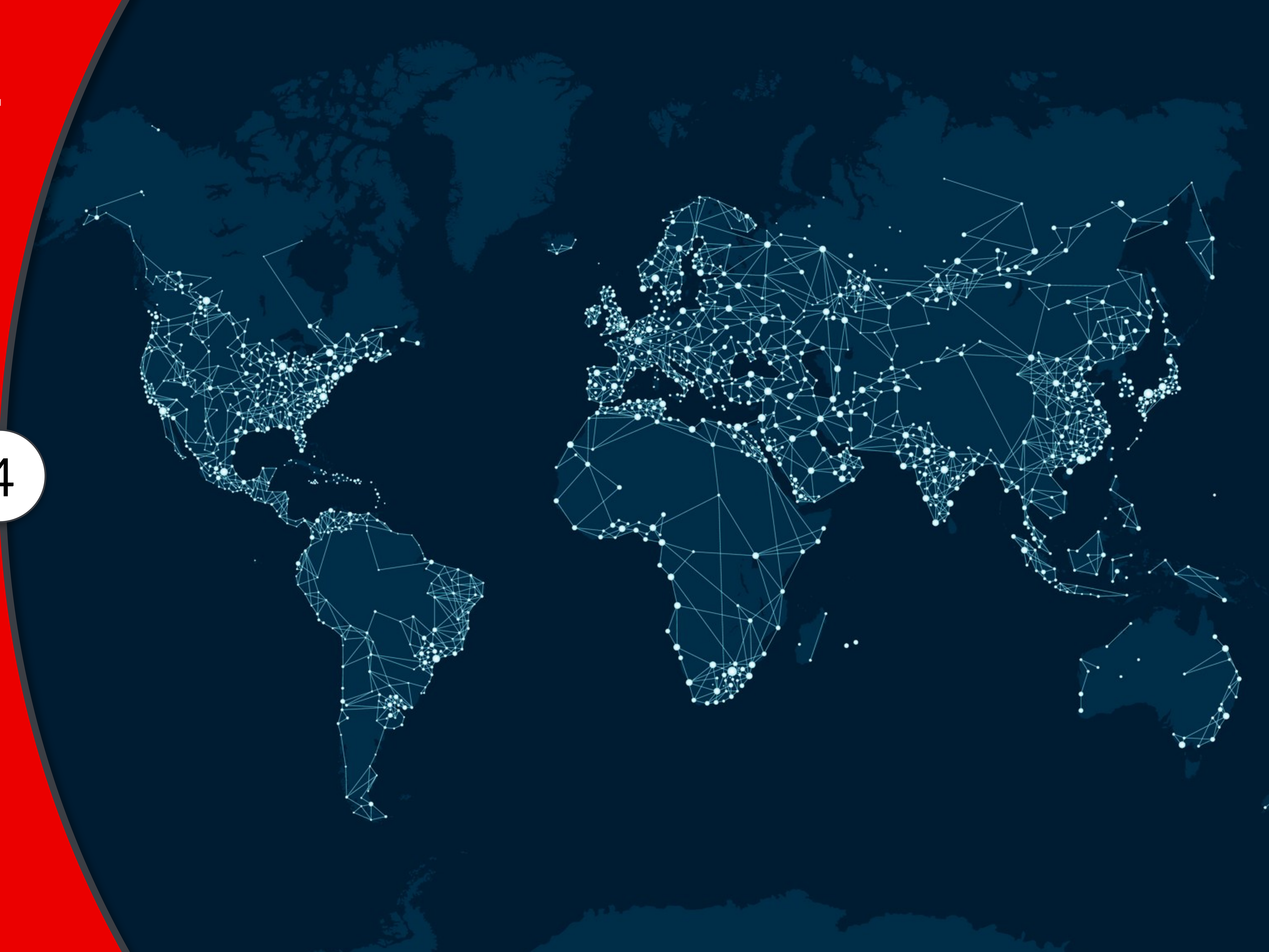
XEvil — easy, fast and flexible tool for automatic recognition of most type of CAPTCHA's (included so hard captchas like Google ReCaptcha v.1 and v.2, Solve Media, Facebook-captcha, etc.).

The application replaces such services as AntiGate (Anti-Captcha), RuCaptcha, DeCaptcher, etc., and at the same time it provides for higher recognition velocity (in 10 times) and is completely free of charge.

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

CREDENTIAL STUFFING

4



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

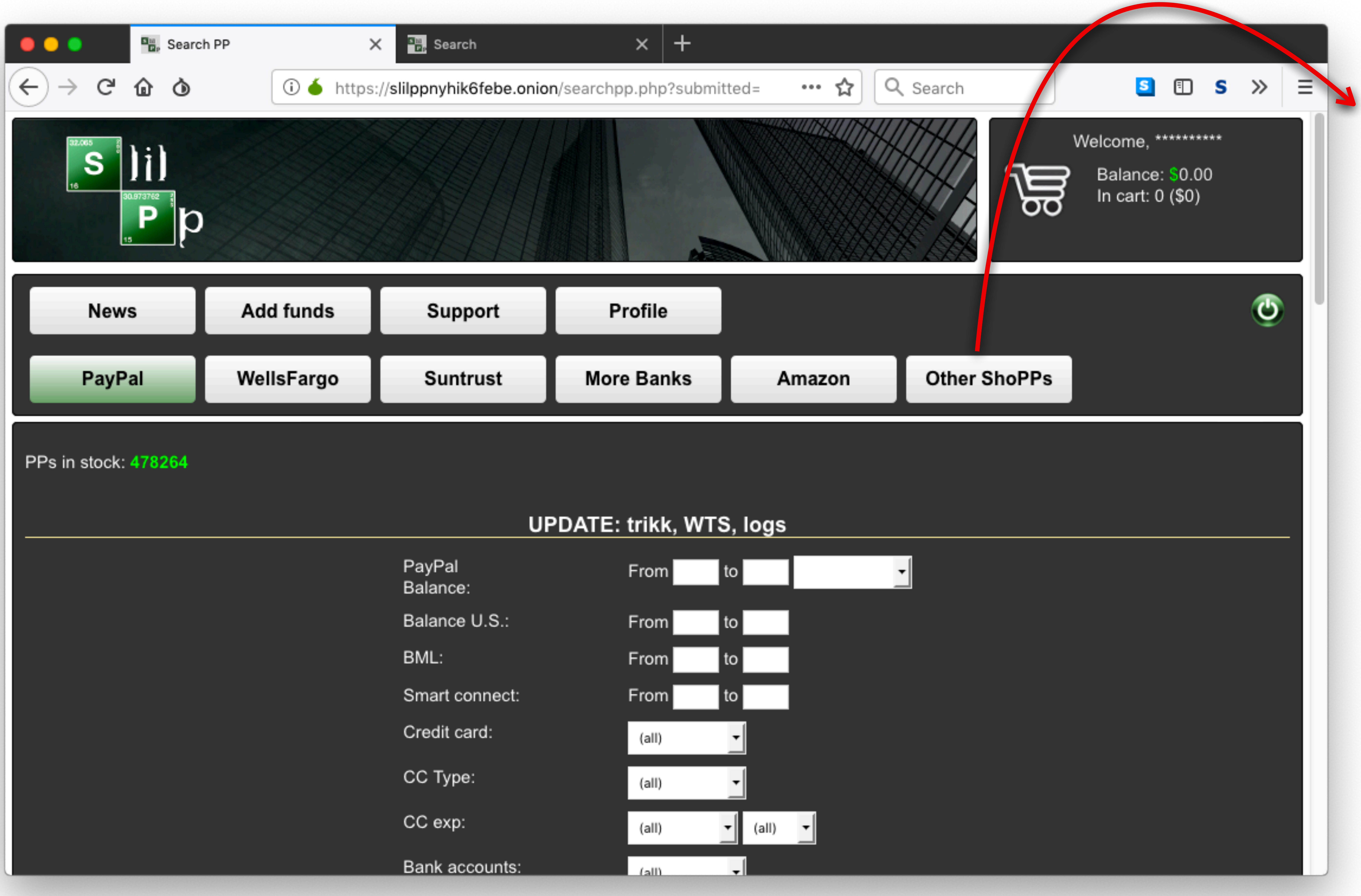
$0 : 2.3 billion credentials

$50 : for tool configuration

$139 : for 100,000 CAPTCHAs

$10 : for 1000 global IPs

Less than $200
for 100,000 ATO
attempts



Welcome, **********

Balance: $0.00

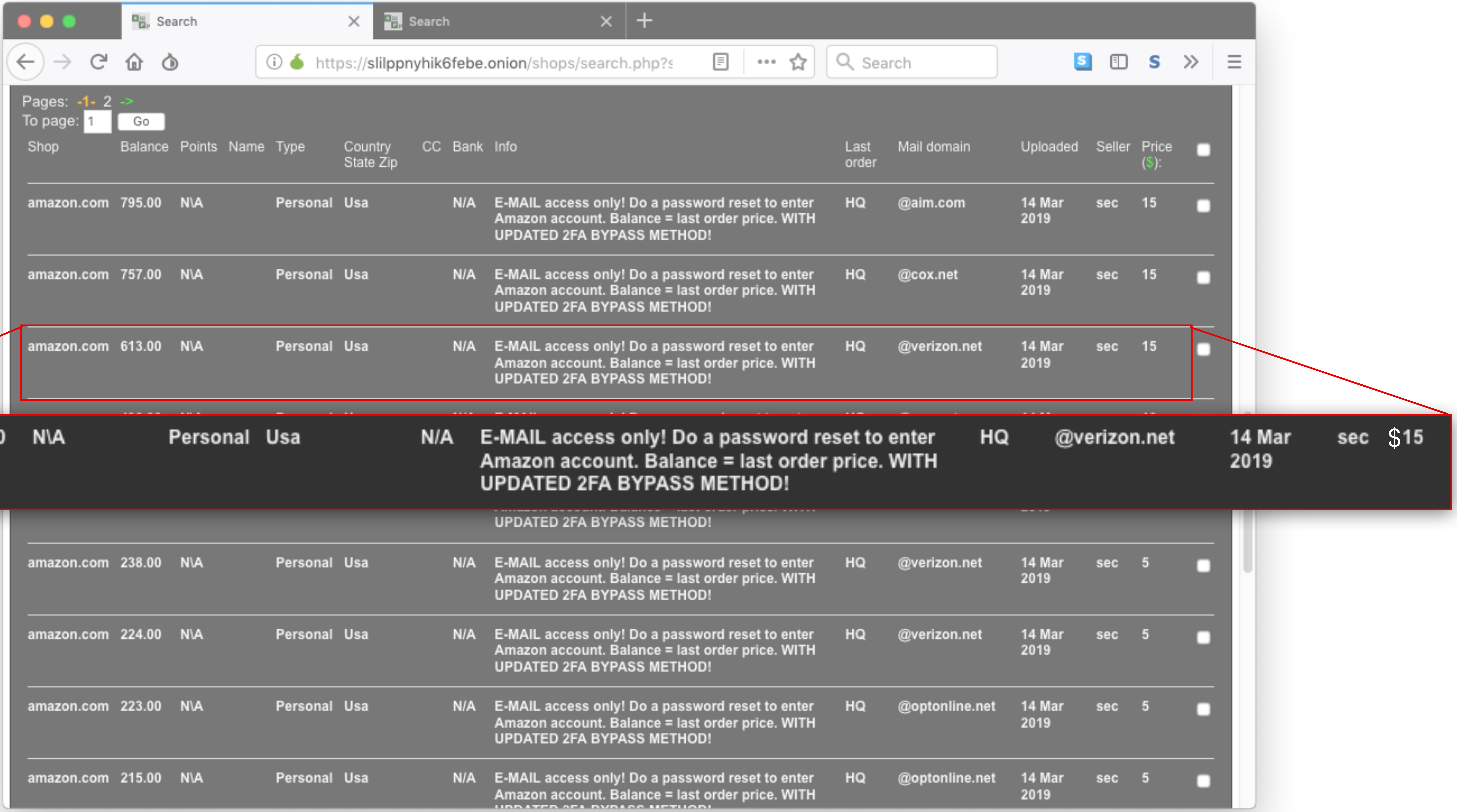
In cart: 0 ($0)

PPs in stock: 478264

UPDATE: trikk, WTS, logs

PayPal Balance:	From to
Balance U.S.:	From to
BML:	From to
Smart connect:	From to
Credit card:	(all)
CC Type:	(all)
CC exp:	(all) (all)
Bank accounts:	(all)

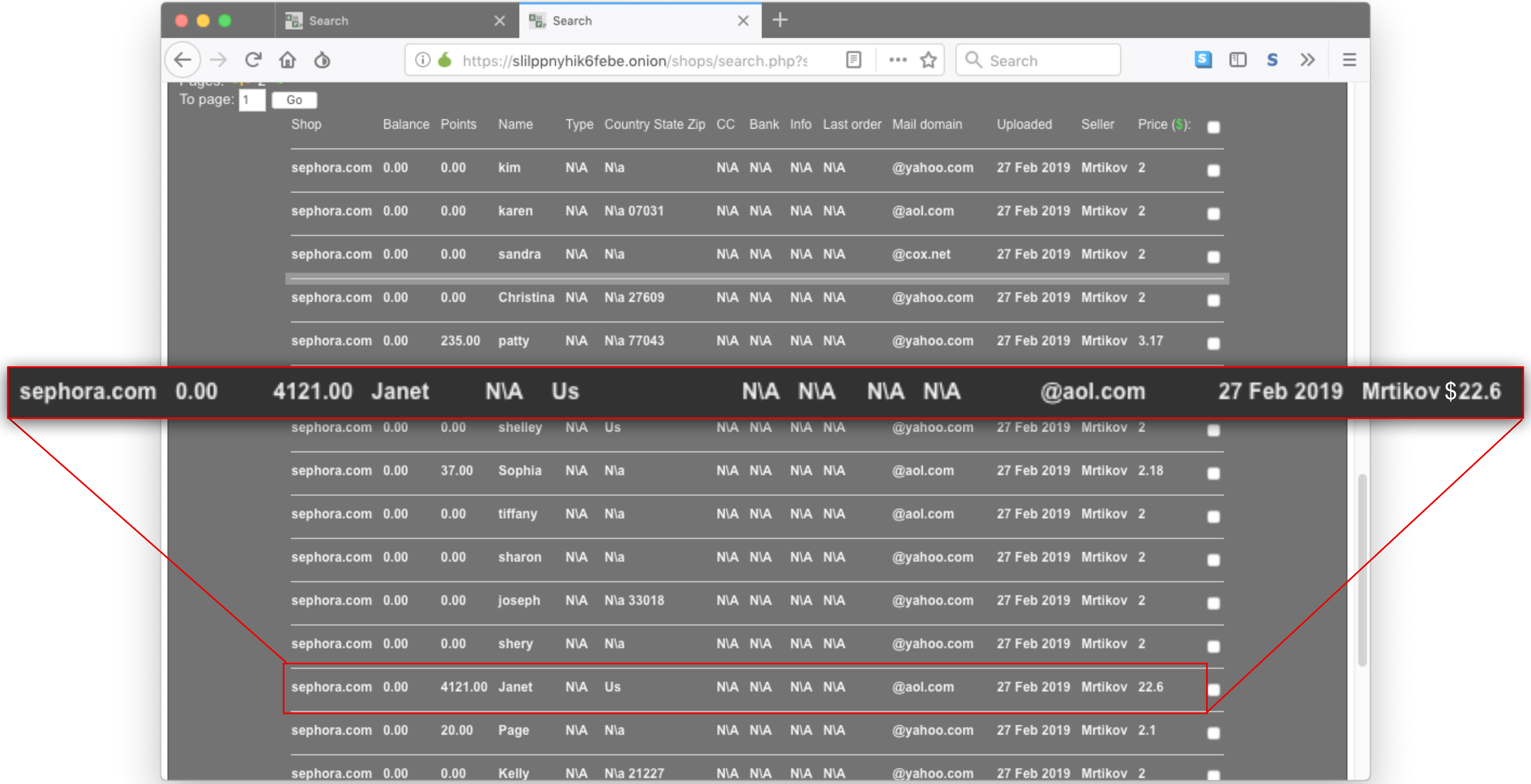
- apple
- airbnb
- bergfreunde
- britishairways
- capitalone
- deliveroo
- discovercard
- epicgames
- facebook
- groupon
- ikea
- marriot
- netflix
- +400 more



Pages: -1- 2 ->
To page: 1 Go

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	□
[illegible]	[illegible]	[illegible]		[illegible]	[illegible]		[illegible]	[illegible] UPDATED 2FA BYPASS METHOD!	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	□
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	□
amazon.com	215.00	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	□

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



To page: 1 Go

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	0.00	shelley	N\A	Us	N\A	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	☐
sephora.com	0.00	0.00	Kelly	N\A	N\a 21227	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

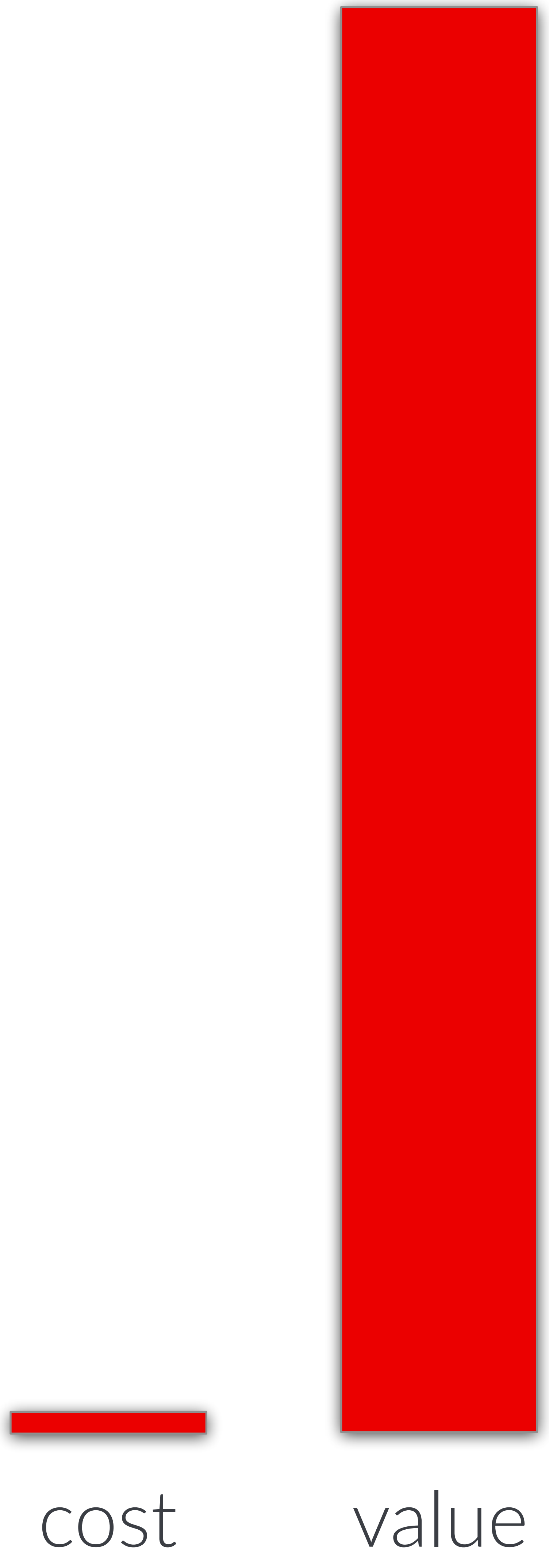
Values range between a couple dollars to >$150

Success rate is around 0.2% - 2%

Cost per attempt is less than $0.002

You're looking at a return with a low of 100% to a high of 150000%+

This is not where we want to be.

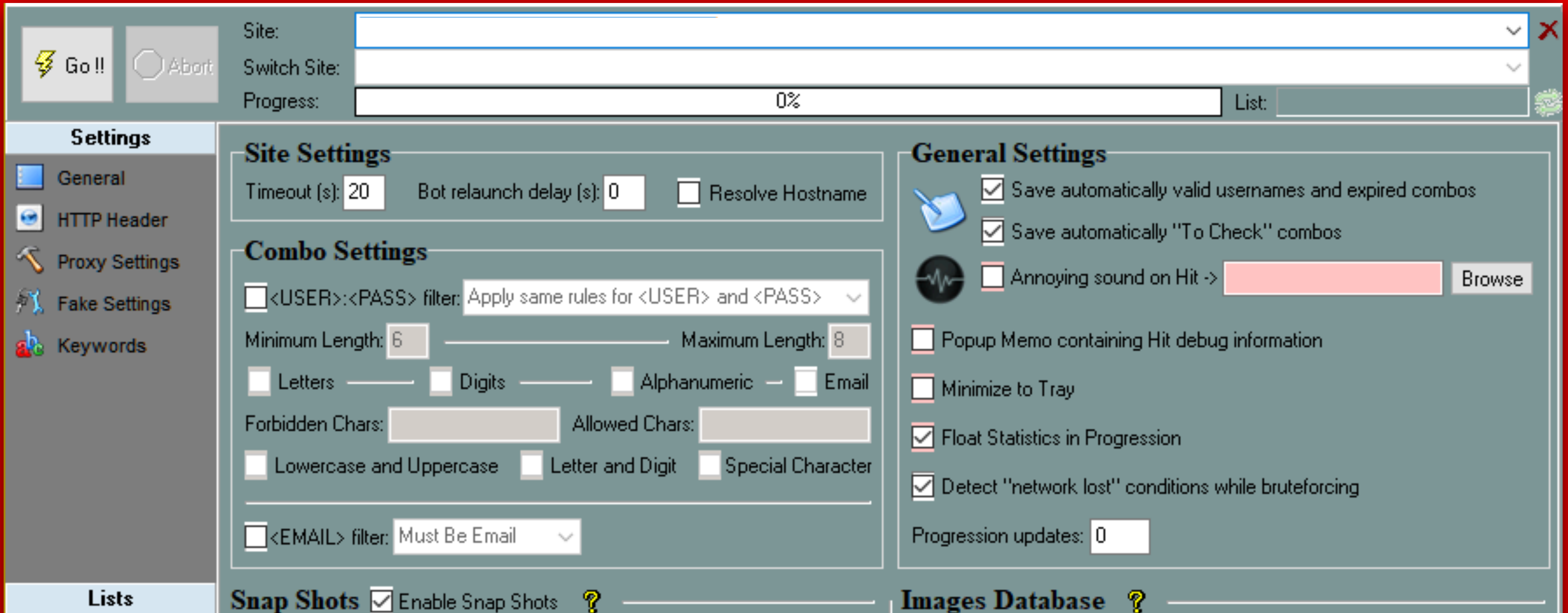


Evolution is constant here.

The value is so great that it is fueling rapid iteration.

SentryMBA

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



Go !! Abort

Site:

Switch Site:

Progress: 0%

List:

Settings

- General
- HTTP Header
- Proxy Settings
- Fake Settings
- Keywords

Lists

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: Allowed Chars:

□ 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 -> Browse

□ Popup Memo containing Hit debug information

□ Minimize to Tray

☑ Float Statistics in Progression

☑ Detect "network lost" conditions while bruteforcing

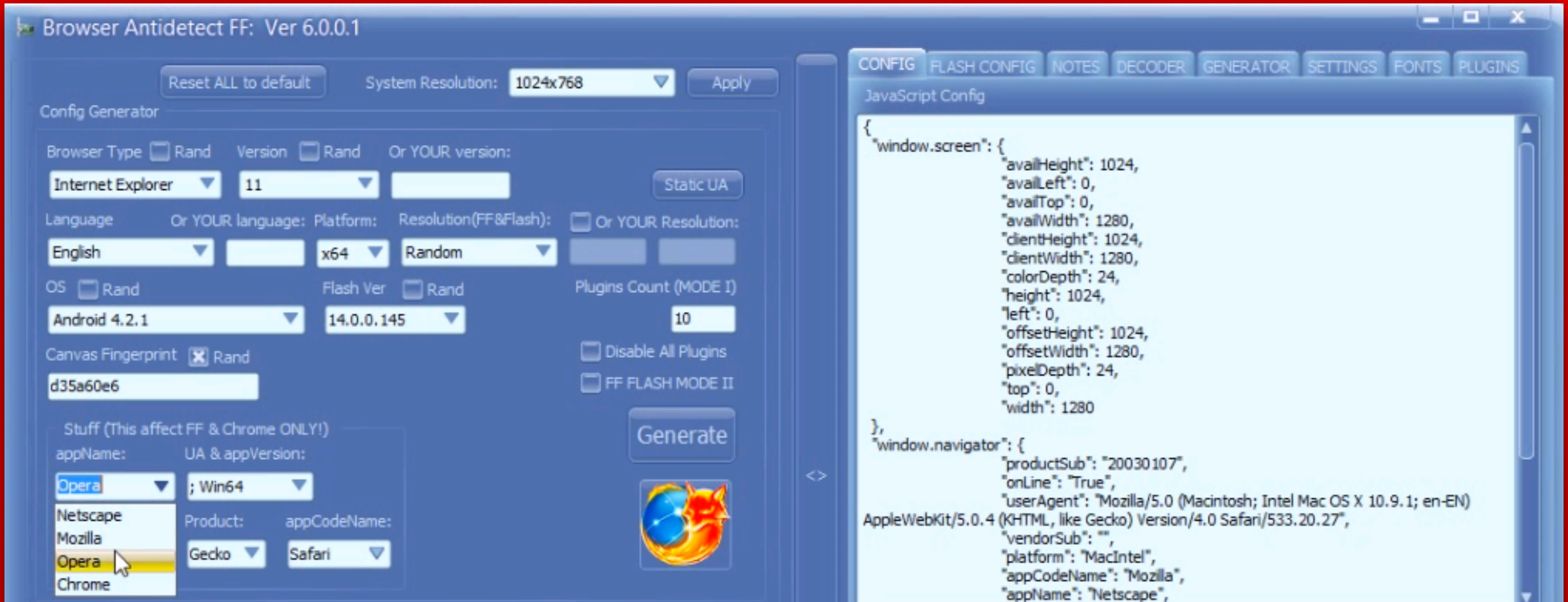
Progression updates: 0

Snap Shots ☑ Enable Snap Shots ?

Images Database ?

Browser AntiDetect

- Extension for FireFox and Chrome.
- Randomizes fingerprintable data points.
- Designed specifically to blend in.



Browser Antidetect FF: Ver 6.0.0.1

System Resolution: 1024x768

Browser Type □ Rand: Internet Explorer

Version □ Rand: 11

Or YOUR version:

Language: English

Or YOUR language:

Platform: x64

Resolution(FF&Flash): Random

□ Or YOUR Resolution:

OS □ Rand: Android 4.2.1

Flash Ver □ Rand: 14.0.0.145

Plugins Count (MODE I): 10

Canvas Fingerprint ☒ Rand: d35a60e6

□ Disable All Plugins

□ FF FLASH MODE II

Stuff (This affect FF & Chrome ONLY!)

appName: Opera

Netscape
Mozilla
Opera
Chrome

UA & appVersion: ; Win64

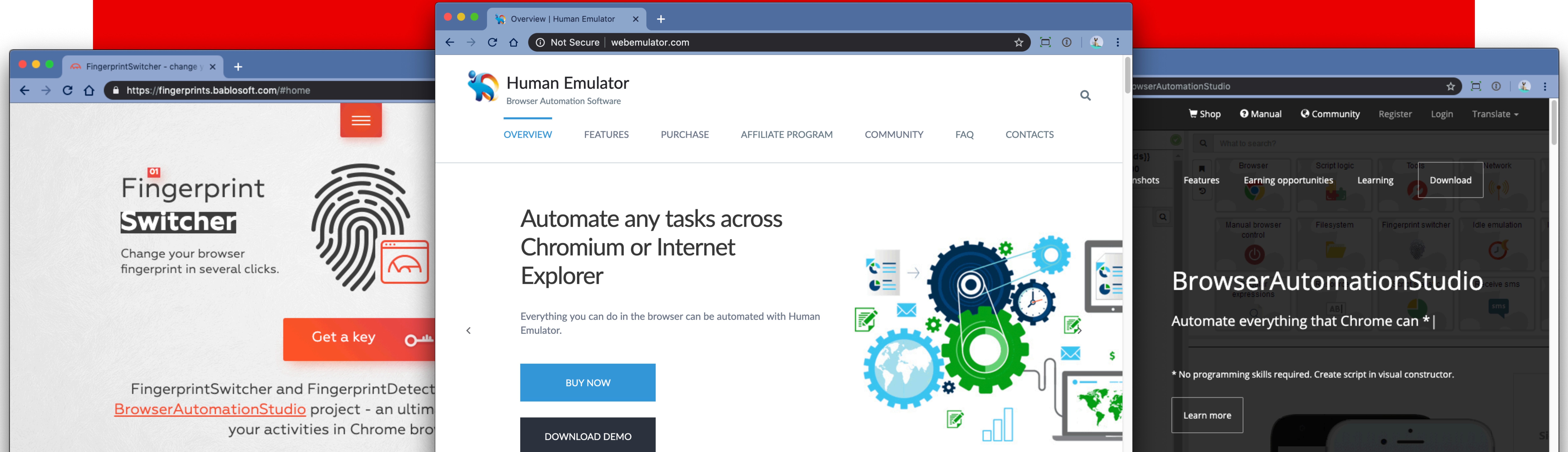
Product: Gecko

appCodeName: Safari

```
{
 "window.screen": {
                     "availHeight": 1024,
                     "availLeft": 0,
                     "availTop": 0,
                     "availWidth": 1280,
                     "clientHeight": 1024,
                     "clientWidth": 1280,
                     "colorDepth": 24,
                     "height": 1024,
                     "left": 0,
                     "offsetHeight": 1024,
                     "offsetWidth": 1280,
                     "pixelDepth": 24,
                     "top": 0,
                     "width": 1280
 },
 "window.navigator": {
                     "productSub": "20030107",
                     "onLine": "True",
                     "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9.1; en-EN)
AppleWebKit/5.0.4 (KHTML, like Gecko) Version/4.0 Safari/533.20.27",
                     "vendorSub": "",
                     "platform": "MacIntel",
                     "appCodeName": "Mozilla",
                     "appName": "Netscape",
```

Loads more

All pushing towards imitating real users with real behavior looking like they are using real devices coming from legitimate networks.



Fingerprint Switcher

Change your browser fingerprint in several clicks.

FingerprintSwitcher and FingerprintDetect
BrowserAutomationStudio project - an ultim
your activities in Chrome bro

Human Emulator
Browser Automation Software

Automate any tasks across Chromium or Internet Explorer

Everything you can do in the browser can be automated with Human Emulator.

BrowserAutomationStudio

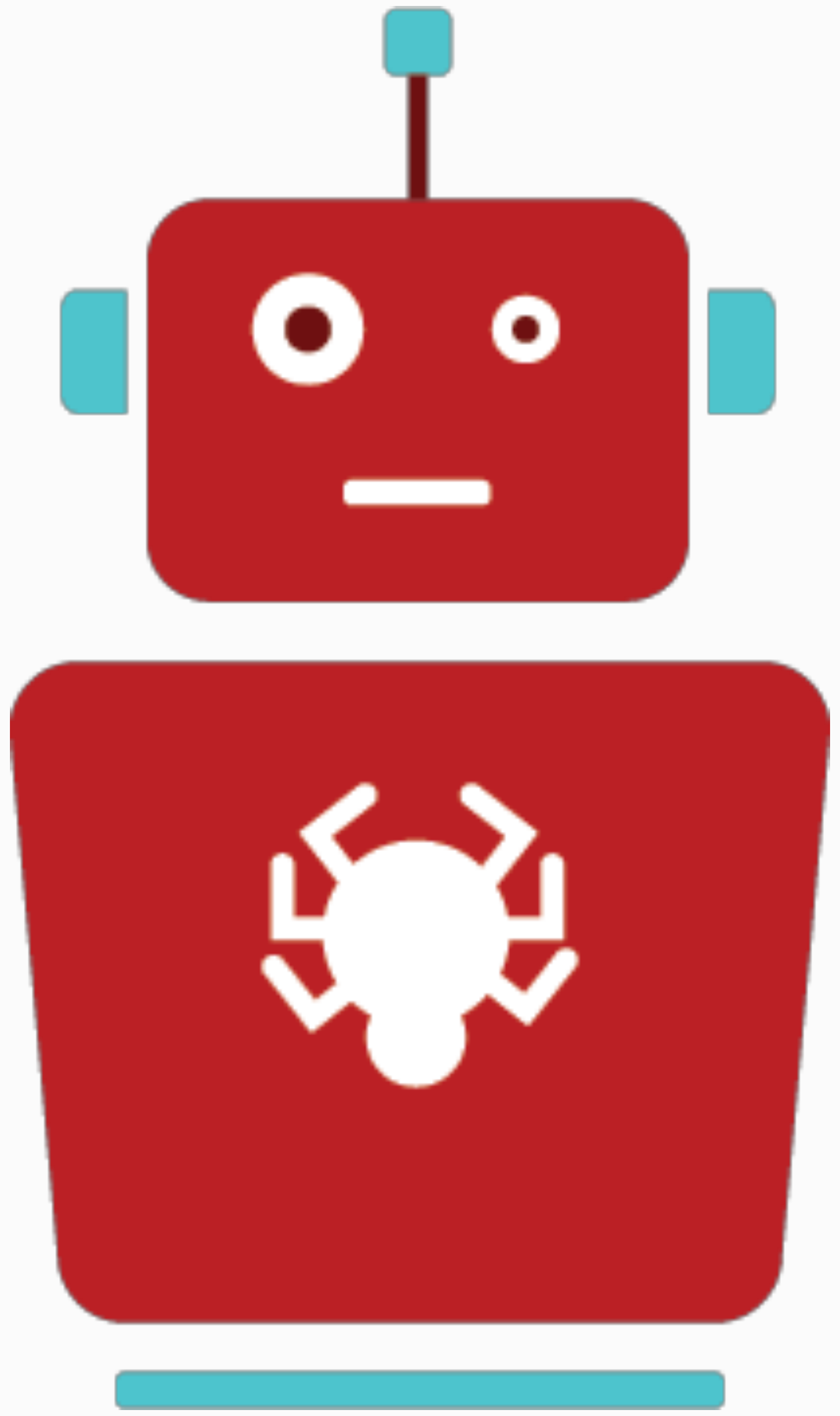
Automate everything that Chrome can * |

* No programming skills required. Create script in visual constructor.

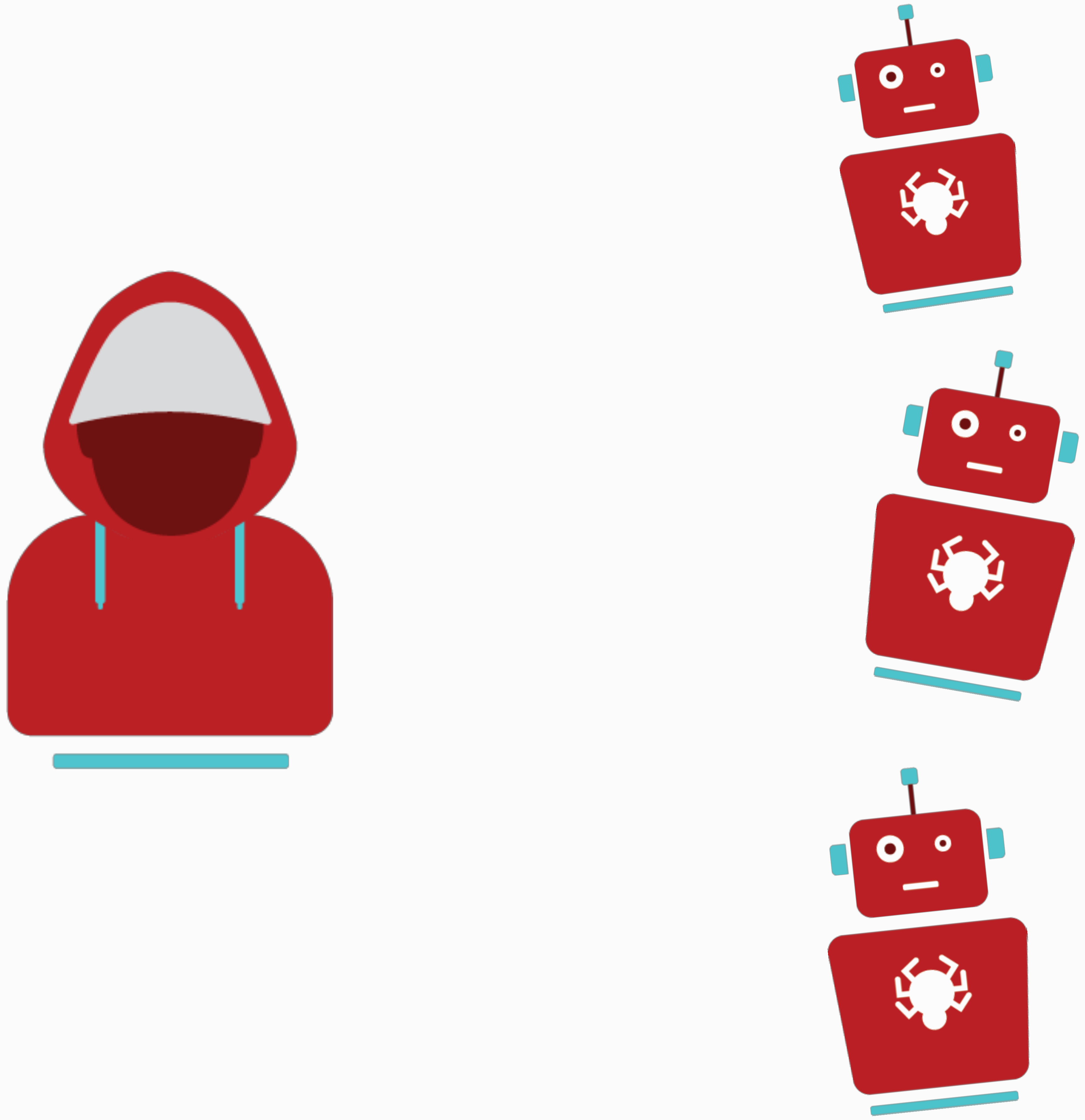
Agenda

1. Cost vs value in security
2. Attack in detail
3. **How to affect cost**
4. Real world example

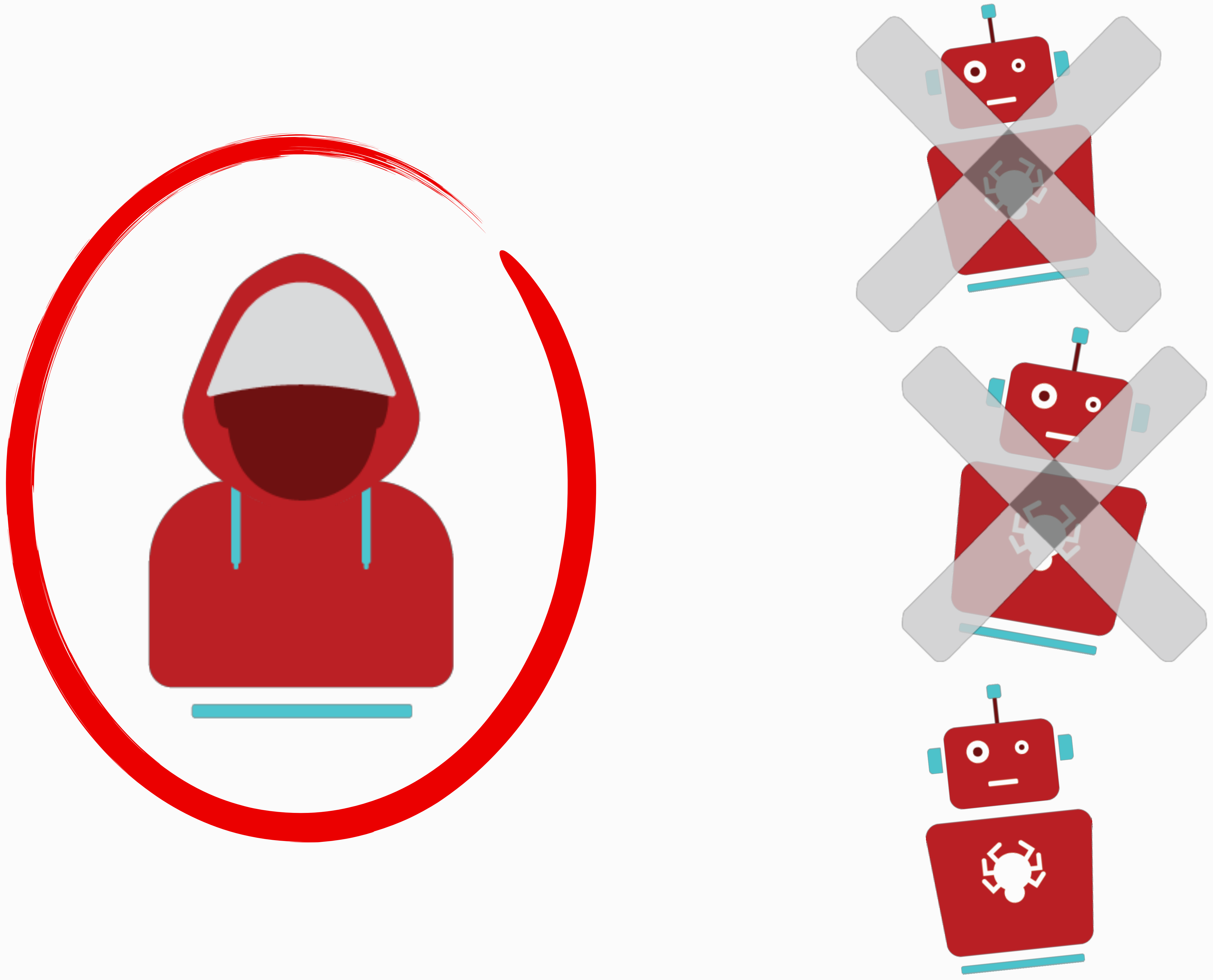
Millions of marketing dollars talk about bots and botnets…

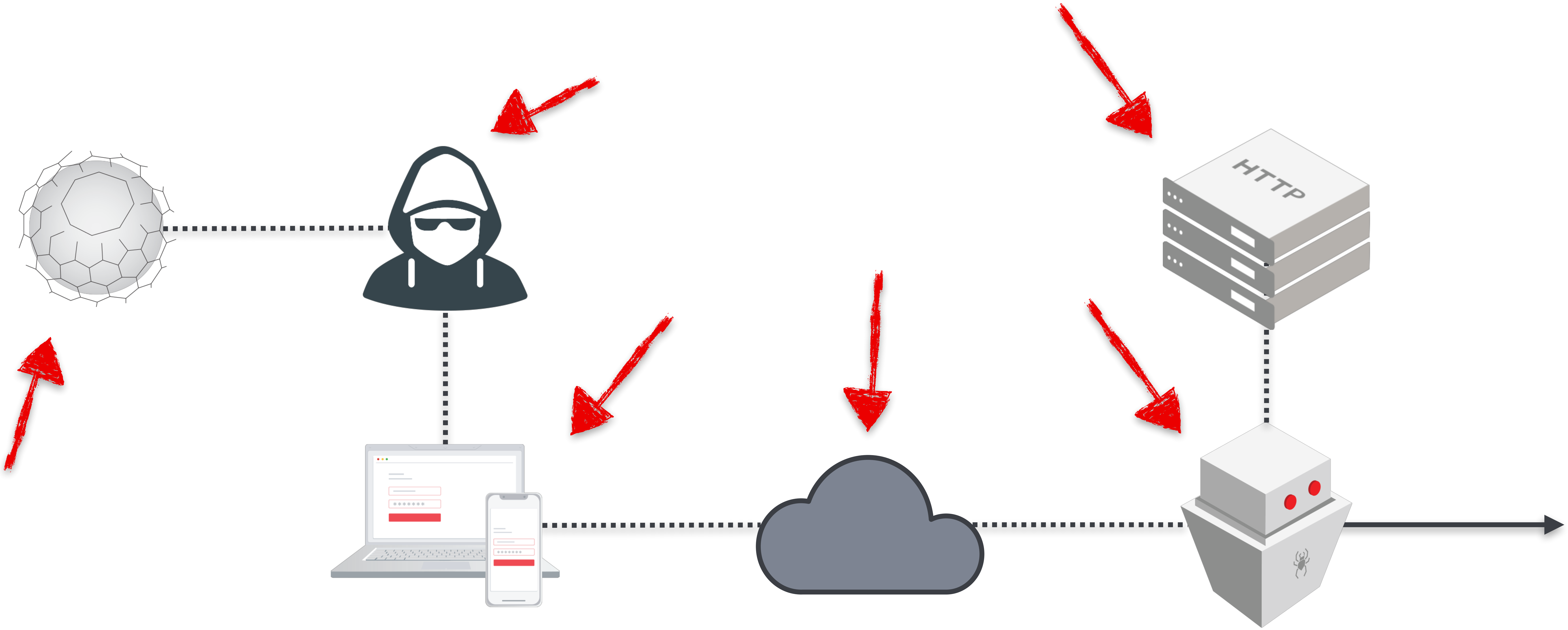


These are just symptoms, not the cause.



Treating the symptom won't fix the problem





It’s not as simple as blocking an IP or a script or a bot or any symptom.

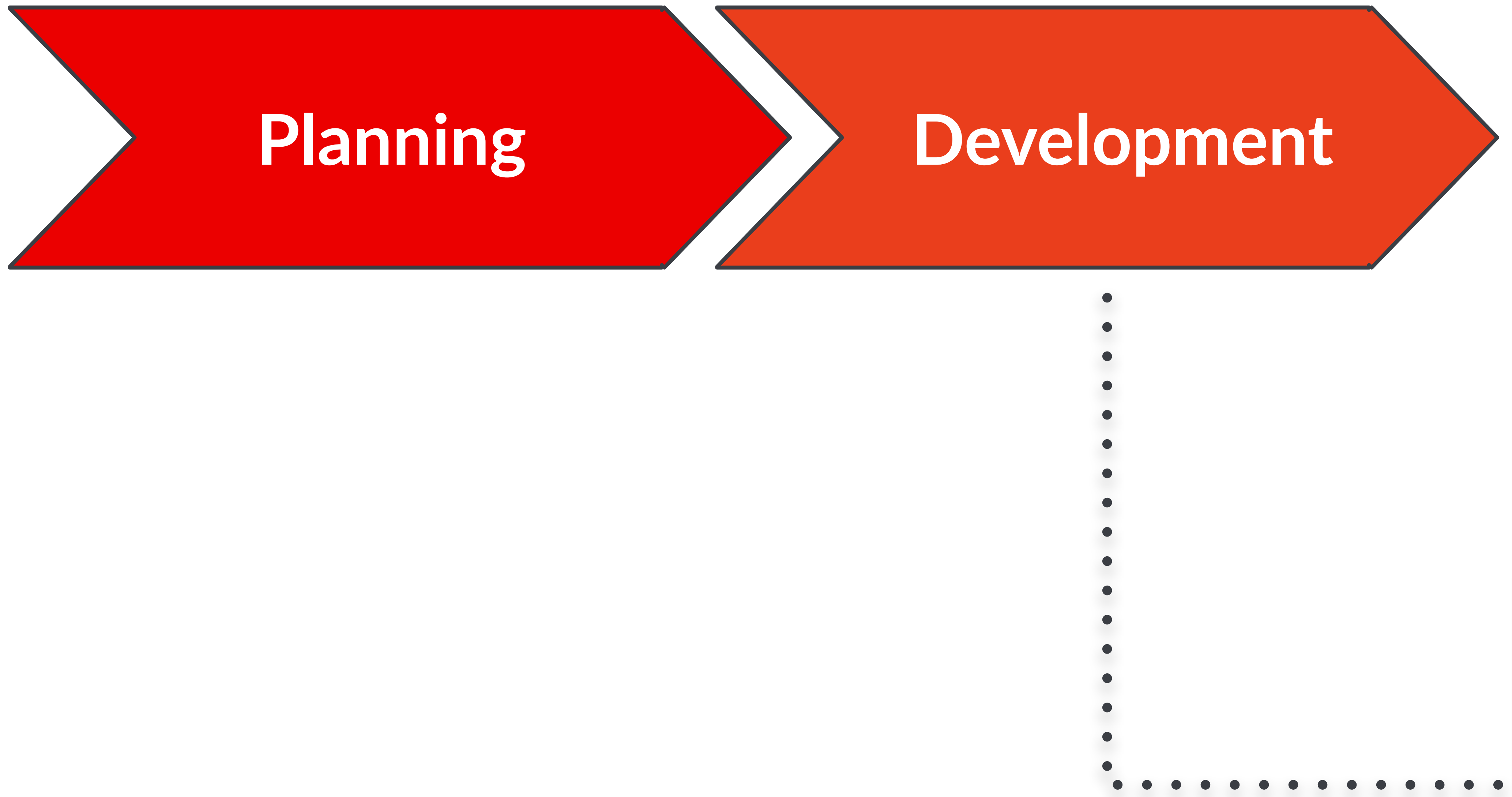
It’s targeting what will cost the attacker the most. Over and over again.

The Software Development Lifecycle

Planning

What tools work, what don’t?
What URLs need to be targeted?
What data do I need?

The Software Development Lifecycle

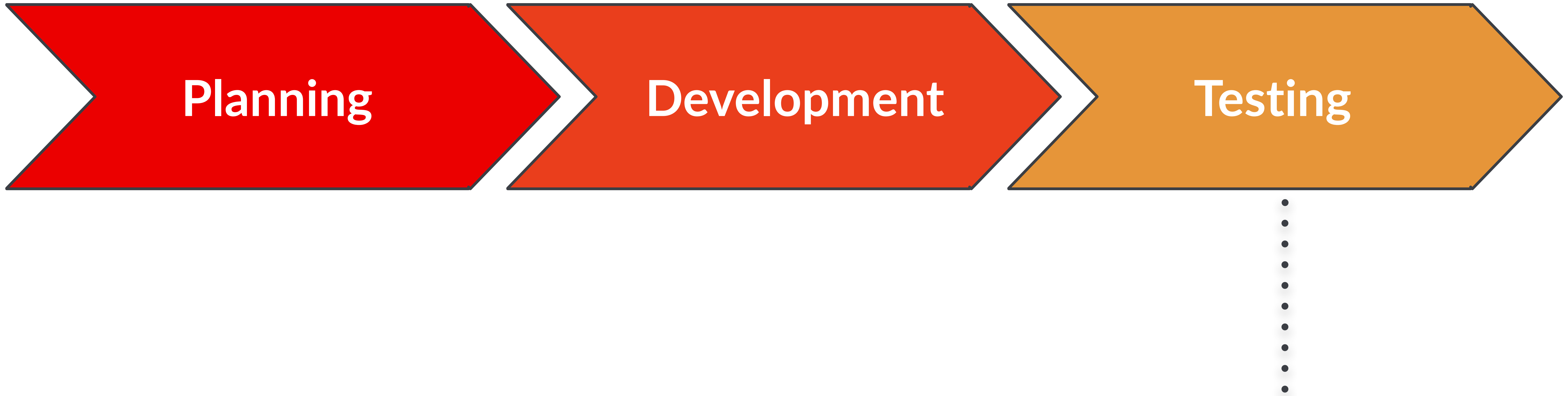


Planning

Development

Investment in a framework of choice.
Custom development against a site.
Building in proxy/botnet hooks.

The Software Development Lifecycle



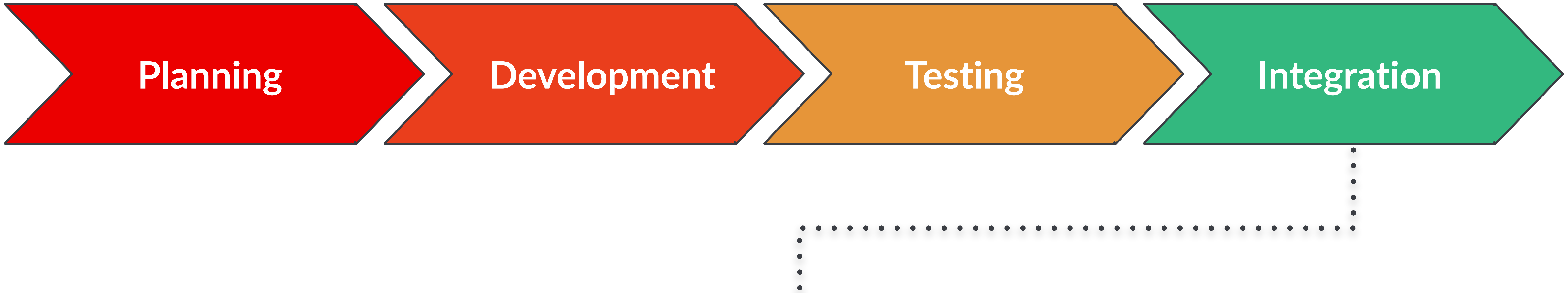
Planning

Development

Testing

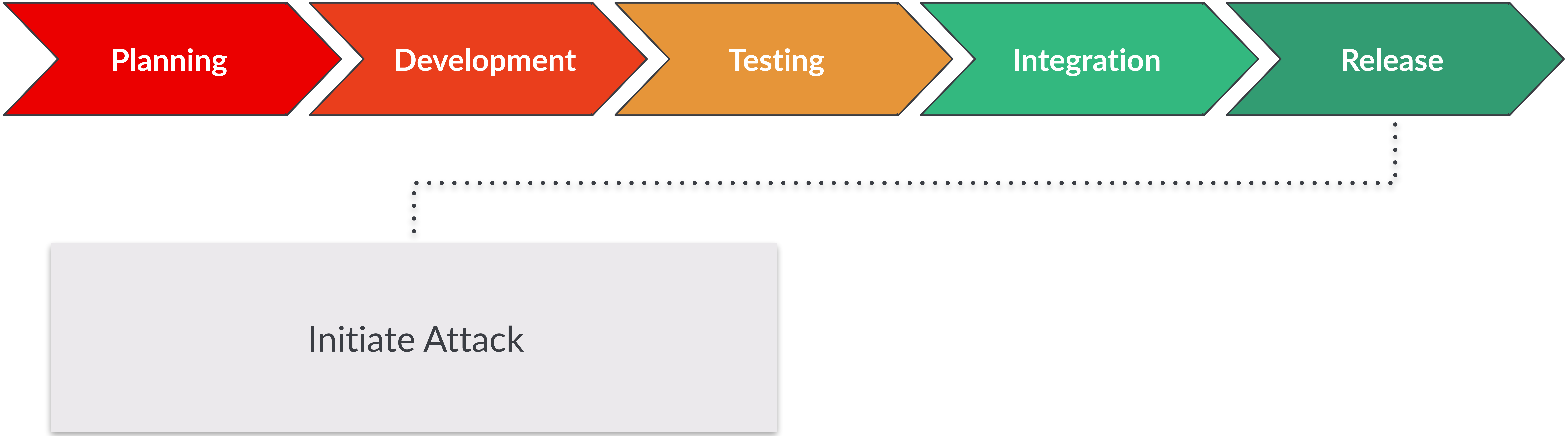
Does it bypass protections?
Does it handle edge case responses?
Does it consume input data properly?

The Software Development Lifecycle



Check integration with services/botnets.
Ensure health checks work.
Deploy to cloud services.

The Software Development Lifecycle



Planning

Development

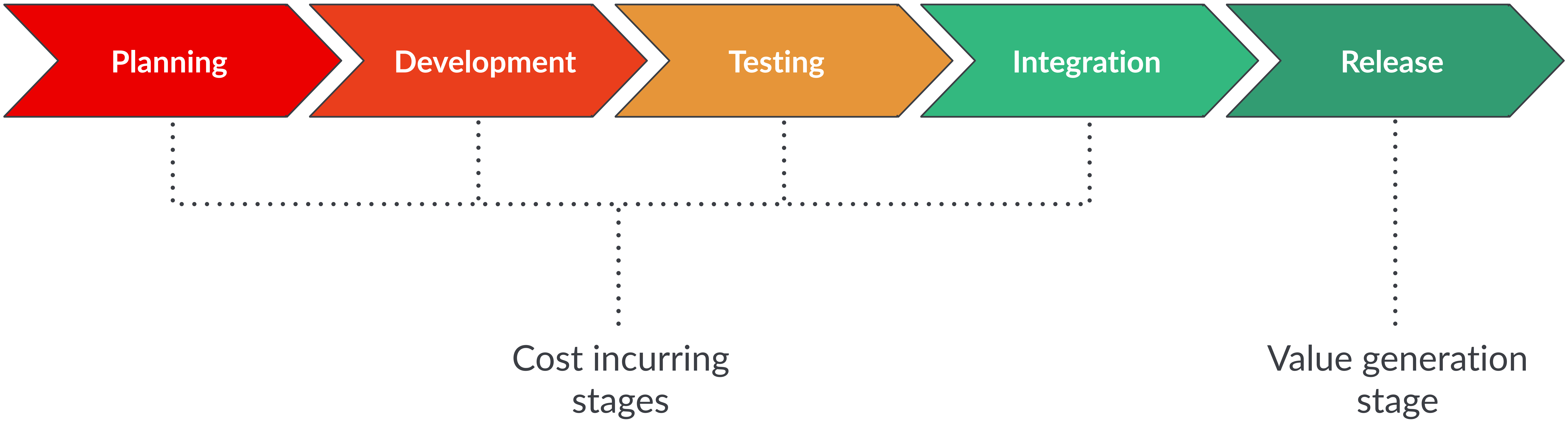
Testing

Integration

Release

Initiate Attack

The Software Development Lifecycle



Agenda

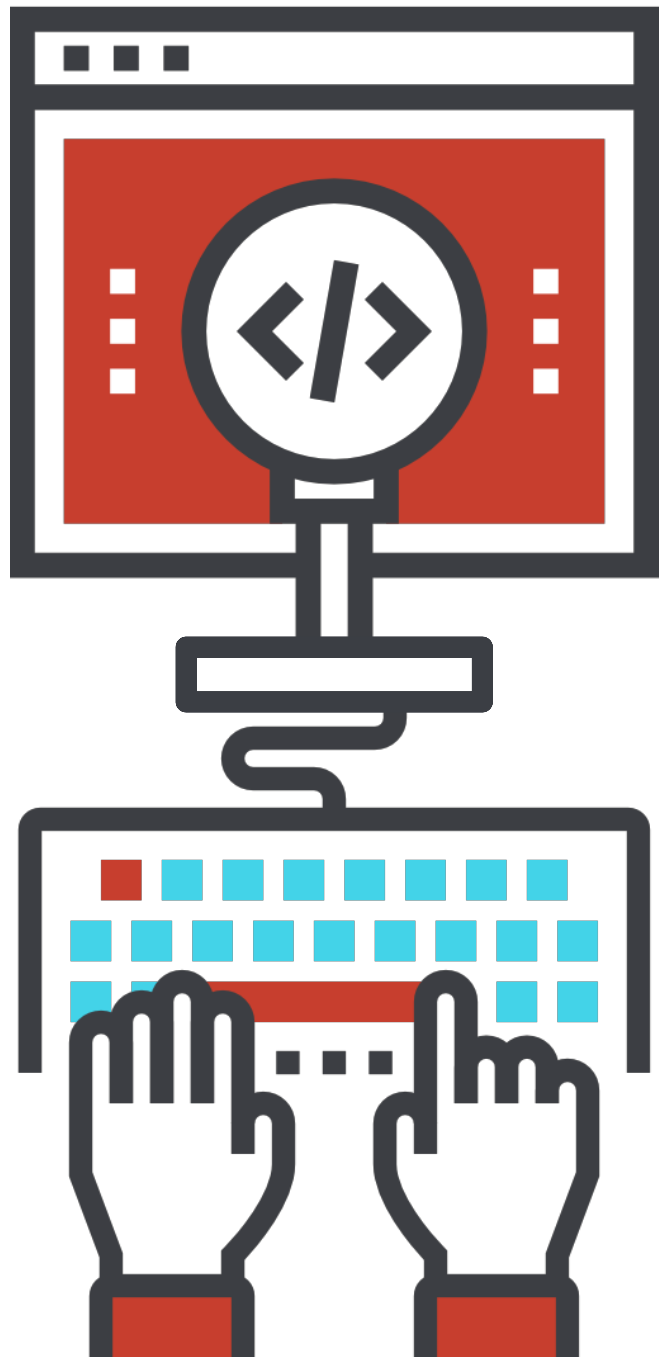
1 Cost vs value in security

2 Attack in detail

3 How to affect cost

4 **Real world example**

Case Study (circa 2015)



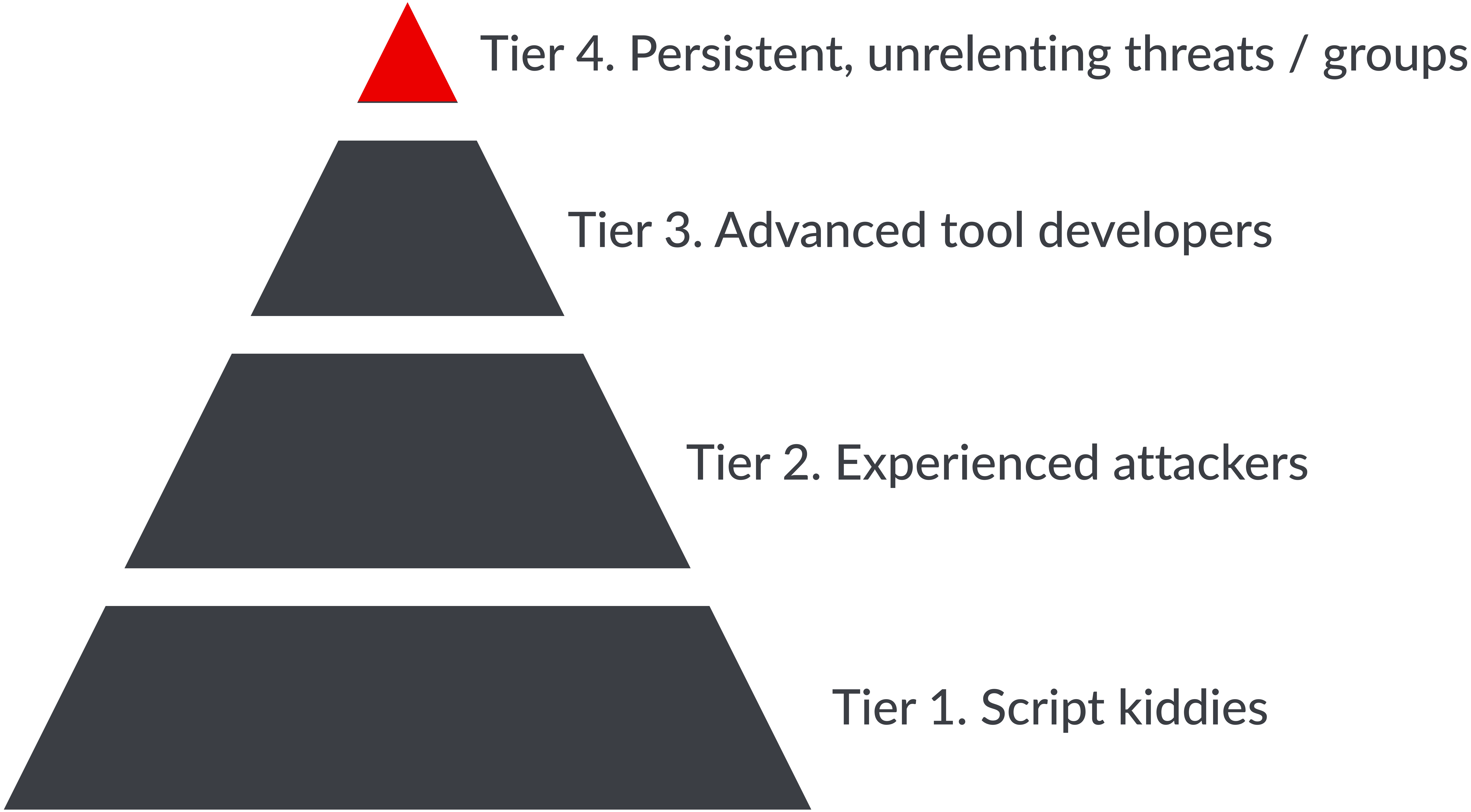
Github Kiddie

Scenario

Credential Stuffer
and Account taker-overer

VS

Big US Retailer



Tier 4. Persistent, unrelenting threats / groups

Tier 3. Advanced tool developers

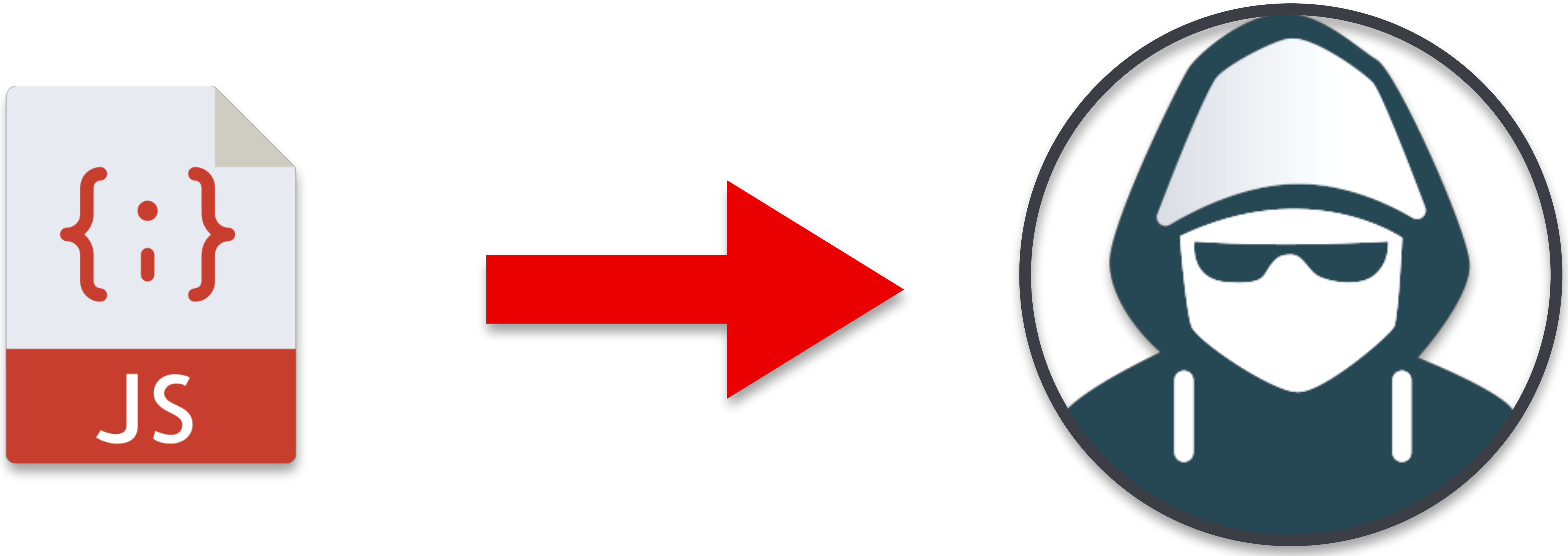
Tier 2. Experienced attackers

Tier 1. Script kiddies

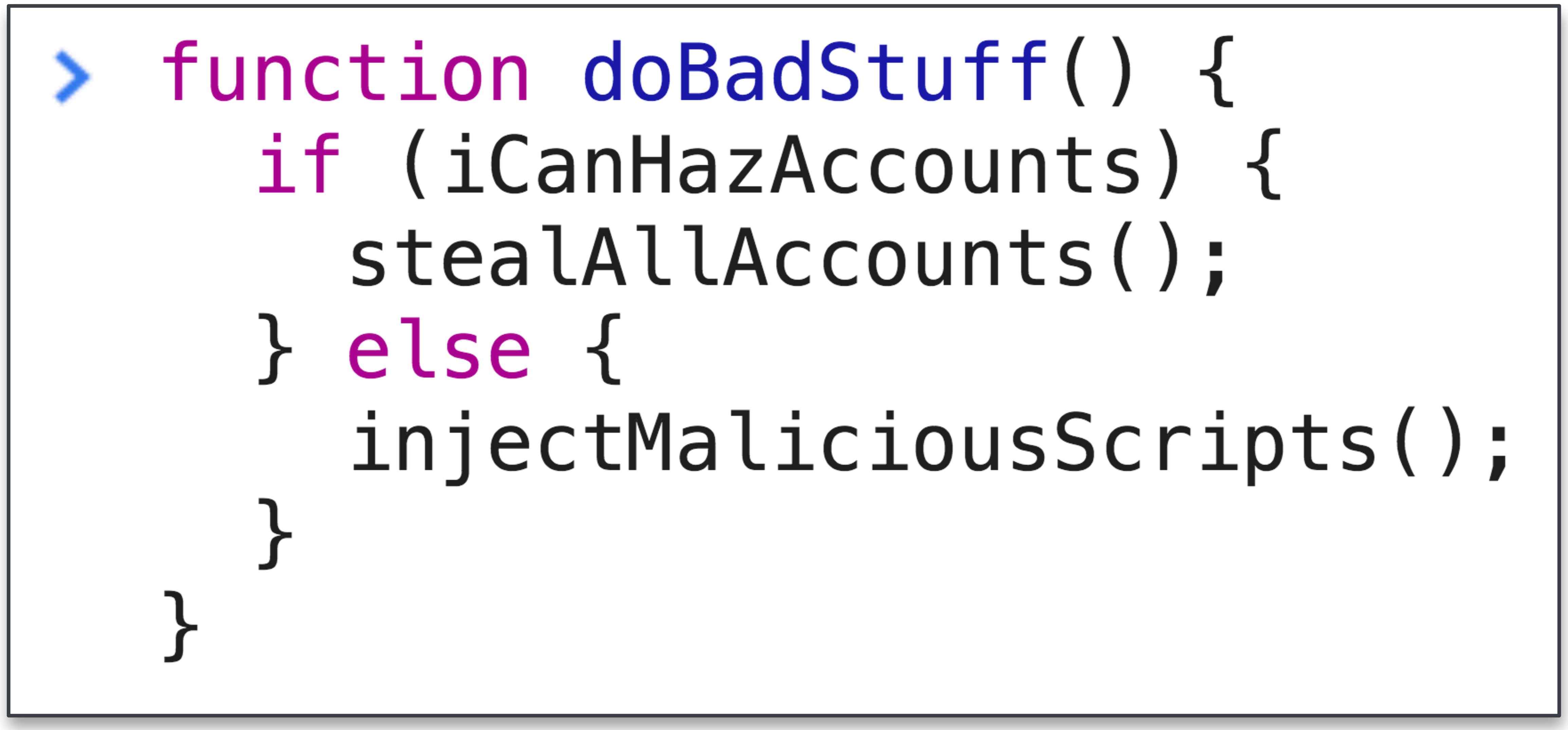
This attacker was a sophisticated, dedicated attacker.

They had been attacking and retooling for months on end, despite blocks.

We sent the attacker a targeted, custom payload.

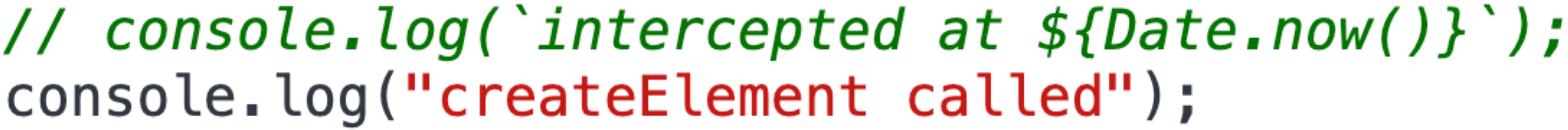


This allowed us to inspect the attacker's retooling effort in real time.



```
> function doBadStuff() {
    if (iCanHazAccounts) {
      stealAllAccounts();
    } else {
      injectMaliciousScripts();
    }
  }
```

We saw the code as it was changed. Comments, logs, typos and all.



```
// console.log(`intercepted at ${Date.now()}`);
console.log("createElement called");
```

The plan

1. Build up defenses based on the tool being used.
2. Provide variable feedback during retooling phase.
3. Turn on just enough to be infuriating. No more, no less.
4. Generalize the work so it can be repeated in the future.

How much does it cost to attack you?

Address weak spots

Audit your versions, your dependencies, your network exposure. Remove all low-hanging fruit.

Hack yourself

Repeat

Address weak spots

Hack yourself

Understand how easy it is to attack your own properties. Operate and prioritize off of evidence not gut feeling.

Repeat

Address weak spots

Hack yourself

Repeat

The landscape evolves constantly. This needs to be a function that is prioritized quarterly at least.

Thank You!

Jarrod Overson - @jsoverson