Psychology and Security
Demotivating Persistent Attackers

Jarrod Overson - @jsoverson
Director of Engineering, Shape Security

HOW DO YOU ENGAGE WITH ATTACKERS WHILE UNDER ATTACK?

IN THE BEGINNING, **ACCESS** WAS GIVEN TO EVERYONE & EVERYTHING

THE MORE WALLS
WE PUT UP

THE HARDER IT
BECAME TO TELL
HUMANS AND
ATTACKERS APART

TO AFFECT BEHAVIOR, YOU NEED TO REMOVE THE **INCENTIVE**
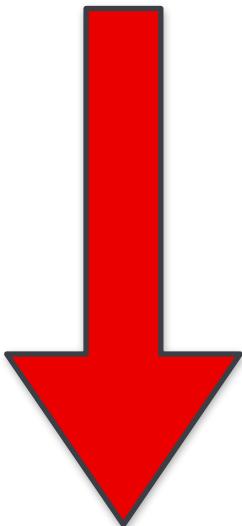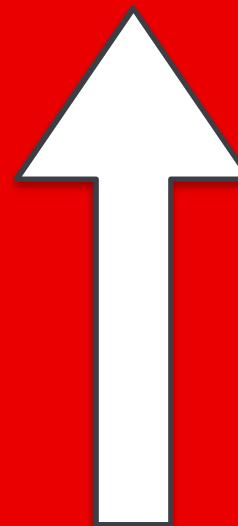
THE SECRET TO DEFEATING ATTACKERS
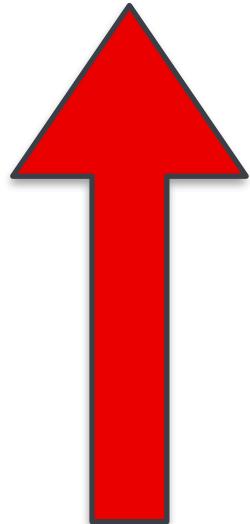
Decrease value

Increase cost
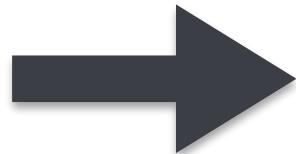
THE SECRET TO HAPPY USERS

Increase value

Decrease cost
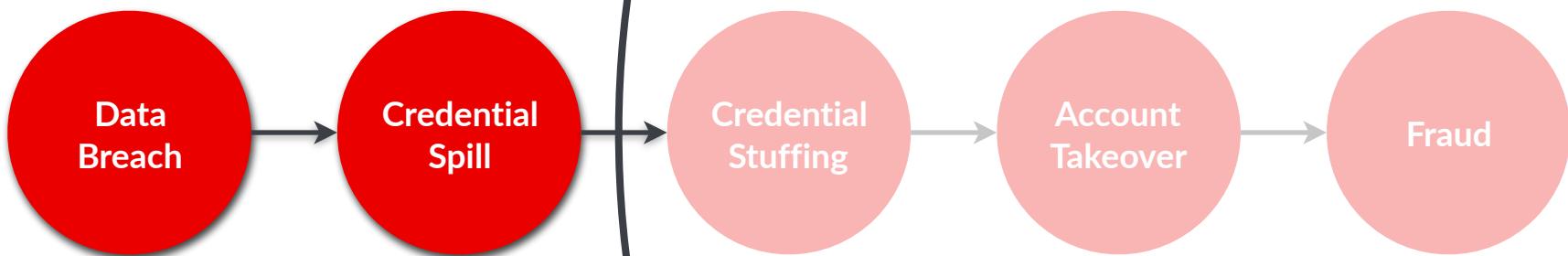
Attack Detail: **Credential Stuffing**

FROM DATA BREACH TO DAMAGE

Outside your control

Data Breach → **Credential Spill** → **Credential Stuffing** → **Account Takeover** → **Fraud**
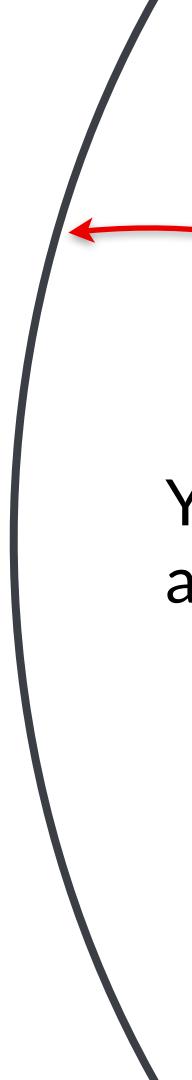
Your web applications and APIs are the battlefield.

CREDENTIAL STUFFING

A STEP BY STEP GUIDE

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.

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

2

HOME GET STARTED INTERNET FINGERPRINT FEATURES SCREENSHOTS SU

ULTIMATE INTERNET PRIVACY

VIRTUAL MACHINE BASED SOLUTION TO BEAT
BROWSER FINGERPRINTING

1. Get Credentials
2. Automate Login

CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login

CREDENTIAL STUFFING

3

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

CREDENTIAL STUFFING

3

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

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

English   Русский

Home | F.A.Q. | API | Order CAPTCHAs | DBC Points | Testimonials | Contact Us

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 s
5 minutes ago: 11 sec
15 minutes ago: 11 sec
Today's average accuracy rate: 90.5 %
(updated every minute)

Create a FREE account

Log In

CREDENTIAL STUFFING

3

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

2Captcha

DASHBOARD   API   Software   StartWork   FAQ   Stat

Solving ReCaptcha V3

2018-06-22 19:02:18

ReCaptcha V3
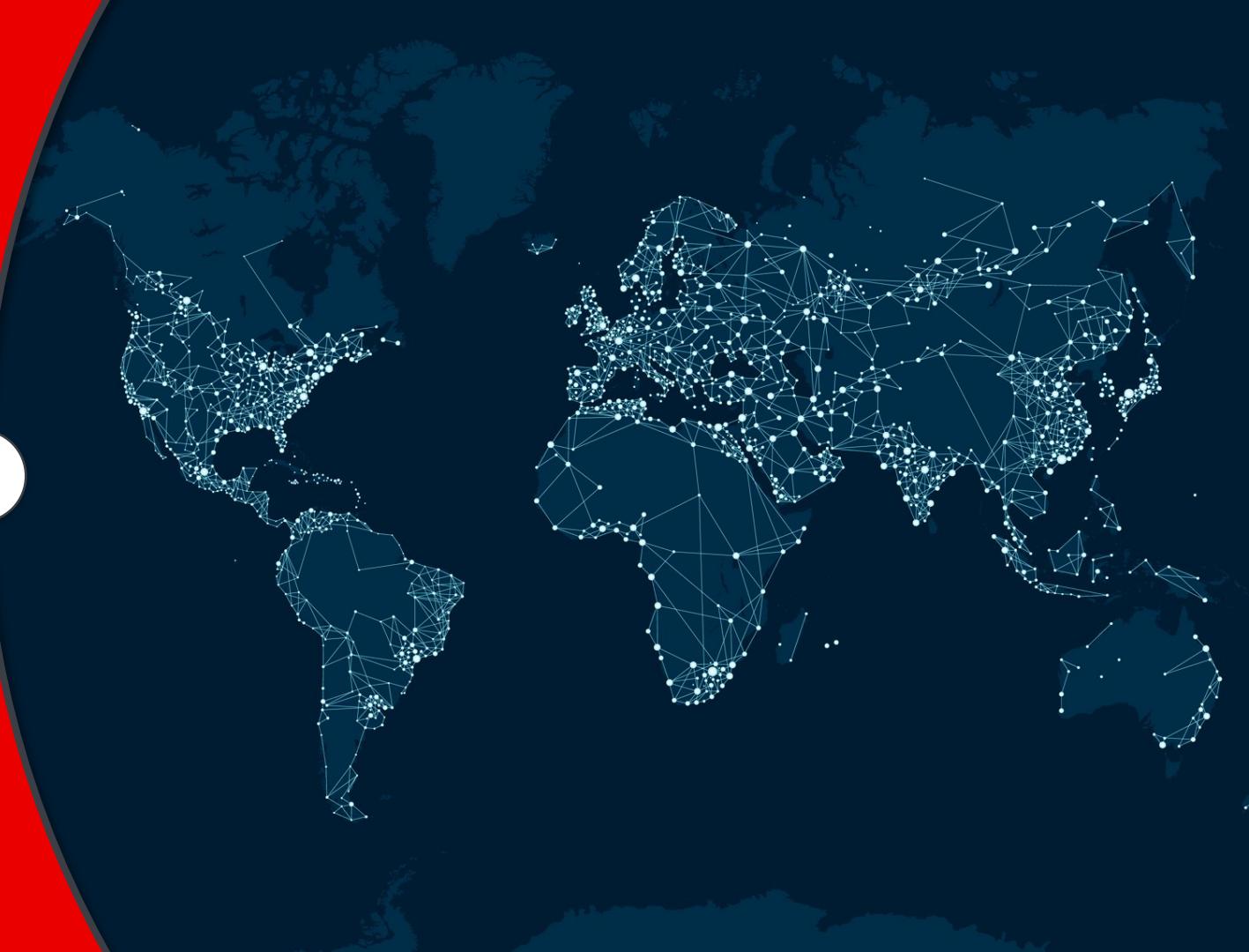
We've been solving ReCaptcha V3 for 3 weeks and are now ready to sh

CREDENTIAL STUFFING

4

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

CREDENTIAL STUFFING

1. Combolists starting at $0
2. $50 per site configuration
3. $1.39 per 1000 CAPTCHAs
4. $2 for 1000 global IPs

Less than $200 for 100,000 ATO attempts

0 Attacker sophistication & where we are

1 The economics of attacks

➡ **2** Flipping the economics in your favor
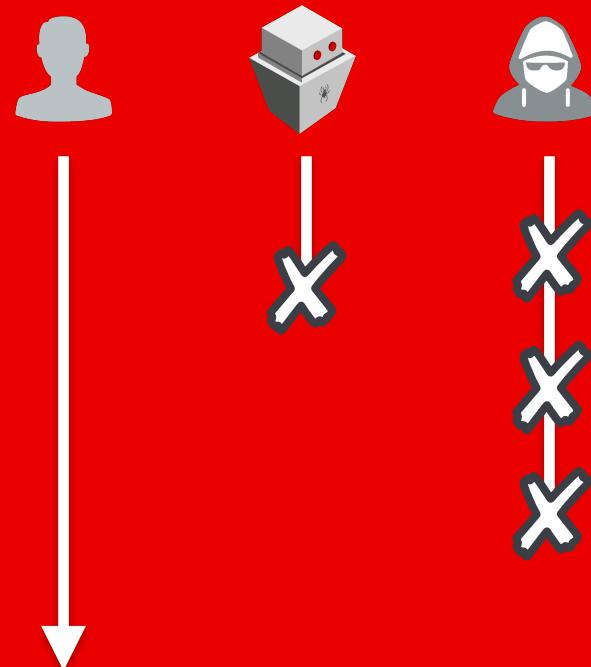
3 Case Studies
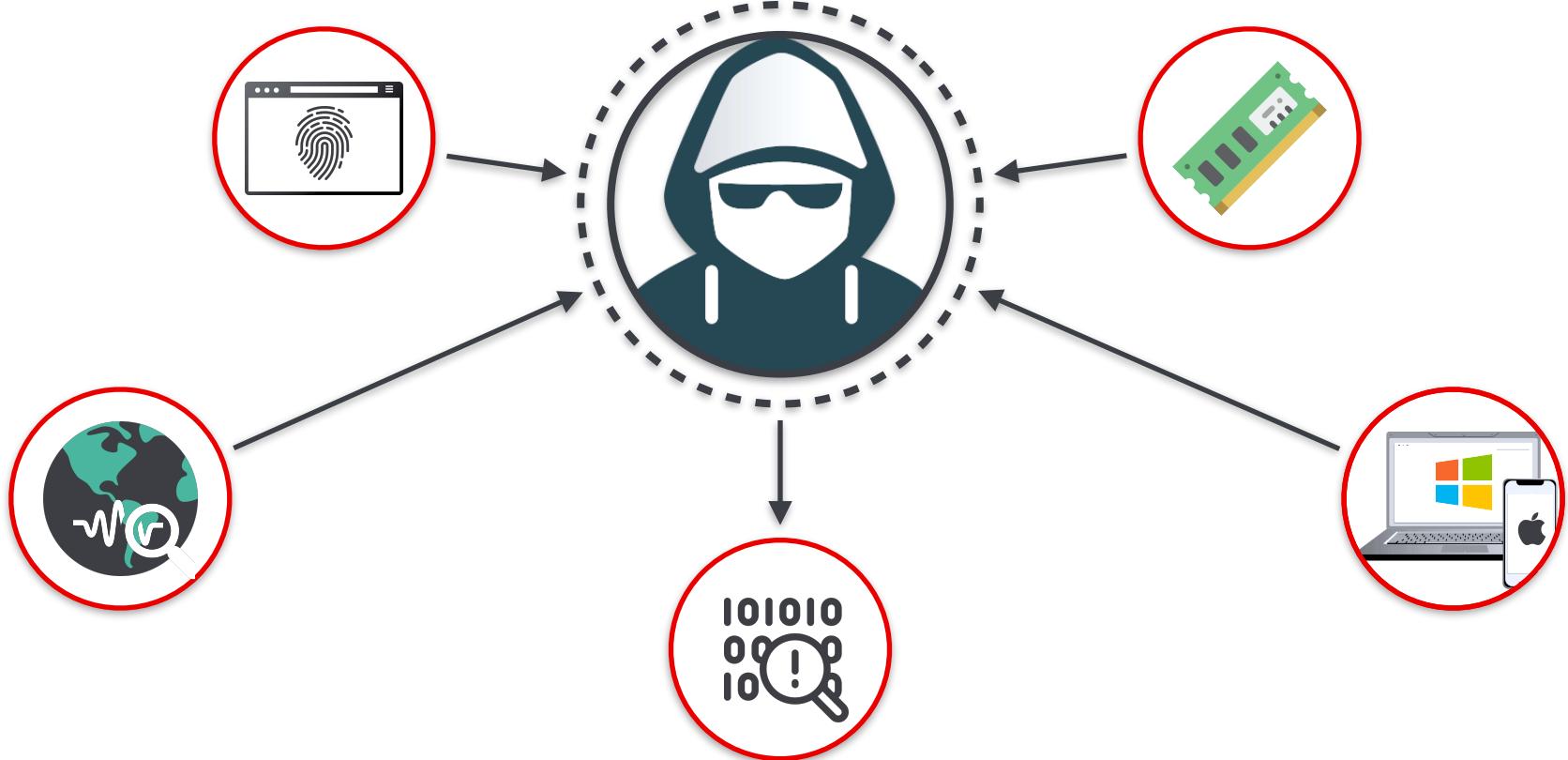
DETECTION VS MITIGATION
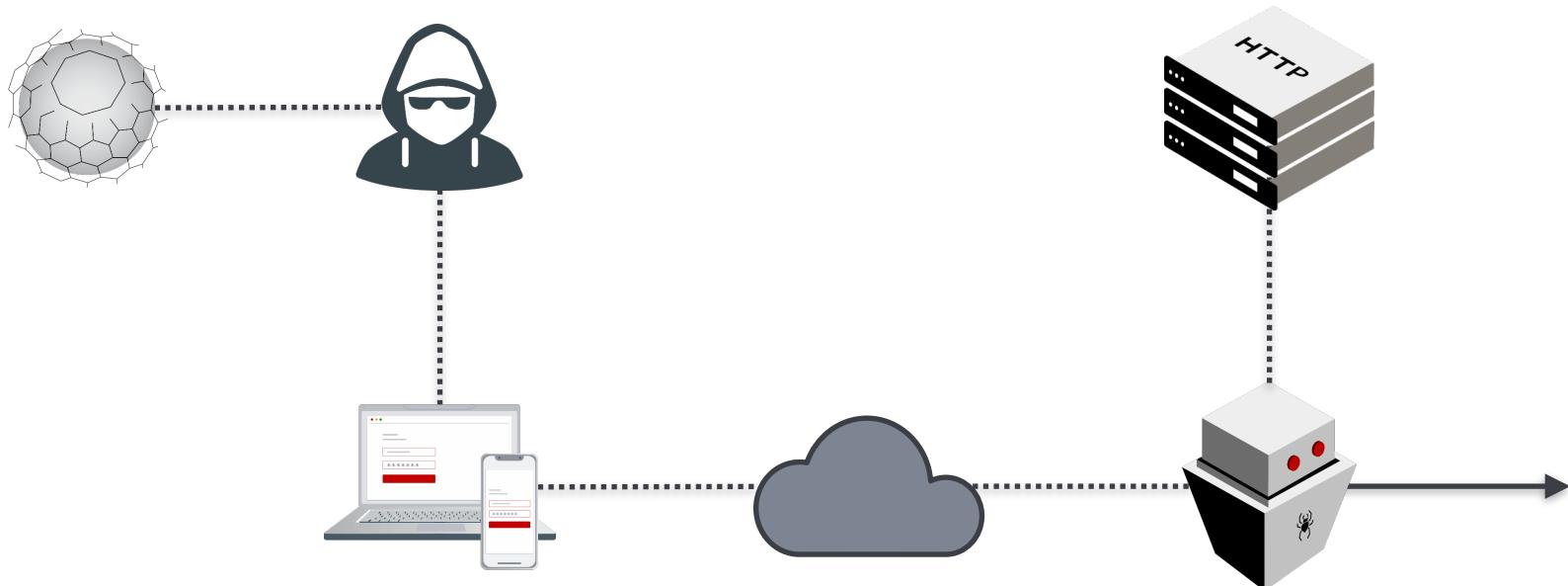
Have multiple ways to detect bad actors

Also have ways to detect when they've started to pry open your systems

TARGET WHAT HURTS THE MOST
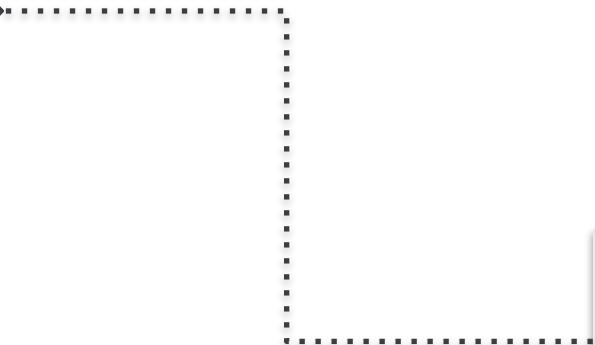
It's not as simple as blocking a baddie.
You need to target what will hurt the most.

THE SOFTWARE DEVELOPMENT LIFECYCLE
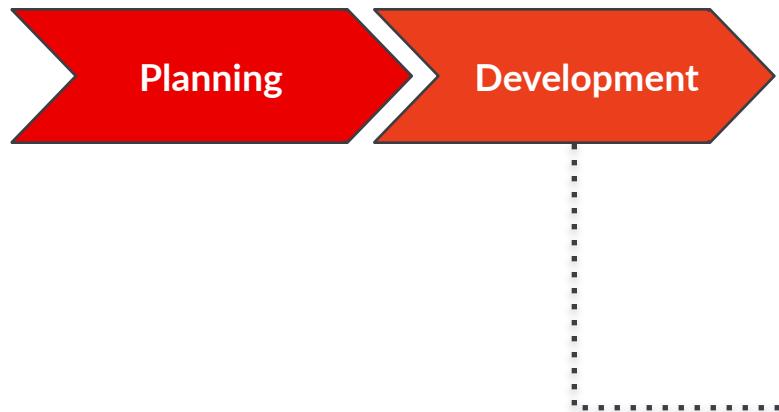
Planning
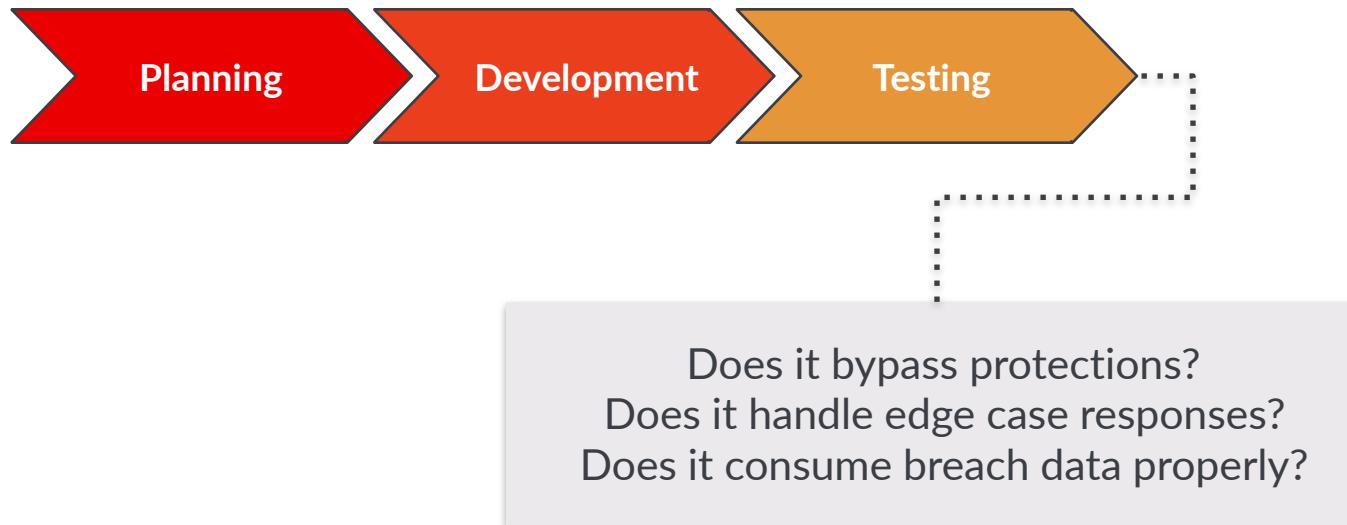
What tools work, what don't?
What URLs need to be targeted?
What dark web data do I need?

THE SOFTWARE DEVELOPMENT LIFECYCLE

Planning
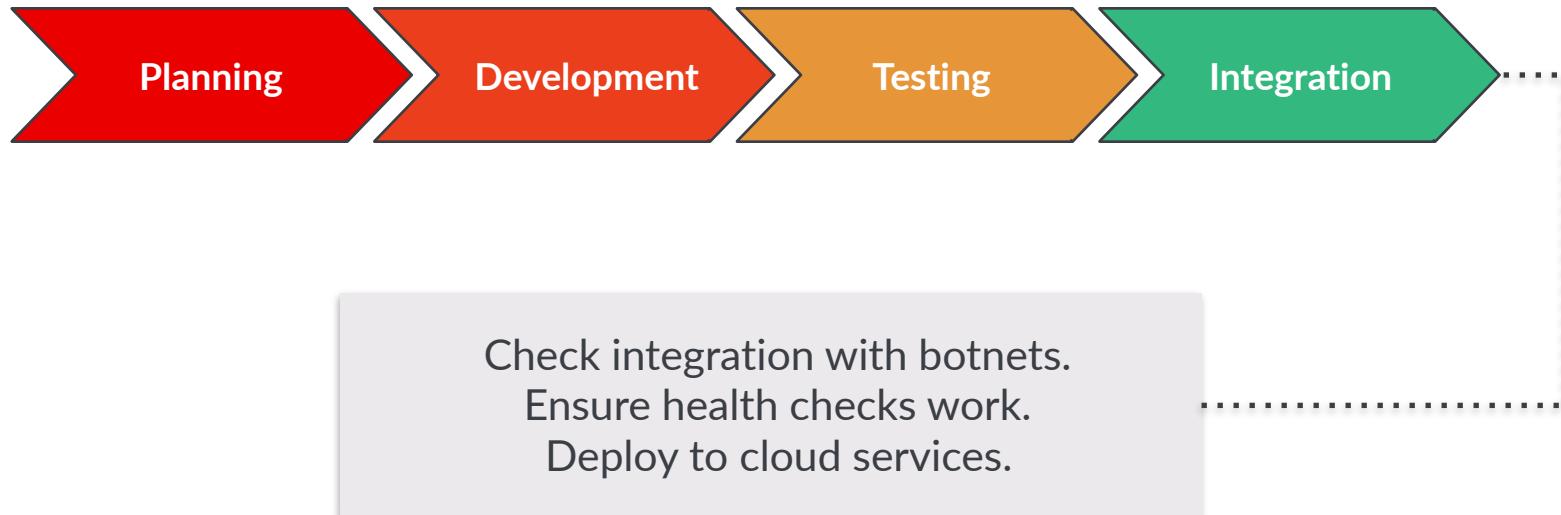
Development

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 breach data properly?

THE SOFTWARE DEVELOPMENT LIFECYCLE

Planning → Development → Testing → Integration

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

THE SOFTWARE DEVELOPMENT LIFECYCLE

| Planning | Development | Testing | Integration | Release |

Initiate Attack

THE SOFTWARE DEVELOPMENT LIFECYCLE

Planning | Development | Testing | Integration | Release

Cost incurring stages

Value generation stage

Case Study 1

Damaging Reputation

Scenario
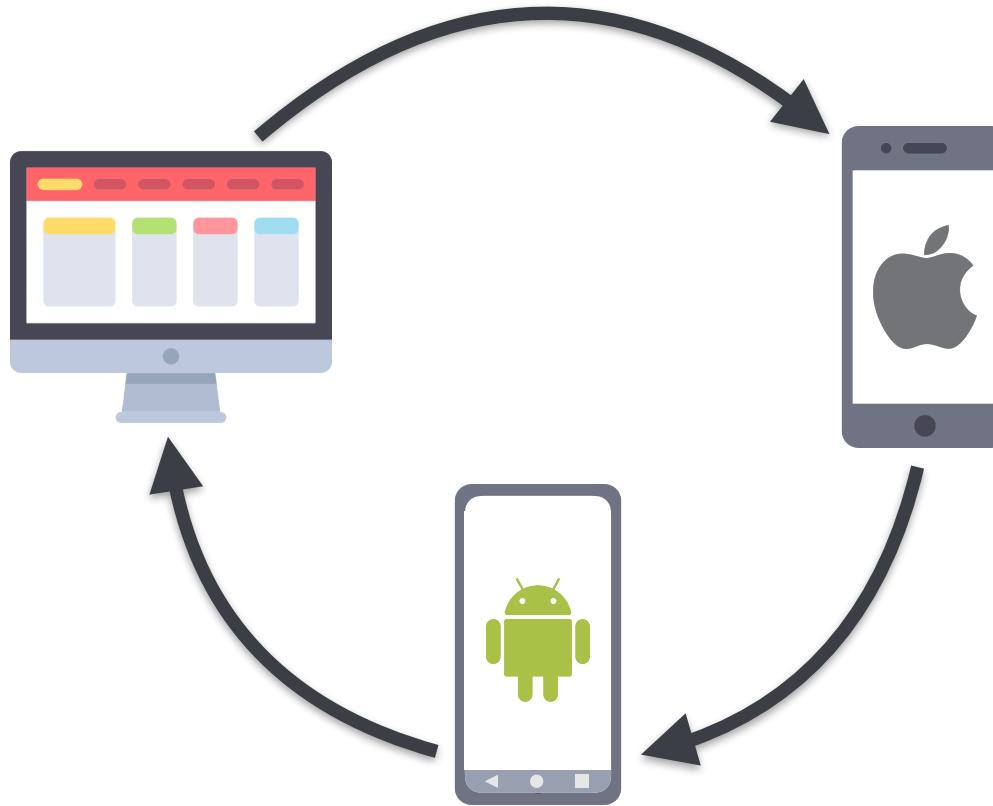
Well funded
scraper

VS
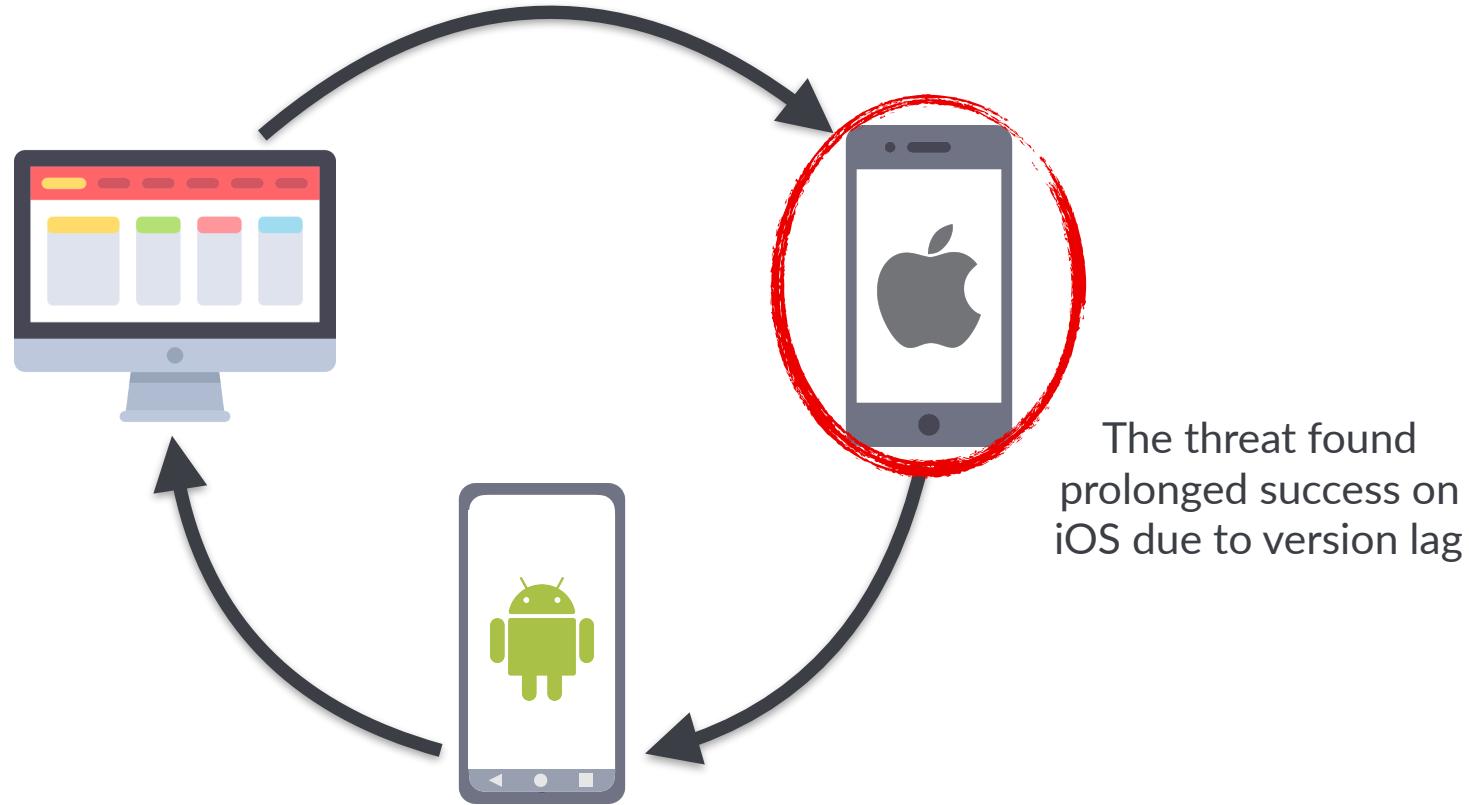
Big US Bank
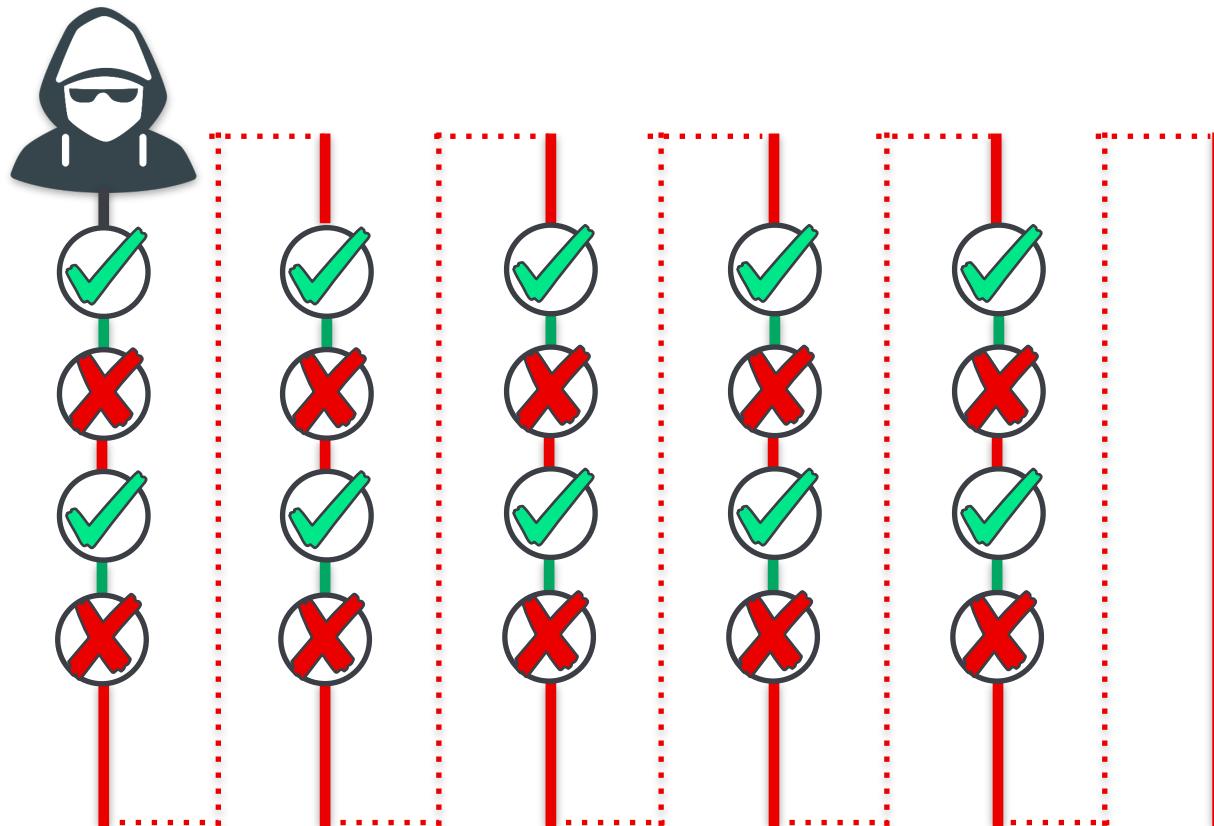
The actor cycled through the softest targets
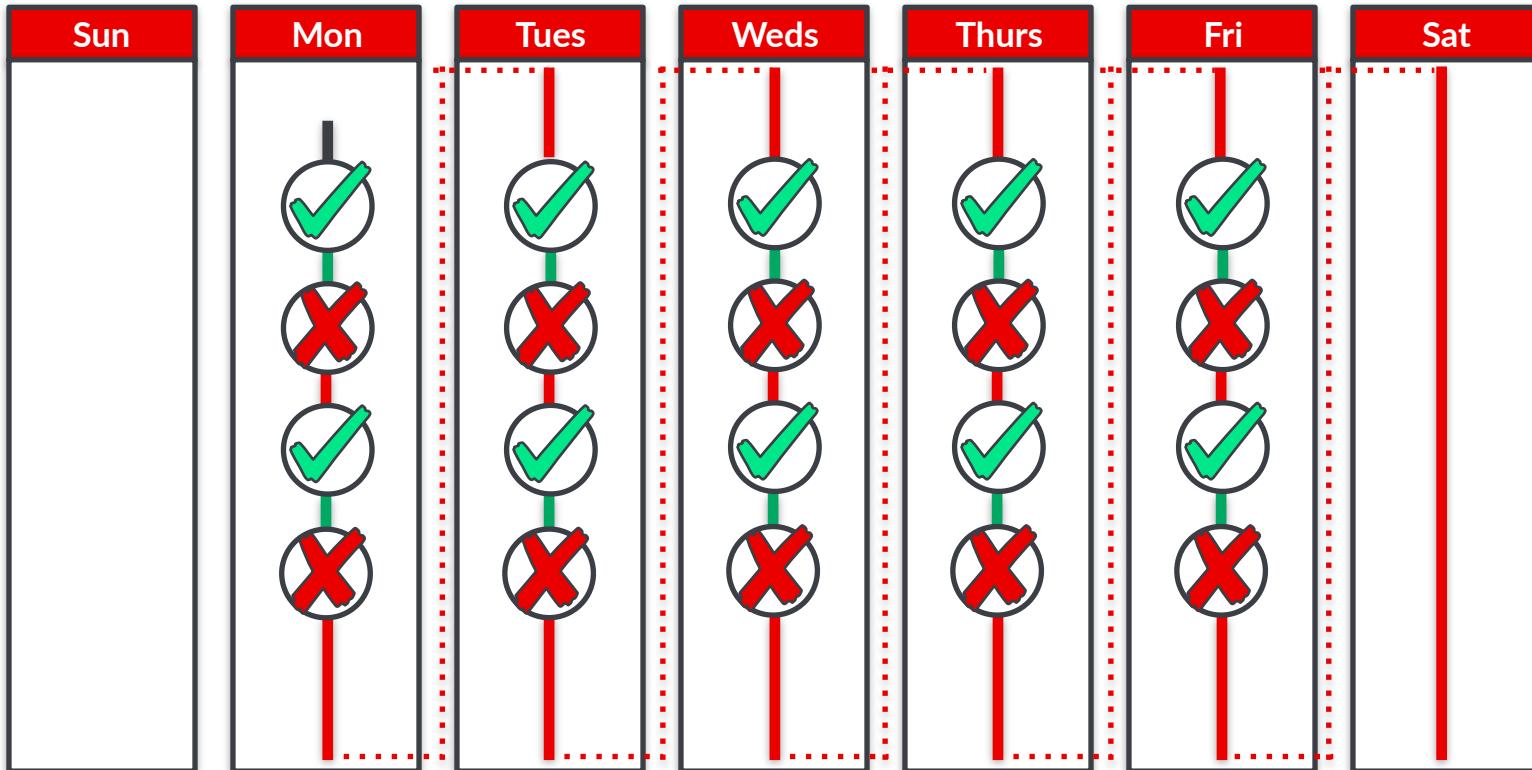
Finally committed to one to dive deeper

The threat found prolonged success on iOS due to version lag

Got around defenses regularly, though not durably

Recognizing patterns in behavior

Analysis

(1) **Regular working schedule**

(2) **Actor's consumers were notified upon success**

(3) **Failure was met with downstream frustration**

(4) **Prolonged failure provoked distress**

Plan of action

1. Target defense out of working schedule

2. Turn on defenses when damage would be highest

3. **Turn off primary mitigation** during working schedule

4. Cycle through defenses even when still working

Case Study 2

Github Kiddies

Scenario
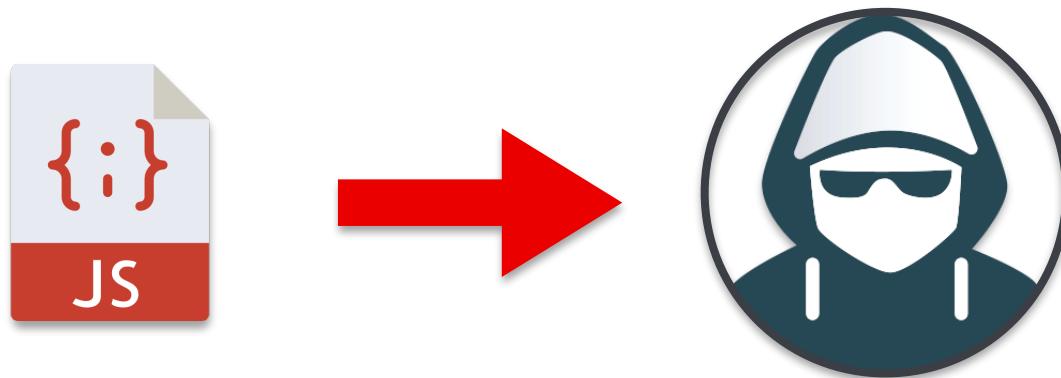
Credential Stuffer
and Account taker-overer

VS

Big US Retailer
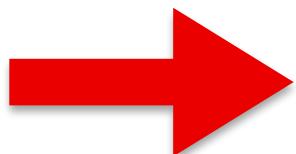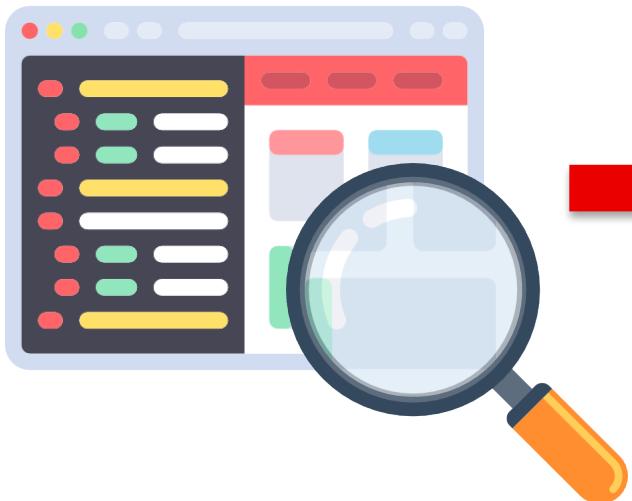
We were down to a fraction of our normal ability to detect
We needed more data

We had enough of a grip to deliver a targeted payload
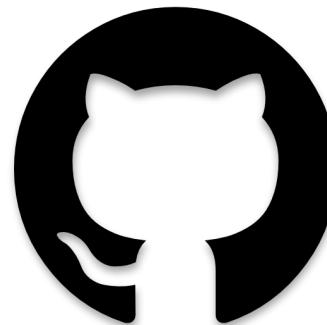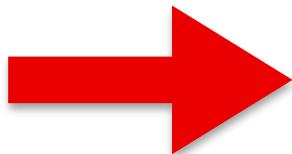
This allowed us to inspect the retooling effort in real time


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

What we learned

Analysis

1 Actor was a competent developer

2 Still relied on community to get around problems

3 Bypassed defenses via trial and error

4 Actor was been lucky, not wildly skilled

Plan of action

1. Build up defenses based on the tool he was using

2. Provide variable feedback during retooling phase

3. Turn on just enough to be infuriating. No more, no less

4. Create new countermeasures that act differently during retooling phase

Recap

1 **Treat detection and mitigation separately.**

2 **Protect the data used to detect.**

3 **Understand what is incentivizing your attackers.**

4 **Work with product to build app-level defenses.**

> *Tactics* is knowing what to do when there is something to do.
>
> *Strategy* is knowing what to do when there is nothing to do.

- Savielly Tartakower