android Bootcamp 2016

Keeping Google Play safe

Thursday January 21, 2016

Agenda

Our mission, our goals, our history

A look at potentially harmful applications

How we protect Android users

Success stories

What the future holds

Our mission, our goals, our history

android

Our Mission

Protect Android users from potentially harmful applications. This includes intentionally harmful applications as well as unintentionally dangerous applications.

Our history

Grown out of the Android Security Team to which we still belong.

Started out protecting Google Play only.

Expanded scope to apps from all sources.

Expanded scope to unintentionally dangerous applications.

Our goals

Of every 1,000,000 downloads from Google Play, only 1 should be a download of an intentionally harmful application.

Of every 10,000 Android devices, only 1 should have an intentionally harmful application installed at any time.

Decrease installation base of unintentionally harmful applications by 95%.

A look at potentially harmful applications

Potentially harmful apps

Intentionally Harmful Applications

- Trojans
- Spyware
- Phishing
- Exploits
- ...

Unintentionally Harmful Applications

- Circumvented security features
- Usage of known vulnerable libraries
- Incorrect use of sensitive APIs
- ...

Image source: https://www.flickr.com/photos/uncalno/8538679708

Media on Android exploits

Cyber-Safe

600 million Samsung Galaxy phones exposed to hackers

Technology

Android Fake ID bug exposes smartphones and tablets

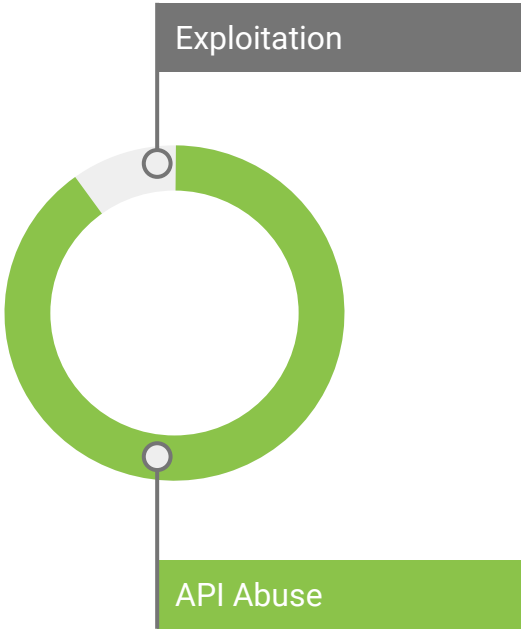
OPINION

Your Android has a Fake ID problem, allowing malware to impersonate trusted apps

Sources: CNN, BBC, Computerworld

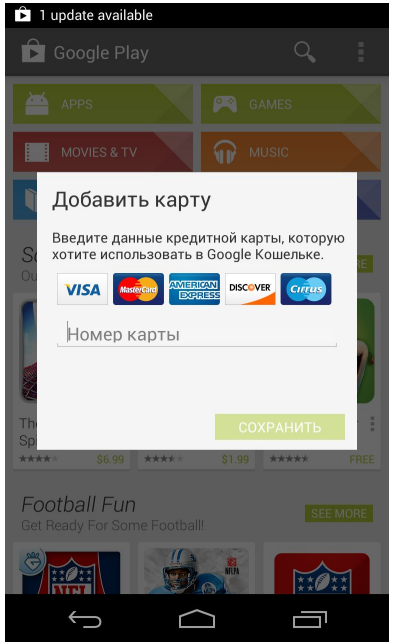
Reality on Android exploits

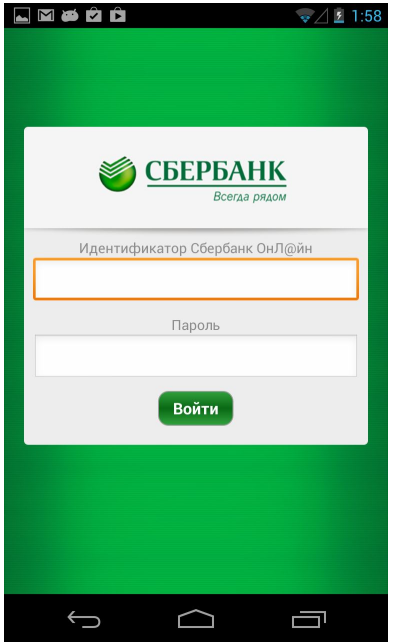
- AOSP provides many APIs that can be abused and are only protected by permissions.
- Much easier to just write apps that abuse APIs than to develop or deploy exploits.
- Lack of incentive for exploitation.



What intentionally harmful apps look like

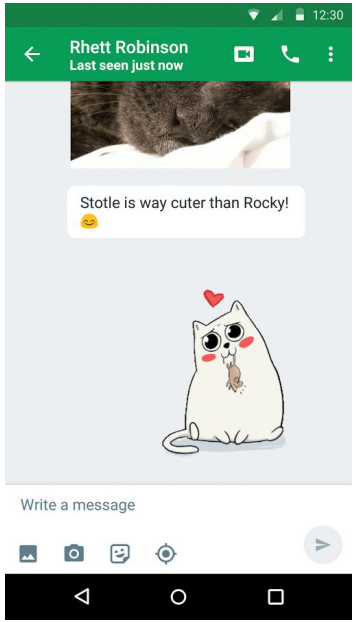
Most intentionally harmful apps do their work in the background: invisible to the user.

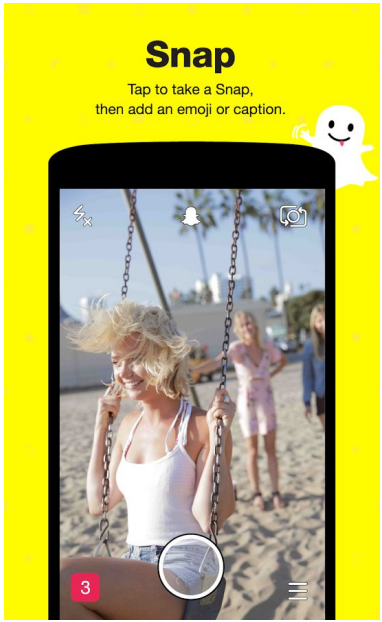




What unintentionally dangerous apps look like

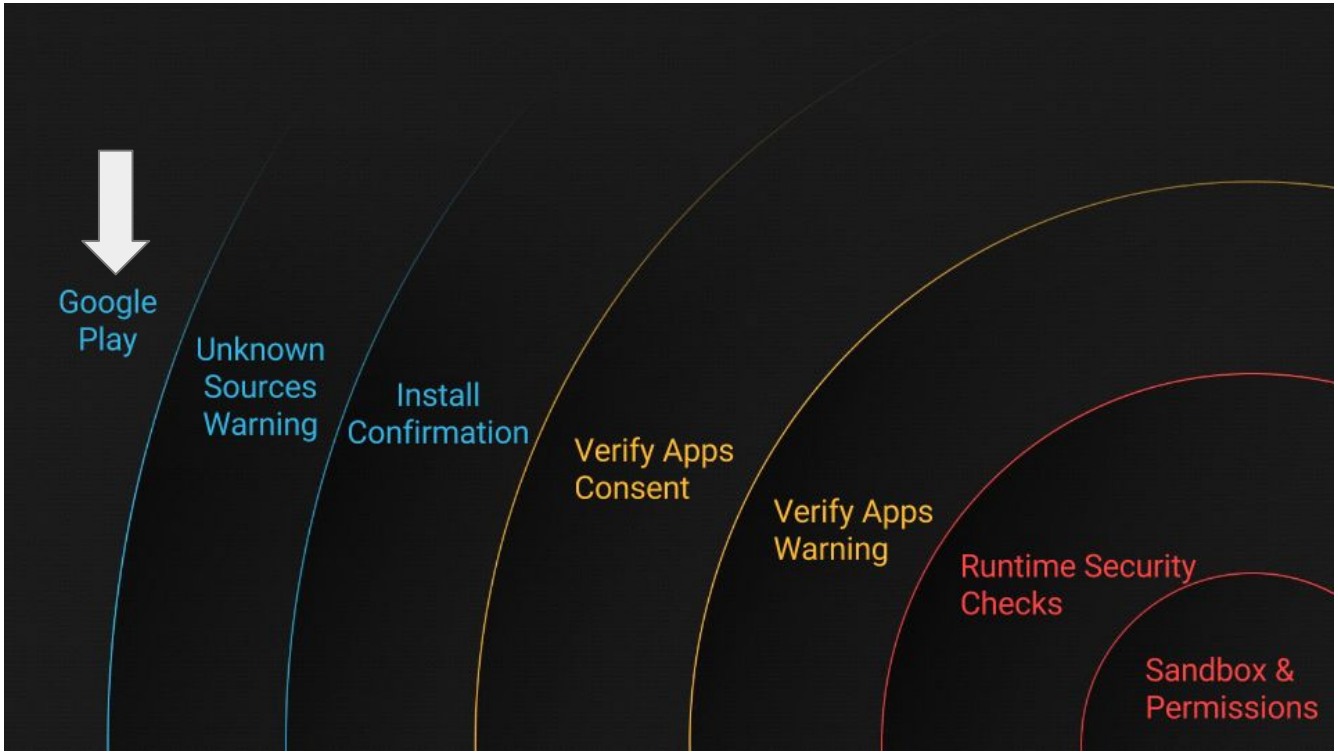
Hangouts, Snapchat, and Facebook used to ship with known vulnerable versions of OpenSSL. So did more than 75,000 other apps in Google Play.



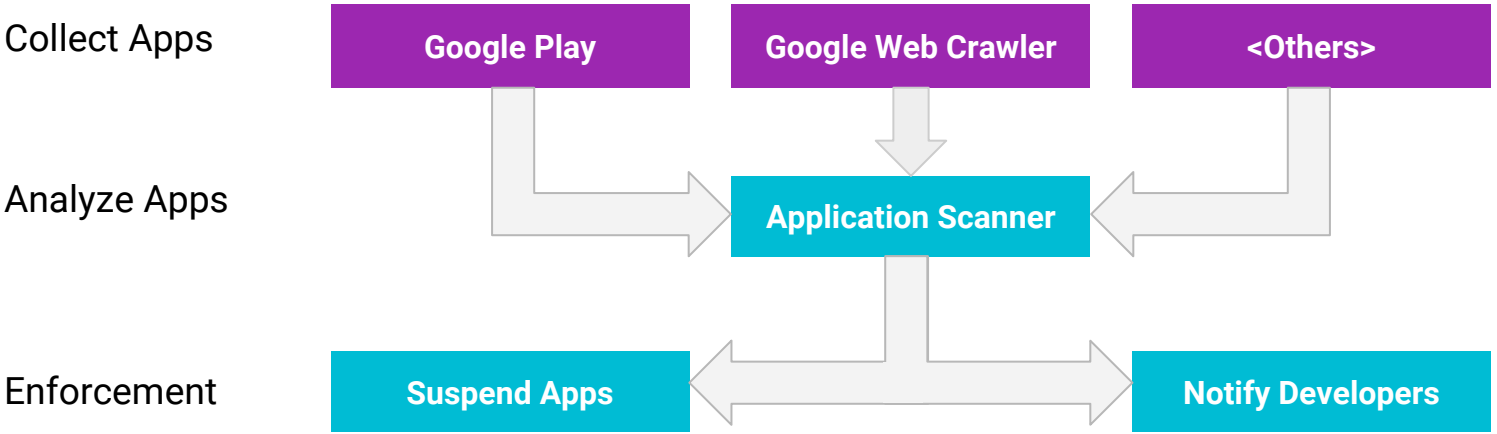


How we protect Android users

We are only a small part of Android security



Our application scanner setup



Application scanner details

Static analysis

Dynamic analysis

Machine learning

Intelligence-based discovery

Signature-based discovery

Handling intentionally harmful apps

Analysis (for most parts) is automated.

Warnings are presented to user at Install time.

In severe cases, we can remotely uninstall apps.

The effects of our application scanning program

Google Play is the most-trusted Android app store.

Attackers look for other targets.

Sideloaded applications are six times more likely to be intentionally harmful compared to Google Play downloads.

Some categories of bad behavior become unprofitable.

Handling unintentionally dangerous apps

Developer guidance must be detailed and actionable.

Developers receive multiple notifications with fix deadlines.

Google Play disallows unfixed app updates after grace period.

The effects of our security and privacy notifications

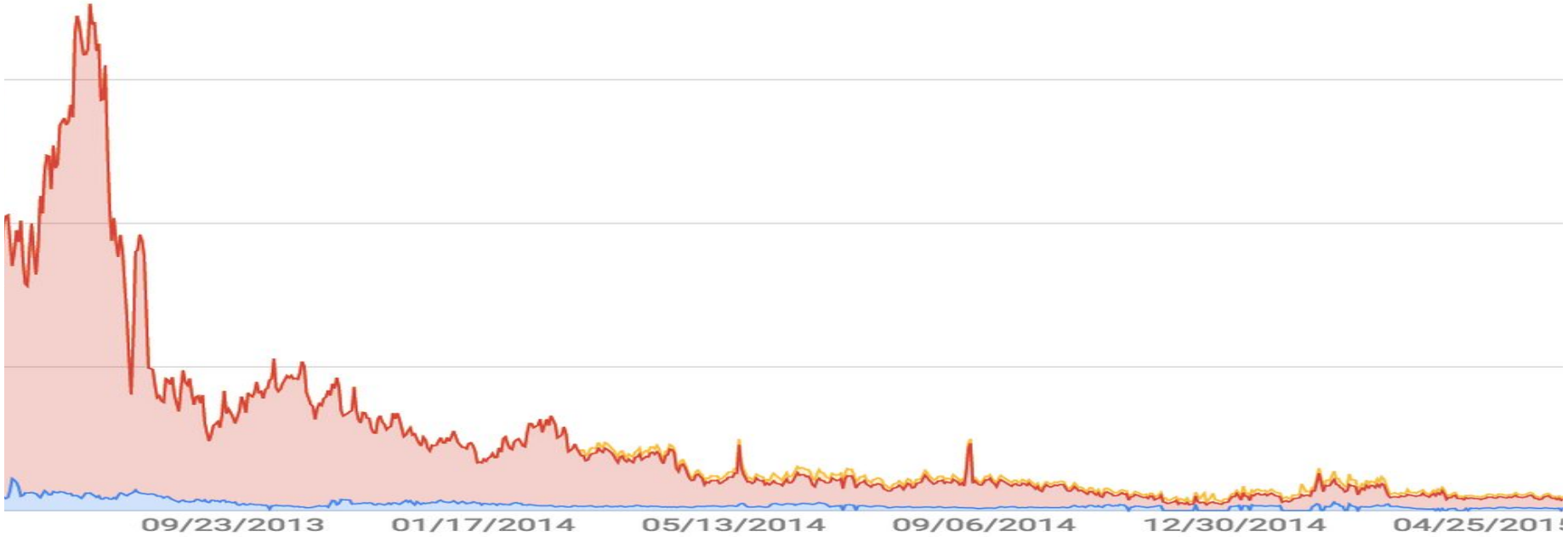
More than 700,000 apps in Google Play notified.

More than 75,000 apps fixed.

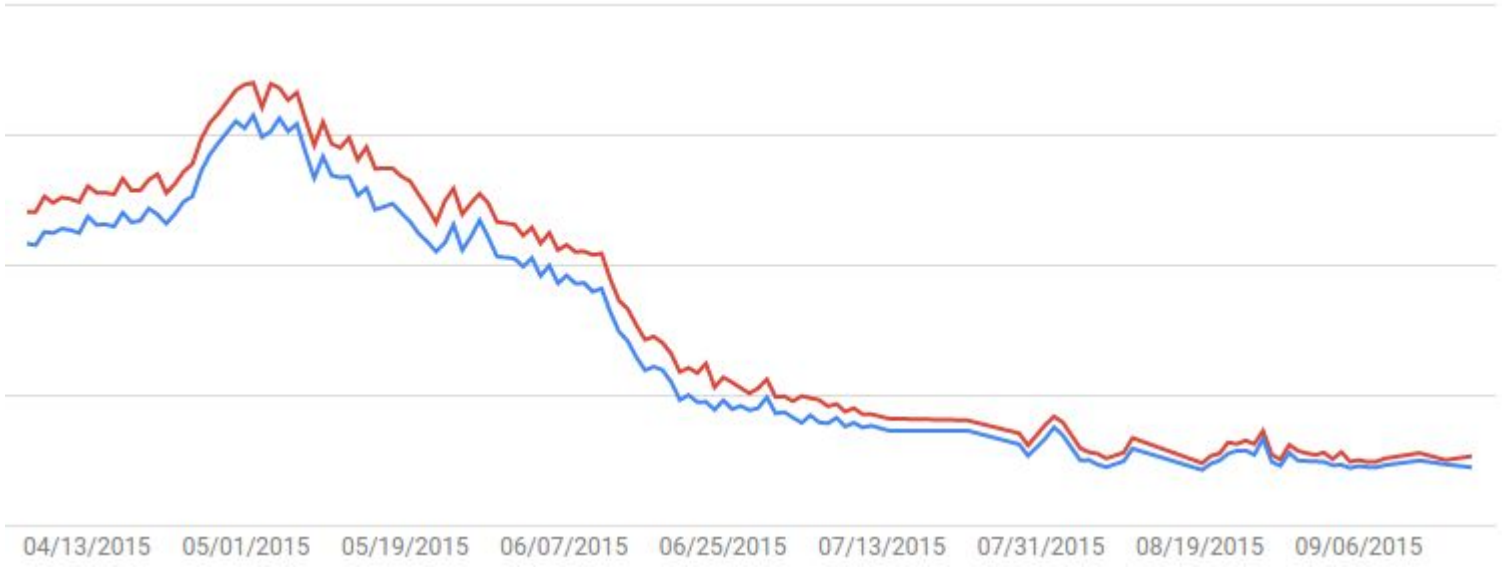
More than 7,600,000,000 security fixes installed on user devices.

Success stories

Near-elimination of SMS fraud

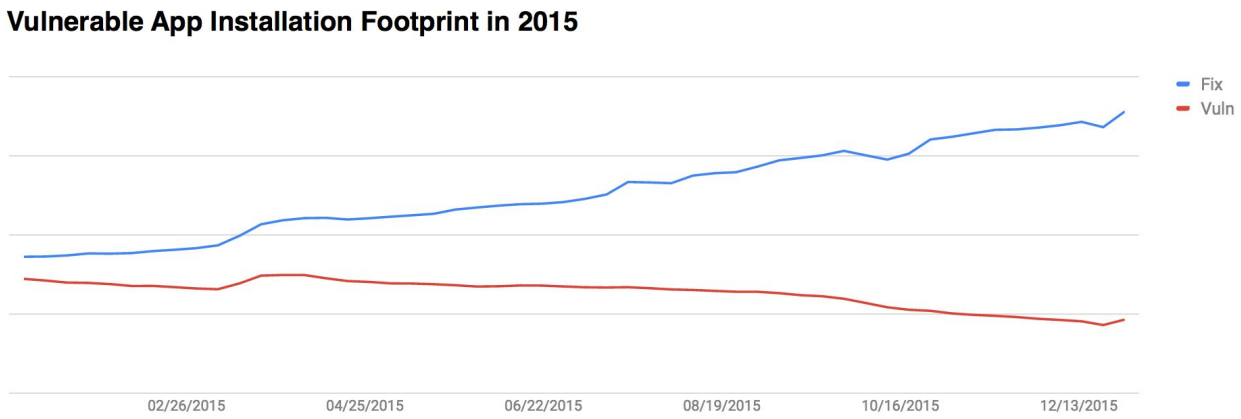


80% Reduction of Russian Bank Phishing Trojans



Infected devices in Russia
Infected devices worldwide

Decreased installation base of insecure app versions

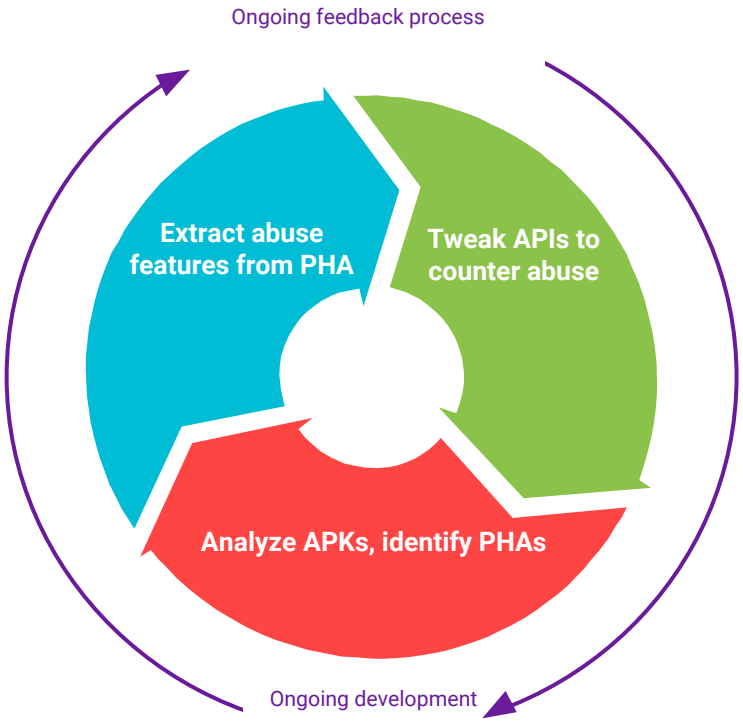


Number of installed apps updated after we warned developers about security problems
Number of installed apps that have not yet been updated to new version

What the future holds

Security is a continuous process

- Look at Platform's security comprehensively.
- Analysis at scale presents interesting data points
  - How are APIs used?
  - How often are APIs used and abused?
- APIs are tweaked to make them resilient to abuse.
- Exploits are used to identify areas for platform hardening.



Looking forward through 2016

Safety Expand our reputation as Android’s safest app store for users.

Scope Provide similar levels of safety to users of side-loaded applications.

Engagement Guide developers to fix their security and privacy issues.

THANK YOU