

Psychology and Security

Demotivating Persistent Attackers

Jarrod Overson - @jsoverson
Director of Engineering, Shape Security

InfoSecon 2018

HOW DO YOU
ENGAGE WITH
ATTACKERS
WHILE
UNDER ATTACK?

HOW DO YOU
KNOW YOU
ARE UNDER

ATTACK

IN THE FIRST PLACE?



0

Imitation attacks and attacker sophistication

1

The economics of attacks

2

Flipping the economics in your favor

3

Case Studies

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





A photograph of a wooden gate in a green field. The gate is made of light-colored wood and has a black rectangular sign attached to its left post. The sign contains the white, bold text "PLEASE CLOSE GATE". The gate is slightly open, revealing a dirt path leading into a large, lush green field. In the background, there is a dense line of trees and bushes. A prominent, very tall and thick tree trunk is visible on the right side of the frame. The entire image is framed by a red border.

PLEASE
CLOSE
GATE

A photograph of a paved walkway with a yellow gate barrier. The walkway is made of grey concrete and has a yellow metal gate arm extending across it. To the right of the gate is a yellow control box with a small screen and a keypad. The background shows a grassy area with some bushes and trees.

GATE, YOU HAD ONE JOB

TO AFFECT BEHAVIOR,
YOU NEED TO
REMOVE THE
INCENTIVE

MANUAL ATTACKS

Sufficient when value is high

Can't scale when value per attack is reduced



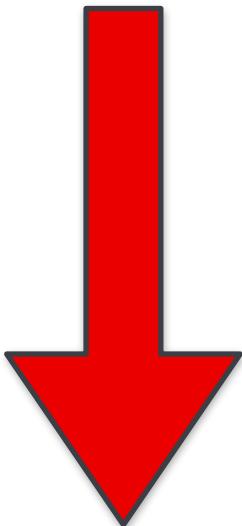
AUTOMATED ATTACKS

Sufficient when value is low

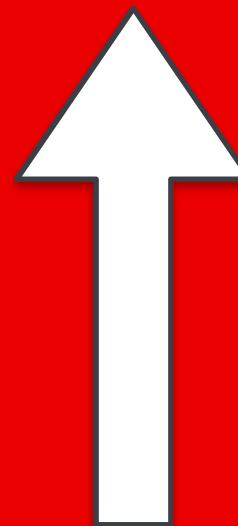


Can't scale when cost per attack is increased

THE SECRET TO DEFEATING ATTACKERS

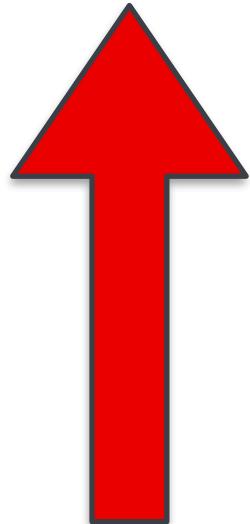


Decrease value



Increase cost

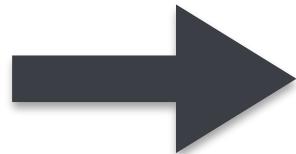
THE SECRET TO HAPPY USERS



Increase value



Decrease cost



0

Attacker sophistication & where we are

1

The economics of attacks

2

Flipping the economics in your favor

3

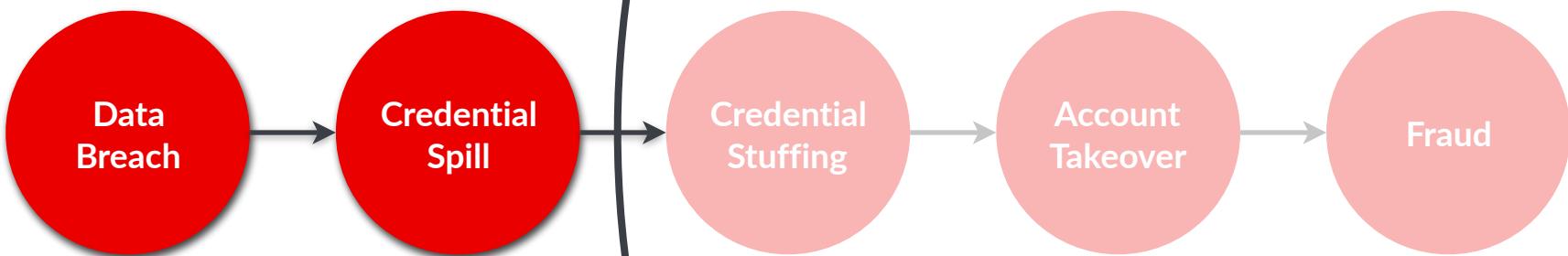
Case Studies

Attack Detail: Credential Stuffing

FROM DATA BREACH TO DAMAGE

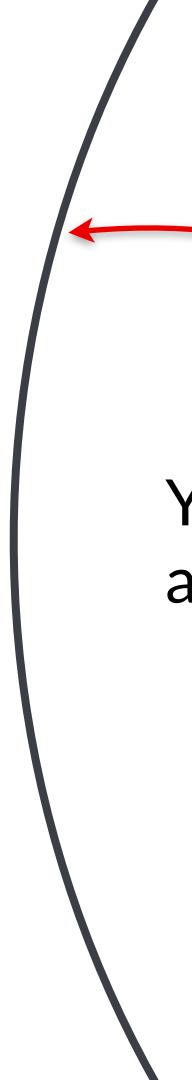


Outside your control



Within your control





Your web applications and APIs
are the battlefield.

CREIDENTIAL STUFFING

cre·den·tial stuff·ing

/krə'den(t)SHəl 'stəfɪNG/

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

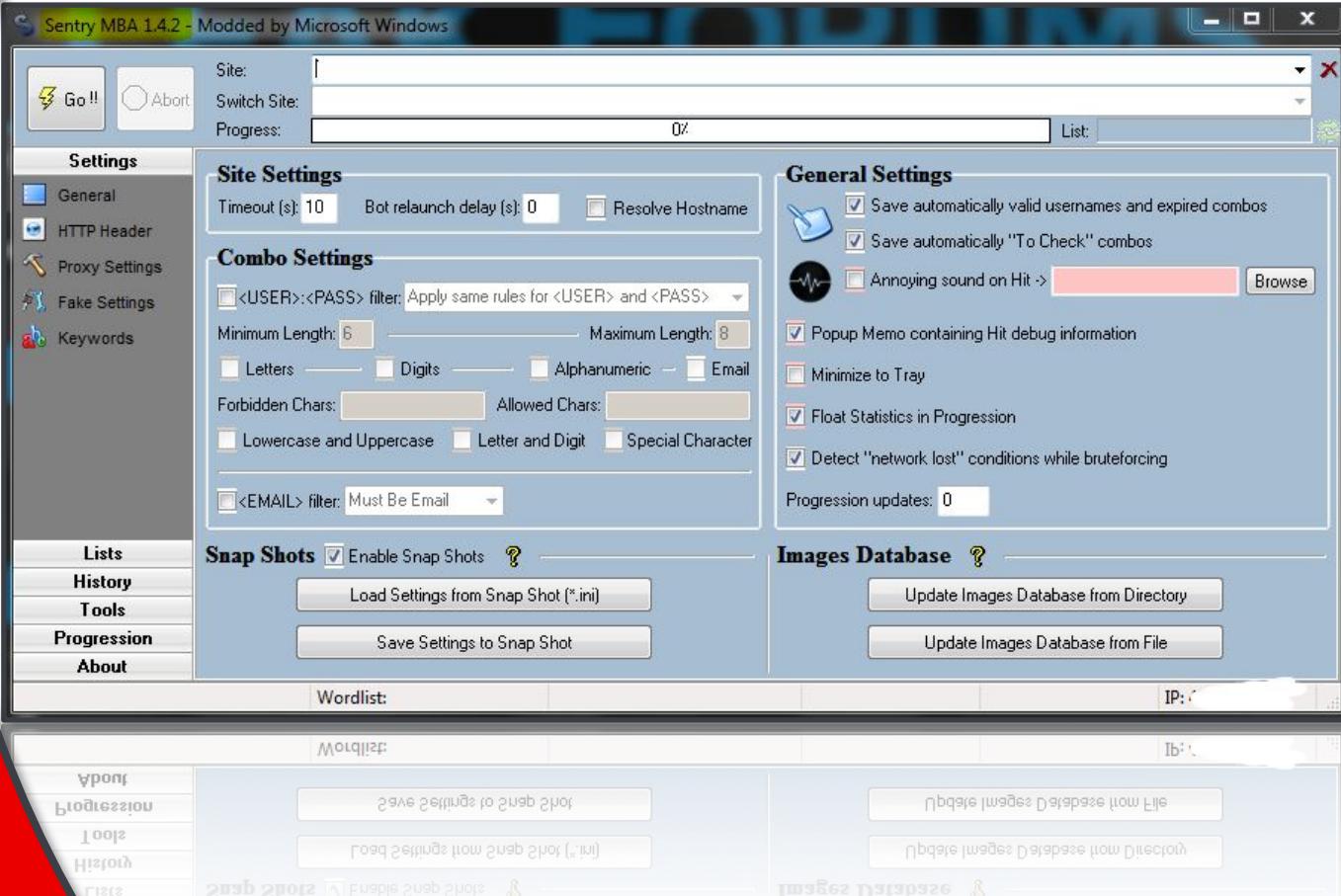
1. Get Credentials

-  **Email:Password** 500K Combo Mixed [EMAIL:PASS] (Netflix, Fortnite, PornHub, Spotify, Cruny) by geroZ
-  **Email:Password** 100K GMAIL Combos[EMAIL:PASS] (Spotify, Deezer, Crunchy, Netflix, uPlay, St by xanoob
-  **Kayo.moe** by jafo
-  **Email:Password** 84k FR Hq Combolist (Music,Shopping,Spotify) 11 Oct 2018 by mzcombo
-  **User:Password** 100k User pass Sqli Paid HQ Combolist (Streaming Sites) 11 Oct 2018 by mzcombo
-  **Email:Password** 572k USA HQ Combolist (Spotify,Netflix,Vpn,Uplay) 11 Oct 2018 by mzcombo
-  **Email:Password** 35k Indian Combo List Private HQ Combo List [1 2] by RuwanMax
-  **Email:Password** [EMAIL:PASS] 401K HQ Combo [Minecraft, VPN, Fortnite, Netflix, Spotify, Por by orlando
-  **Email:Password** 215K HQ Combo [Email:Pass][Minecraft, VPN, Fortnite, Netflix, Spotify, Porn by geroZ
-  **Email:Password** [EMAIL:PASS] 340K HQ Combo [Minecraft, VPN, Fortnite, Netflix, Spotify, P by xanoob
-  **Email:Password** 532K HQ Compro [Email:Pass][Minecraft, VPN, Fortnite, Netflix, Spotify, P by geroZ
-  **Email:Password** 532K HQ Compro [Email:Pass][Minecraft, VPN, Fortnite, Netflix, Spotify, P by geroZ

CREDENTIAL STUFFING

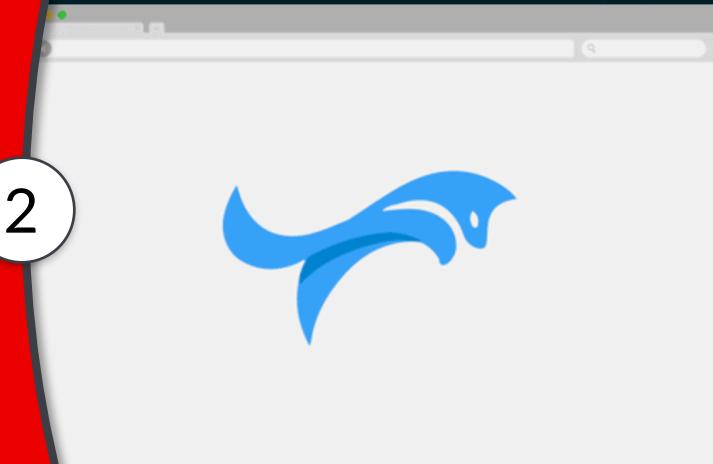
1. Get Credentials
2. Automate Login

2



CREDENTIAL STUFFING

1. Get Credentials
2. Automate Login



2

HOME

GET STARTED

INTERNET FINGERPRINT

FEATURES

SCREENSHOTS

SU

ULTIMATE INTERNET PRIVACY

VIRTUAL MACHINE BASED SOLUTION TO BEAT
BROWSER FINGERPRINTING



CREIDENTIAL STUFFING

2

1. Get Credentials
2. Automate Login

Browser Antidetect FF+IE: Ver 5.0.0.2 C927-EA72-CBF6-9438

Change Skin Resolution (IE & System): 1024x768 Apply

Profiles & Generator Directories, to save with profiles and load with profiles: Configs:

Save Load

Firefox Exactly Generator

Browser Type: Opera Language: English-US (en-US) Or YOUR language: Static UA

OS (name, ver): Windows NT 6.1 Browser Version: 12.00a Or YOUR version: OSCPU

Mobile Device: LG-L160L Build/IML74K Flash Version: 11.6.602.180 Resolution (FF & Flash): Random

Shortcut to browsers: + IE + System language + Reboot + Resolution Generate

License Registered to: Realy | Special for Opensource

CONFIG NOTES NEWS DECODER PHONES

JavaScript Config

```
{ "window.screen": { "availHeight": 768, "availLeft": 1366, "availTop": 768, "availWidth": 1366, "clientHeight": 768, "clientWidth": 1366, "colorDepth": 32, "height": 768, "left": 1366, "offsetHeight": 768, "offsetWidth": 1366, "pixelDepth": 32, "top": 768, "width": 1366 }, "window.navigator": { "userAgent": "Opera/12.00a (Windows NT 6.1; en-US) Presto/4.1.23 Version/12.00a", "comment": "" } }
```

HTTP Headers

```
{"headers": [{"action": "Add", "name": "User-Agent", "value": "1122", "comment": "", "enabled": true}, {"action": "Modify", "name": "Accept-Language", "value": "en-us", "comment": "", "enabled": true} ]}
```

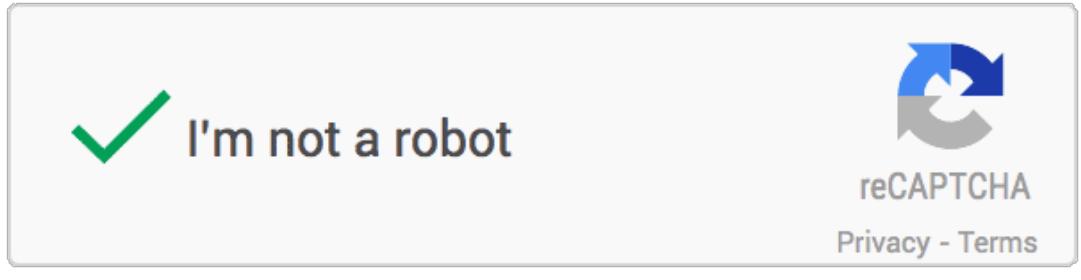
SAVE ALL CONFIGS

DISCLAIMER: This software is designed for ethical hacking and penetration testing. It is illegal to use this software for unauthorized access to computer systems. The developer is not responsible for any misuse of this software.

CREDENTIAL STUFFING

3

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



CREDENTIAL STUFFING

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

The screenshot shows the homepage of Death by CAPTCHA. At the top, there's a navigation bar with links for Home, F.A.Q., API, Order CAPTCHAs, DBC Points, Testimonials, and Contact Us. Below the navigation is a large green banner with the text "STATUS: OK". To the right of the banner, there's a sidebar with a timestamped log of solving times and accuracy rates. On the left side of the main content area, there's a large number "3" inside a white circle. The main content area features a heading "Best CAPTCHA Solver Bypass Service" and a paragraph explaining how the service works. It also includes a note about research projects and legal use, a section for offers, and a "Create a FREE account" button.

DEATH BY CAPTCHA
FASTEAST DISCOUNT CAPTCHA SOLVERS

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

STATUS: OK

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

3

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.

Create a FREE account

Log In

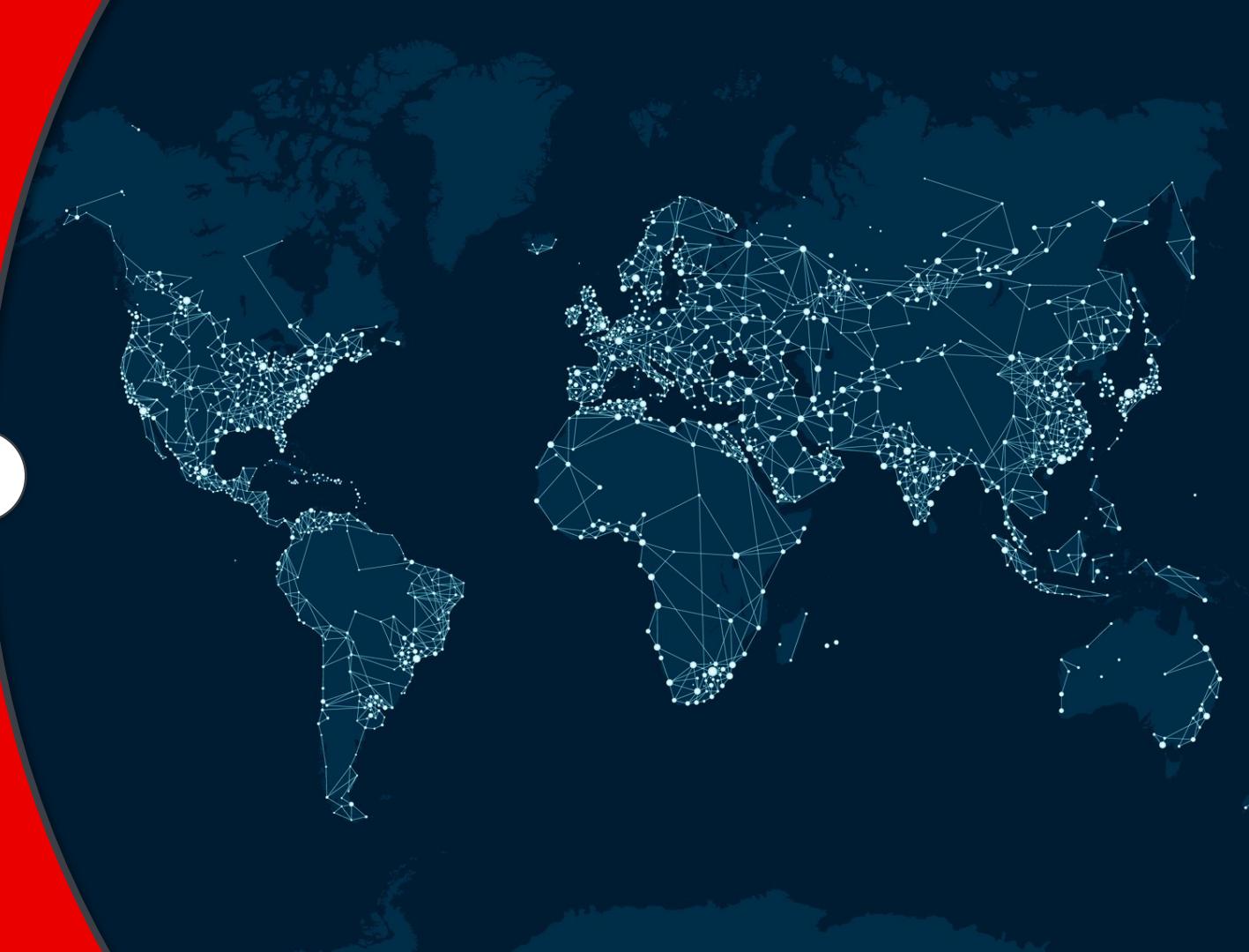
Forgot password?

Create a FREE account

CREDENTIAL STUFFING

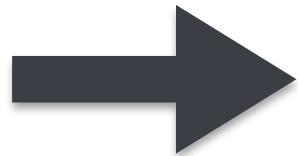
4

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

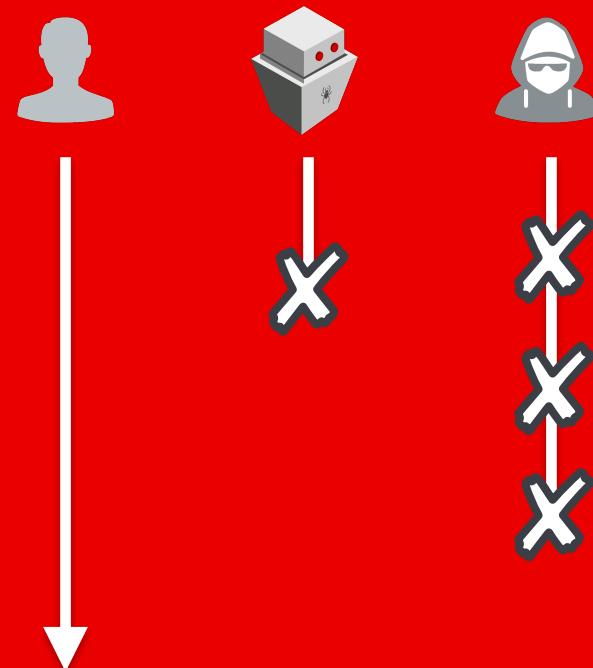
3

Case Studies

DETECTION

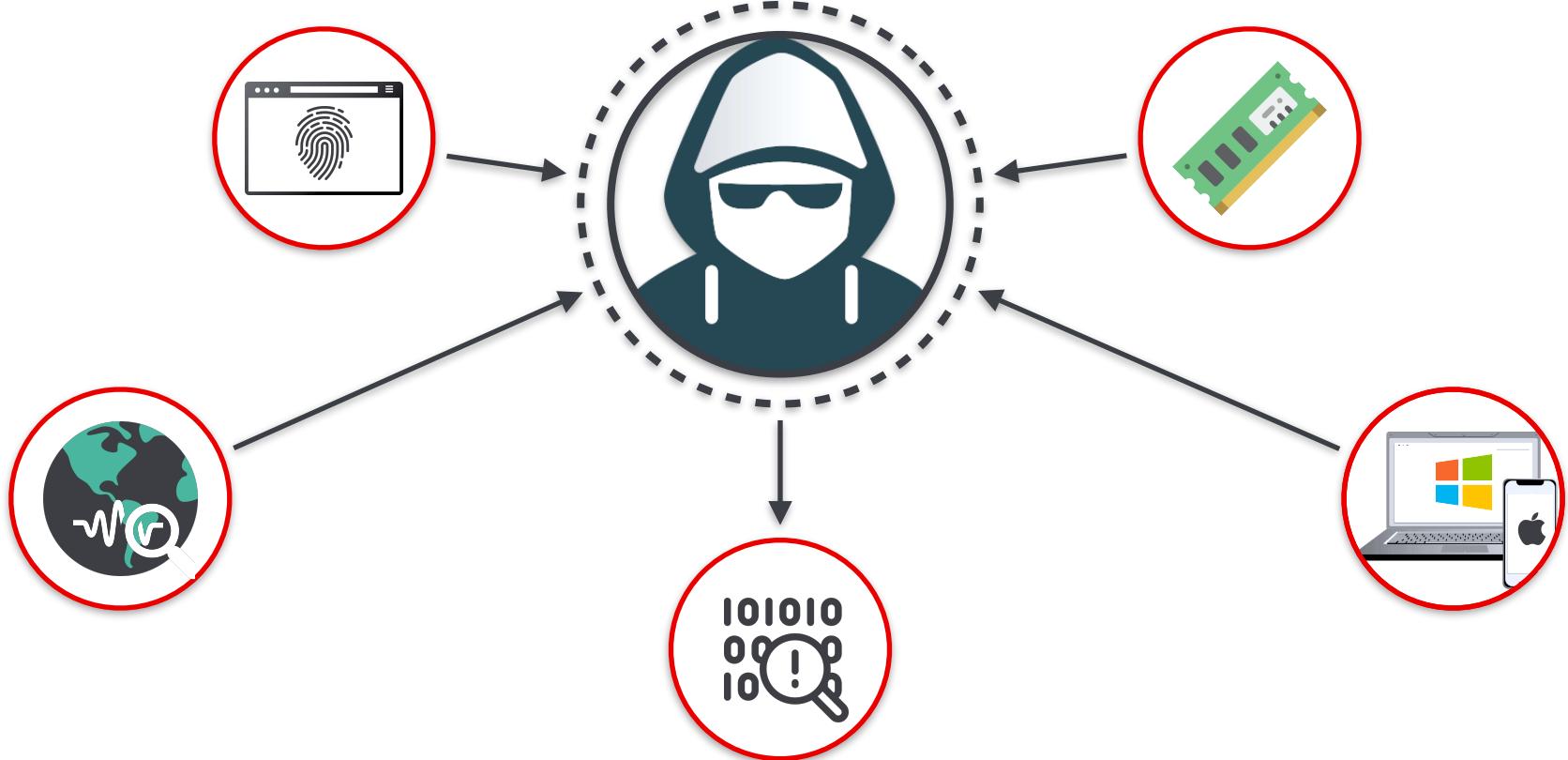
VS

MITIGATION



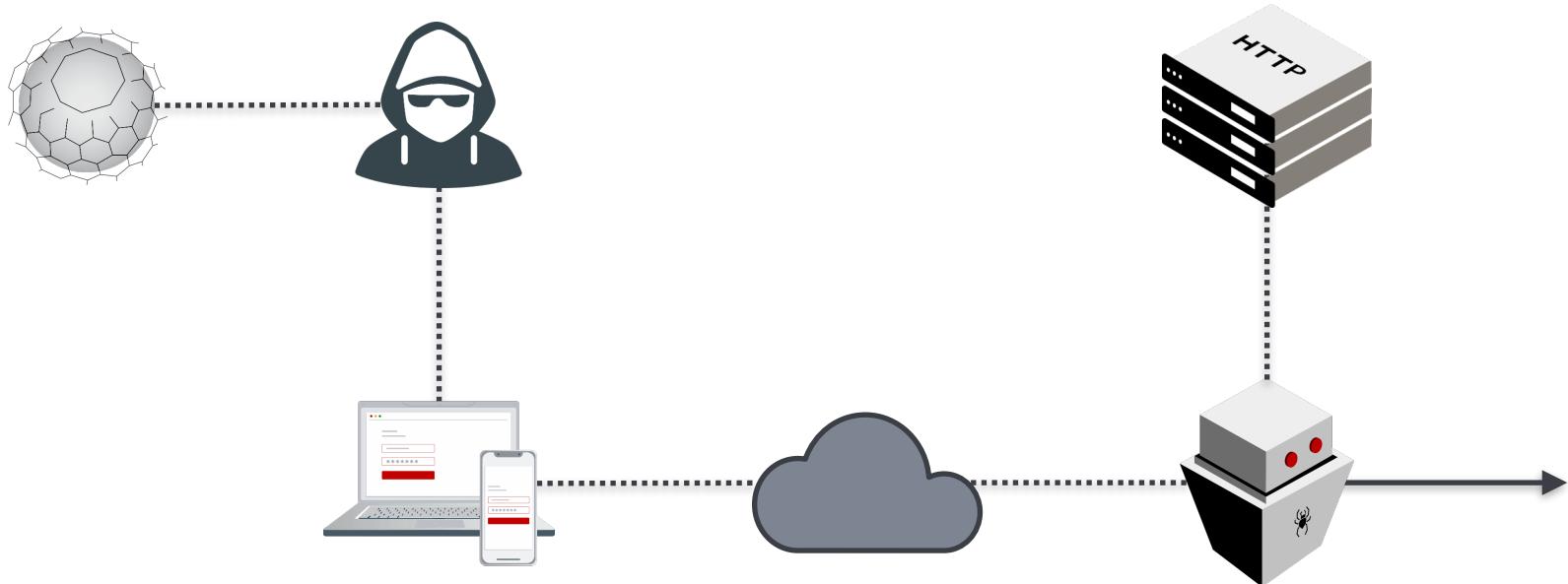


Have multiple ways to detect bad actors



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

TARGET WHAT HURTS THE MOST

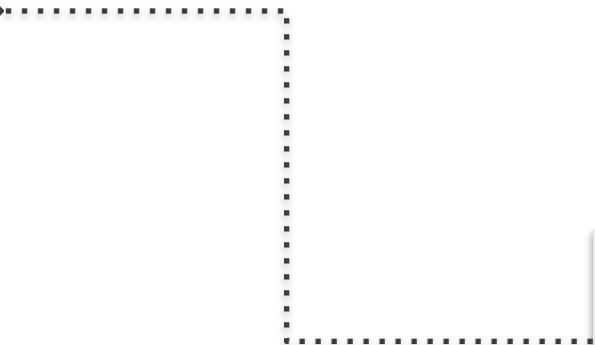


It's not as simple as blocking a baddie.
You need to target what will hurt the most.

THE SOFTWARE DEVELOPMENT LIFECYCLE

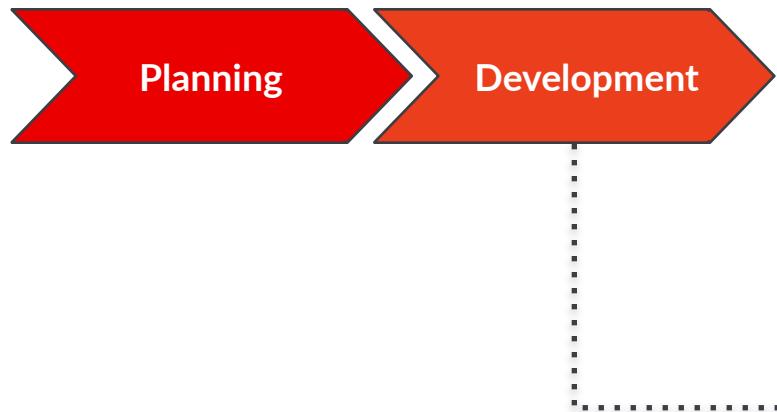


Planning



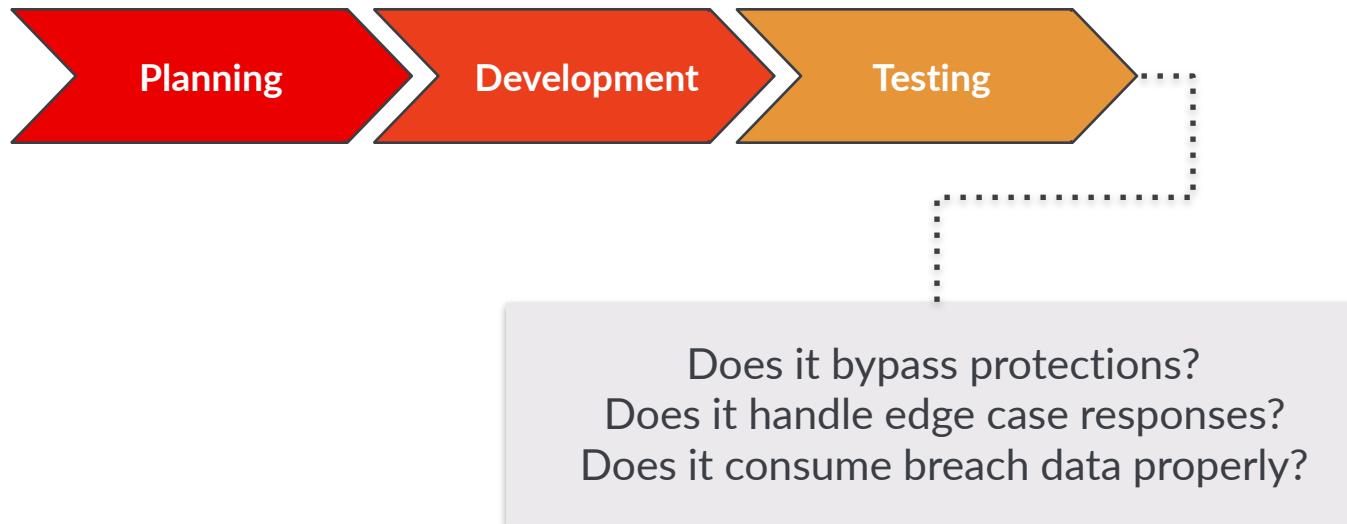
What tools work, what don't?
What URLs need to be targeted?
What dark web data do I need?

THE SOFTWARE DEVELOPMENT LIFECYCLE

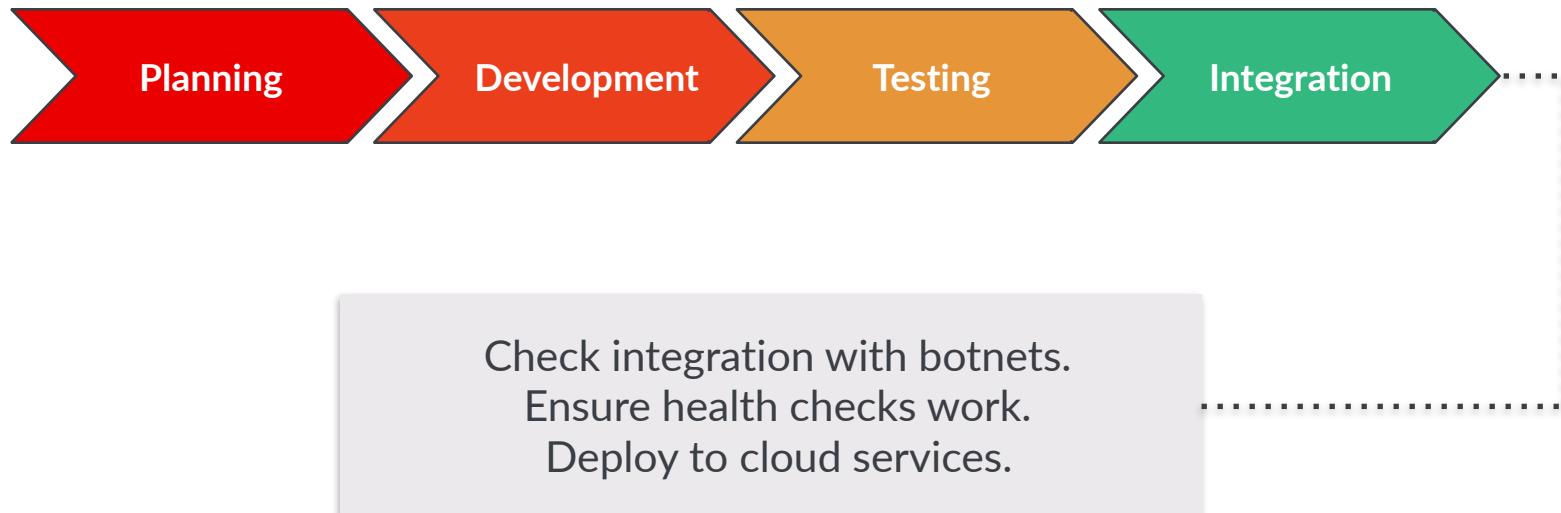


Investment in a framework of choice.
Custom development against a site.
Building in proxy/botnet hooks.

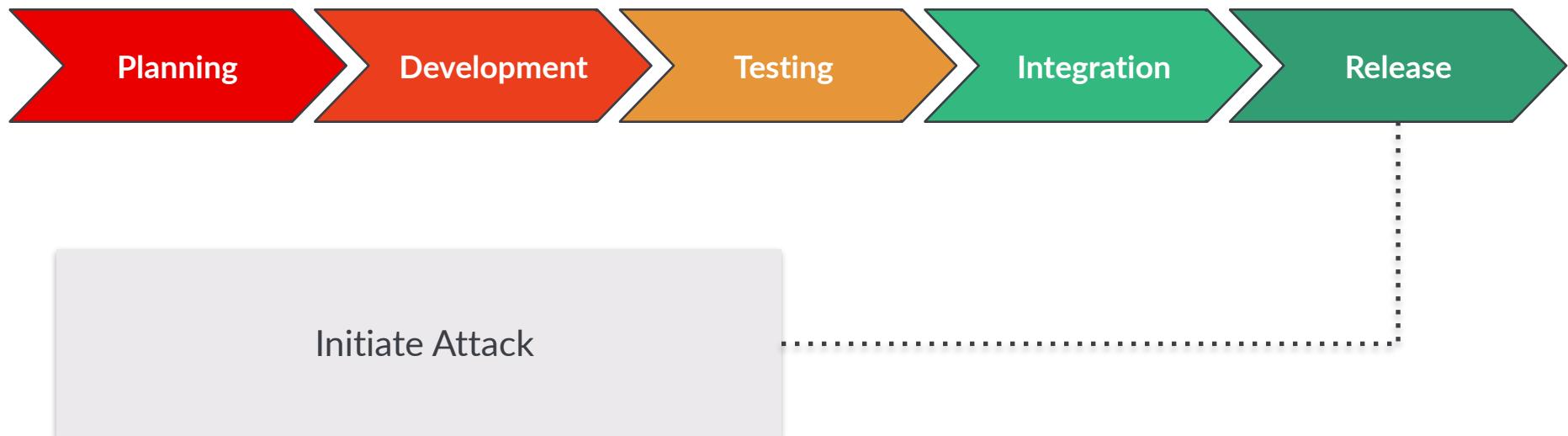
THE SOFTWARE DEVELOPMENT LIFECYCLE



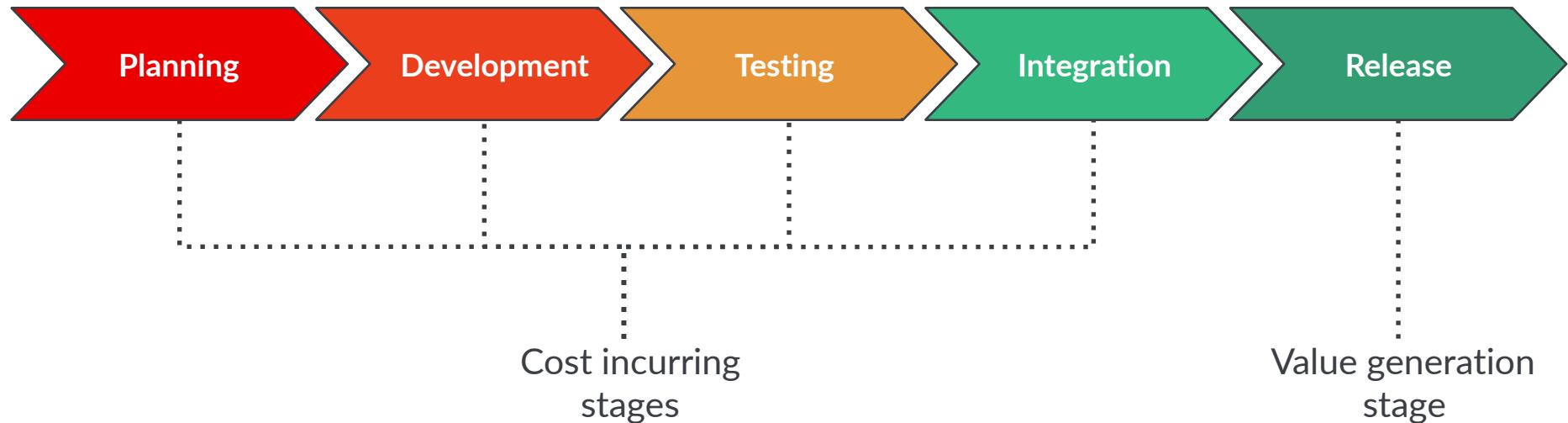
THE SOFTWARE DEVELOPMENT LIFECYCLE



THE SOFTWARE DEVELOPMENT LIFECYCLE



THE SOFTWARE DEVELOPMENT LIFECYCLE





0

Attacker sophistication & where we are

1

The economics of attacks

2

Flipping the economics in your favor

3

Case Studies

Case Study 1



Damaging Reputation

Scenario

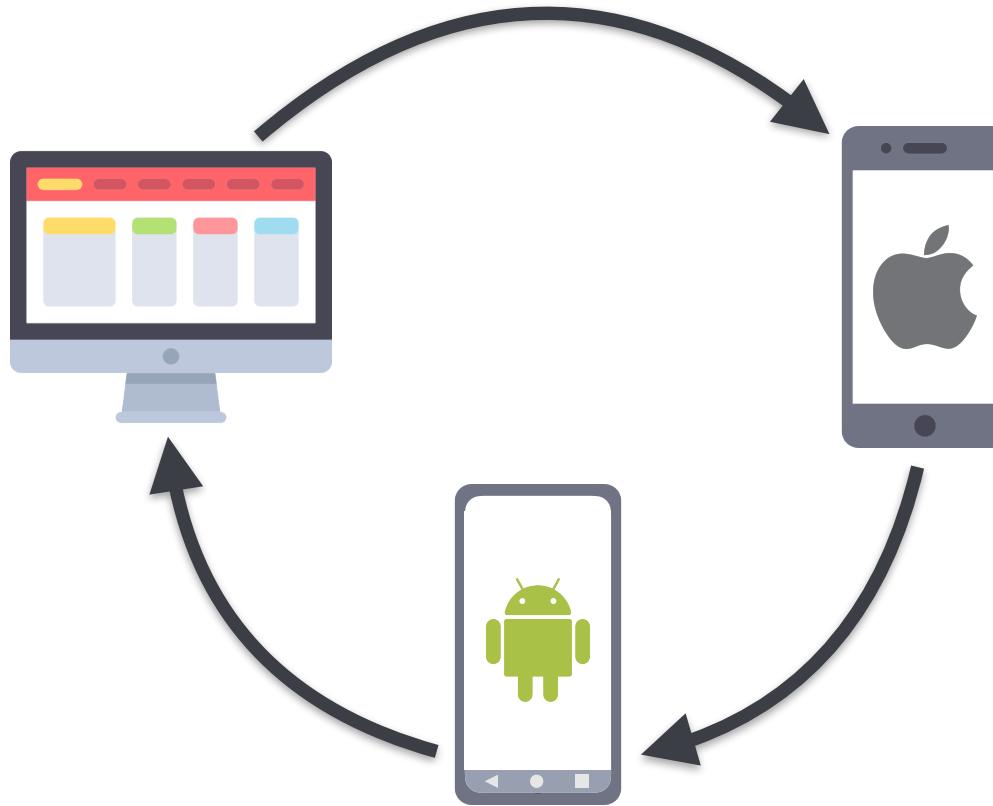


Well funded
scraper

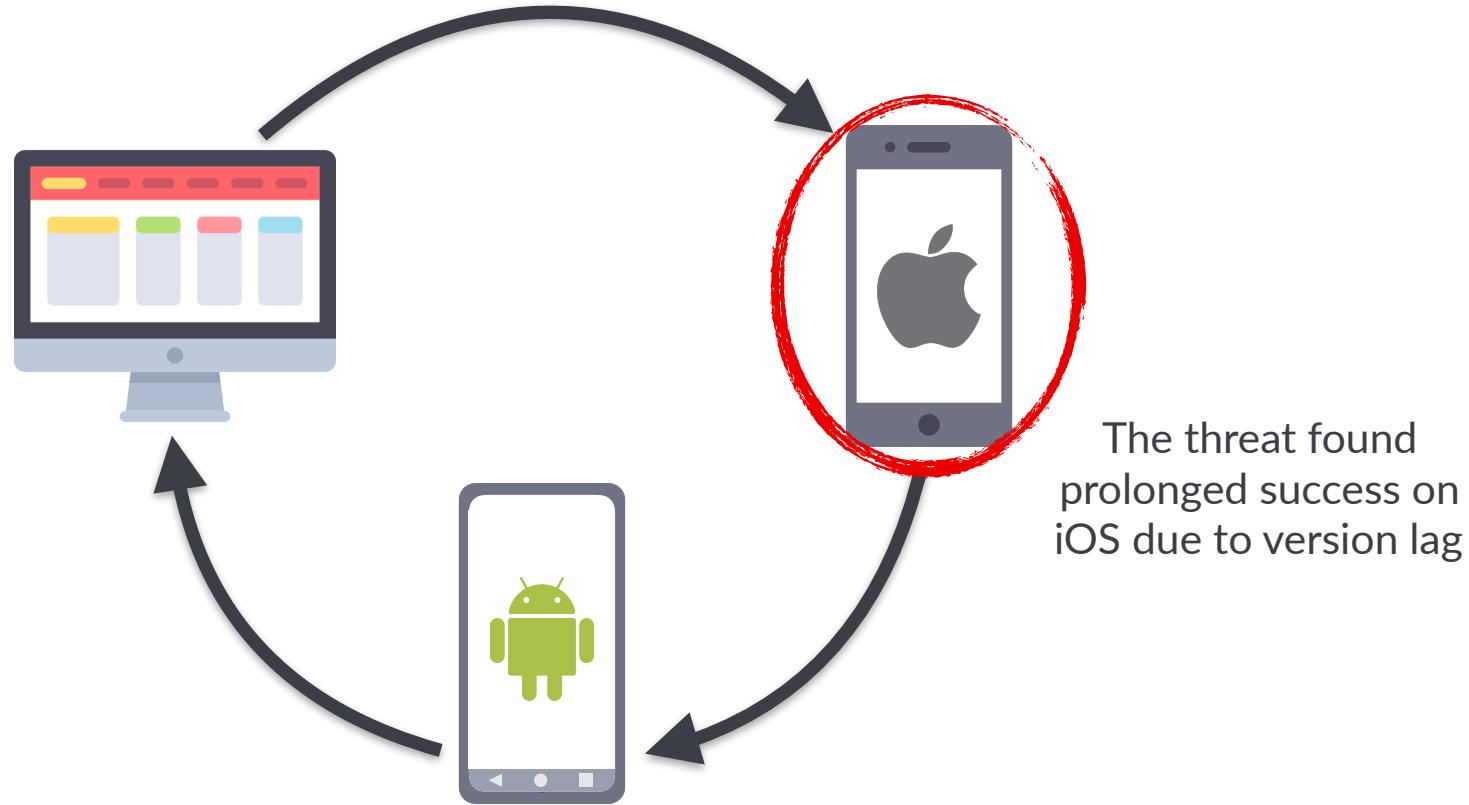


Big US Bank

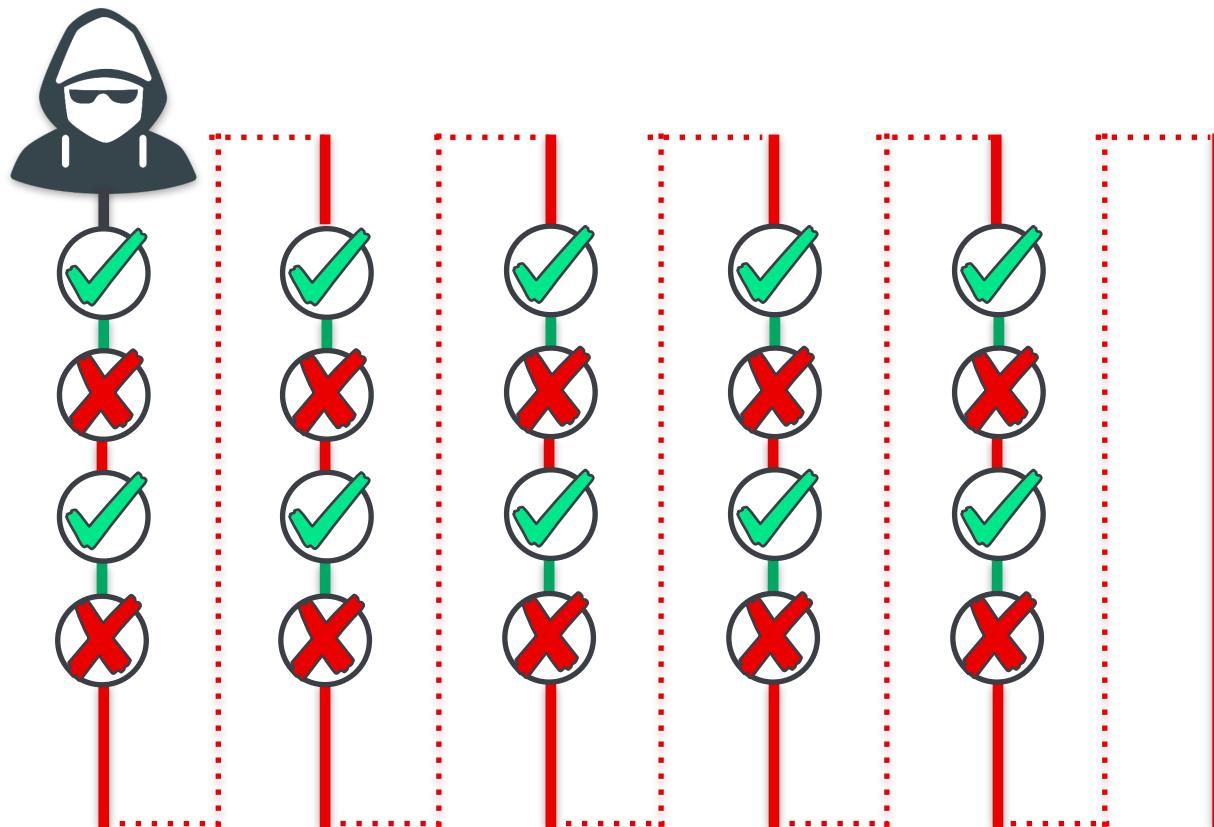
The actor cycled through the softest targets



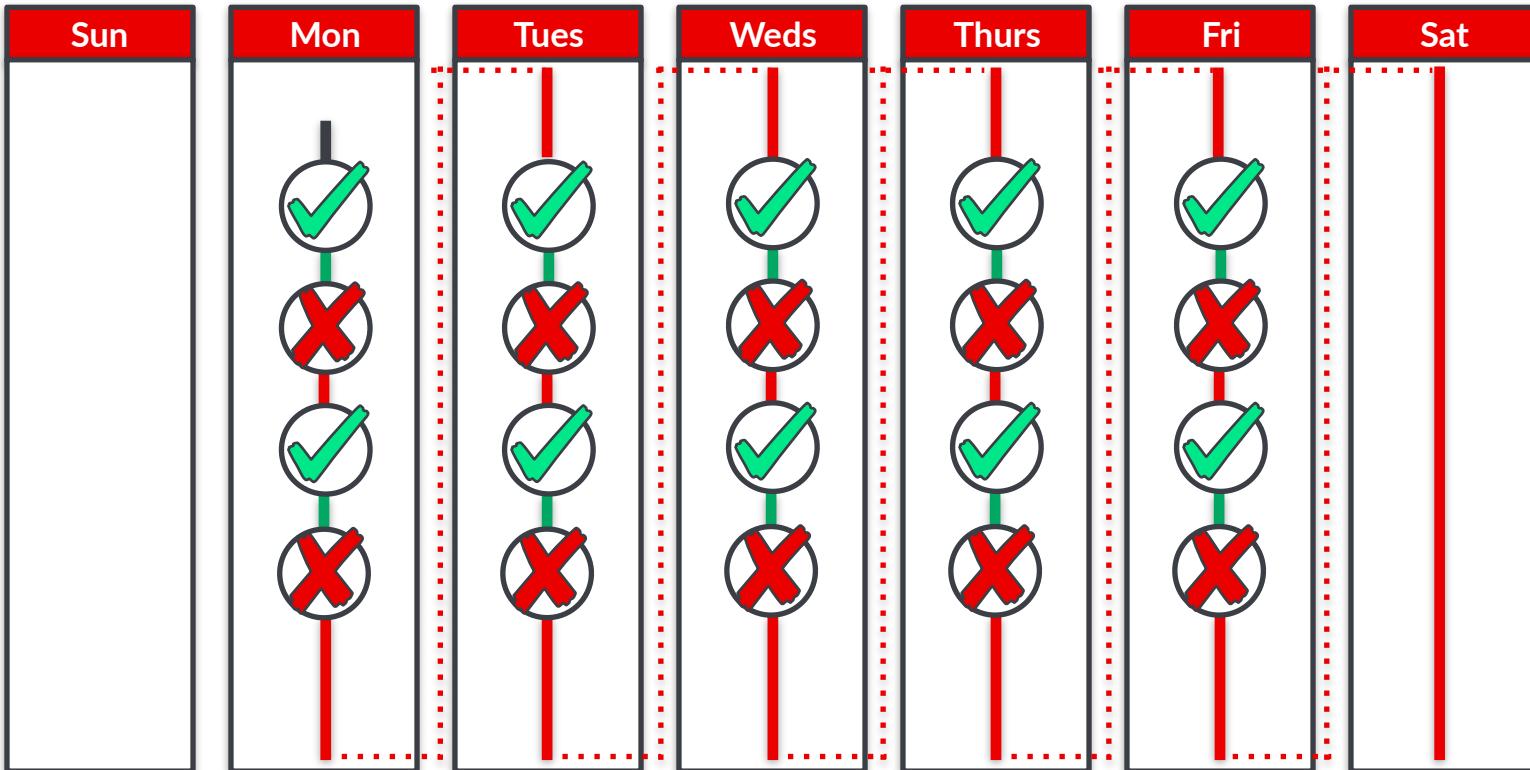
Finally committed to one to dive deeper



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



VS



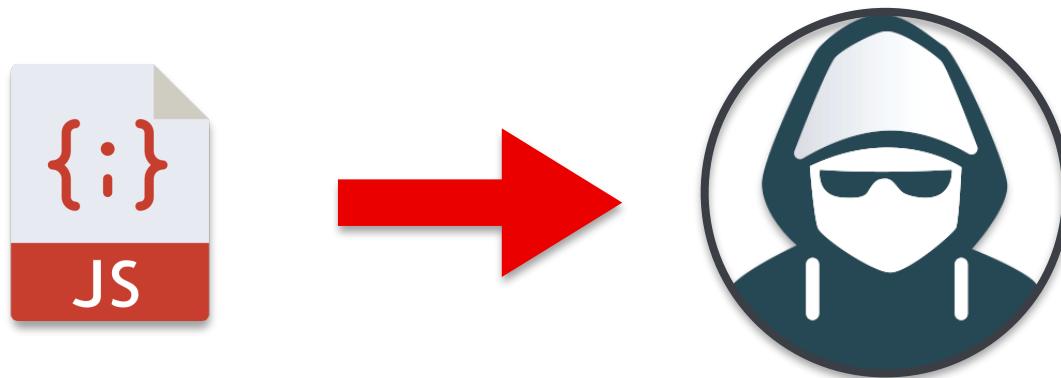
Credential Stuffer
and Account taker-overer

Big US Retailer

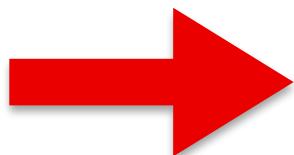
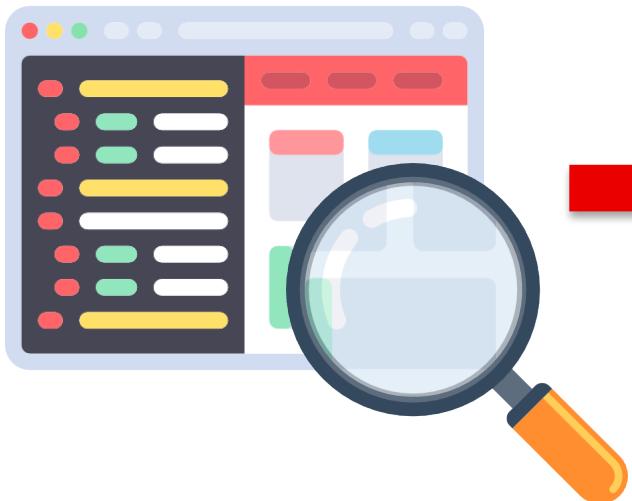


We were down to a fraction of our normal ability to detect
We needed more data

We had enough of a grip to deliver a targeted payload

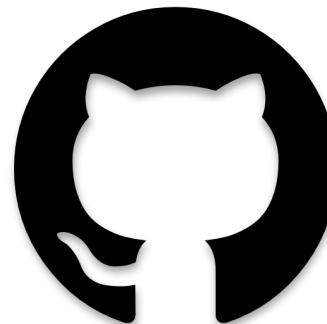
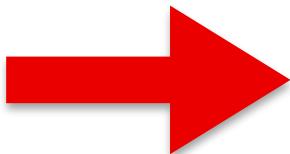


This allowed us to inspect the retooling effort in real time



```
> 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 in app-level defenses.

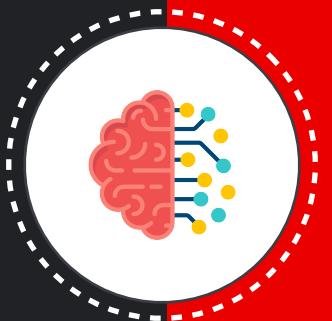


Tactics is knowing what to do when there is something to do.

Strategy is knowing what to do when there is nothing to do.



- Savielly Tartakower



Psychology and Security

Demotivating Persistent Attackers

Jarrod Overson - @jsoverson
Director of Engineering, Shape Security

InfoSecon 2018