Hunting Them

Detecting app abuse, fraud and other badness

Steve Davies | @northvein

Who am I?

Twitter: @northvein
KeyBase: keybase.io/northvein
LinkedIn: /in/sldavies
Blog: https://northve.in

- Independent Security Consultant / Contract dude
- Blue team Architect, Analyst, Auditor
- Security Lumberjack

“(…) look for attacks that **get past security systems** and to catch intrusions in progress rather than after attackers have completed their objectives and done worse damage to the business.”

SANS Institute | *The Who, What, Where, When, Why and How of Effective Threat Hunting*

Monday morning…

- So we need some help…
- Stumbled onto something weird…
- Leadership are worried…
- Found some ‘dark web’ stuff…
- Something bad happened to a competitor…

Security Systems = Controls

- But we've got a WAF…
- Security Controls are important but they typically monitor network activity or hosts for known-bad
- They don't (usually) look at how someone is using (or abusing) your apps' functionality or user journey
- Security isn't just about the Cyberz…

Question

How well do **you** know your app?

Not just functionality

Do you understand all the supporting processes and sub-processes?

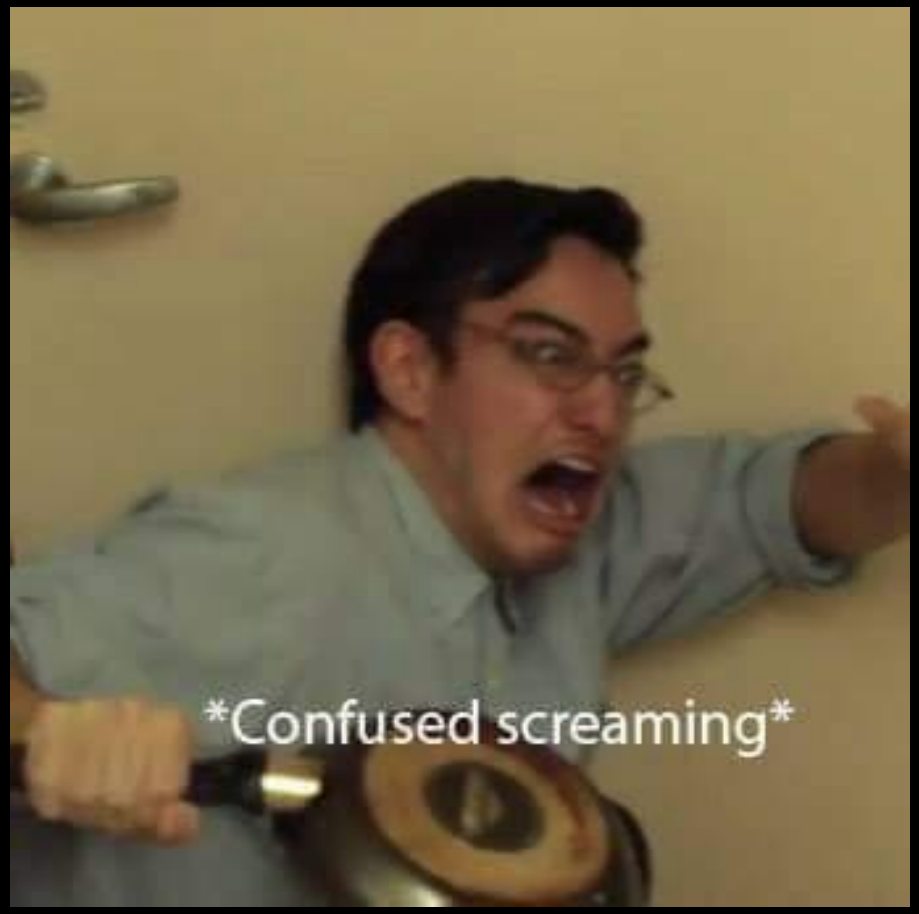
- Registration | How customer’s sign-up, what details they (need to) provide?
- Payments | Do you understand the mechanics for deposits and withdrawals?
- Risk & Fraud | Does your app employ ID verification, confidence tests, perform industry lookups, mandate payment method and verification at registration?
- Device fingerprinting | Does your app register and track customer devices?
- Customer Support | Does your app include support, IM/chat or case functionality?

Question

How well do you understand the customer journey?

Question

Do you know what ‘normal’ looks like?



Normal|

- Registration| Completion time, route/path, potential deviations?
- Logins| Per user, per demographic, per market, per event?
- Devices| Per user, per region, per market?
- Sources| IPs, ISPs, VPNs, Tor(!)?
- Everything per Presentation| desktop, mobile app(s), desktop via mobile?

Question

Do you have

Affiliates?

Affiliates |

- Registration | How do they ‘colour’ registrations?
- Logins | Do they affect or shape later visits? Do they market to your existing customers?
- Abuse | Are they capable of abuse? Are you capable of detecting it?

Question

How do you track affinity between users and ...?

Affinity|

- Users & Devices| Manufacturer? OS Version? Browser Version?
- Users & Sources| IPs, CG Nat, VPN, Tor?
- Users & Account(s)| Do you limit customers to one...?
- Users & Payment methods| Same name? Same address?
- Users & Geolocation| ?
- Users & E-mail addresses| Unique? Restrict providers? Restrict TLDs?

Question

Do you monitor for trends in activity?

Trends|

- Registrations| Do you track registrations in line with marketing and other business events?
- Logins| Can you predict spikes in registration/deposits/withdrawals?
- Abuse| Can you predict indicative spikes in network activity?

Question

Can you trivially differentiate these trends from suspicious or malicious activity? E.g:

- Site crawling / scraping / bug bounty(?)
- Enumeration attack
- GET flood
- Affiliate abuse

Thanks!

Twitter: @northvein
KeyBase: keybase.io/northvein
LinkedIn: /in/sldavies
Blog: https://northve.in