Imitation Attacks

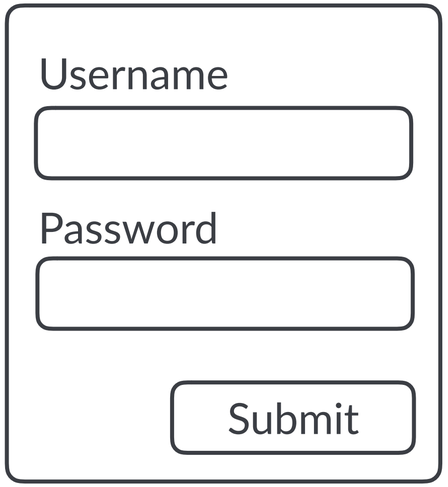
How account takeovers are evolving.

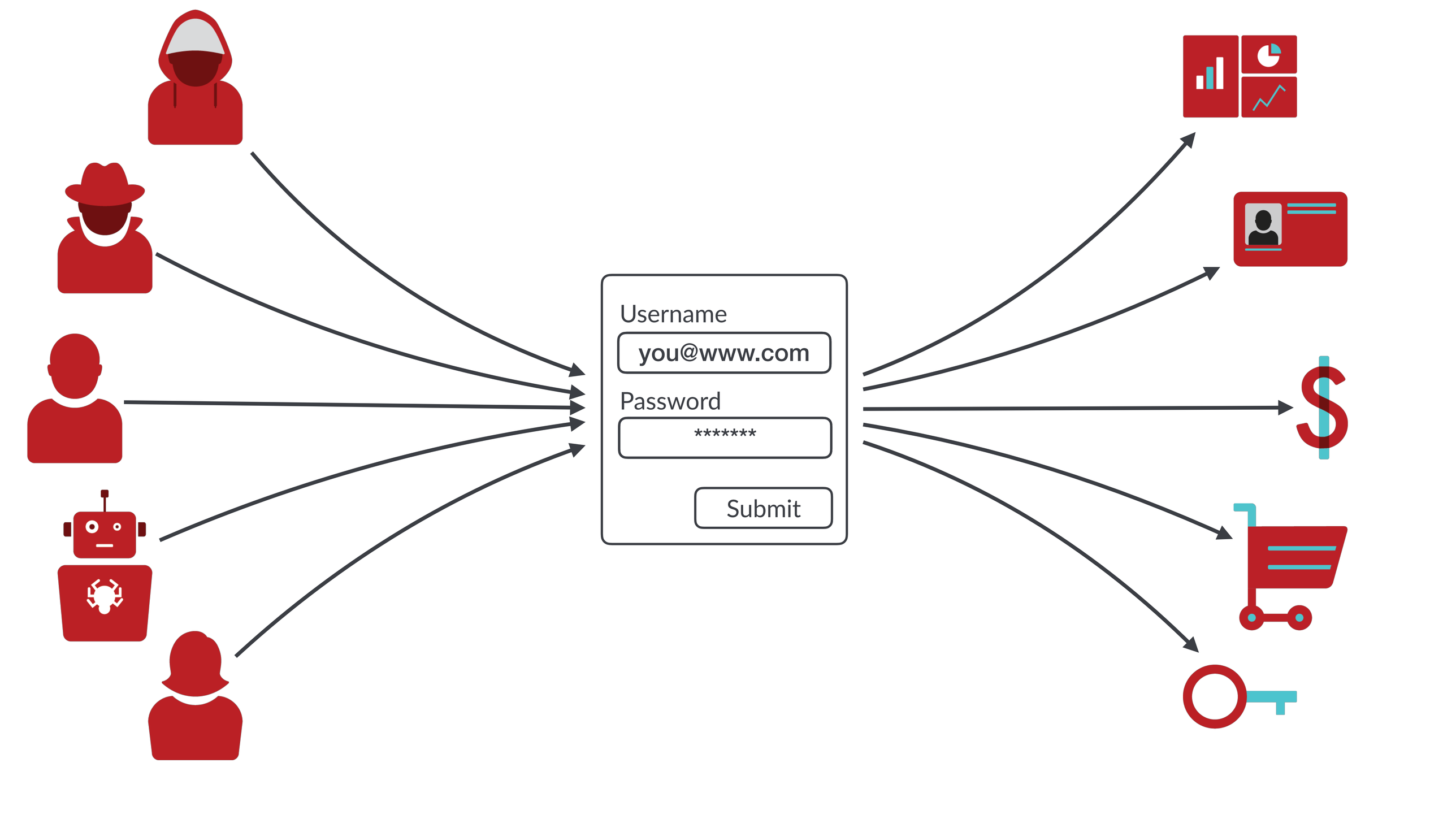
Jarrod Overson, Director @ShapeSecurity

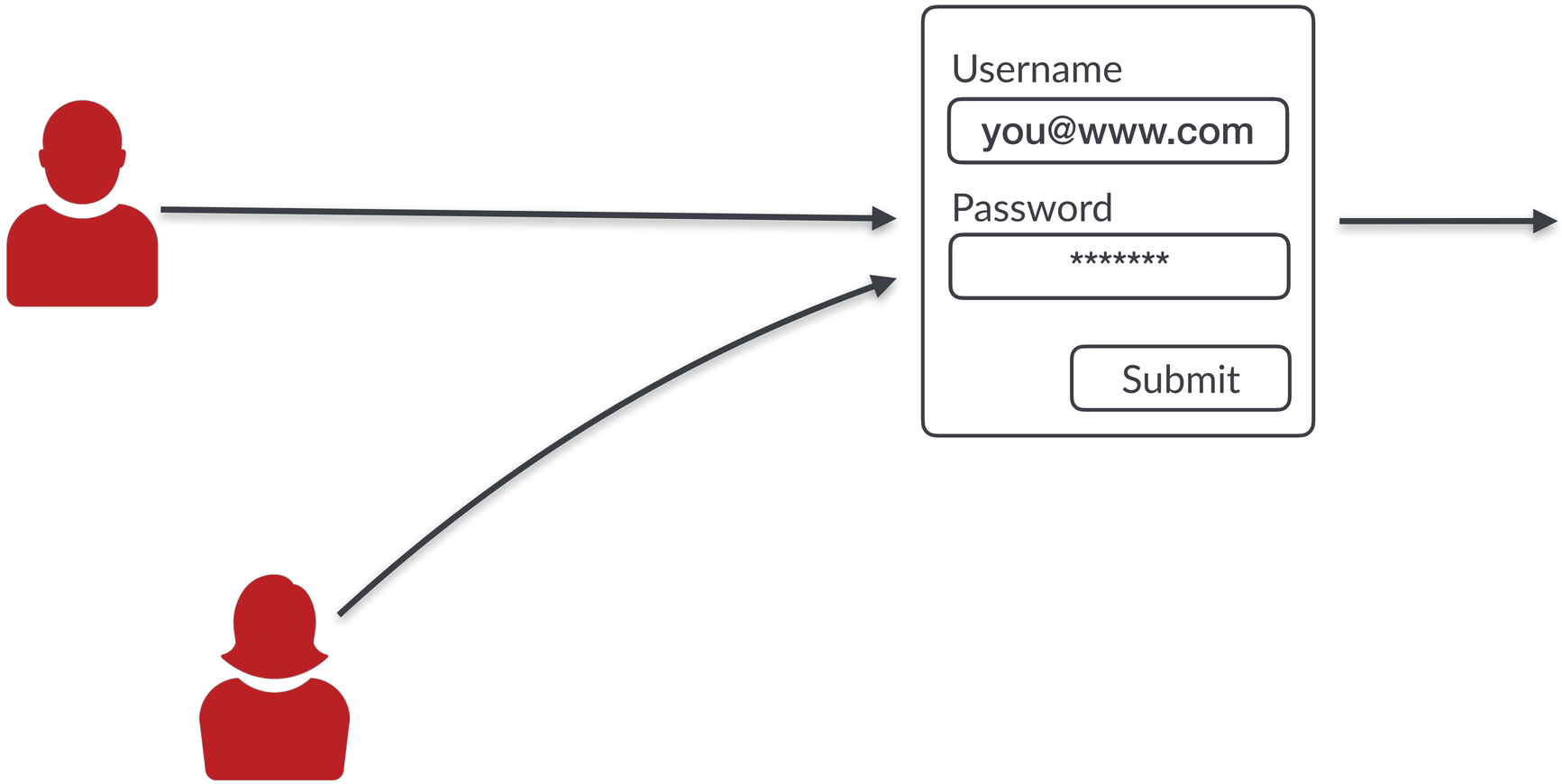
Two themes to keep in mind

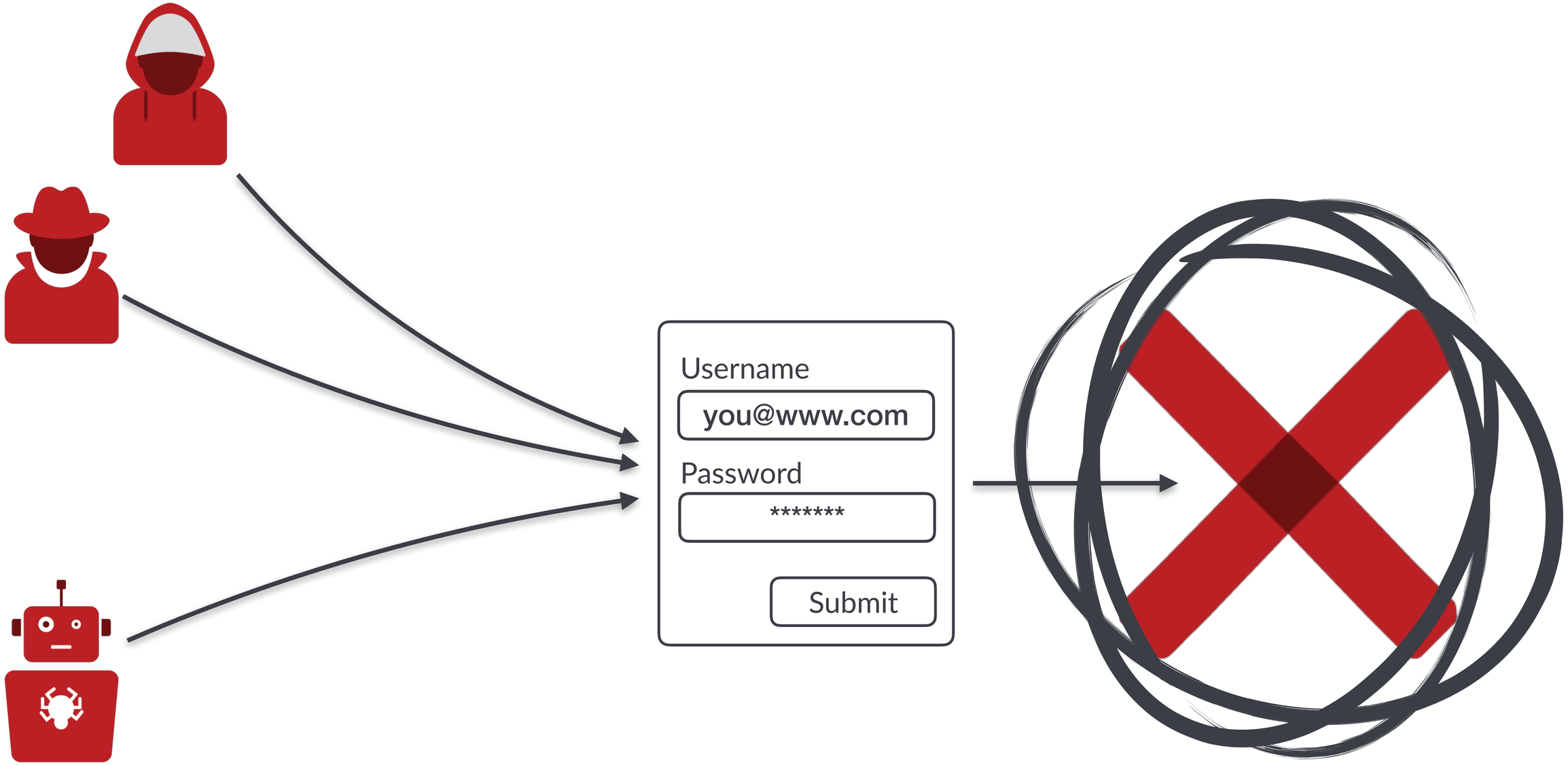
Imitation

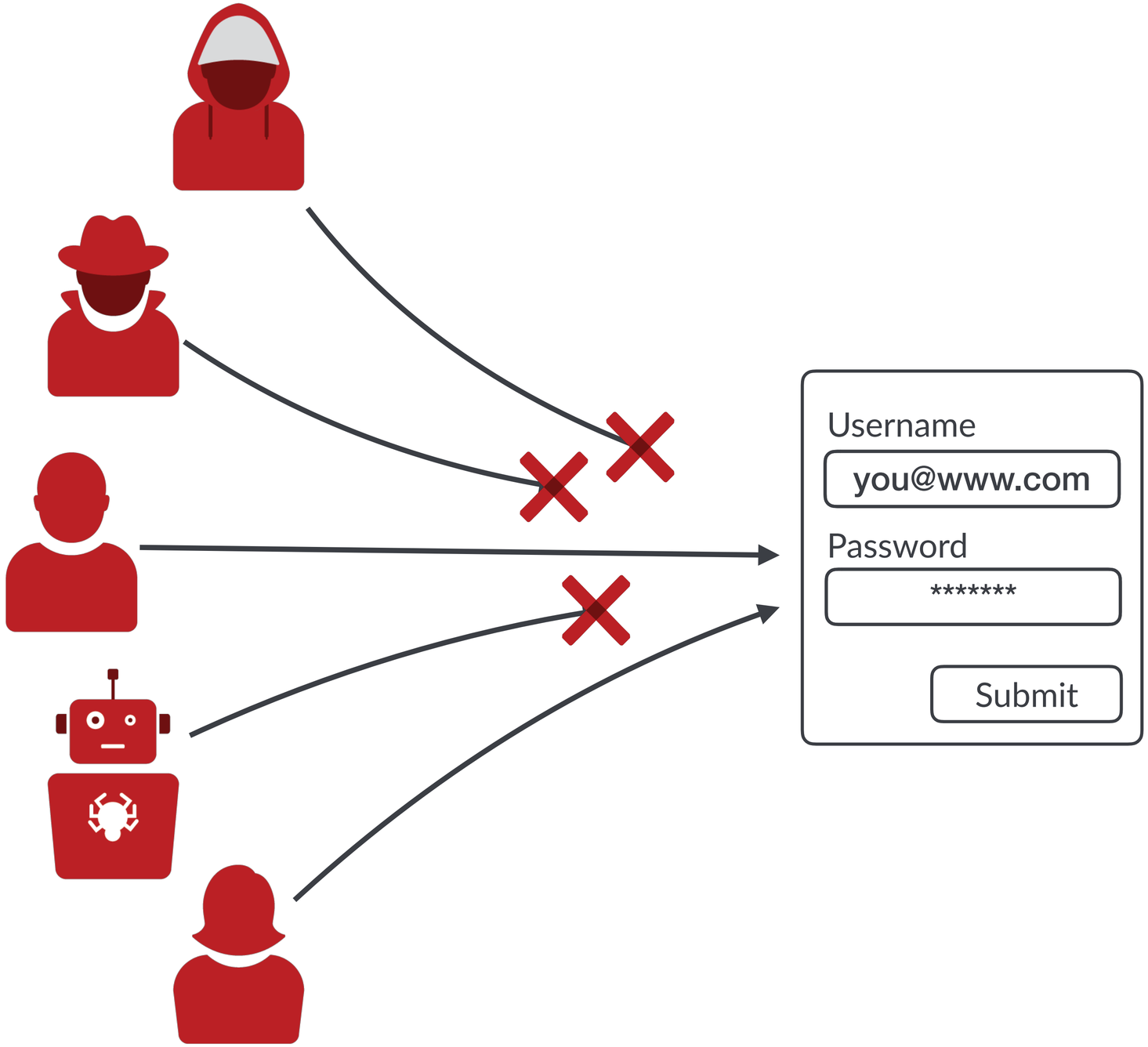
Cost vs Value

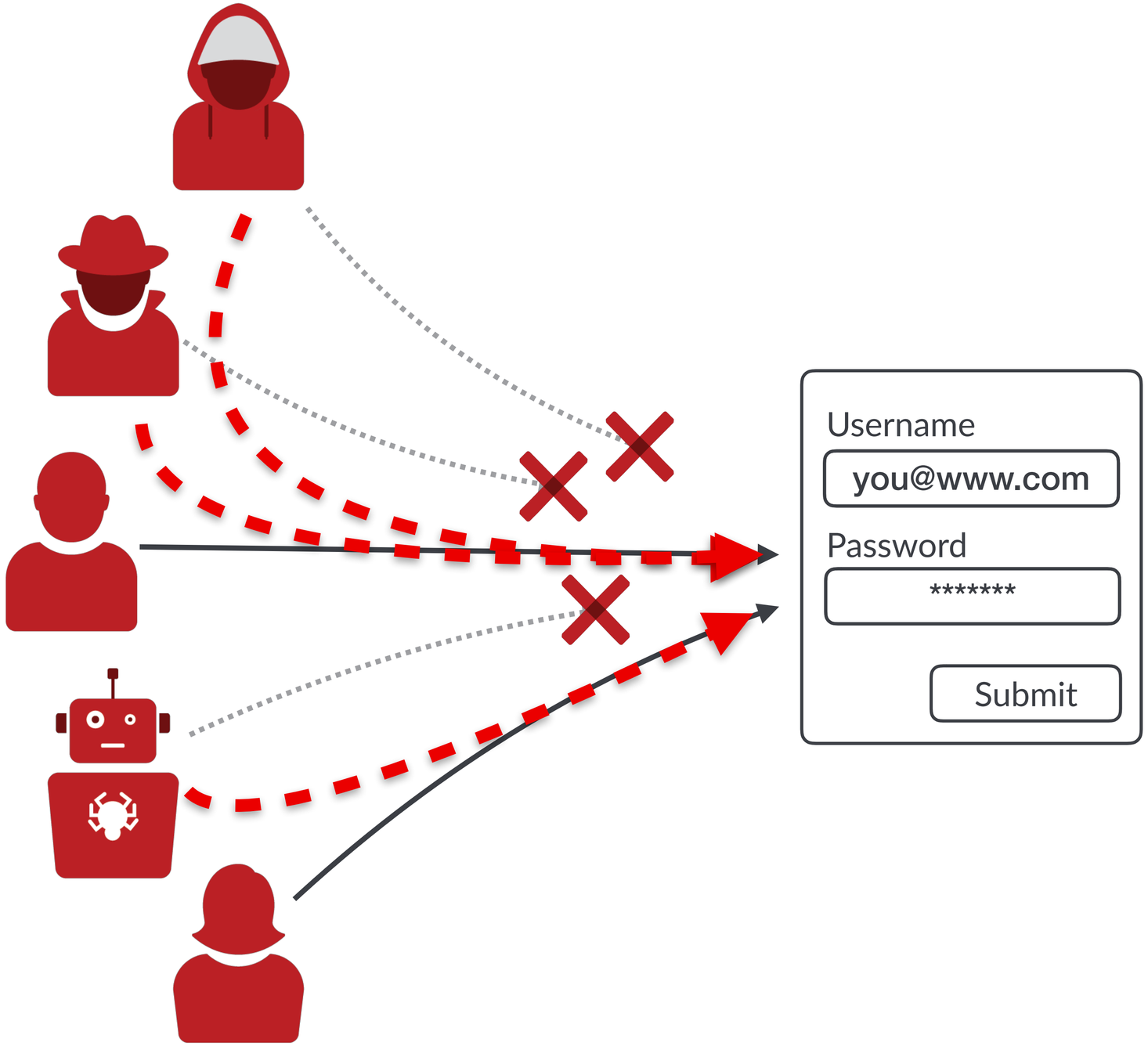

Username
Password
Submit


Username
you@www.com
Password
****
Submit


Username
you@www.com
Password
****
Submit


Username
you@www.com
Password
****
Submit

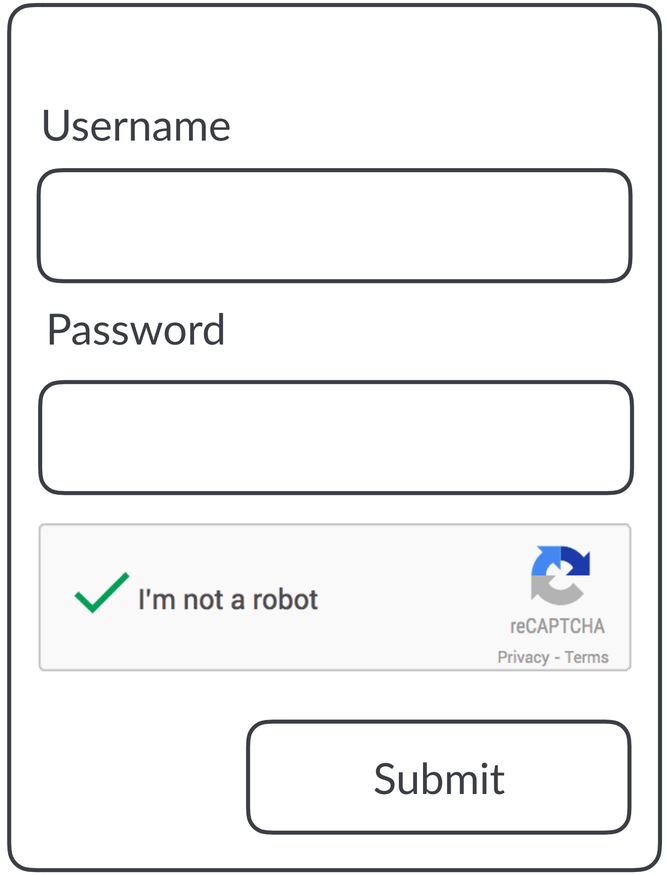

Username
you@www.com
Password
****
Submit

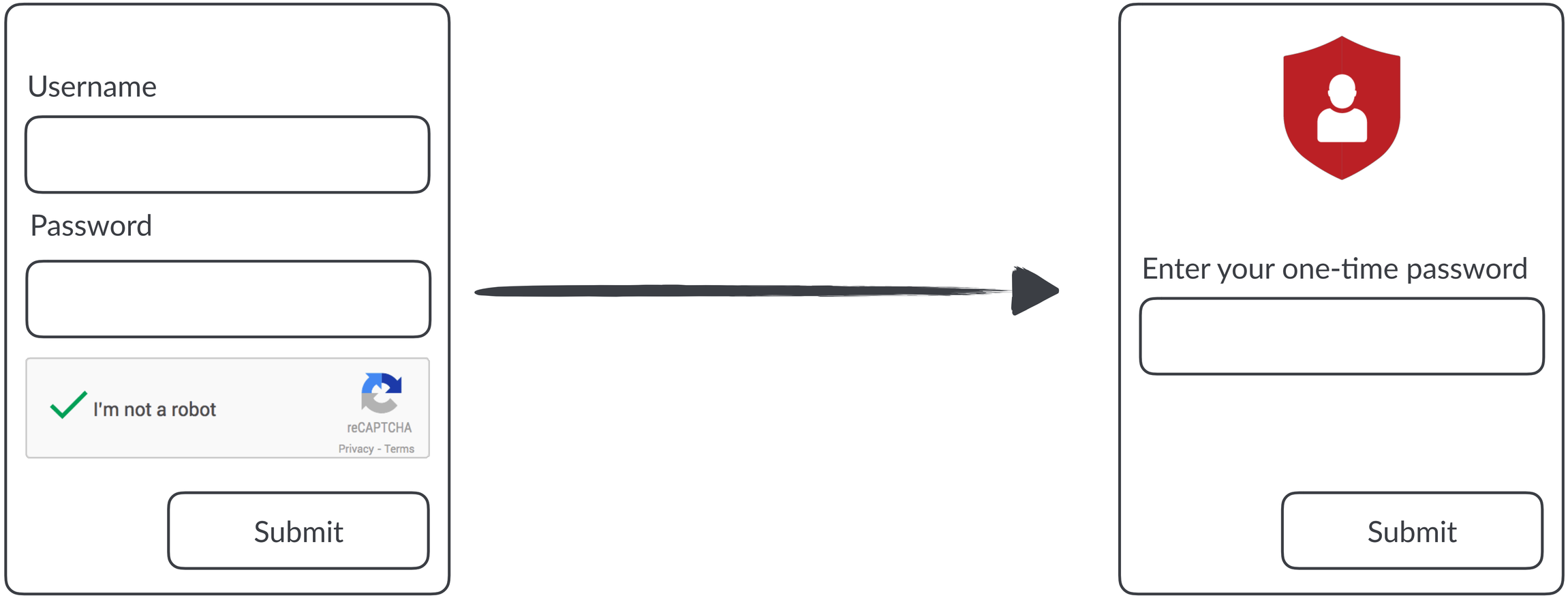


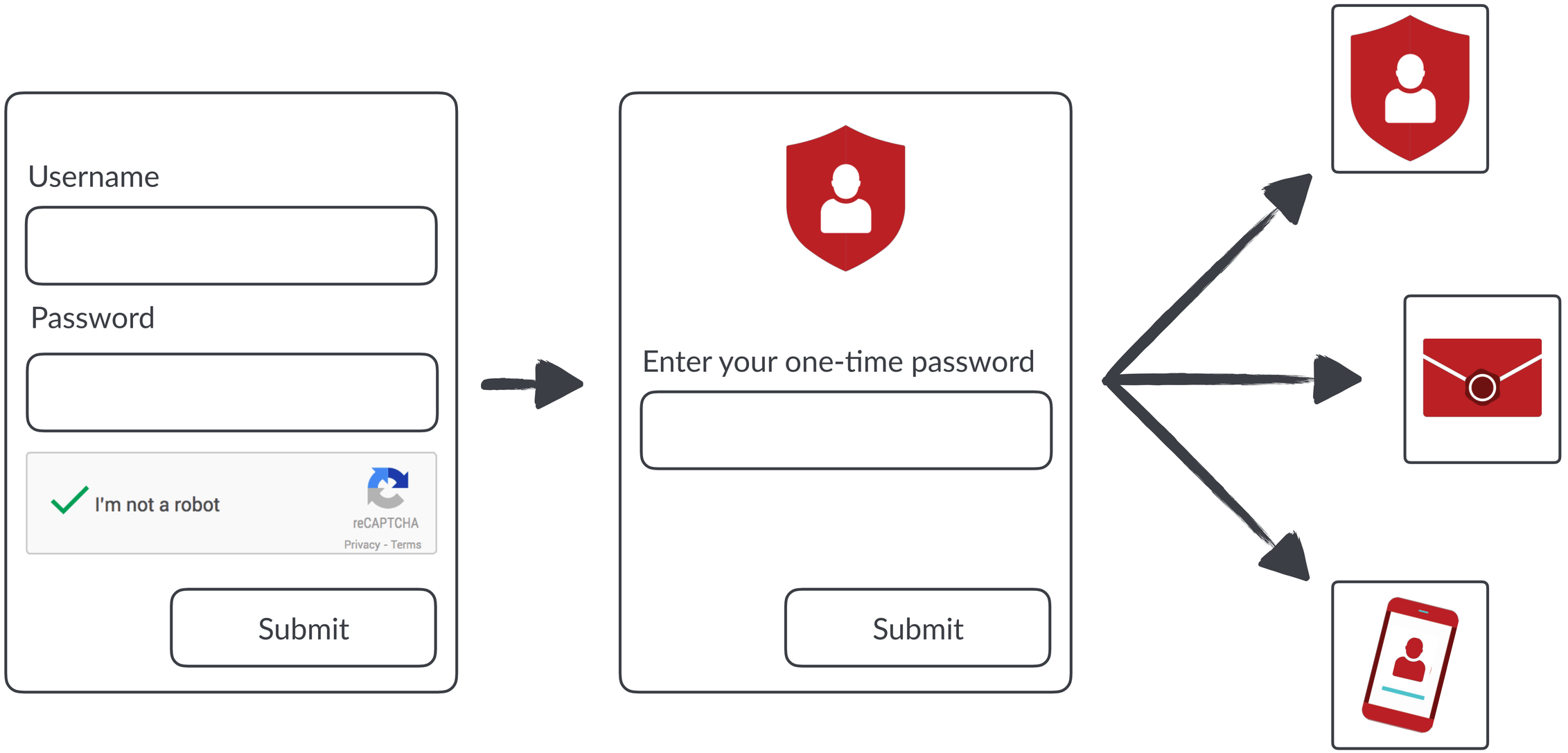
Imitation Attacks

Attacks through publicly accessible APIs or websites that can only be successful if they mimic legitimate user behavior.

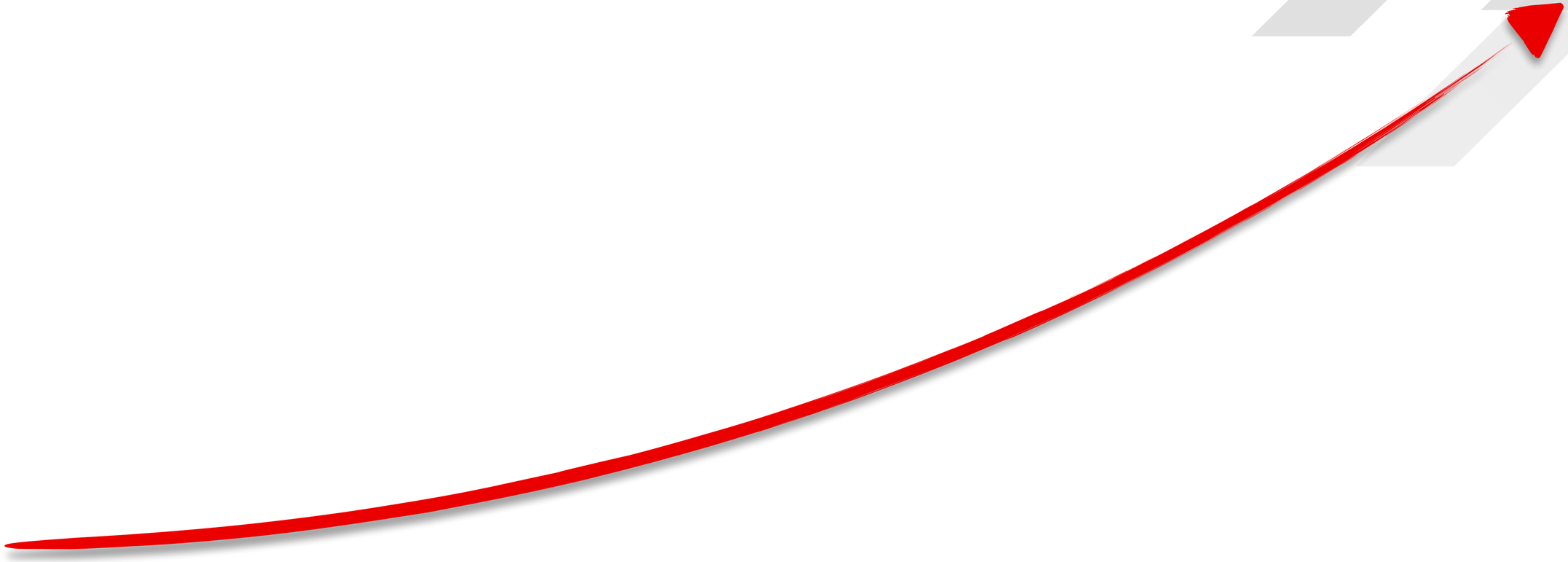
User behavior may mean demographics, traffic origin, User-Agent, mouse and keyboard input, challenge responses, sensor data, et al.


Username
Password
I'm not a robot
reCAPTCHA
Privacy - Terms
Submit


Username
Password
I'm not a robot
reCAPTCHA
Privacy - Terms
Submit
Enter your one-time password
Submit


Username
Password
I'm not a robot
reCAPTCHA
Privacy - Terms
Submit
Enter your one-time password
Submit

Even with all these defenses, attacks are increasing,



and they are only getting easier to perform.

IN THE **FIRST 6 WEEKS** OF 2019

IN THE **FIRST 6 WEEKS** OF 2019

2.3 BILLION

credentials were leaked to the open web.

Shape recorded its largest ever attack

2.93 BILLION TRANSACTIONS

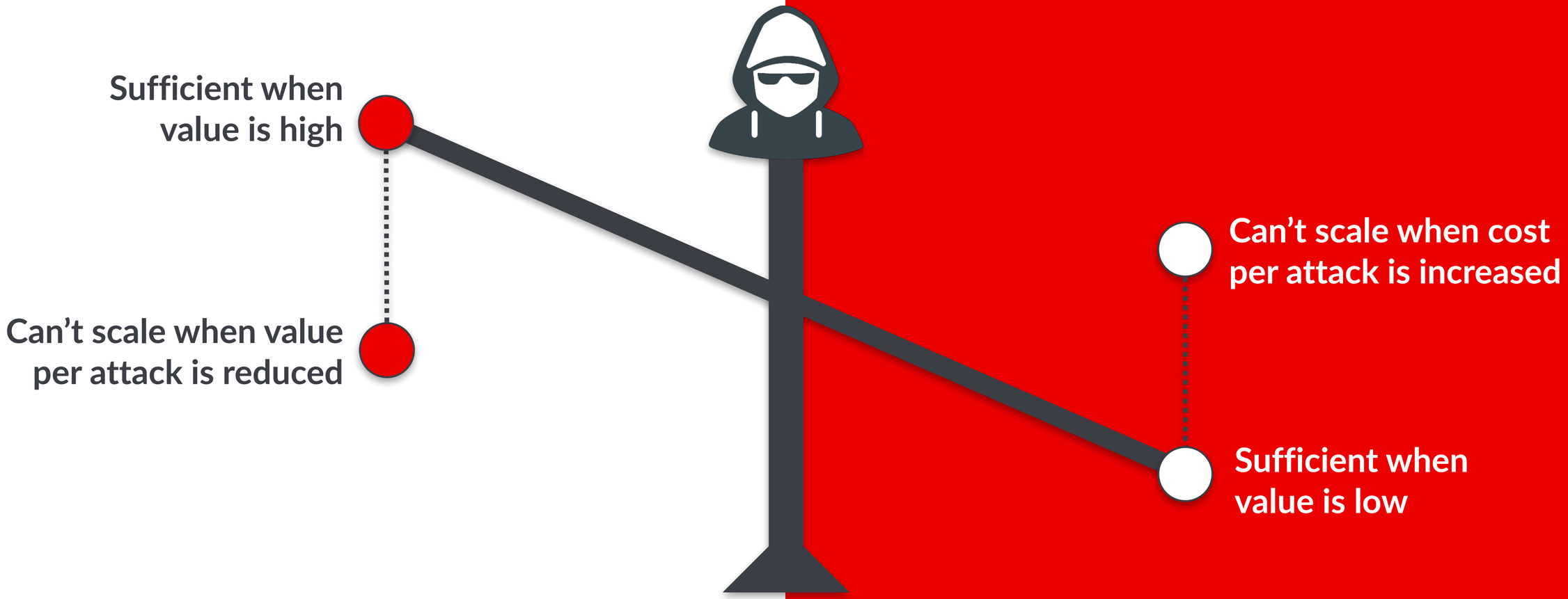
For **1 CUSTOMER** against **1 FLOW** in **1 WEEK**

Agenda

1. **Current attack landscape**
2. Attacks in detail
3. The arms race
4. How do we adapt?

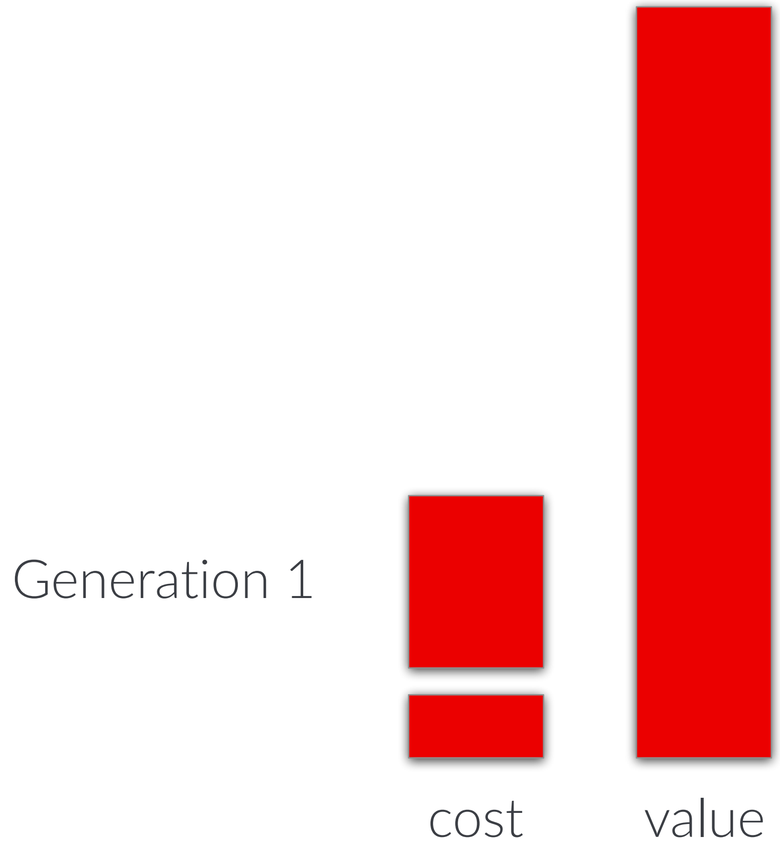
MANUAL ATTACKS

AUTOMATED ATTACKS

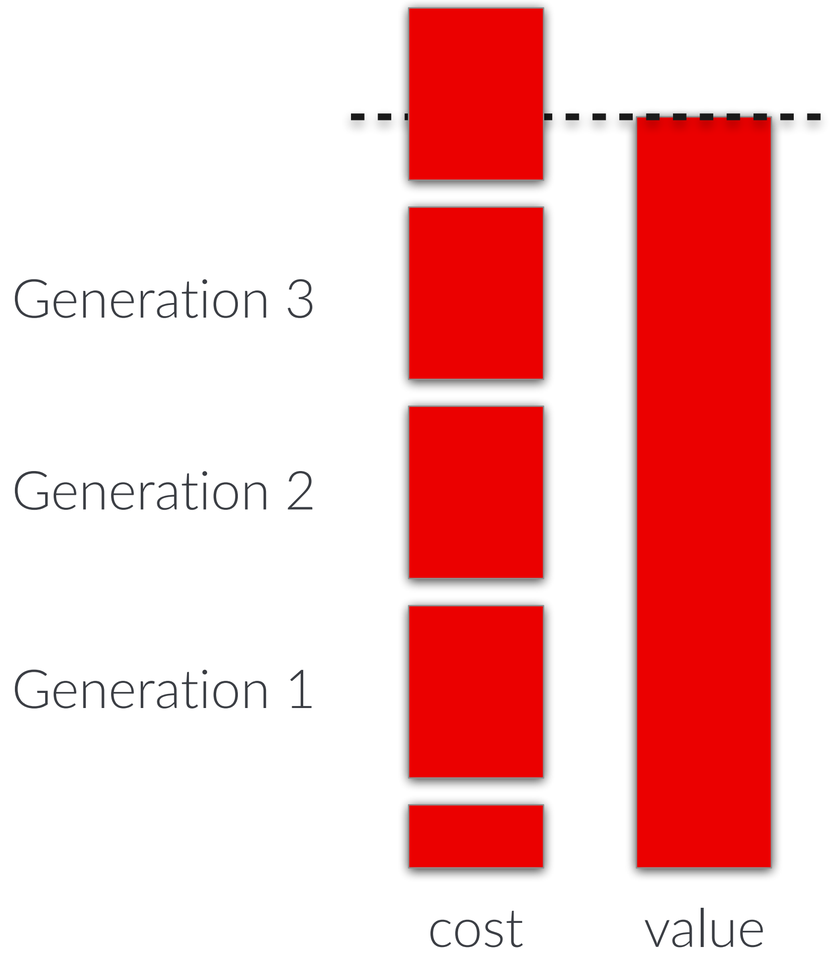


If there are no defenses in place, costs are negligible.

Any defense increases the cost by forcing a generational shift.



The sophistication increases until it is unsustainable.

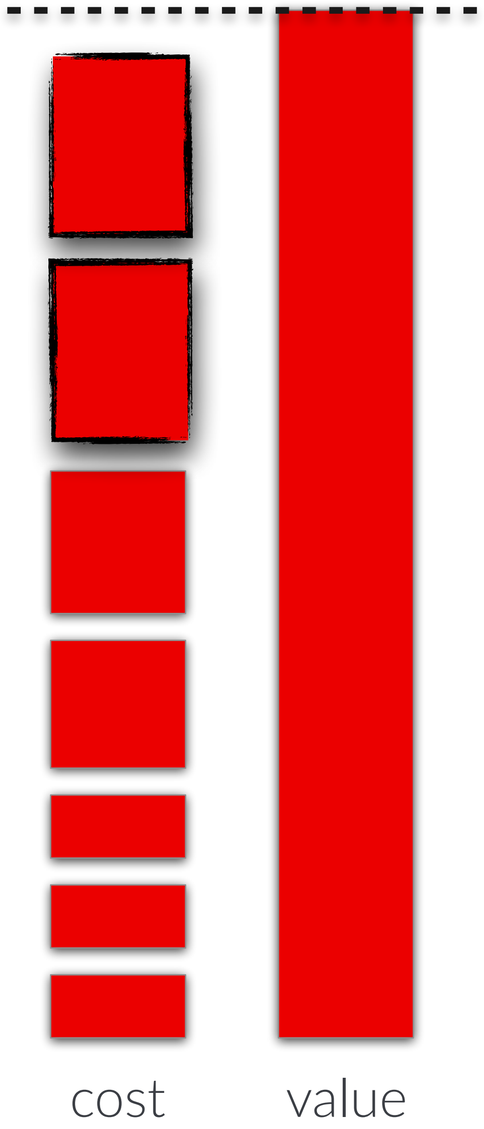


The cost of entry for each generation decreases over time.

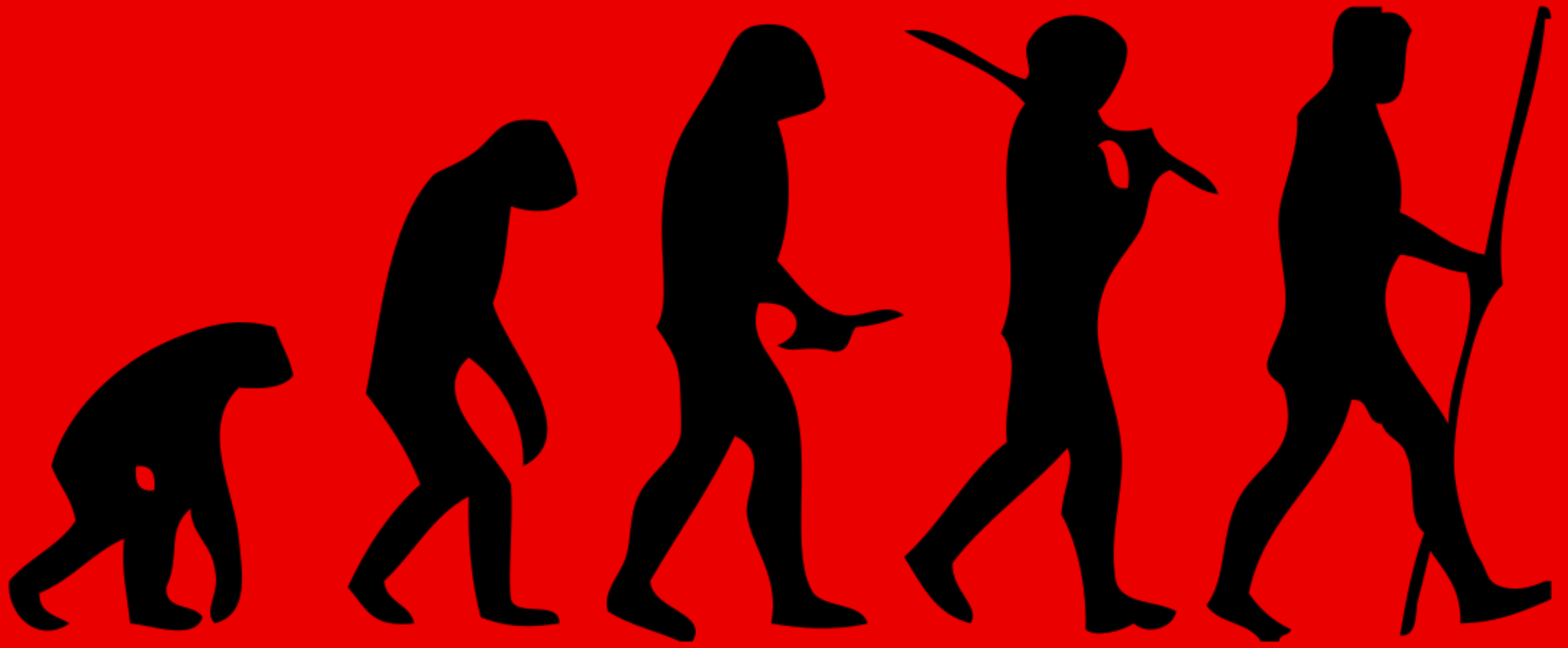
Not only that, the value of these accounts only goes up.

And every generation necessitates new defenses.

and sophistication is growing **rapidly**



THE EVOLUTION OF ATTACK TOOLS



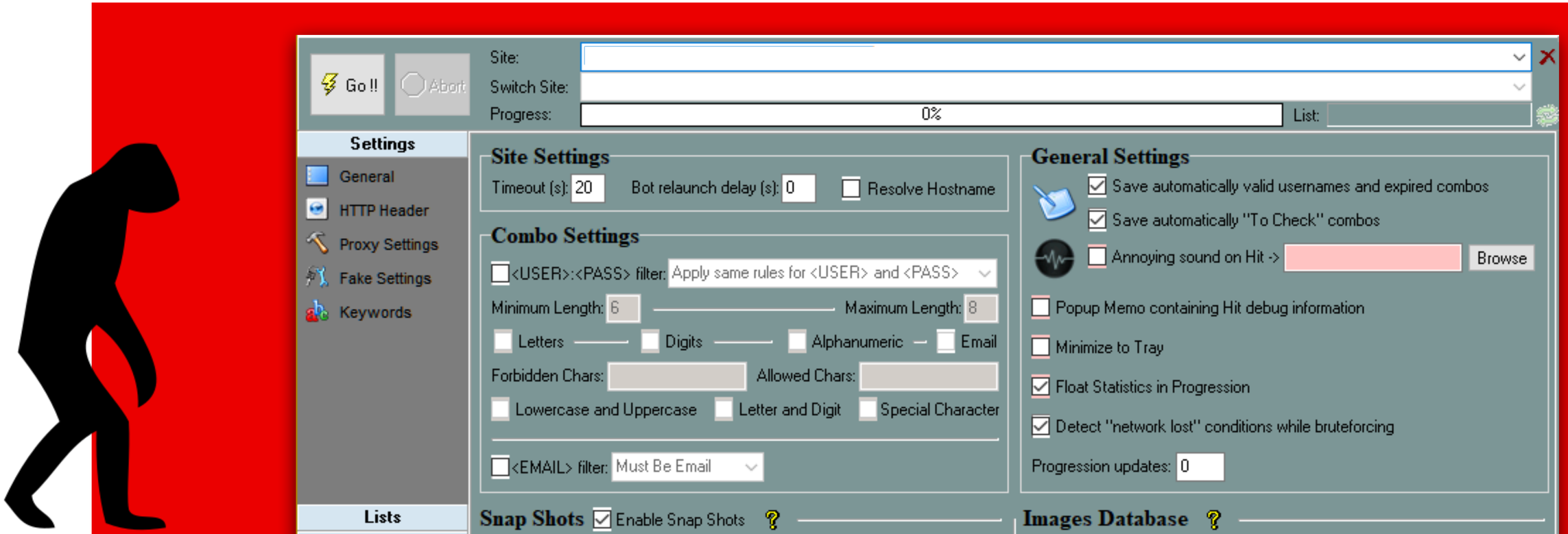
curl / wget

- Basic HTTP requests.
- Replaying tokens or reusing cookies.
- Changing form data for each transaction.

```
* About to connect() to google.com port 443 (#0)
*   Trying 172.217.10.14... connected
* successfully set certificate verify locations:
*   CAfile: none
  CApath: /etc/ssl/certs
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using ECDHE-ECDSA-AES128-SHA
* Server certificate:
*       subject: C=US; ST=California; L=Mountain View; O=Google Inc; CN=*.google.com
*       start date: 2017-05-16 14:17:12 GMT
*       expire date: 2017-08-08 13:41:00 GMT
*       subjectAltName: google.com matched
*       issuer: C=US; O=Google Inc; CN=Google Internet Authority G2
*       SSL certificate verify ok.
> GET / HTTP/1.1
```

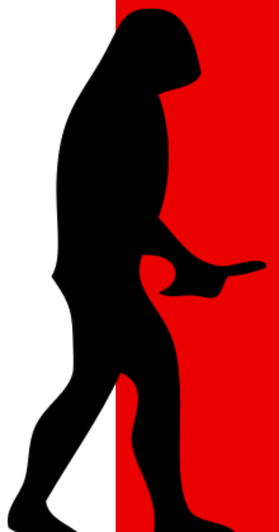
SentryMBA

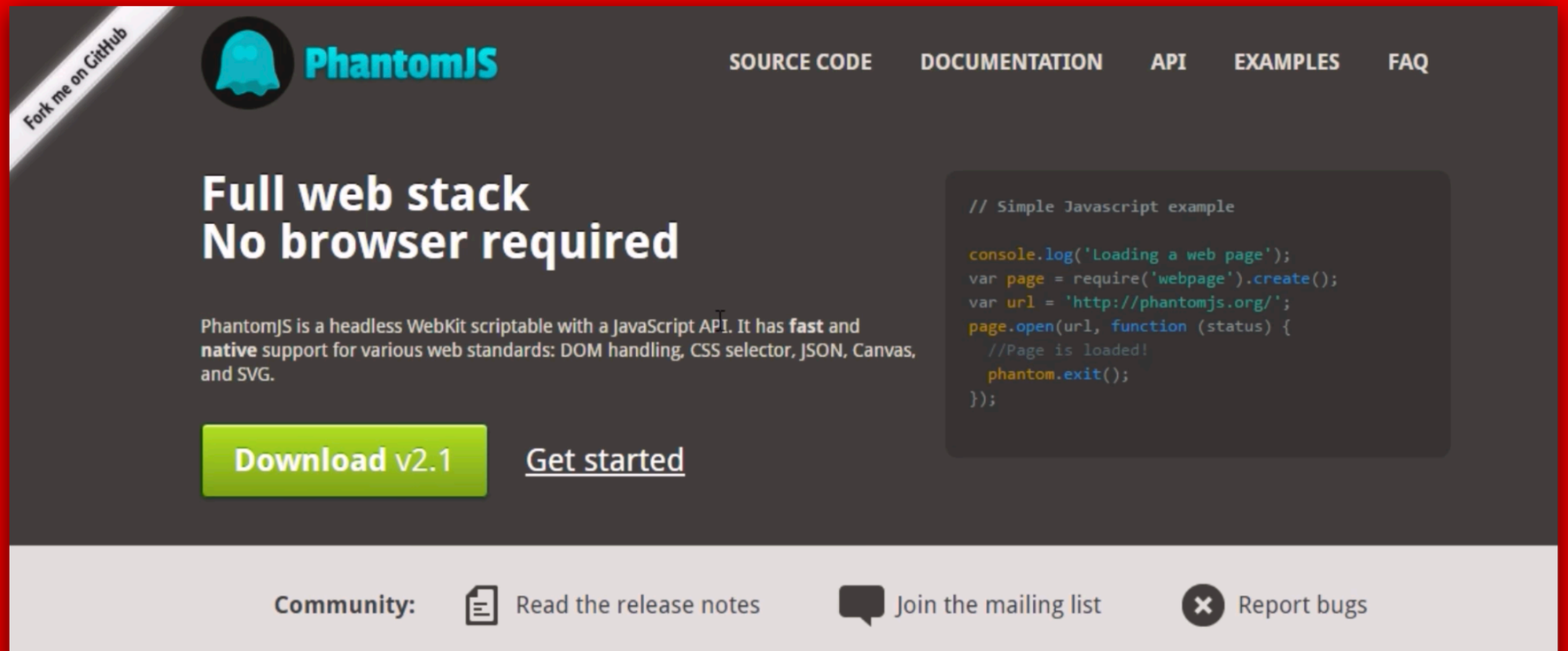
- Still Basic HTTP requests.
- Extensible and highly configurable.
- Tailored towards specific attack use cases.



PhantomJS

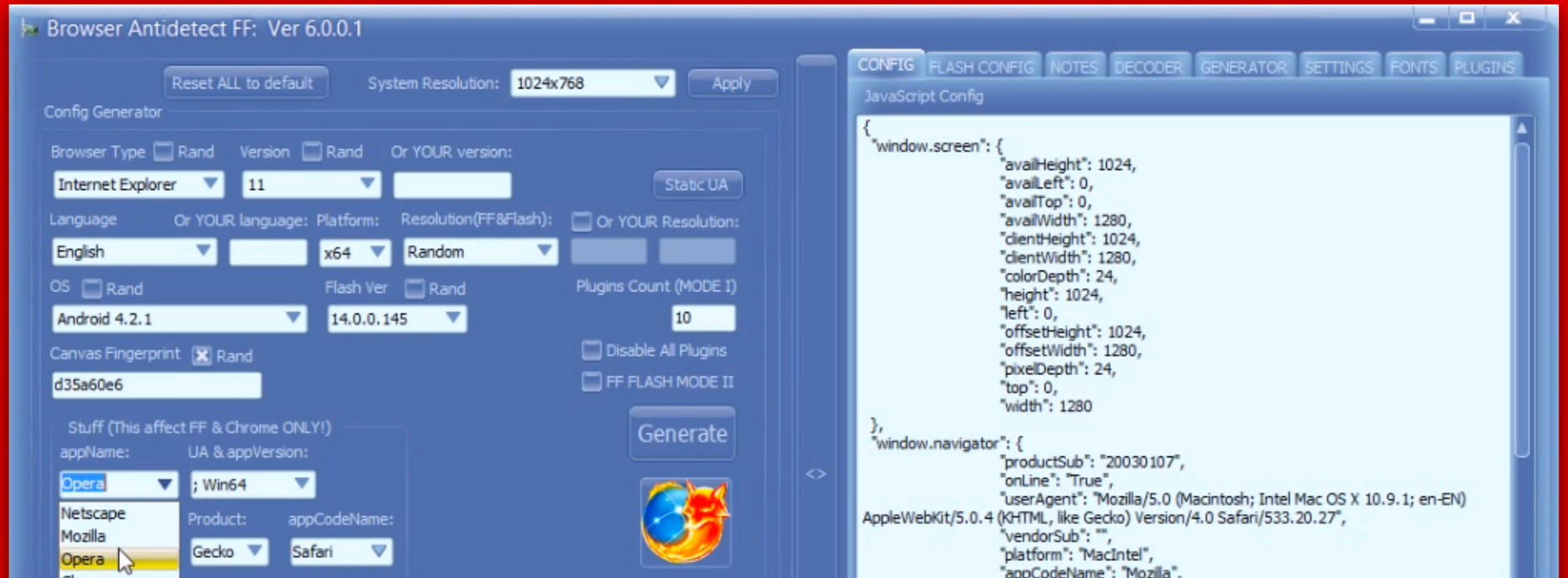
- Full browser environment for developers.
- Scriptable and headless.
- Bypasses trivial protection with no effort.





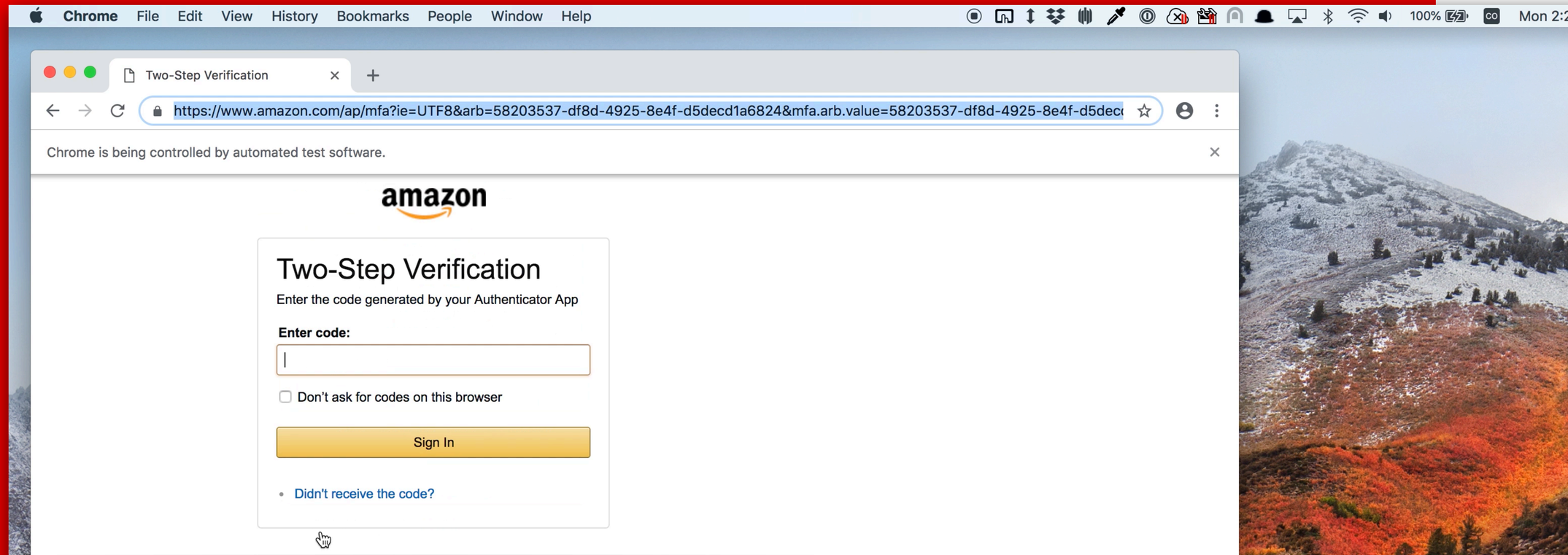
Browser AntiDetect

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



Headless Chrome & Puppeteer

- Drives Production Chrome, the world's most-used browser.
- Scriptable with low level features that benefit attackers.
- Powerful foundation for imitation attacks.



Agenda

1. Current attack landscape
2. **Attacks in detail**
3. The arms race
4. How do we adapt?

Attack Detail: Credential Stuffing

CREDENTIAL STUFFING

cre·den·tial stuff·ing

/krəˈden(t)SHəl ˈstəfiNG/

The automated replay of breached username/password pairs across many sites in order to take over accounts where passwords have been reused.

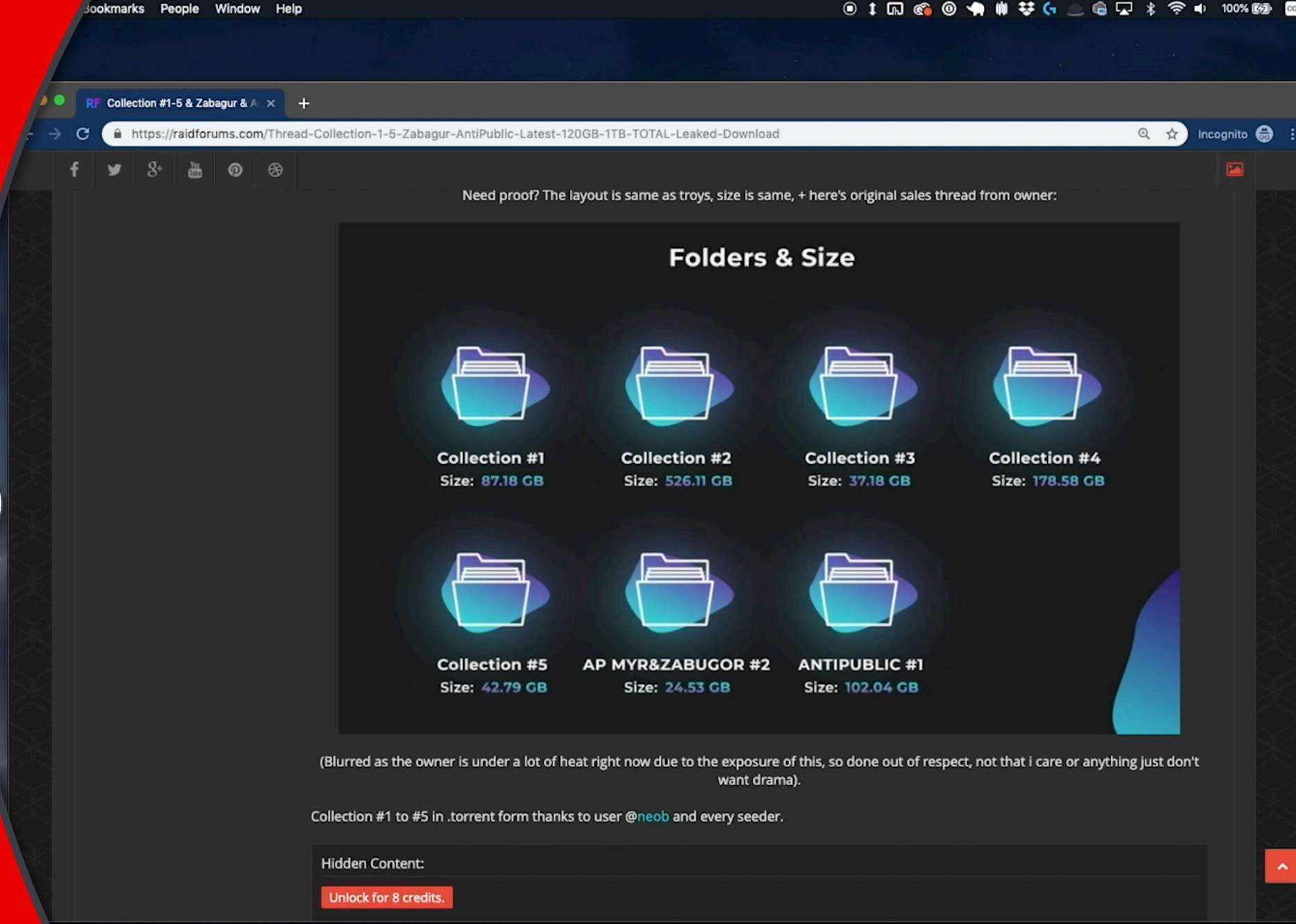
A STEP BY STEP GUIDE

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

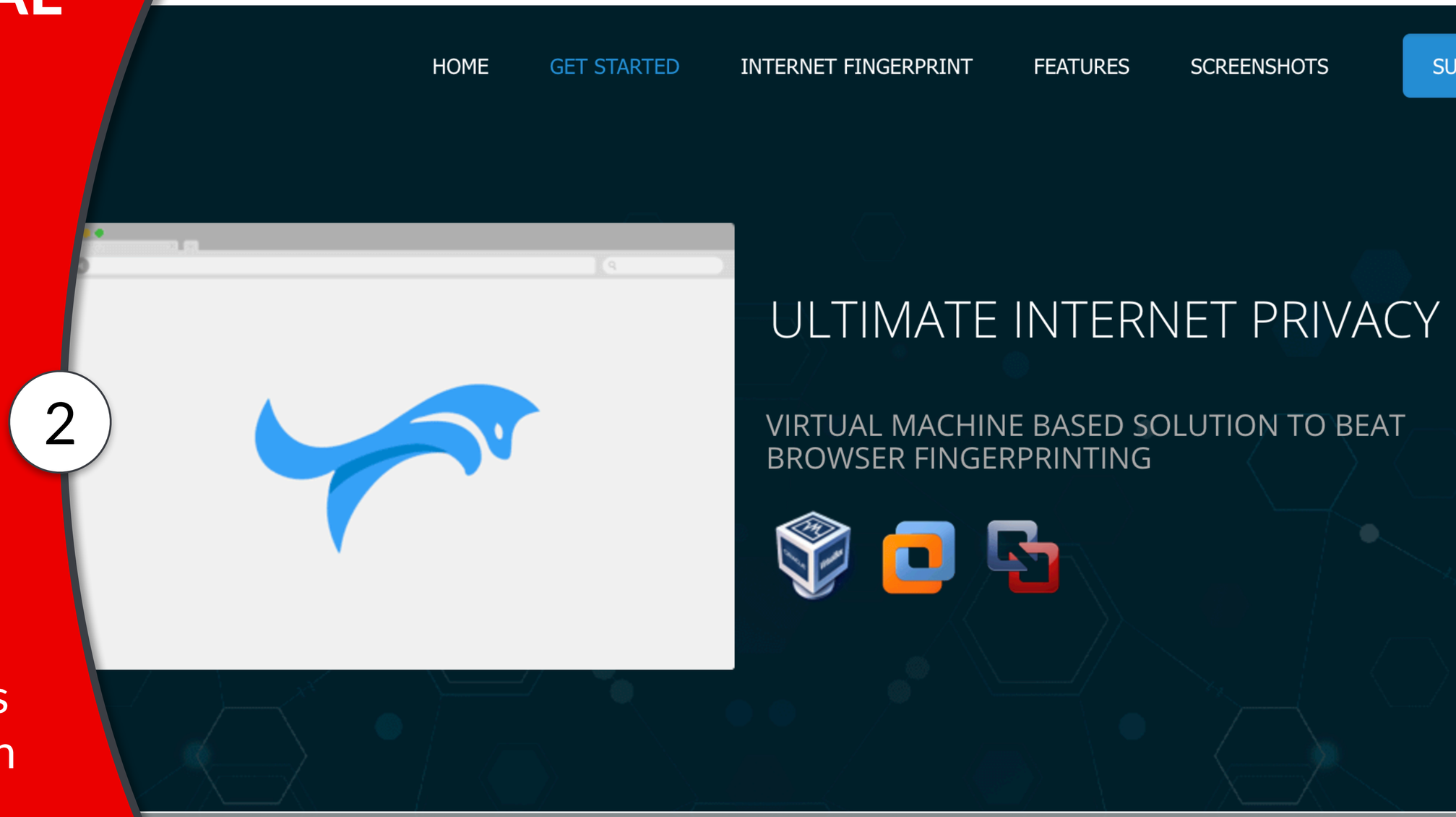
CREDENTIAL STUFFING

1

1. Get Credentials



CREDENTIAL STUFFING

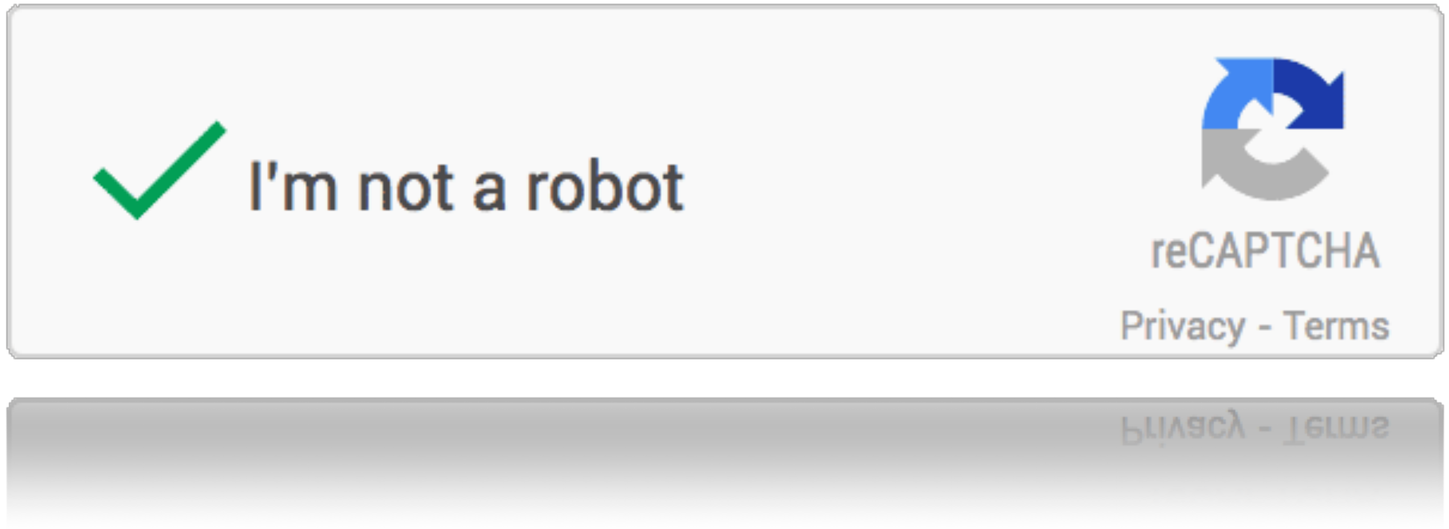


2

1. Get Credentials
2. Automate Login

CREDENTIAL STUFFING

3

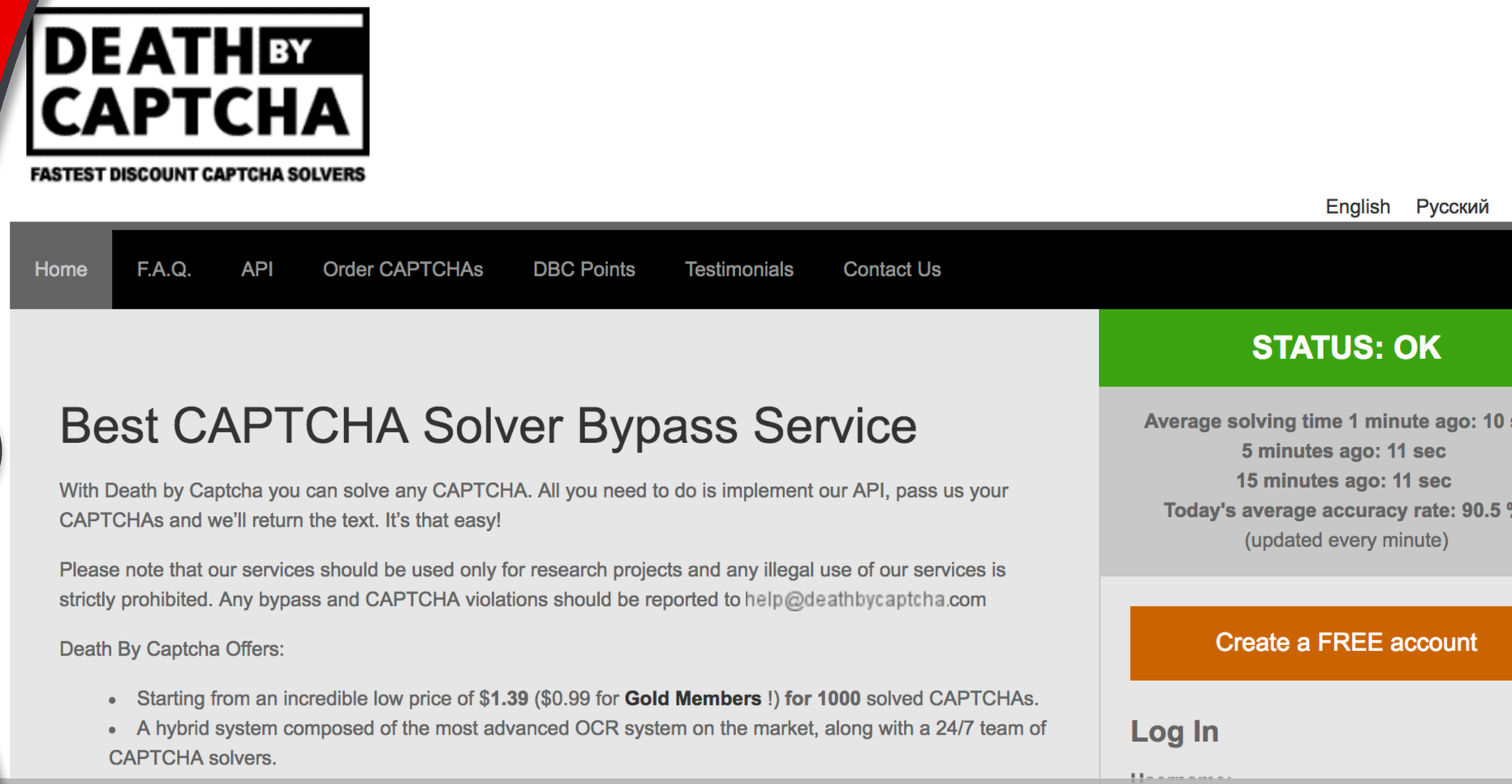


1. Get Credentials
2. Automate Login
3. Defeat Defenses

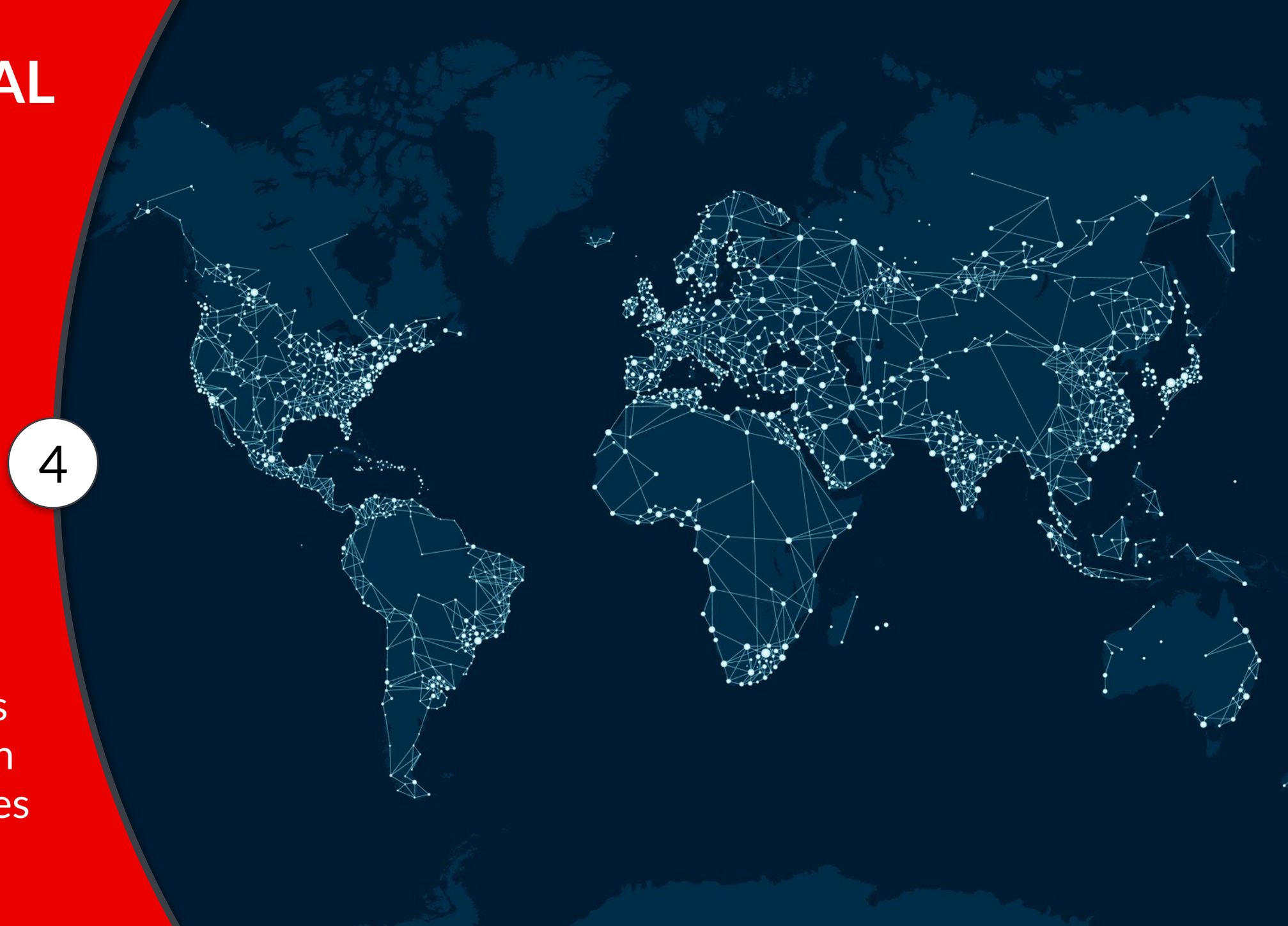
CREDENTIAL STUFFING

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

3



CREDENTIAL STUFFING



4

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

CREDENTIAL STUFFING

4

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

CREDENTIAL STUFFING

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

4

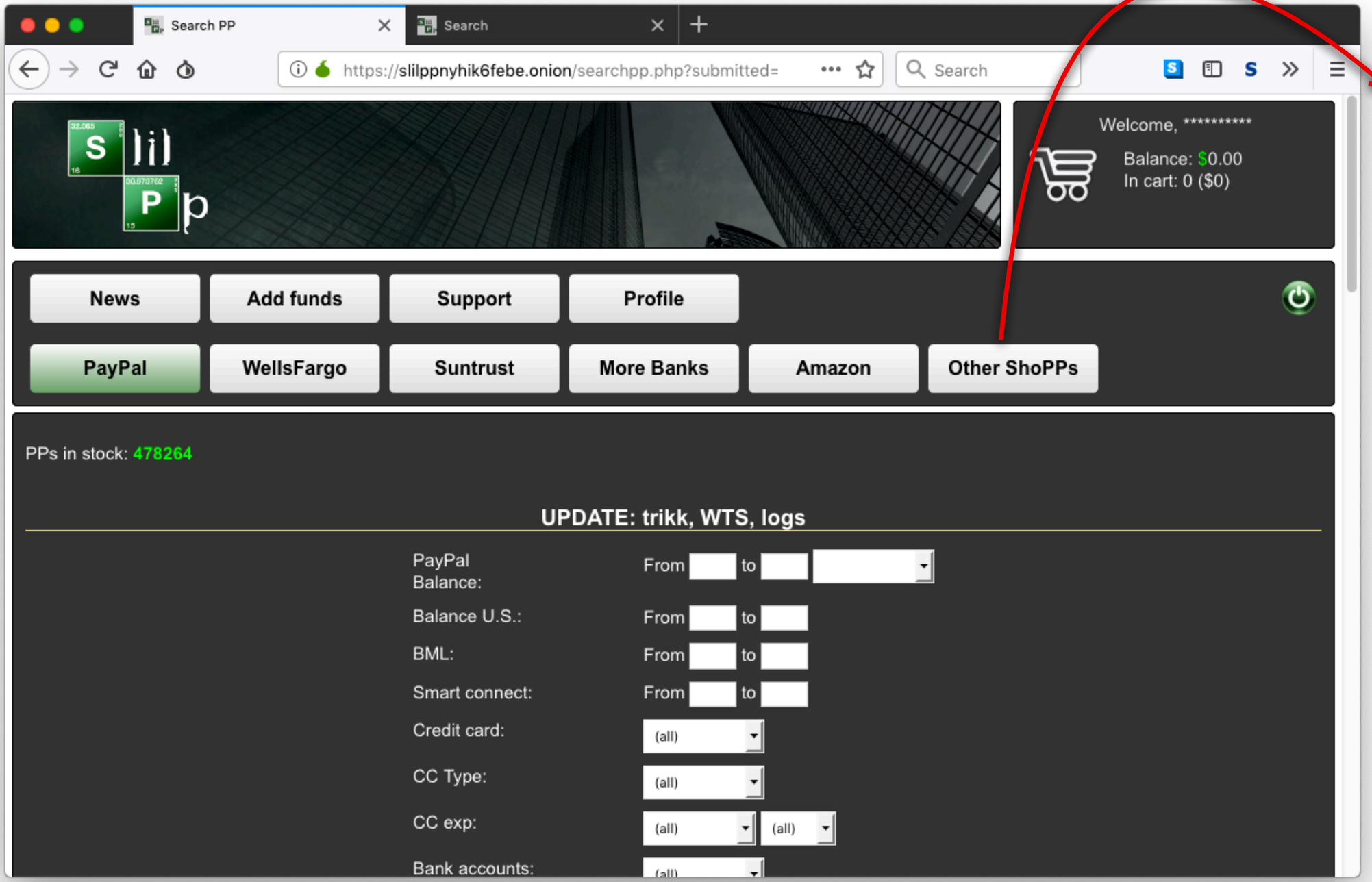
$0 : 2.3 billion credentials

$50 : per site configuration

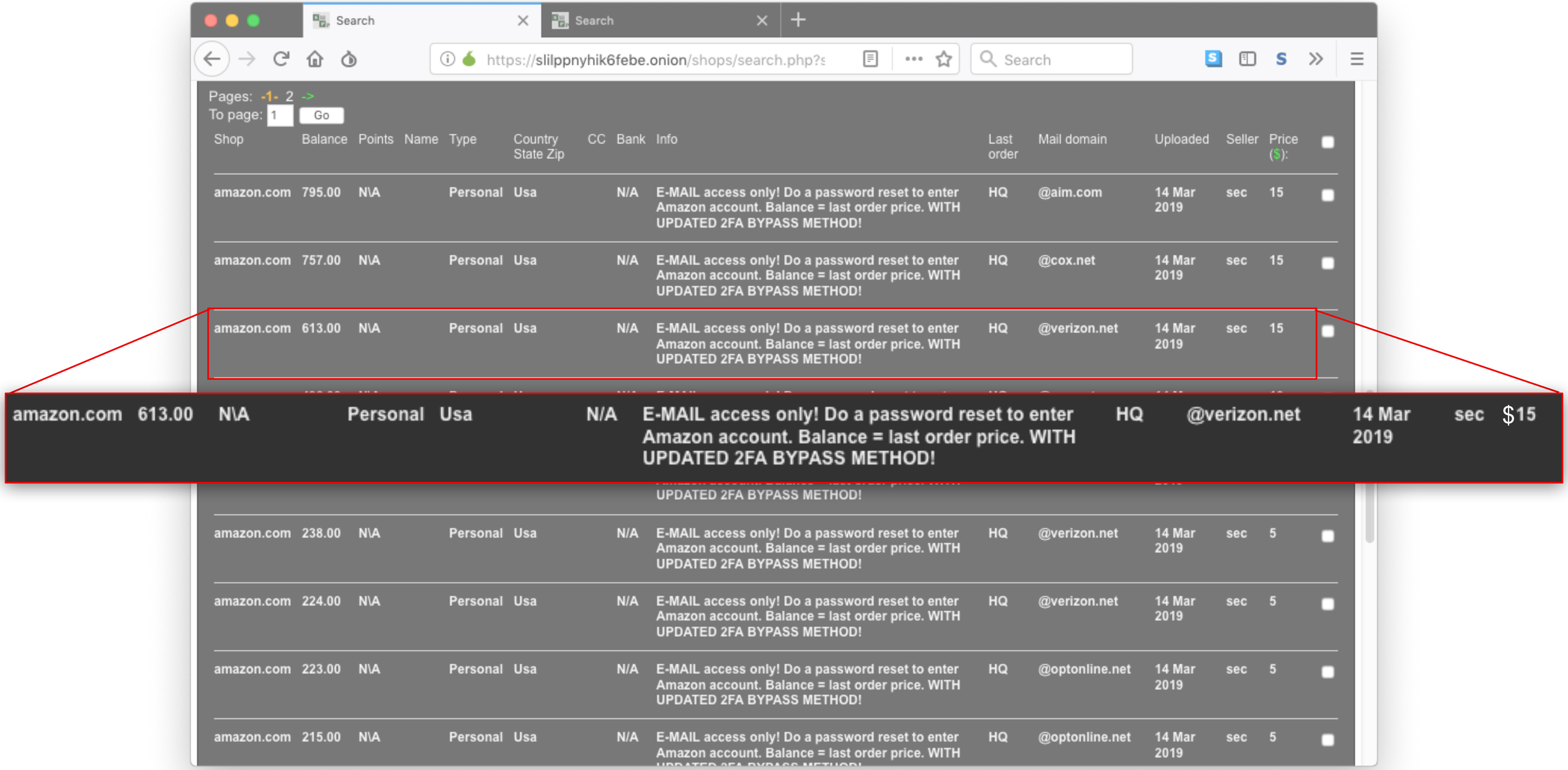
$139 : for 100,000 CAPTCHAs

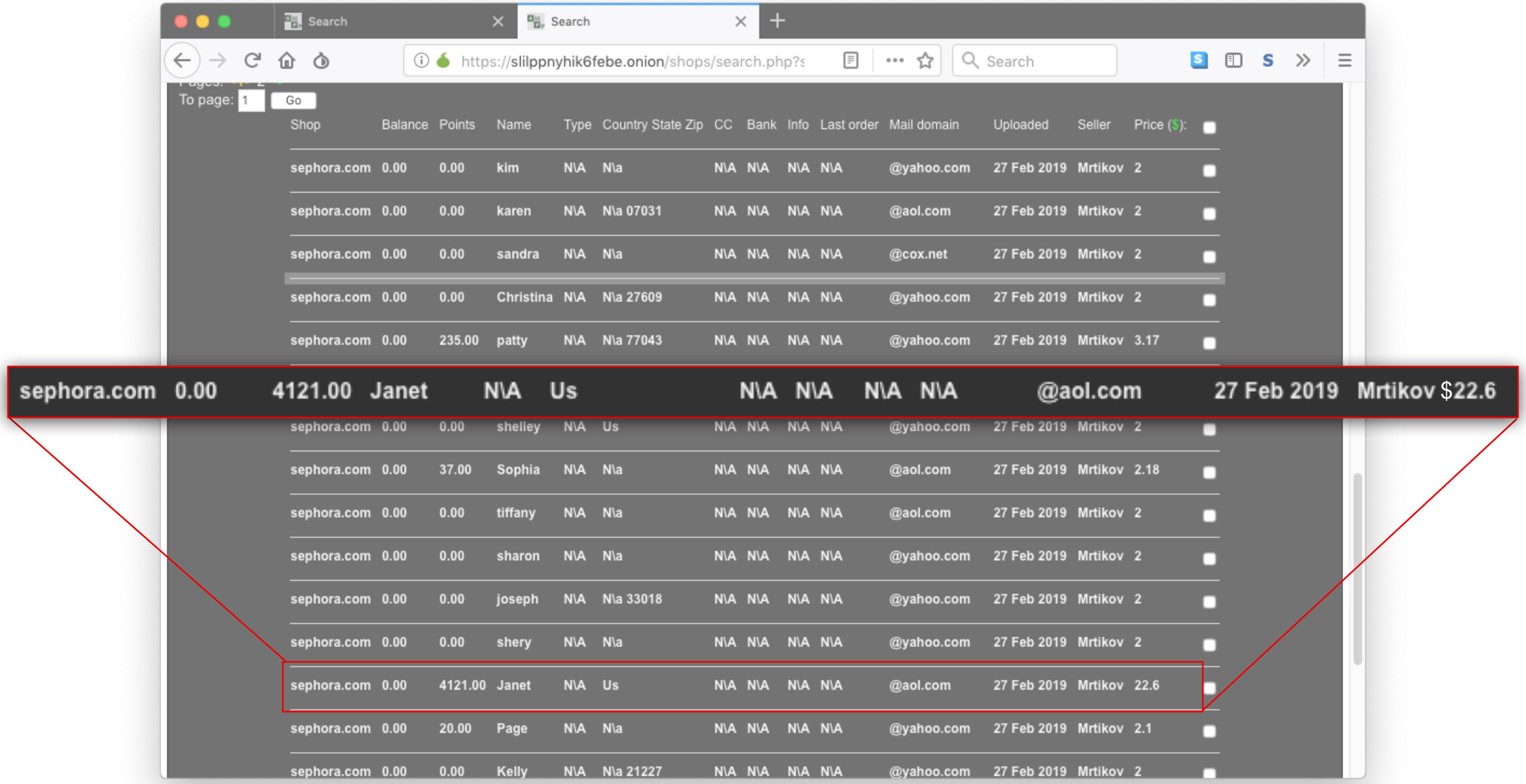
$2 : for 1000 global IPs

Less than $200 for 100,000 ATO attempts



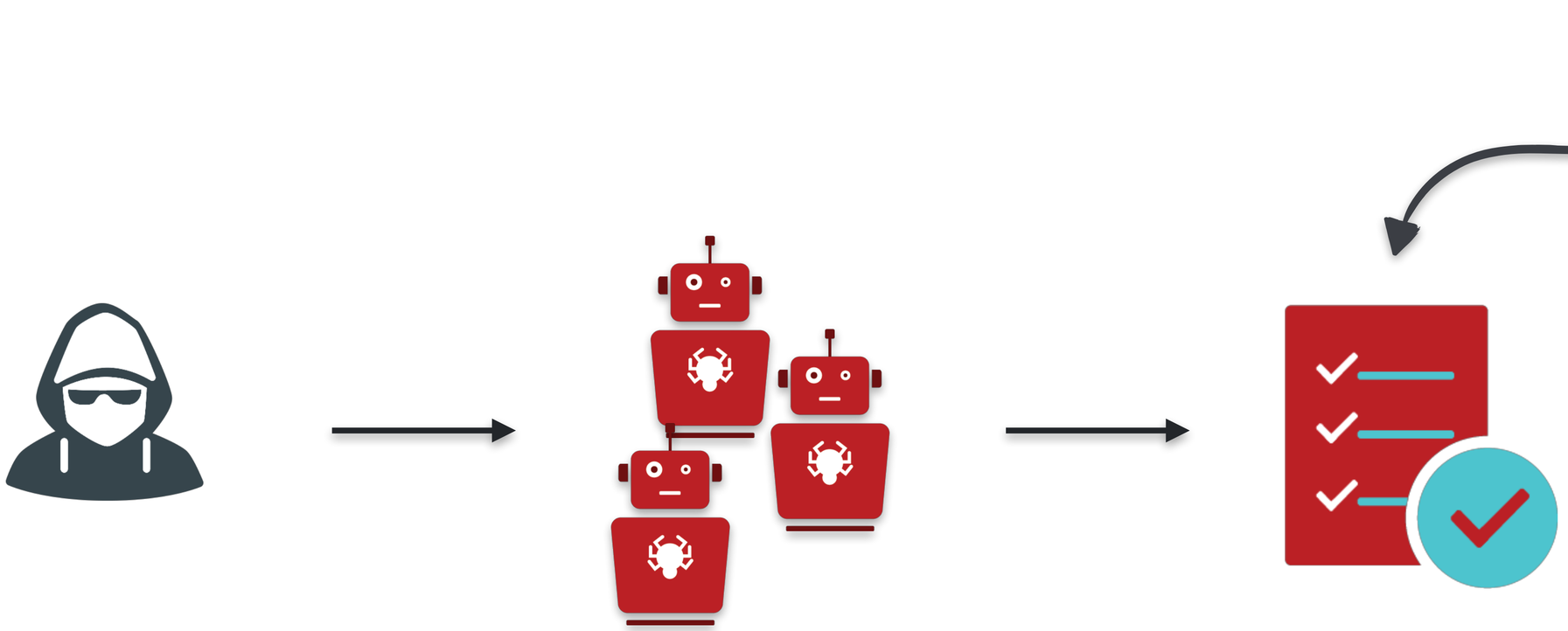
- apple
- airbnb
- bergfreunde
- britishairways
- capitalone
- deliveroo
- discovercard
- epicgames
- facebook
- groupon
- ikea
- marriot
- netflix
- +400 more


Search
Search
https://slilppnyhik6febe.onion/shops/search.php?s
Search
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
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 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 HQ @optonline.net 14 Mar 2019 sec 5

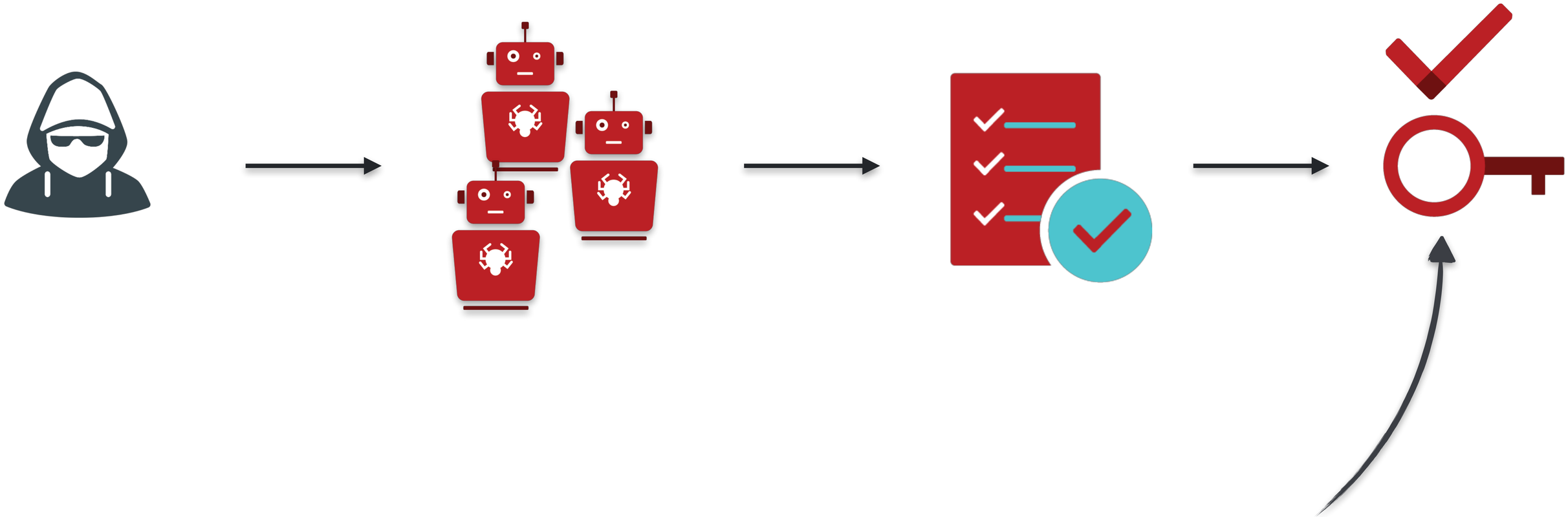

Search
Search
https://slilppnyhik6febe.onion/shops/search.php?s
Search
To page: 1 Go
Shop Balance Points Name Type Country State Zip CC Bank Info Last order Mail domain Uploaded Seller Price ($):
sephora.com 0.00 0.00 kim N\A N\a N\A N\A N\A N\A @yahoo.com 27 Feb 2019 Mrtikov 2
sephora.com 0.00 0.00 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 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 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

But Multi-Factor Authentication solves this, right?

The purpose of credential stuffing is to find valid accounts.

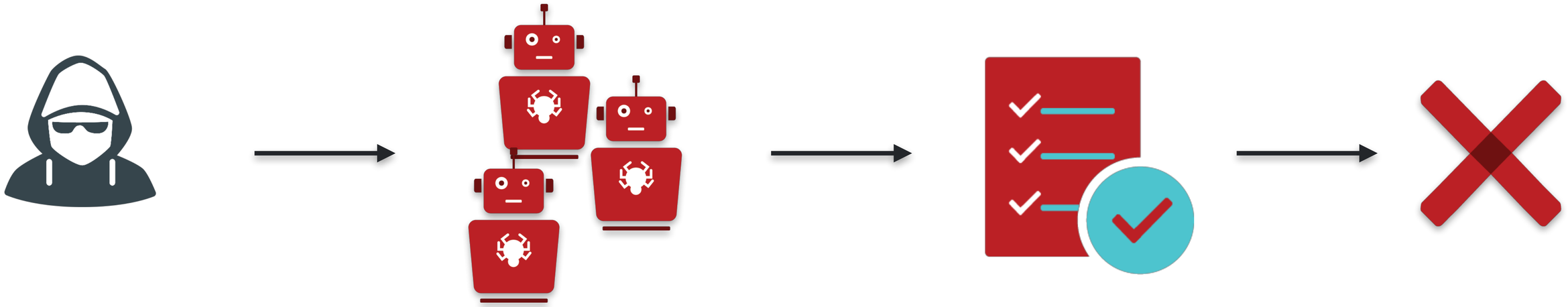


The purpose of credential stuffing is to find valid accounts.



Valid accounts **without MFA** lead directly to account takeovers.

Valid accounts **with MFA** do not lead *directly* to ATOs.

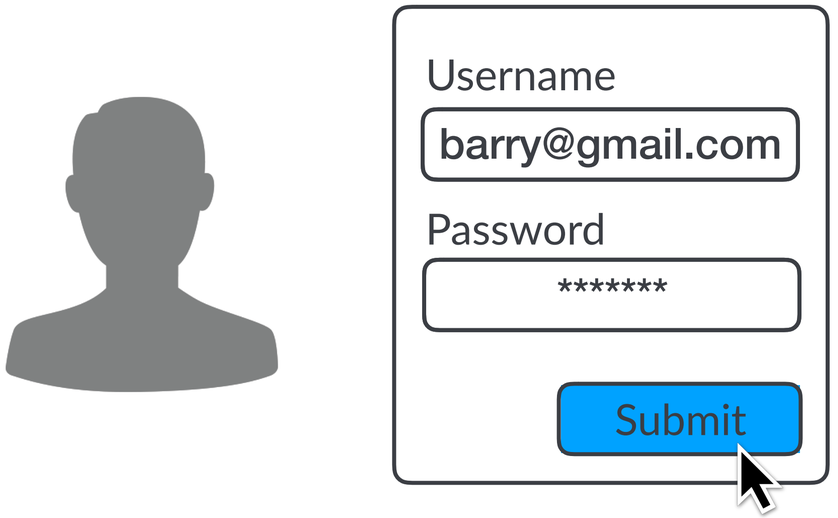


But the attacker still has valid accounts.

MFA is a hurdle that adds cost to the attack.

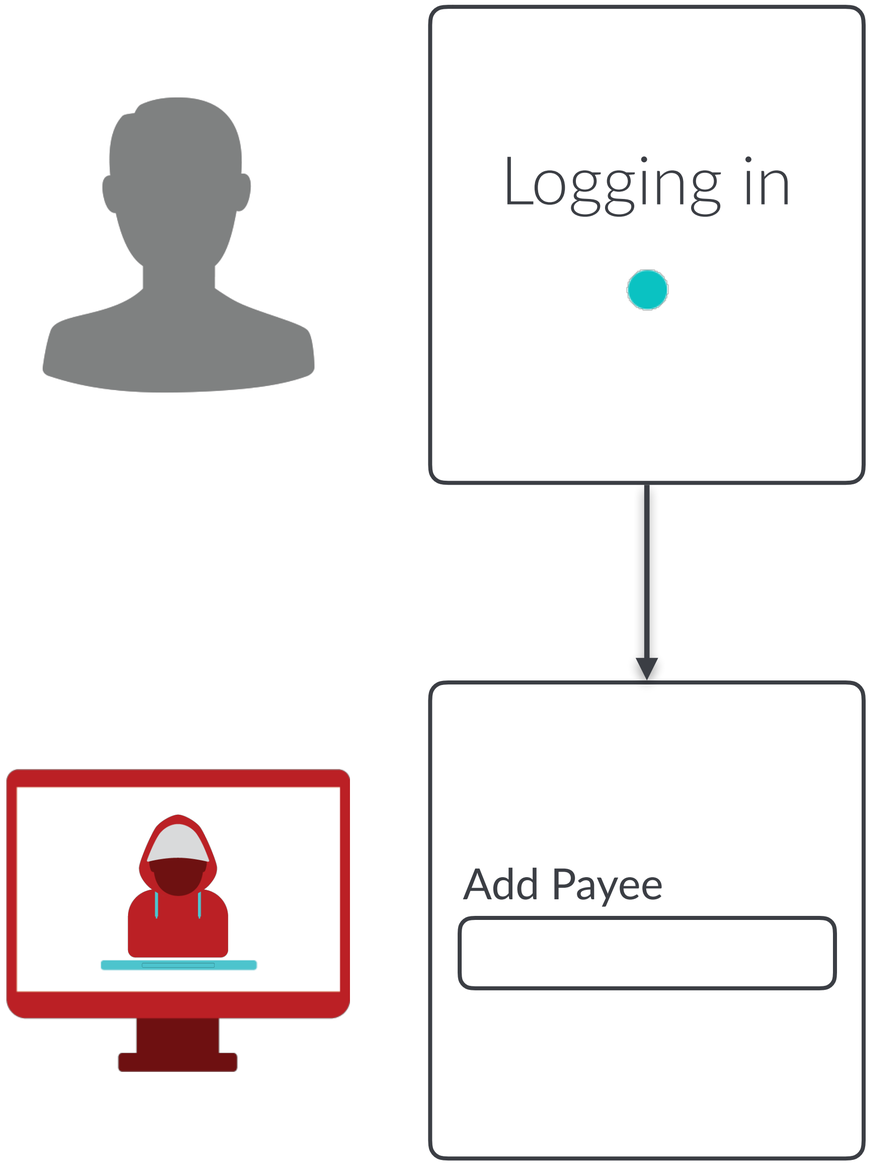
It is good but it is **not** a silver bullet.

All hurdles will be crossed if the value is there.

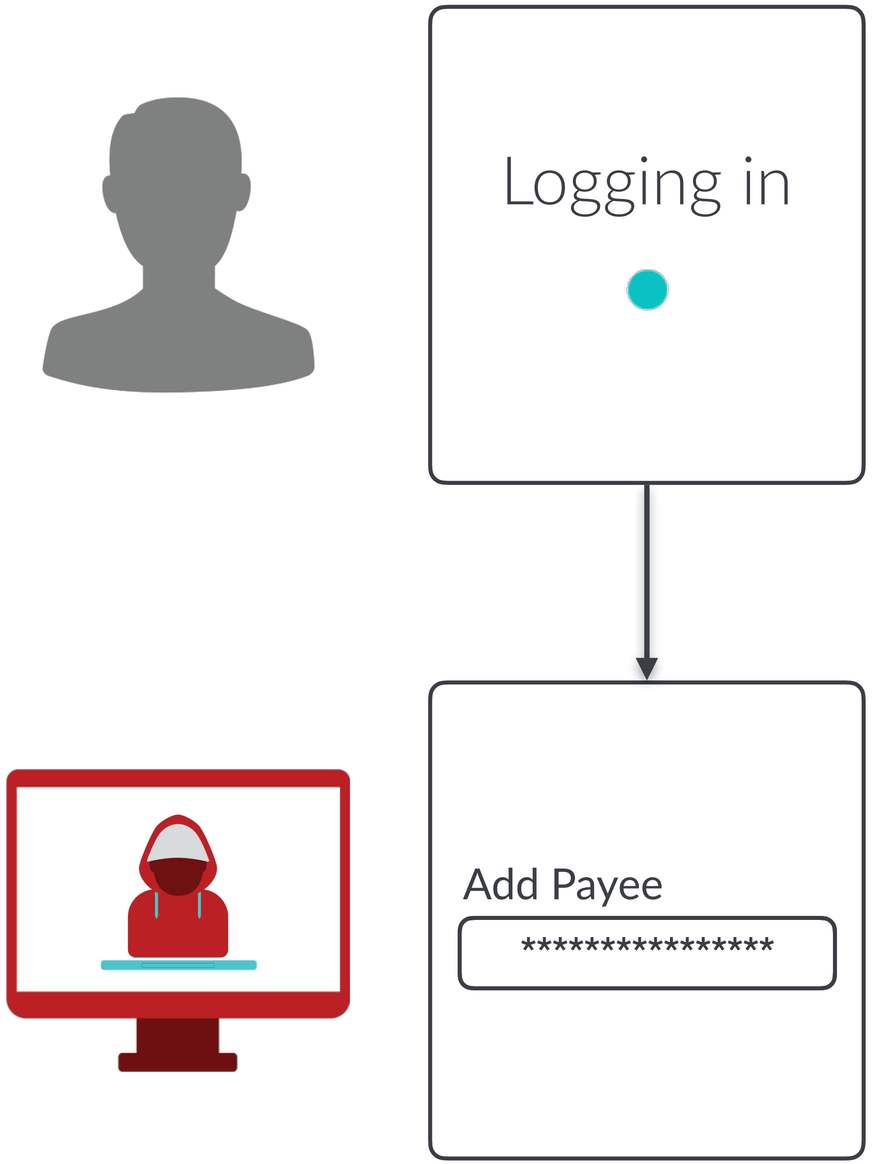


Take Barry, for example. An everyday user logging in as normal.

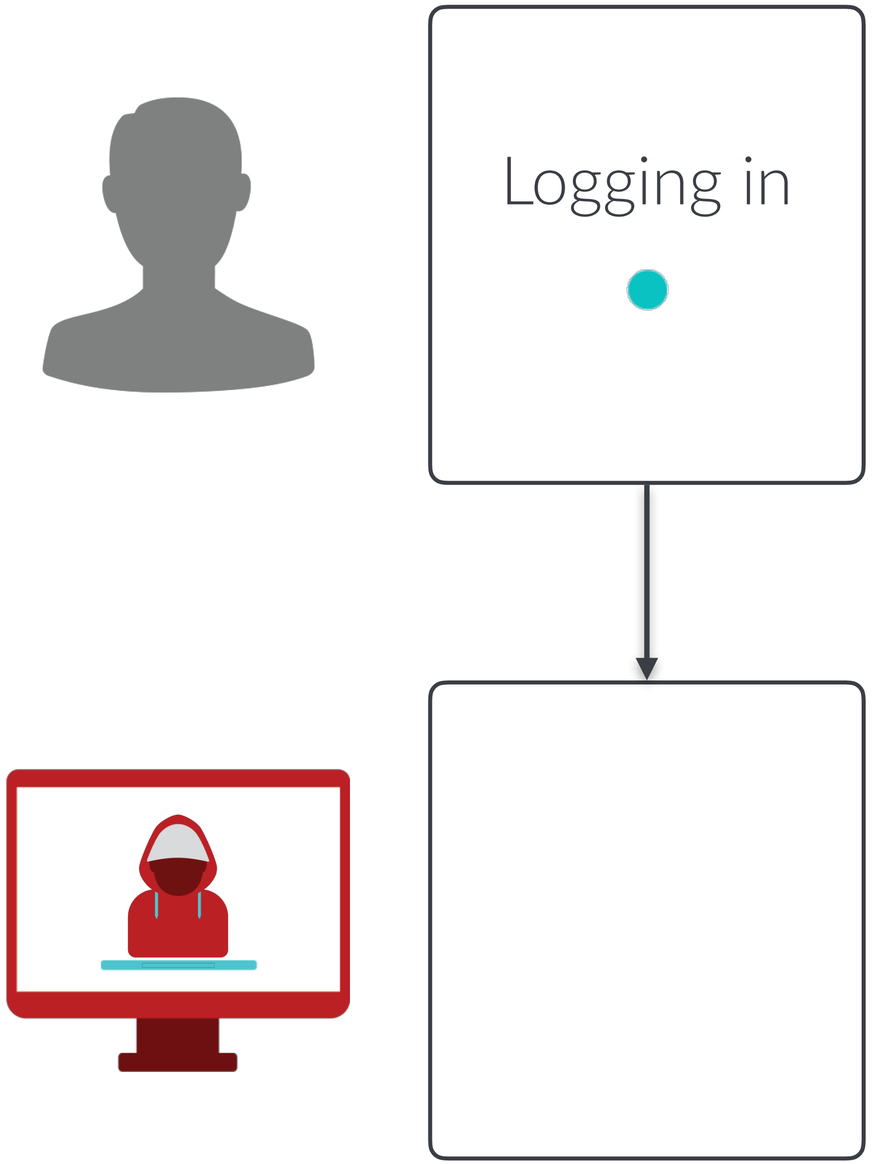
Barry experiences a login delay but he is used to that.



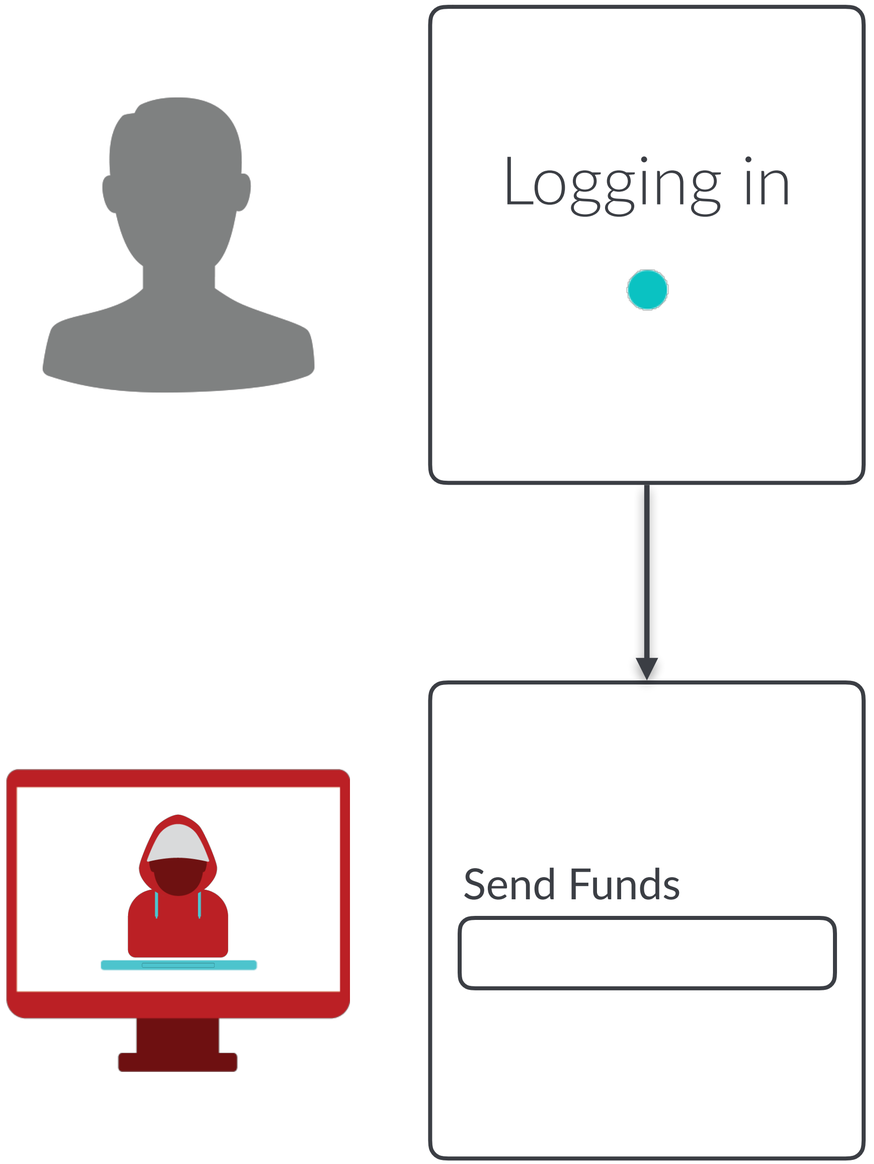
Uh oh. An injected script or malicious extension kicks in.



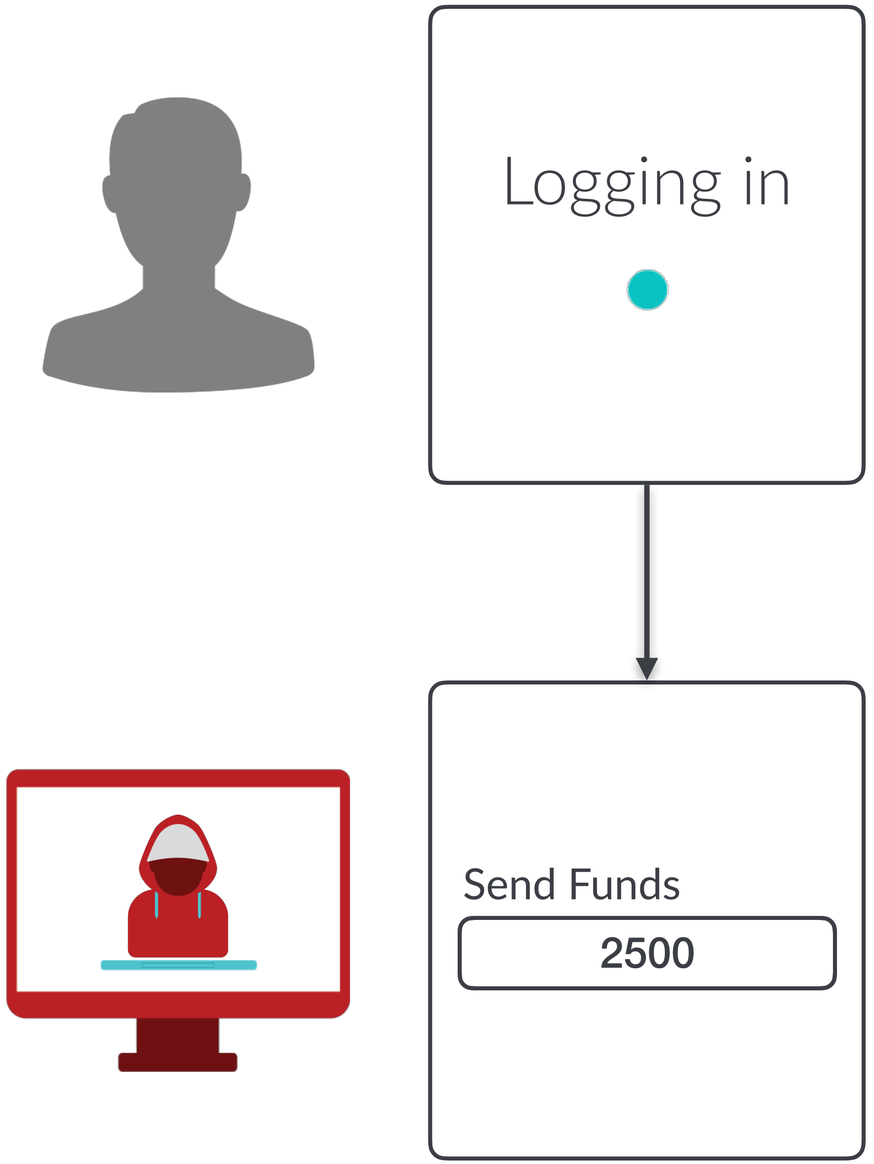
This script tries to add a new payee...



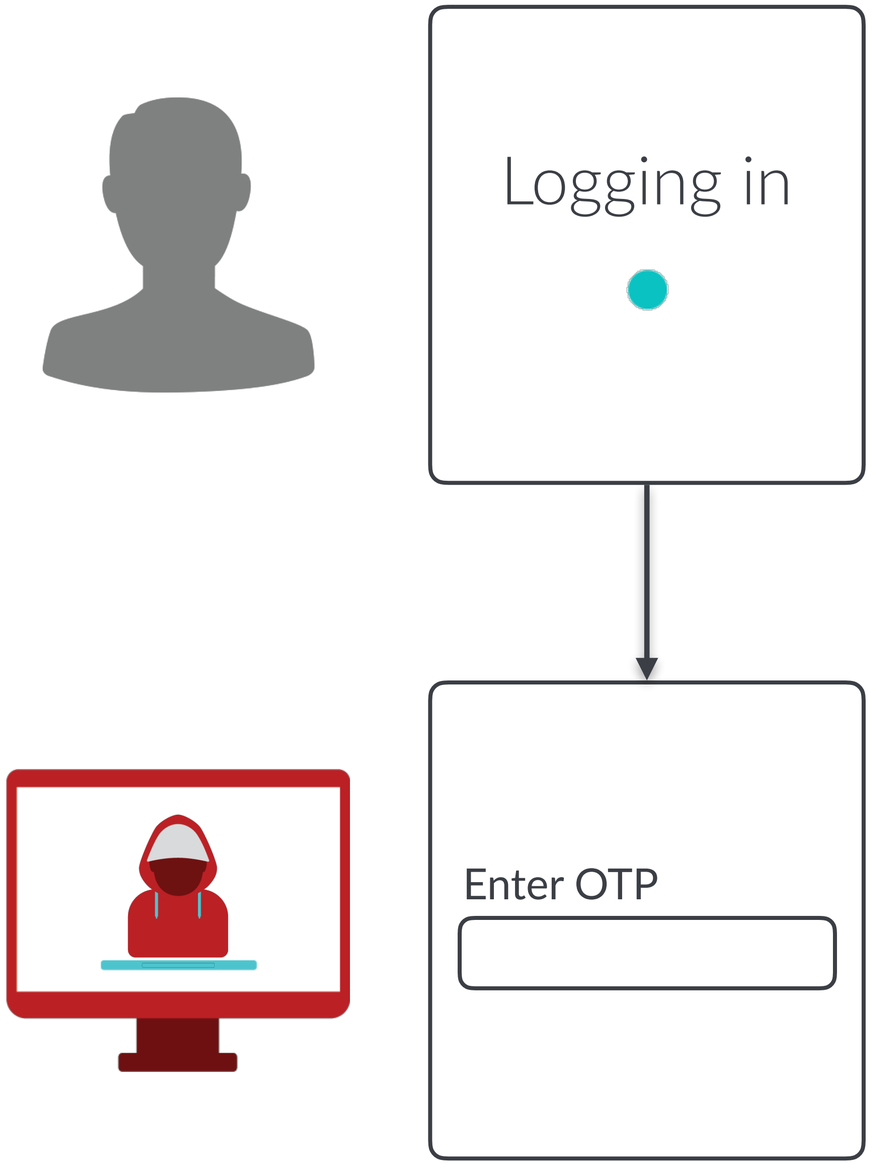
...which is successful because why wouldn't it be?



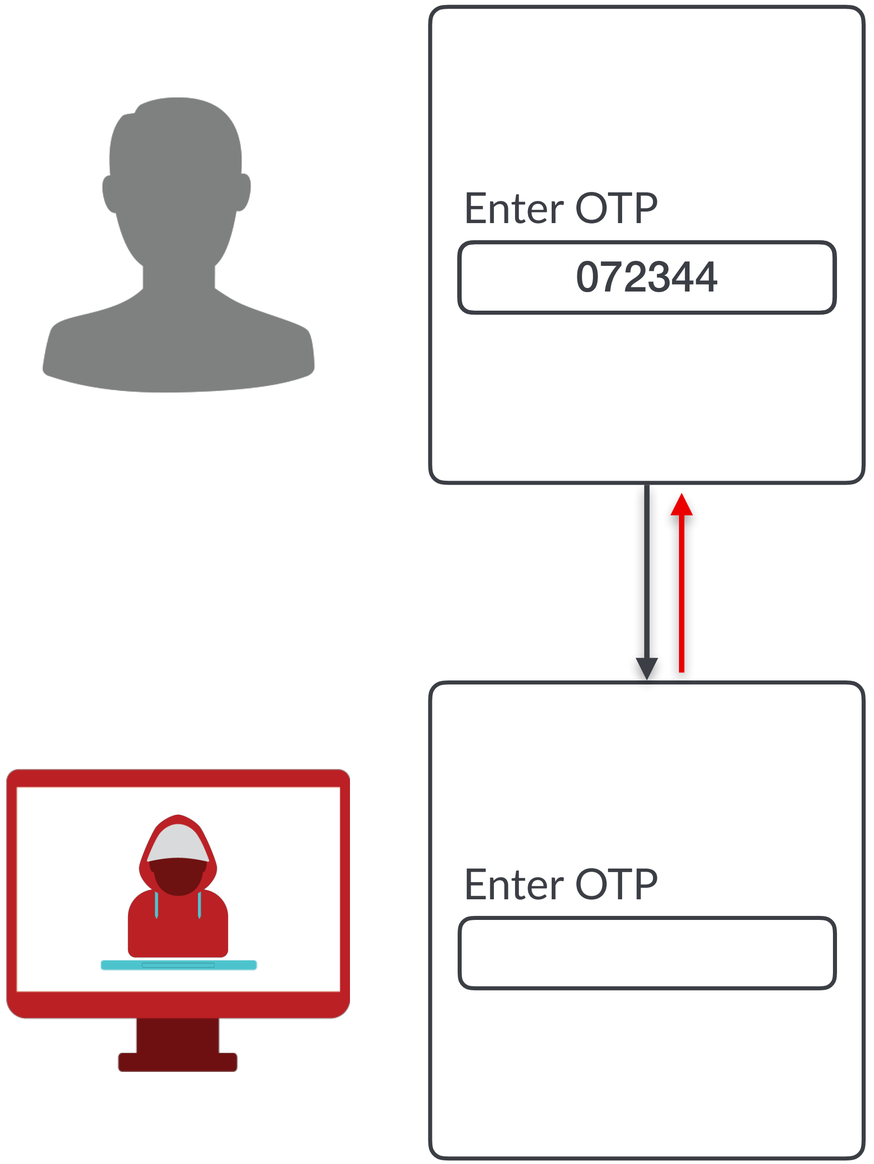
The script then attempts to transfer funds.



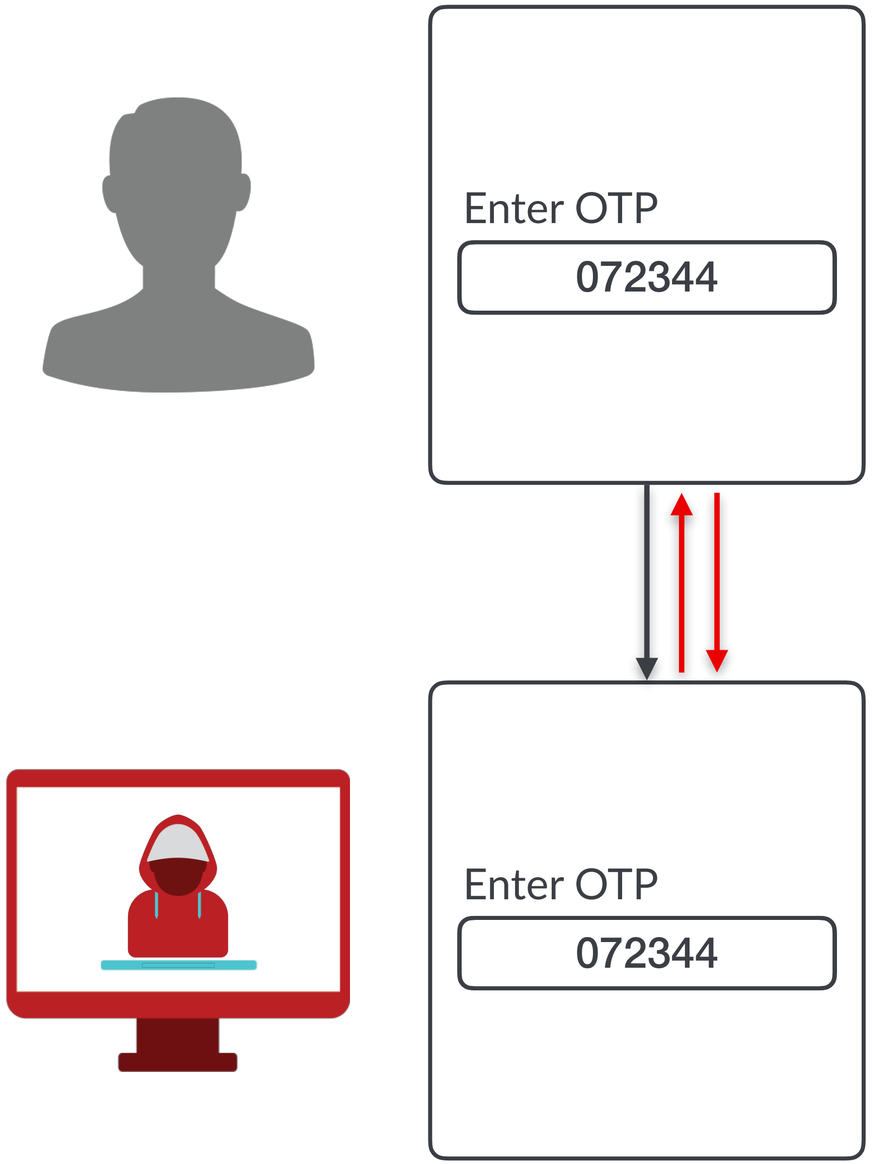
Usually a flat number or percentage, whichever is lower.



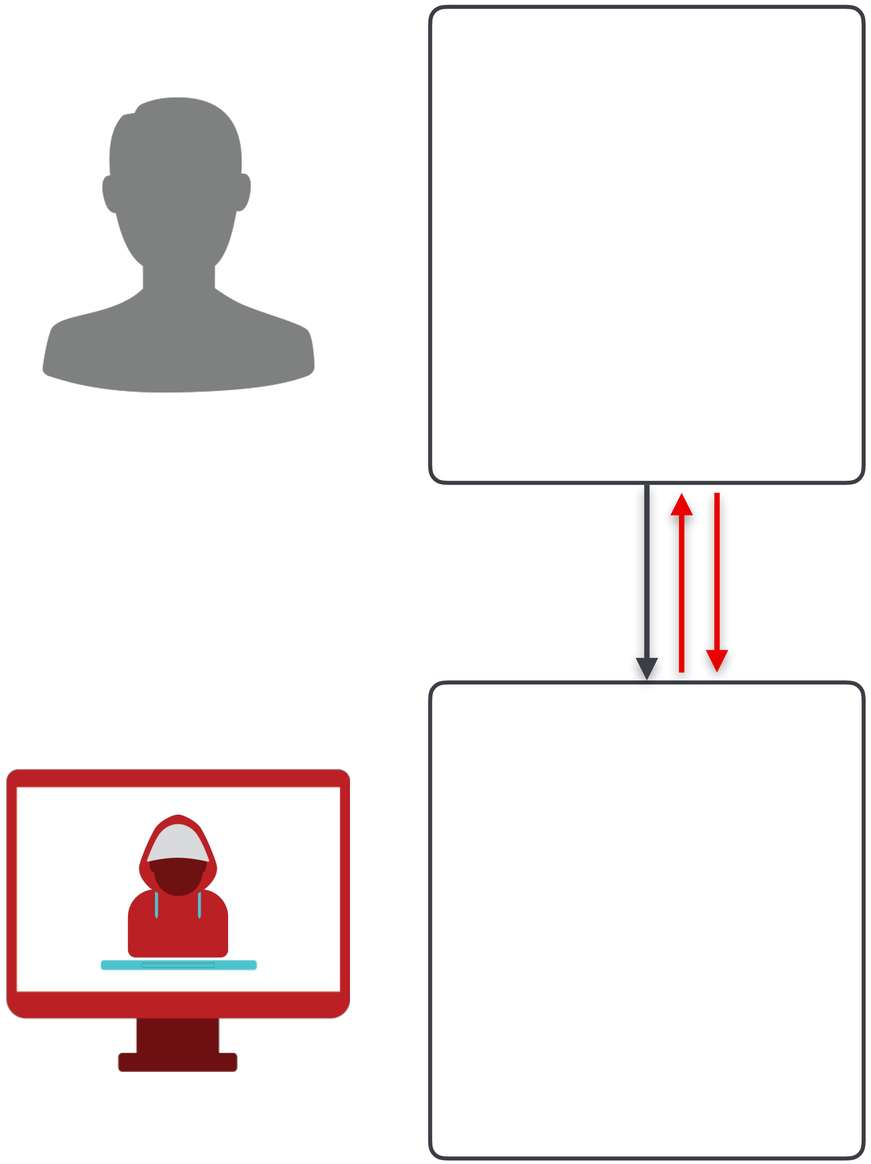
The risk score is too high, time to ask for a one-time password.



But wait, Barry's used to this flow and doesn't see a problem.



The script grabs the token and funds are transferred.



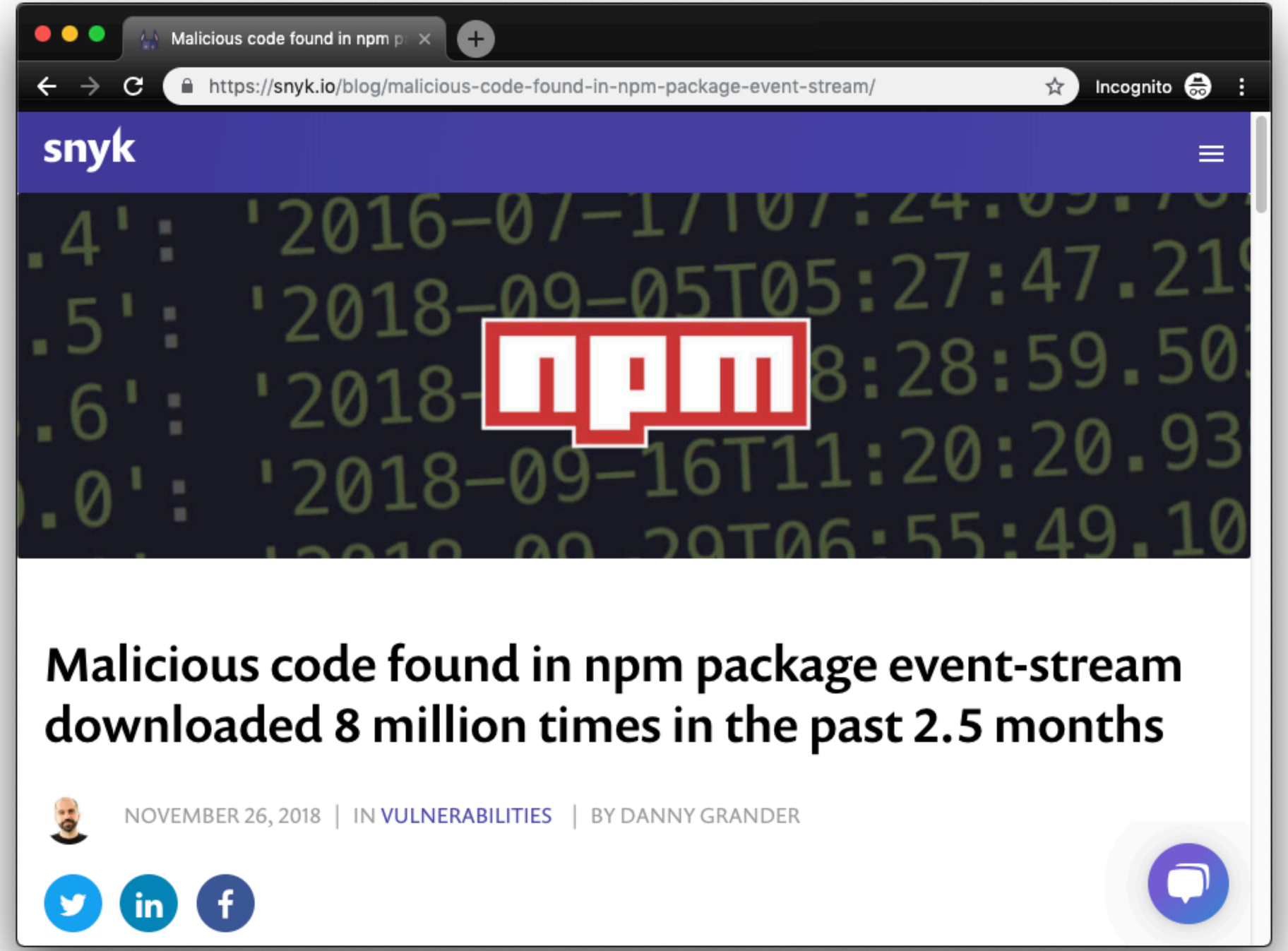
NEWS

Spammers buy Chrome extensions and turn them into adware

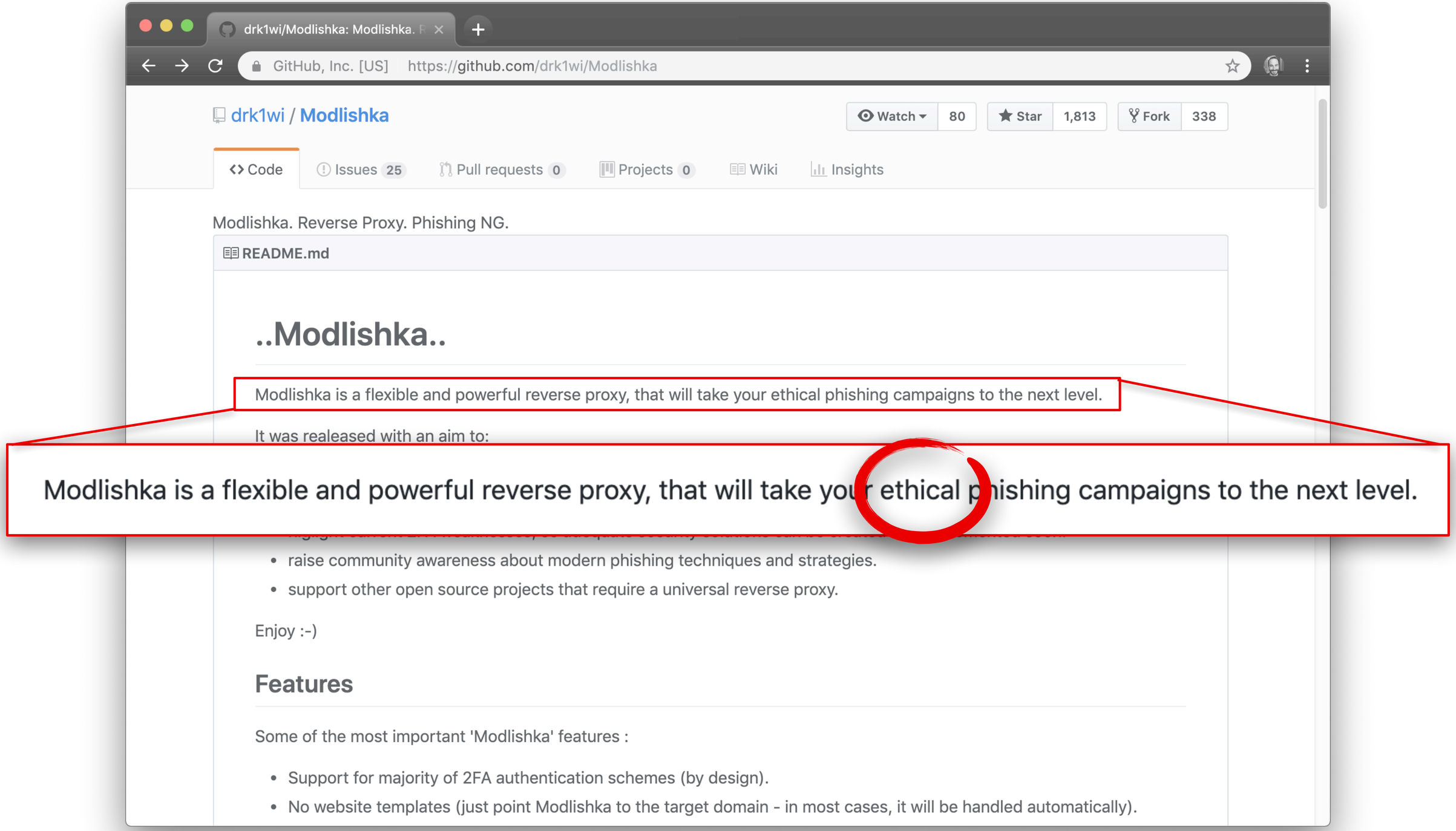
Two developers who sold their popular Chrome extensions saw them misused for aggressive advertising

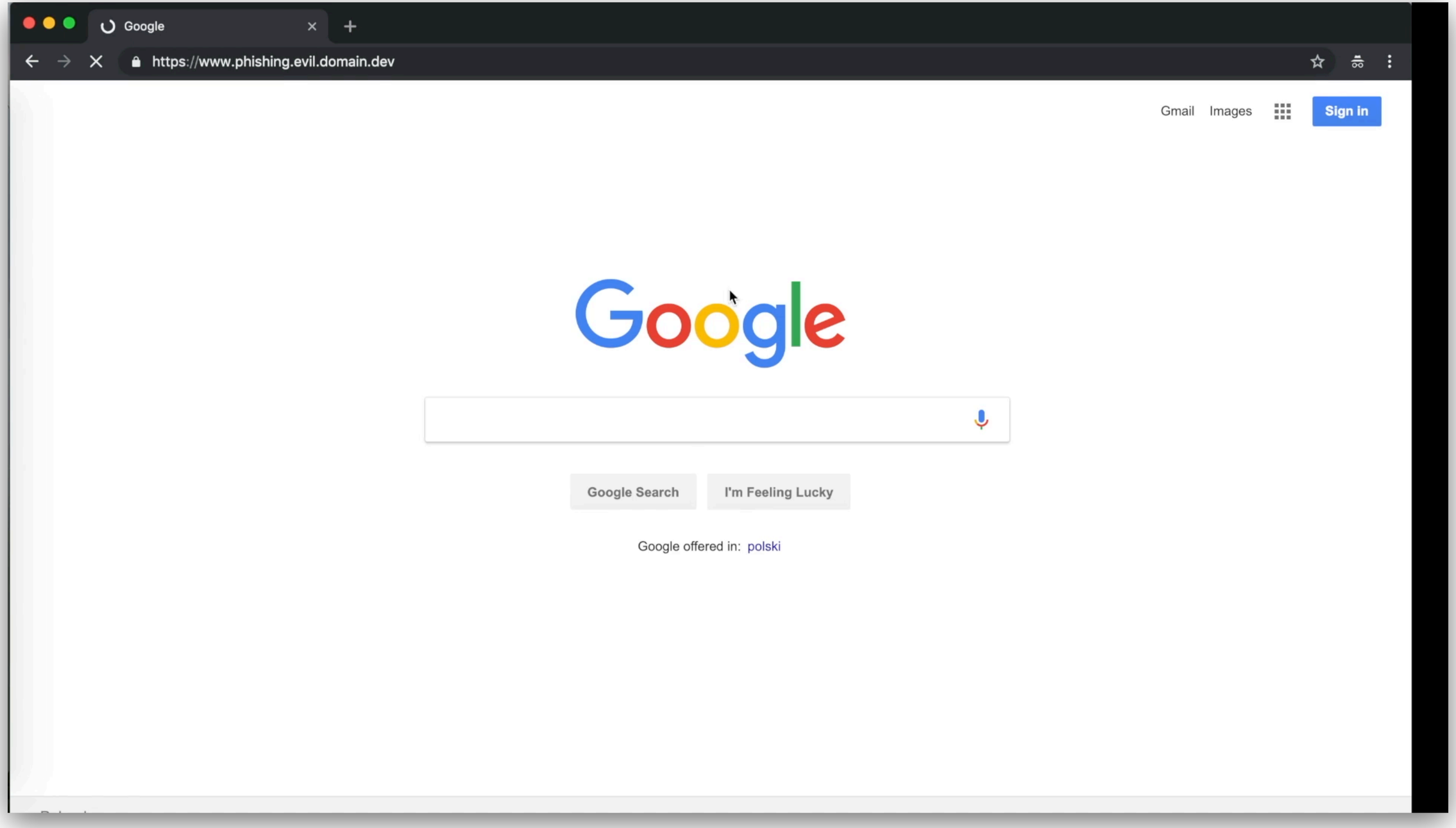
By Lucian Constantin

Romania Correspondent, IDG News Service | JANUARY 20, 2014 08:03 AM PT


Malicious code found in npm p
https://snyk.io/blog/malicious-code-found-in-npm-package-event-stream/
Incognito
snyk
npm
Malicious code found in npm package event-stream downloaded 8 million times in the past 2.5 months
NOVEMBER 26, 2018 | IN VULNERABILITIES | BY DANNY GRANDER

"I'm mostly concerned about phishing"

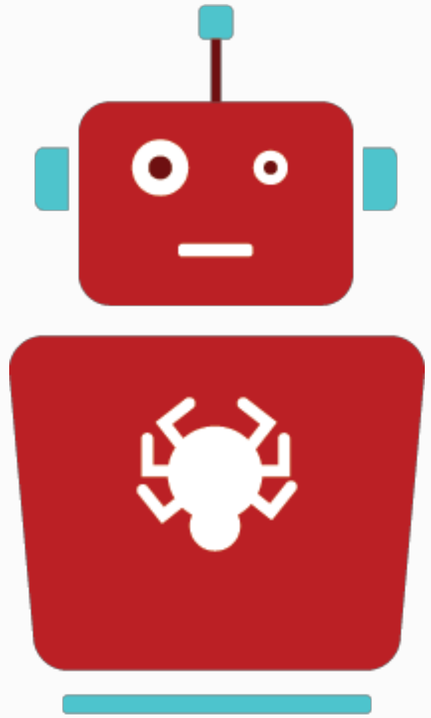

drk1wi/Modlishka: Modlishka.
GitHub, Inc. [US] https://github.com/drk1wi/Modlishka
drk1wi / Modlishka
Watch 80
Star 1,813
Fork 338
Code
Issues 25
Pull requests 0
Projects 0
Wiki
Insights
Modlishka. Reverse Proxy. Phishing NG.
README.md
..Modlishka..
Modlishka is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level.
It was realeased with an aim to:
raise community awareness about modern phishing techniques and strategies.
support other open source projects that require a universal reverse proxy.
Enjoy :-)
Features
Some of the most important 'Modlishka' features :
Support for majority of 2FA authentication schemes (by design).
No website templates (just point Modlishka to the target domain - in most cases, it will be handled automatically).
Modlishka is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level.


Google
https://www.phishing.evil.domain.dev
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: polski

Agenda

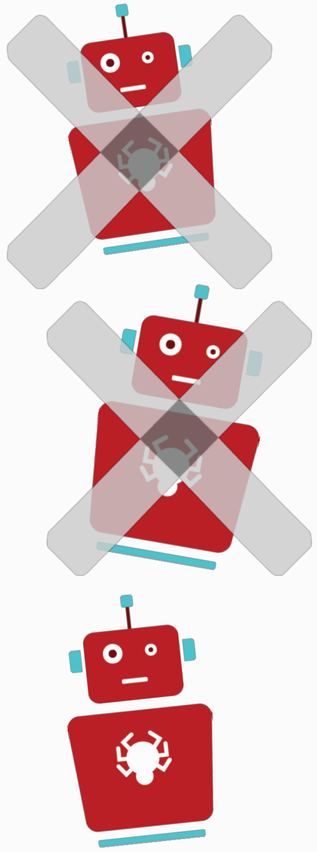
1. Current attack landscape
2. Attacks in detail
3. **The arms race**
4. How do we adapt?

Millions of marketing dollars talk about bots...



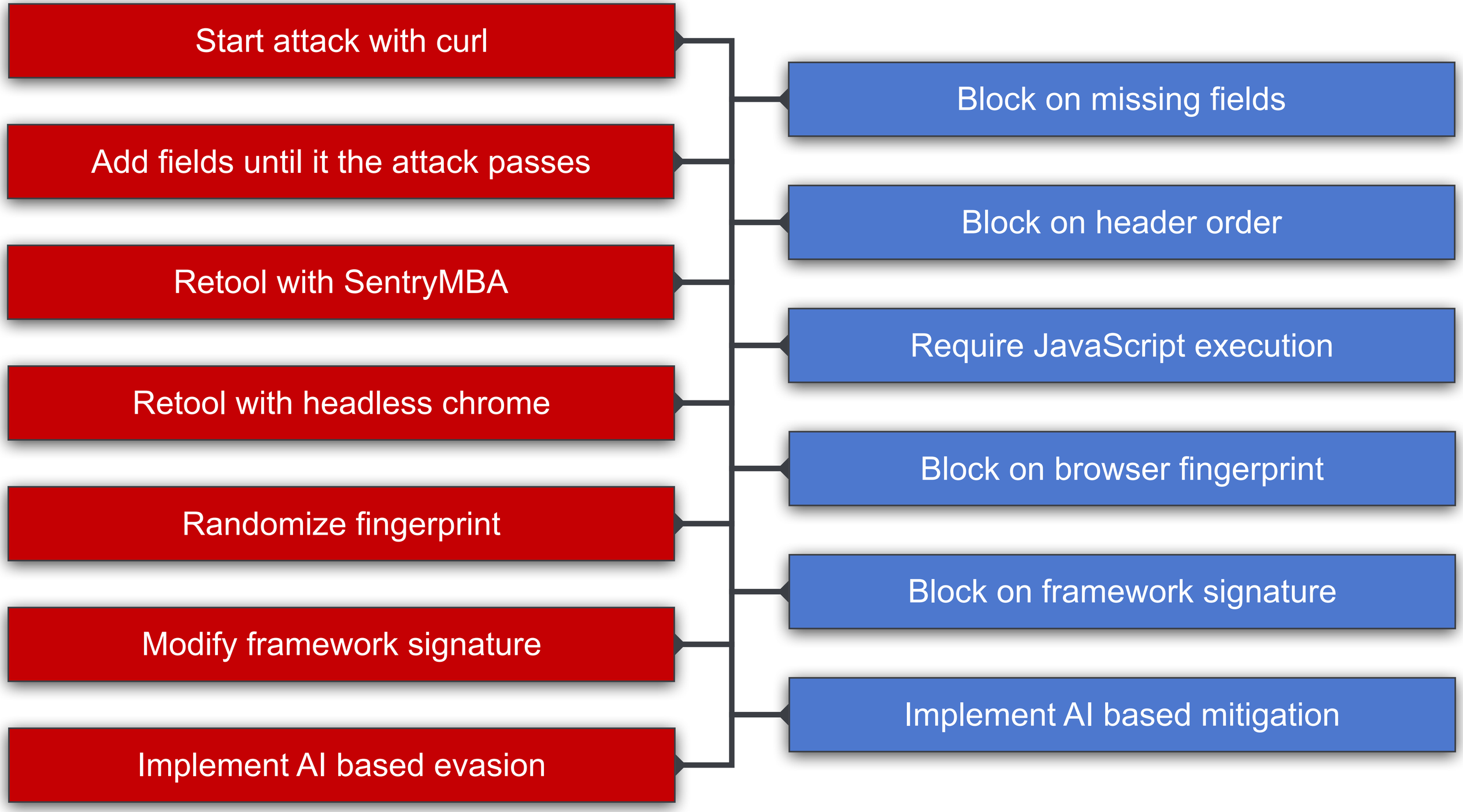
Bots are just one symptom, not the cause

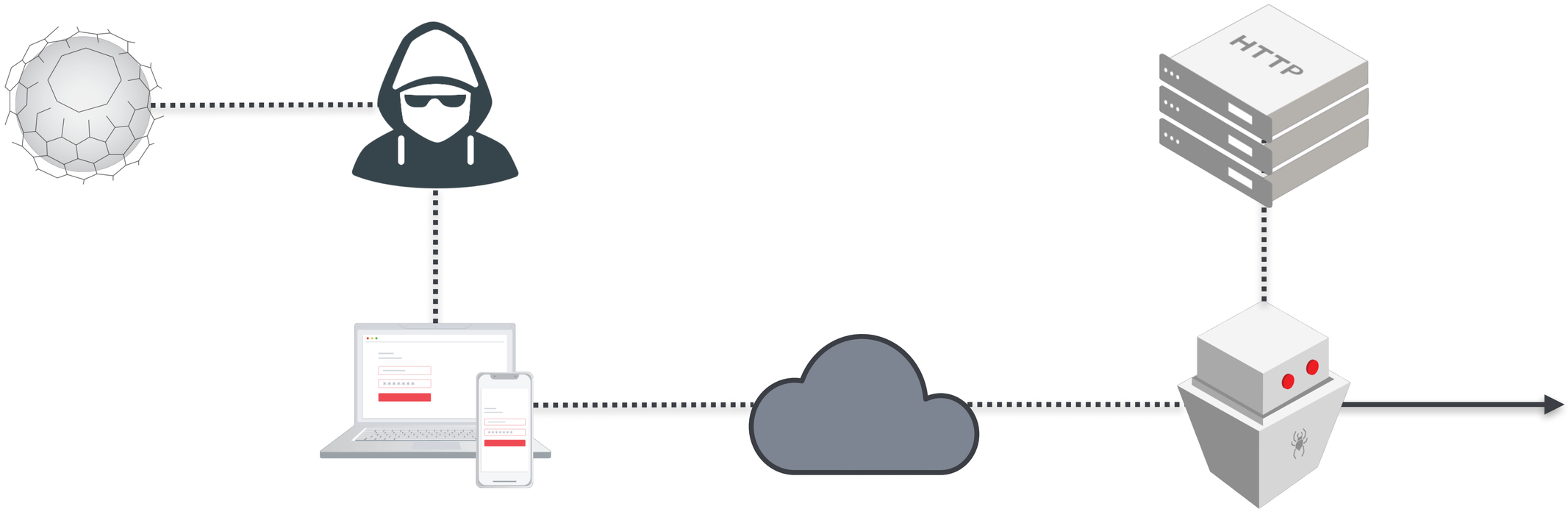
Treating the symptom won't fix the problem



There are no silver bullets

There will always be a back and forth


Start attack with curl
Add fields until it the attack passes
Retool with SentryMBA
Retool with headless chrome
Randomize fingerprint
Modify framework signature
Implement AI based evasion
Block on missing fields
Block on header order
Require JavaScript execution
Block on browser fingerprint
Block on framework signature
Implement AI based mitigation



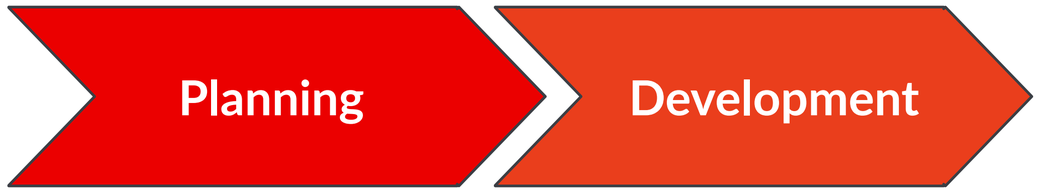
It’s not as simple as blocking a bot.
It’s targeting what will cost the attacker the most. Over and over again.

The Software Development Lifecycle

Planning

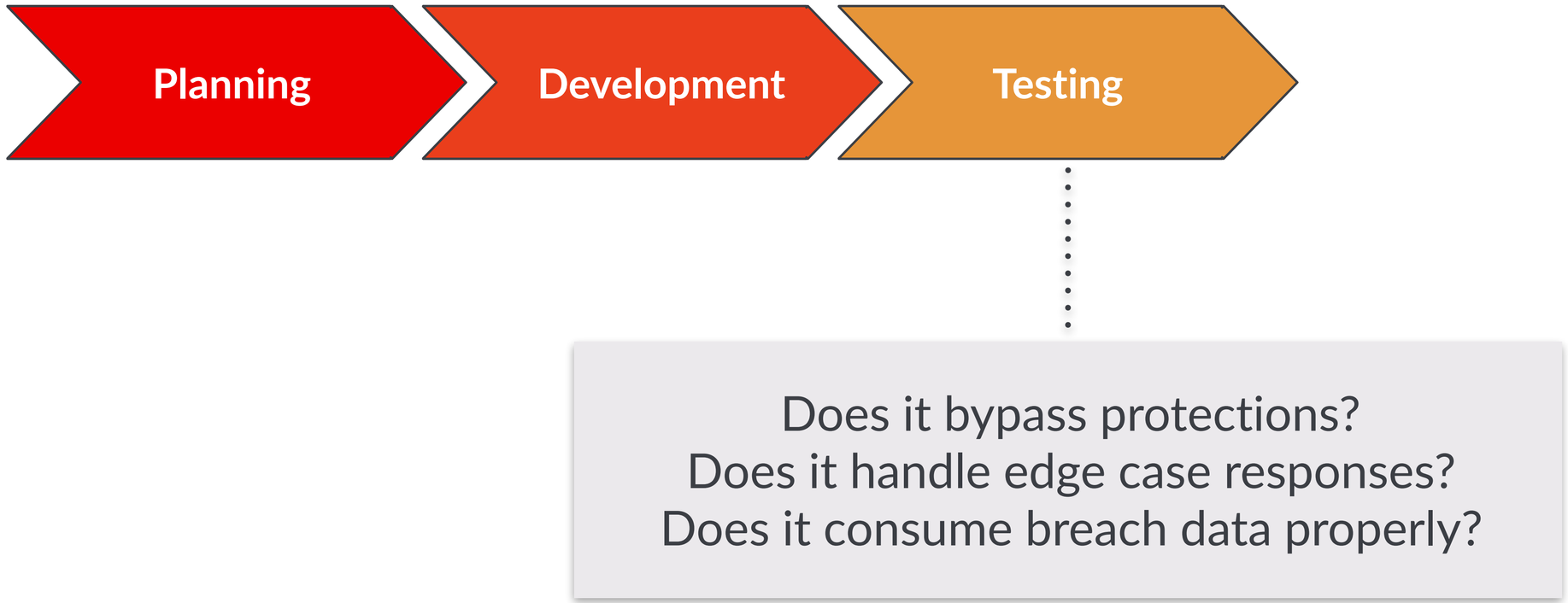
What tools work, what don’t?
What URLs need to be targeted?
What dark web data do I need?

The Software Development Lifecycle

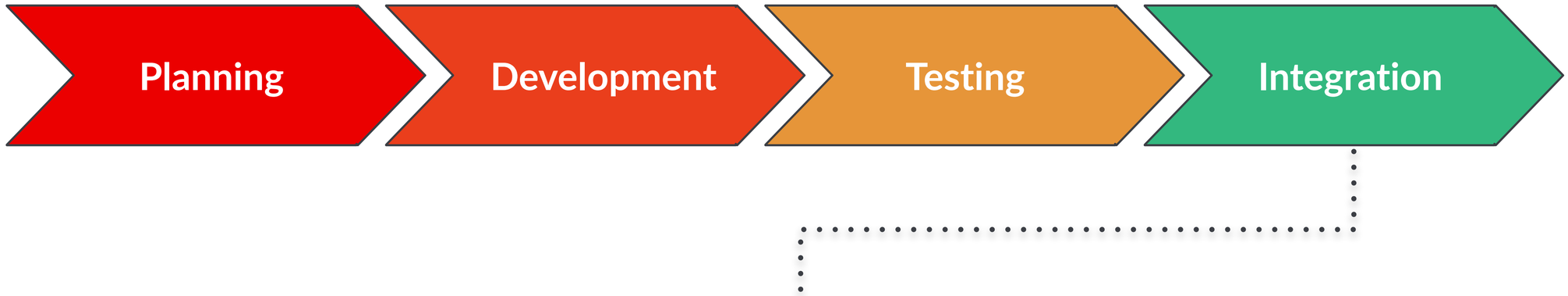


Investment in a framework of choice.
Custom development against a site.
Building in proxy/botnet hooks.

The Software Development Lifecycle

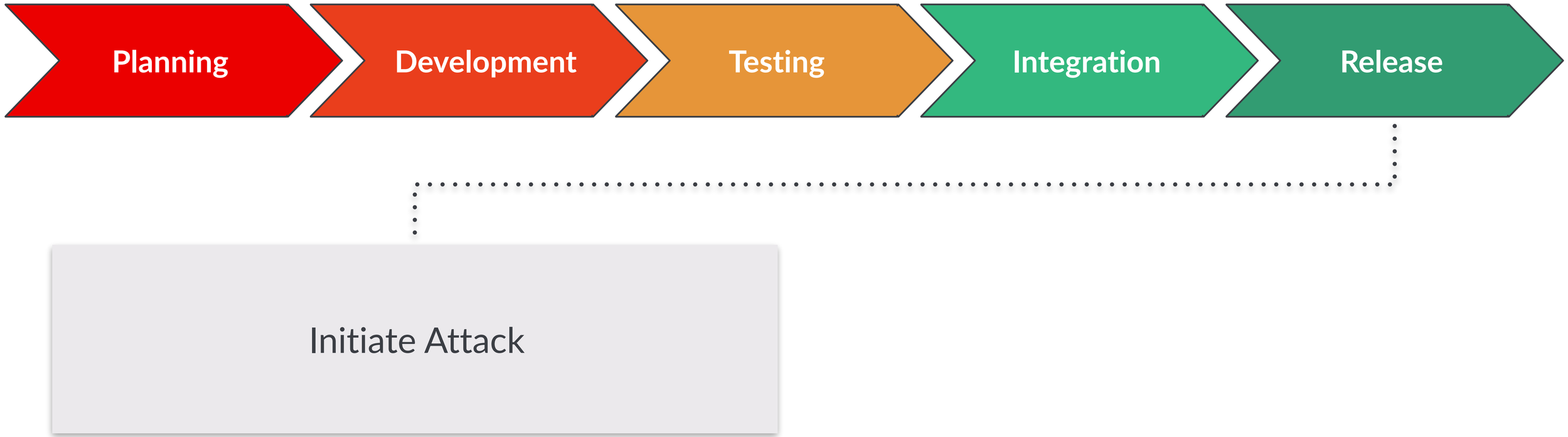


The Software Development Lifecycle

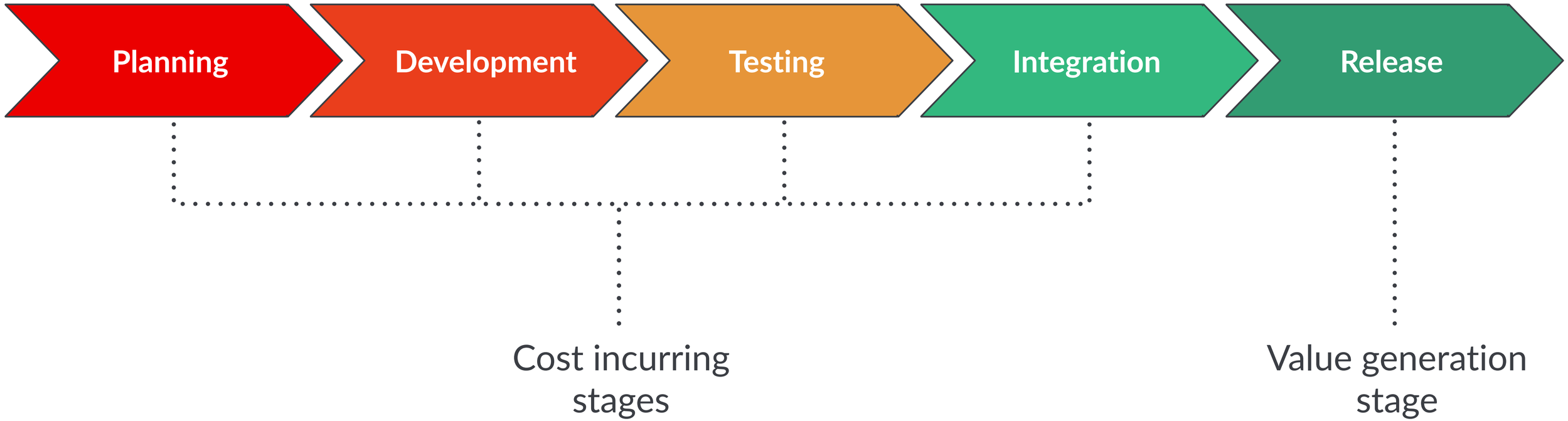


Check integration with botnets.
Ensure health checks work.
Deploy to cloud services.

The Software Development Lifecycle

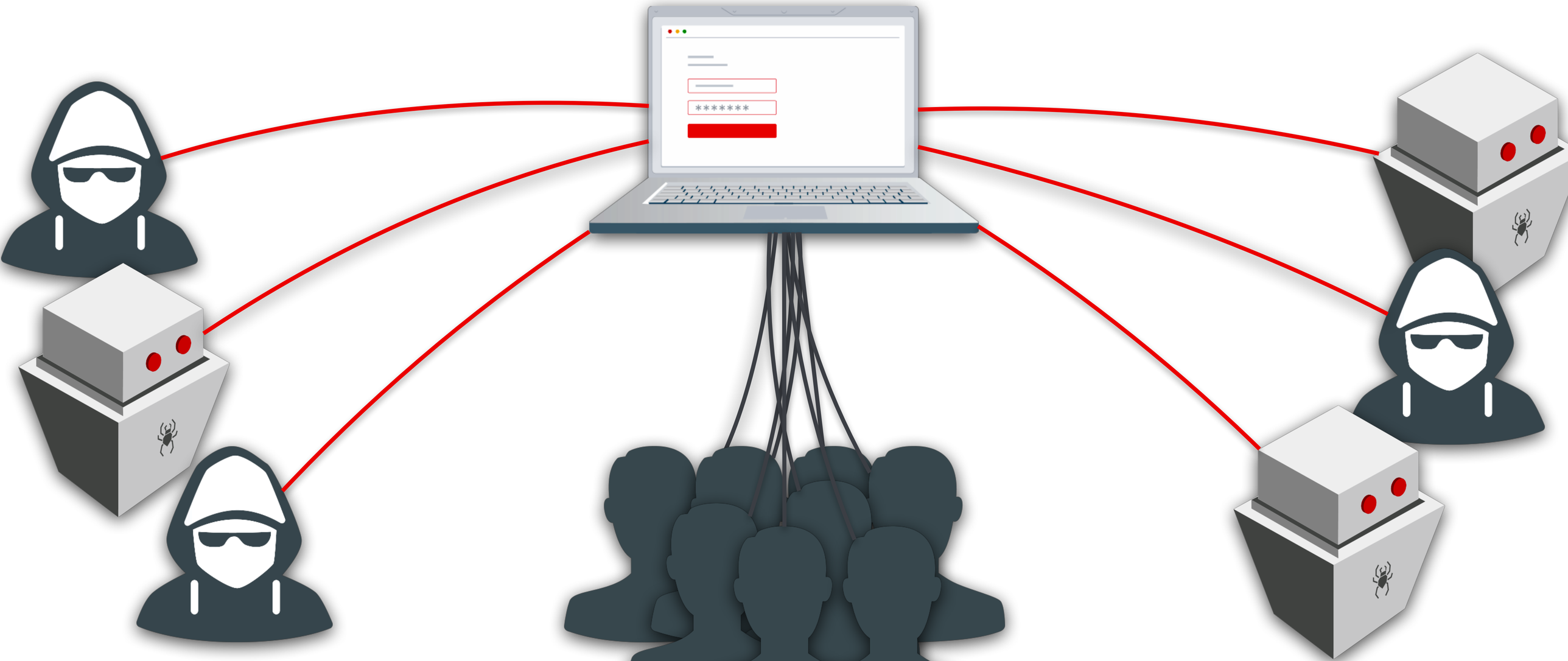


The Software Development Lifecycle

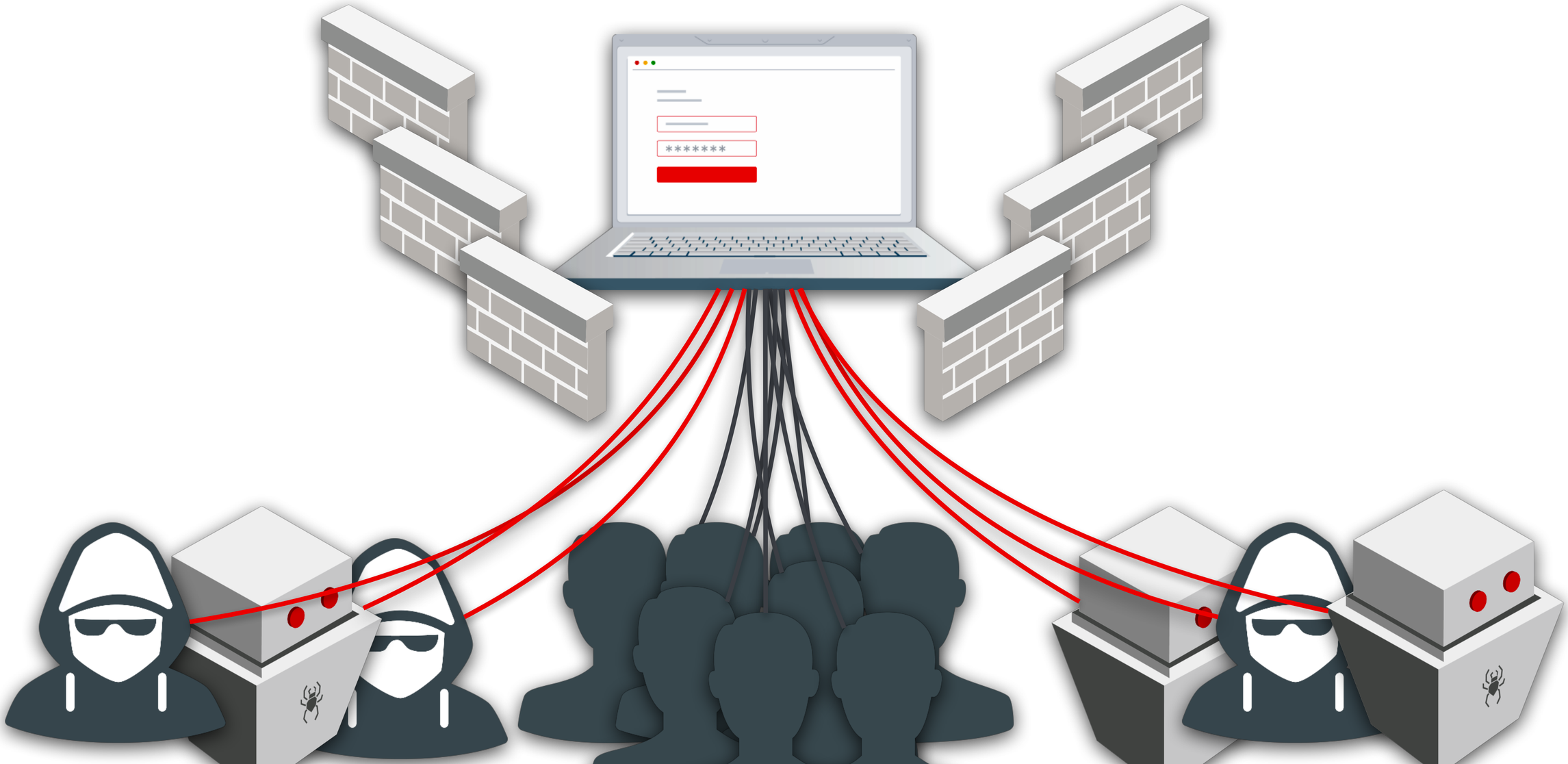


REMEMBER THE WALLS WE PUT UP?

Without feedback, attacks don't evolve.



With feedback the attackers learn how to evolve the tools



This is a problem well suited for AI *on the attacker's side*.

Getting better is a matter of getting the right data.

Apps Installed On Millions Of A

https://www.buzzfeednews.com/article/craigsilverman/how-a-massive-ad-fraud-scheme-exploited-android-phones-to

BuzzFeed News Apps Installed On Millions Of Android Phones Tracke...

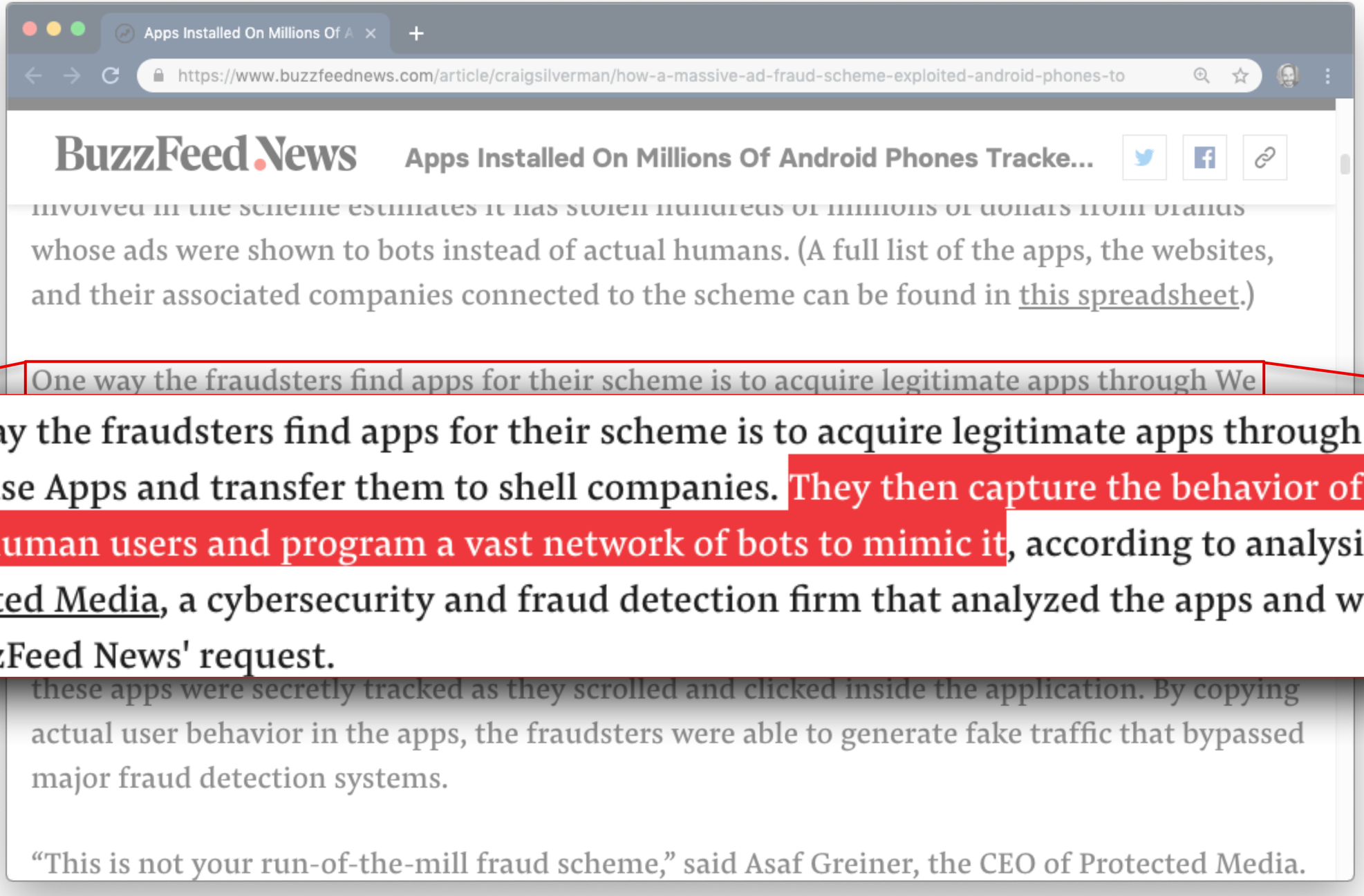
Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme

A BuzzFeed News investigation uncovered a sophisticated ad fraud scheme involving more than 125 Android apps and websites, some of which were targeted at kids.

Craig Silverman
BuzzFeed News Reporter

Posted on October 23, 2018, at 1:07 p.m. ET

Tweet Share Copy



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.

Any score based solution can be gamed.

Researchers Created Fake 'Ma

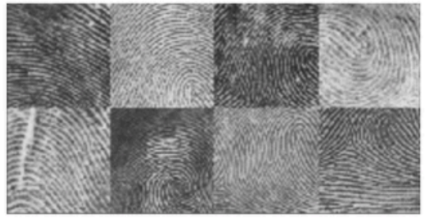
https://motherboard.vice.com/en_us/article/bjenyd/researchers-created-fake-master-fingerprints-to-unlock-smartphones

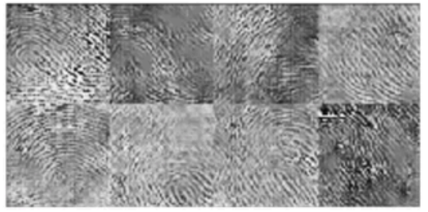
MOTHERBOARD Moveable Hacking Environment Space Gaming Health

Researchers Created Fake 'Master' Fingerprints to Unlock Smartphones

It's the same principle as a master key, but applied to biometric identification with a high rate of success.

SHARE TWEET





Agenda

1. Current attack landscape
2. Attacks in detail
3. The arms race
4. **How do we adapt?**

How do we adapt?

Optimize for speed to response.

- Security & Fraud teams need security features built into products.
- Defenses need dials and knobs that can be adjusted in real time.
- Embrace collaboration and trust across industry and with vendors.

How do we adapt?

Optimize for speed to response.

- Security & Fraud teams need security features built into products.
- Defenses need dials and knobs that can be adjusted in real time.
- Embrace collaboration and trust across industry and with vendors.

Develop hurdles that slow down attackers.

- Vary responses to attackers, limit direct feedback.
- Only enable countermeasures when they're necessary.
- Invest in client side protection.

How do we adapt?

Optimize for speed to response.

- Security & Fraud teams need security features built into products.
- Defenses need dials and knobs that can be adjusted in real time.
- Embrace collaboration and trust across industry and with vendors.

Develop hurdles that slow down attackers.

- Vary responses to attackers, limit direct feedback.
- Only enable countermeasures when they're necessary.
- Invest in client side protection.

Invest in continuous improvement.

- No silver bullet exists, don't be fooled into resting.
- Security & Fraud teams need to be proactive.
- Red teams are worth the cost.

How we do it at SHAPE

Optimize for speed to response.

- Fully scriptable platform. New defenses can be deployed in a day.
- Client-side code generated and composed on the fly.
- Shape collaborates with teams to demotivate sophisticated attackers.

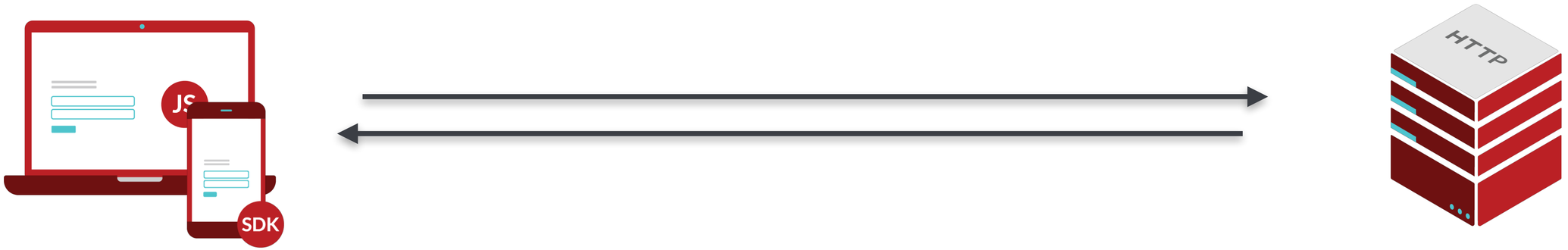
Develop hurdles that slow down attackers.

- JavaScript is compiled to bytecode and randomized automatically.
- Tamper evidence checks alert Shape when a retool is occurring.
- Payloads can be delivered to an attacker to sabotage the development.

Invest in continuous improvement.

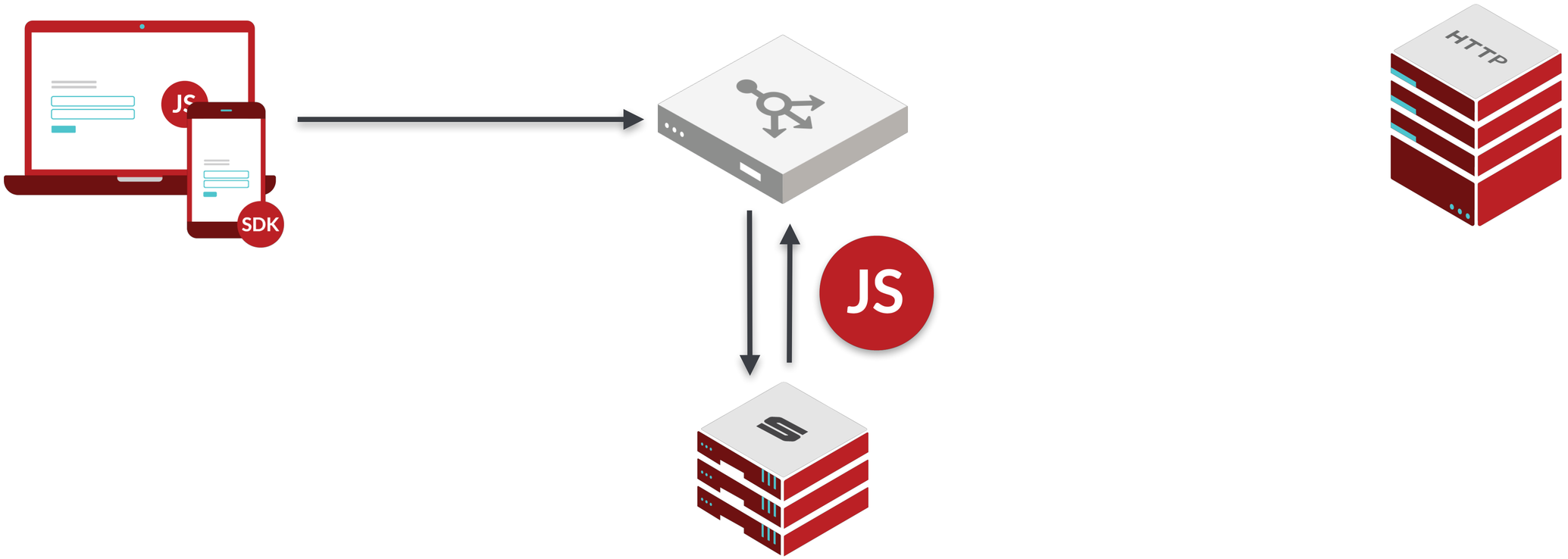
- Shape has been a member of TC-39 (the JS committee) for 4+ years.
- Shape works with browser vendors on specs like CSP, SRI, WebDriver.
- Shape's open source tools are being used to improve the entire internet.

How we do it at Shape



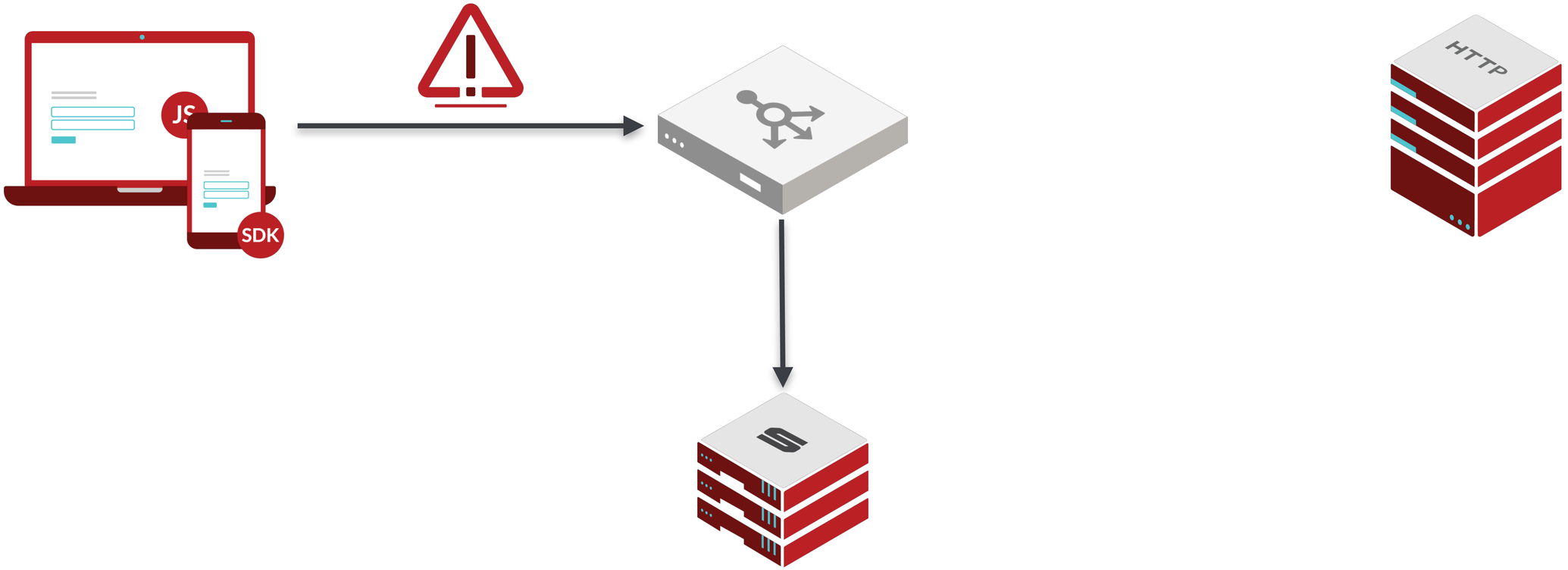
A client makes a request as normal

How we do it at Shape



The client then makes a request for a Shape's JavaScript

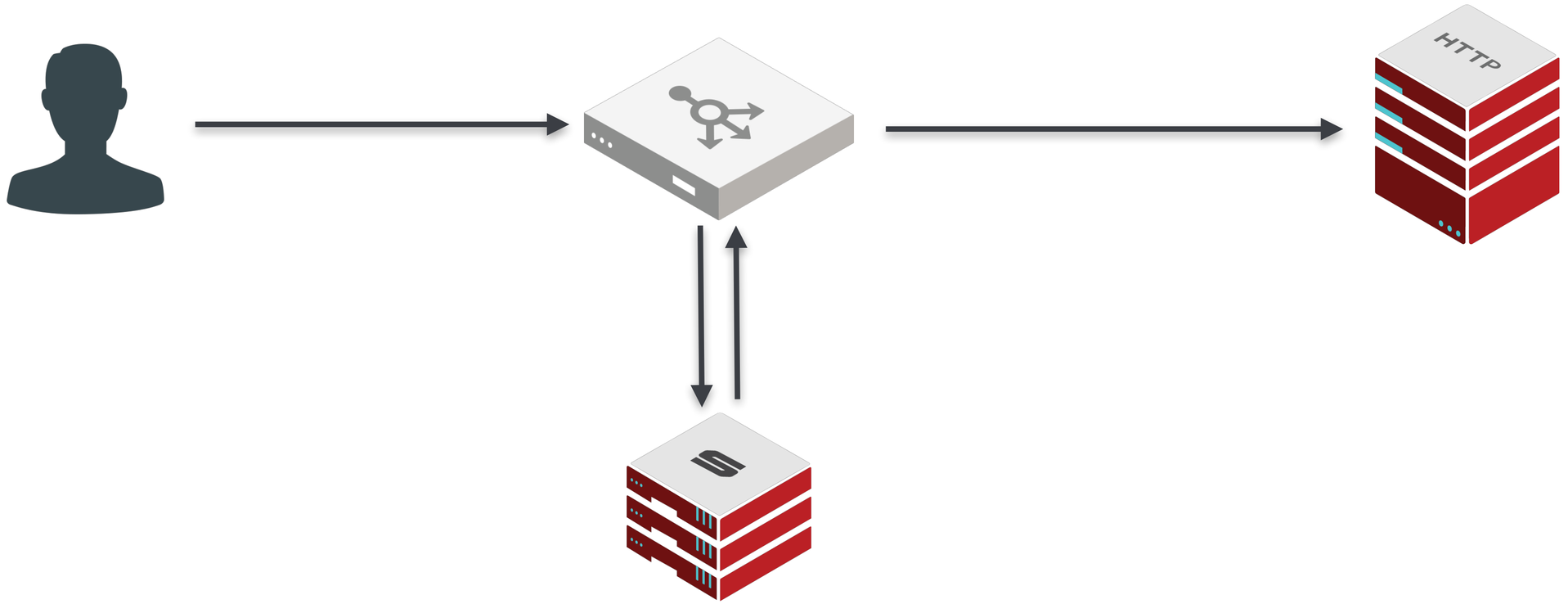
How we do it at Shape



When the client makes a request to a protected URL,

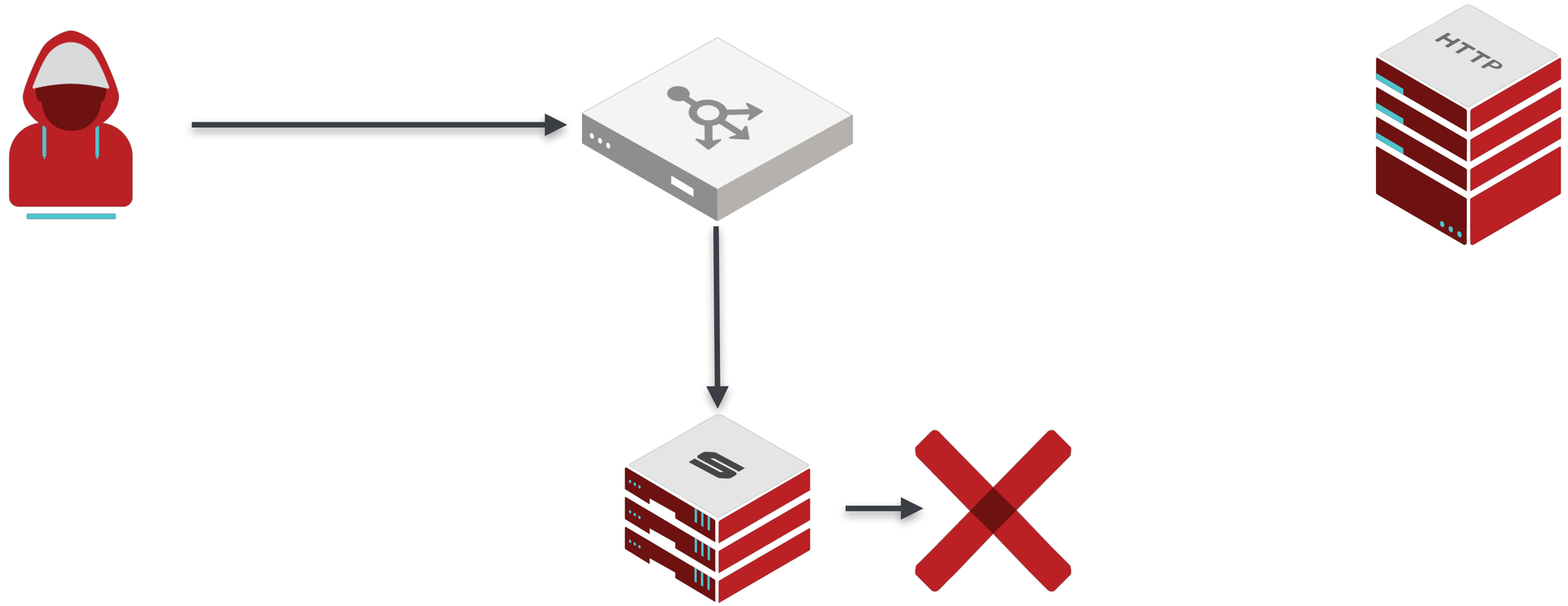
the request is decorated with Shape execution results and telemetry

How we do it at Shape



Legitimate traffic passes through to the originating servers.

How we do it at Shape

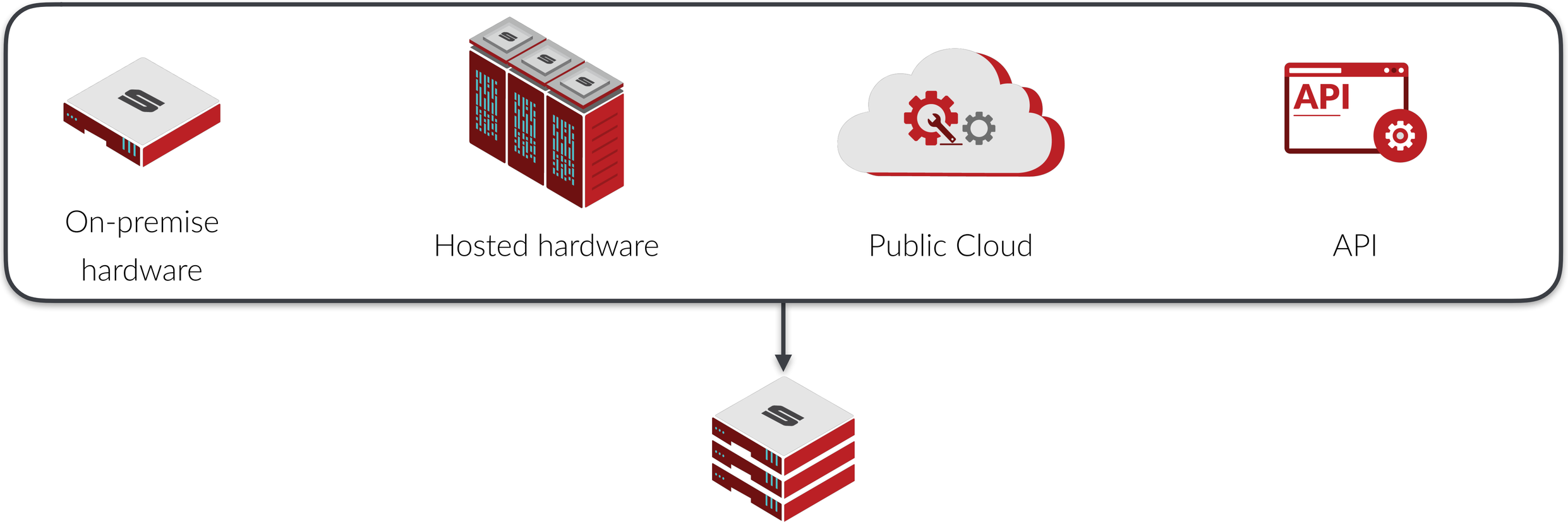


When Shape detects an illegitimate transaction it's stopped.

How we do it at Shape

- JavaScript is compiled to bytecode on the fly
- All JavaScript is generated per-request
- Bytecode + Virtual Machine is regenerated every 5 minutes
- Dozens of tamper evidence checks
- 120+ configurable countermeasure modules
- Returns...
  - User, Environment, Browser Telemetry
  - Execution characteristics
  - Proofs of hardware
  - Proofs of work
  - and much more...

How we do it at Shape

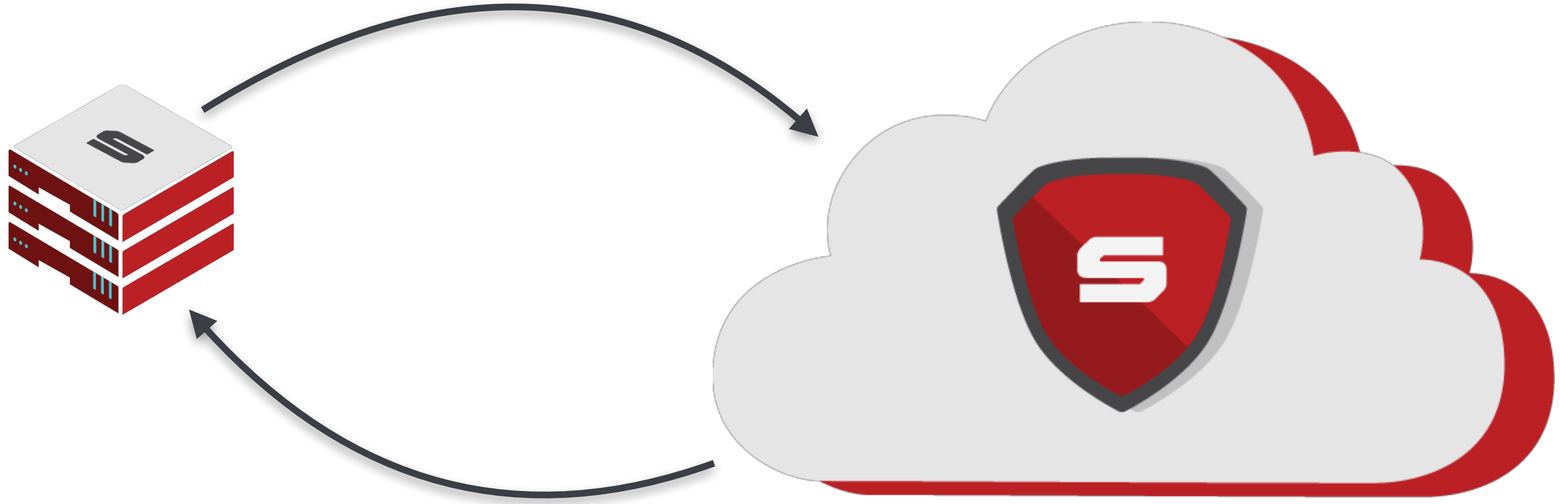


The service is available in many different configurations

How we do it at Shape

The service asynchronously sends the data to Shape's cloud

How we do it at Shape



Where 3 layers of analysis find anomalies and update the service

How we do it at Shape

Service updates regularly to run…

- Generated machine learning models per attacker.
- Custom rules written by security analysts.
- Variable responses designed for advanced attackers.

Thank You!

Jarrod Overson
@jsoverson