From: Eric Friedman (██████████)
To: Raj Ramamurthy (█████████████)   Trystan Kosmynka (██████████)   Ritwik Kumar (████████████)   Jeremy Stober (██████████)
CC:
BCC:
Subject: virus scanner abuse
Attachments: AMP Virus Scanner Abuse - EF.key; smime.p7s;
Sent: 06/29/2017 12:49:57 PM 0000 (GMT)

Collaboration gave up on me last night, so I had to edit locally. Please send feedback as you can. Trystan especially, call out any misstatements. I'm just summarizing and not trying to speak for you now or in the ERB.

Jeremy, if you see mitigations we should propose, please do. If you see mitigations we think are not realistic, let's not put them out there. External campaigns is a hard one — Figaro reversing would yield poor results.

Idea: can you please rank order the mitigations from most=>least effective? That would be something worth closing with.

Raj, after this group looks at it, we need to push it past iAds. I don't know what they are realistically going to do.

App Store abuse case study

A retrospective on https://medium.com/@johnnylin/how-to-make-80-000-per-month-on-the-apple-app-store-bdb943862e88
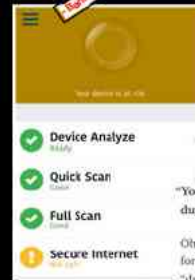
Apple Confidential Internal Use Only

Agenda

- Summarize issues raised by the article
- Map these to current and future work across store functions
  - Discovery
  - Content quality & pricing
  - Search Ads

Apple Confidential nternal Use Only
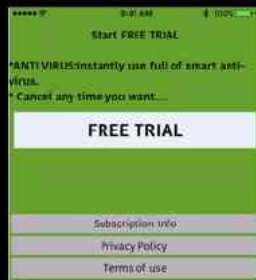
Article highlights

Abuse timeline

1. Developer submits app with prohibited terms, rejected twice

2. Developer removes problem terms, passes review but with problematic content

3. Once in store, developer:

   1. updates keywords and description post-review

   2. increases in-app pricing post-review

   3. stuffs positive reviews

   4. buys iAd keywords, including banned concept terms

   5. launches <u>external</u> marketing campaign with banned terms

4. Users gulled into subscribing with aggressive call to action

5. Conversion rate sufficient to enter Top Grossing chart

Apple Confidential Internal Use Only

Content quality/compliance
How did this get through App Review?

Start FREE TRIAL

*ANTI VIRUS:instantly use full of smart anti-virus.
* Cancel any time you want....

FREE TRIAL

Subscription Info
Privacy Policy
Terms of use

Problem

Third reviewer not made aware of findings of prior two rejections.

Mitigation

High risk team for submissions following egregious rejections [complete]

Improve tooling for bad content discovery [in progress]

Apple Confidential Internal Use Only

Rejections made correctly the first 2 times. Developer removed problem terms and got through. App was launched, but some content overlooked.

Charting
Why did this appear in Top Grossing?

Problem

Top Grossing is a straight revenue count.

Mitigation

Chart removed in store redesign [complete]

High-value in-app drives revenue from small # of victims
How did they get a $99.99 in-app into the store?

Problem

Easy to avoid ERB review by raising price after approval

Mitigation

Flag suspicious price changes for review [proposed]

Not a trivial undertaking — a motivated adversary can beat a simple threshold check (as demonstrated). Needs developer reputation and a pipeline for handling these escalations, as well as policy about what happens while under review.

Banned concept shows up in Search
Why does "malware scan" yield results?

Problem

Keywords can change post submission

results for "malware scan"

Malware
Analysis 101-...

Hotspot Shield
Free VPN Pros...

Best vpn proxy
Betternet -...

Mitigation

Live moderation team for discovery [in progress, not scoped to Ads]

Reduce reliance on keywords; lock down description post-review [in progress]

Apply banned concepts globally: app review, discovery, ads [proposed]

Apple Confidential Internal Use Only

Not a trivial undertaking — a motivated adversary can beat a simple threshold check (as demonstrated). Needs developer reputation and a pipeline for handling these escalations, as well as policy about what happens while under review. Also, it's OK to sell books/videos about these topics — the leftmost icon is one example.

Banned concept shows up in Search ads
Why does "virus scanner" yield results?

Problem

Keywords can change post submission and ads are
heavily keyword based

Mitigation

Apply banned concepts globally: app review, discovery,
ads [proposed]

Ads runs its own fraud program.

Low quality / low sentiment reviews

Problem

Fraud algorithm scope today is review ranking: not deletion, not banned concept identification

Review moderation is manual and prioritized by scale abuses

Mitigation

Live moderation team for discovery [in progress]

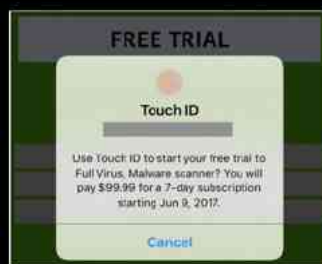Automated review deletion [proposed]

"Excellent virus removal recommended" uses a banned concept
"Best app / OK" is a low quality review
Reviews from real uses are overwhelmingly negative

Aggressive in-app solicitation

FREE TRIAL

Touch ID

Use Touch ID to start your free trial to Full Virus, Malware scanner? You will pay $99.99 for a 7-day subscription starting Jun 9, 2017.

Cancel

Problem

Developer can display inApp purchase dialogs repeatedly

Mitigation

Add "report a problem" action in the StoreKit purchase sheet, trigger investigations [proposed]

High cancellation rates trigger investigation [proposed]

Apple Confidential Internal Use Only

May even catch the user trying to exit the app by the home button

Misleading external campaigns

iphone malware

iphone malware
iphone malware **scanner**
iphone malware **protection**
iphone malware **removal**

iPhone Malware - #1 Anti-Malware & Security
[Ad] www.norton.com/Android/Malware ▾
Better Protection. Faster Installs. Download Now & Save.
Money-Back Guarantee · Instant Download · Limited Time Offer
Services: Malware Detection, App Risk Advisor, Call Blocker, Rem

Problem

Developer can drive conversions with external
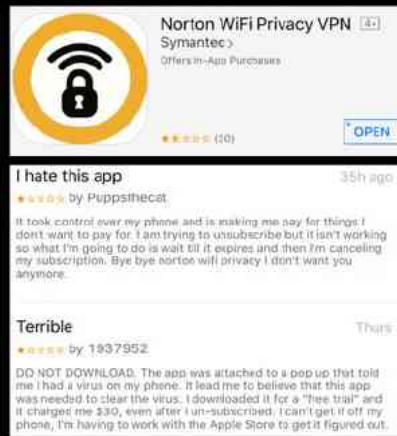campaigns, yet keep content within guidelines

Mitigation

?

Apple Confidential Internal Use Only

Customer confusion around subscriptions
How do I cancel?

Norton WiFi Privacy VPN 4+
Symantec›
Offers In-App Purchases
★★★★★ (10)   OPEN

I hate this app   35h ago
★★★★★ by Puppsthecat

It took control over my phone and is making me pay for things I don't want to pay for. I am trying to unsubscribe but it isn't working so what I'm going to do is wait till it expires and then I'm canceling my subscription. Bye bye norton wifi privacy I don't want you anymore.

Terrible   Thurs
★★★★★ by 1937952

DO NOT DOWNLOAD. The app was attached to a pop up that told me I had a virus on my phone. It lead me to believe that this app was needed to clear the virus. I downloaded it for a "free trial" and it charged me $30, even after I un-subscribed. I can't get it off my phone, I'm having to work with the Apple Store to get it figured out.

Problem

Reviews indicate that customers don't know how to cancel

Mitigation

Apple Care feedback loop [proposed]

Subscription-specific review sentiment feedback loop [proposed]

Apple Confidential Internal Use Only

Search today is ONLY for discovery. Why doesn't it help users resolve problems? (search for cancel my subscriptions yields no results)

PX-0253.14
APL-APPSTORE_09567772

Customer confusion around subscriptions
How do I cancel?
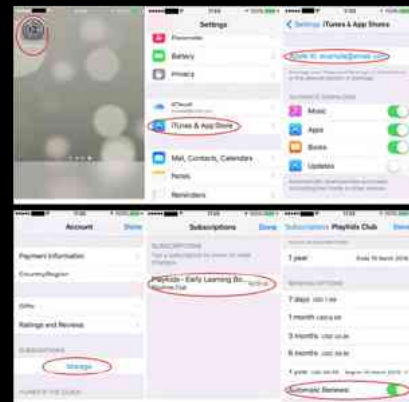
Problem

Numerous web sites providing 6+ step illustrated guides

Mitigation

Clear paths for "managing your subscriptions"

~~when an app is deleted~~ [proposed]

in Search

on Report A Concern

with less than six steps + auth?

Search today is ONLY for discovery. Why doesn't it help users resolve problems? (search for cancel my subscriptions yields no results)
Use CK for subscription cancellation: lower friction

Abuses identified

- Chart manipulation
  - No more top grossing section in the new app store
  - Currently fraudulent apps are taken off from free and paid charts
    - Algorithmically based on untrusted account activity
    - Manually when escalated/ reviewed
  - Upcoming enhancements includes
    - Live moderation
    - Excluding activity from untrusted devices
    - Behavioral anomaly detection
    - Randomized charting algorithm
    - Cohort based charting

Apple Confidential nternal Use Only

Abuses identified

- Suspicious reviews
  - Fake reviews/ sentiment was low
  - Currently fake reviews are removed manually
    - Model driven review ranking is performed
- Upcoming work includes
  - Model driven review removal and ranking
  - Live moderation
  - Analytical average rating computation
  - Behavioral anomaly detection
  - Review sentiment risking

Abuses identified

- High value in-app/ app
  - Should price range be based on category/ complexity (complexity calculated thru algorithms)?
  - Should >$99 app be approved by a board?
  - Proposal to push to app review if price changes post review

- Aggressive/ misleading marketing/ subscription
  - Should we terminate or action for over aggressive sales?
  - Proposal to
    - Impose hard limits
    - Targeted 'report a problem' (StoreKit action using Fraud signal)
    - Metric on per capita/ ratio of downloads vs $ made
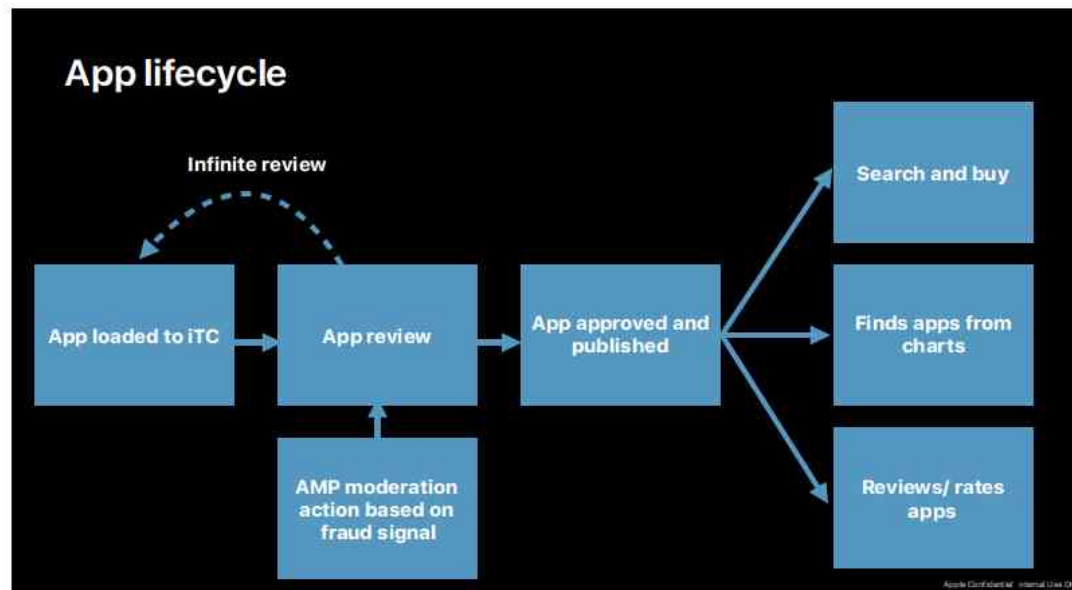
Apple Confidential nternal Use Only

Abuses identified

- Suspicious app
  - Proposal to
    - Rate limit repeated app review submission
    - Mass actioning capability
    - Reduce sensitivity for clone app identification

- Bad category of app (anti-virus)
  - Not allowed today (users were mislead by external marketing sources)
  - Proposal to look into referrer anomalies and reputation

- Search Ads abuse
  - Search ads for banned concepts
  - Currently apps can buy keywords un-related to app to increase visibility
  - Proposal to remove/ blacklist banned concepts and utilize common blacklist with discovery features

Apple Confidential nternal Use Only

Appendix

Apple Confidential nternal Use Only

CONFIDENTIAL

Nature of AMP Search abuse

Abuse vector	Why?	How?	What we do today?	Upcoming enhancements
Manipulate search query app ranking	Increase visibility of the app	Scripted and incentivized conversion	Search session filtering based on factory device data, device profiles, purchase behavior and account type Title keyword filtering	Behavioral Anomaly Detection Live moderation
Manipulate search hints			Search hints blacklist	Use fraud filtered sessions Blacklisting banned concepts Live moderation

Apple Confidential Internal Use Only

Nature of AMP Search abuse

Abuse vector	Why?	How?	What we do today?	Upcoming enhancements
Manipulate search query app ranking	Increase visibility of the app	Scripted and incentivized conversion	Search session filtering based on factory device data, device profiles, purchase behavior and account type Title keyword filtering	Behavioral Anomaly Detection Live moderation
Manipulate search hints			Search hints blacklist	Use fraud filtered sessions Blacklisting banned concepts Live moderation

Apple Confidential Internal Use Only

Nature of AMP Charts abuse

Abuse vector	Why?	How?	What we do today?	Upcoming enhancements
Apps in top charts due to fraudulent purchase activity	Increase visibility of the app Get more downloads Investor manipulation	Scripted and incentivized conversion	Account neutralization Chart algorithm tuning	Device neutralization Behavioral anomaly detection Randomized charting algorithm Cohort based charting Live moderation

Apple Confidential Internal Use Only

PX-0253.24
APL-APPSTORE_09567782

Nature of AMP Rating and Review abuse

Abuse vector	Why?	How?	What we do today?	Upcoming enhancements
Creating fake ratings	Increase average rating	Scripted/ fake ratings	Manual removal of fake ratings	Model driven rating risking Analytical average rating computation Live moderation
Inject fake reviews	Mislead customers De value competitor app		Rank reviews in order of usefulness Manual removal of reviews	Model driven removal of reviews Behavioral anomaly detection Review sentiment risking

Apple Confidential Internal Use Only

Nature of iAd abuse

Abuse Vector	Why?	How?	What we do today?	Proposal
Search ads abuse	Increase app visibility	Buy keywords un related to app	Policy controls on banned categories	??
External marketing		Out of guidelines 3rd party marketing	None	Referrer anomalies and reputation

Apple Confidential Internal Use Only

Nature of iTC abuse

Abuse vector	Why?	How?	What we do today?	Proposal
Repetitive submission on rejection	Attempting to target weakest link	Repetitive attempts with minimal changes	No penalty	Rate limit
Change app price	Defraud customers	Price changes are not reviewed	None	Push change in price to app review Policy category/ complexity based pricing Process price change to >$99 apps ERB ed

Apple Confidential Internal Use Only

Nature of iTC abuse

Abuse vector	Why?	How?	What we do today?	Proposal
Clone apps	Get multiple similar apps to increase coverage/ visibility	Submit similar apps	Similarity scanning	Adjust similarity sensitivity Mass actioning capability Risk guided App Review
DDOS customer for subscriptions	Defraud customers	Prompting for subscription repetitively	None	Impose hard limits Targeted report a problem Policy terminate app over aggressive sales

Apple Confidential Internal Use Only

Apple Confidential Internal Use Only

PX-0253.29

APL-APPSTORE_09567787