android Bootcamp 2016

SafetyNet

How we actively detect and prevent security problems

Thursday January 21, 2016

Agenda

Do devices need security apps?

What is SafetyNet?

Verify Apps: Detecting and removing harmful apps

SafetyNet APIs: Attestation and anti-phishing

SafetyNet Sensor Network: Vulnerability logging

Android Device Manager: Find/wipe lost or stolen devices

Do devices need security apps?

No

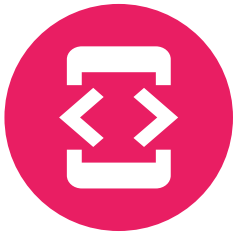
It’s already in the platform and Google apps.

SafetyNet

android

Scope

Verify Apps



APIs

Sensor Network

Android Device Manager

Protect 1.4B Android users through data-driven security apps and services.

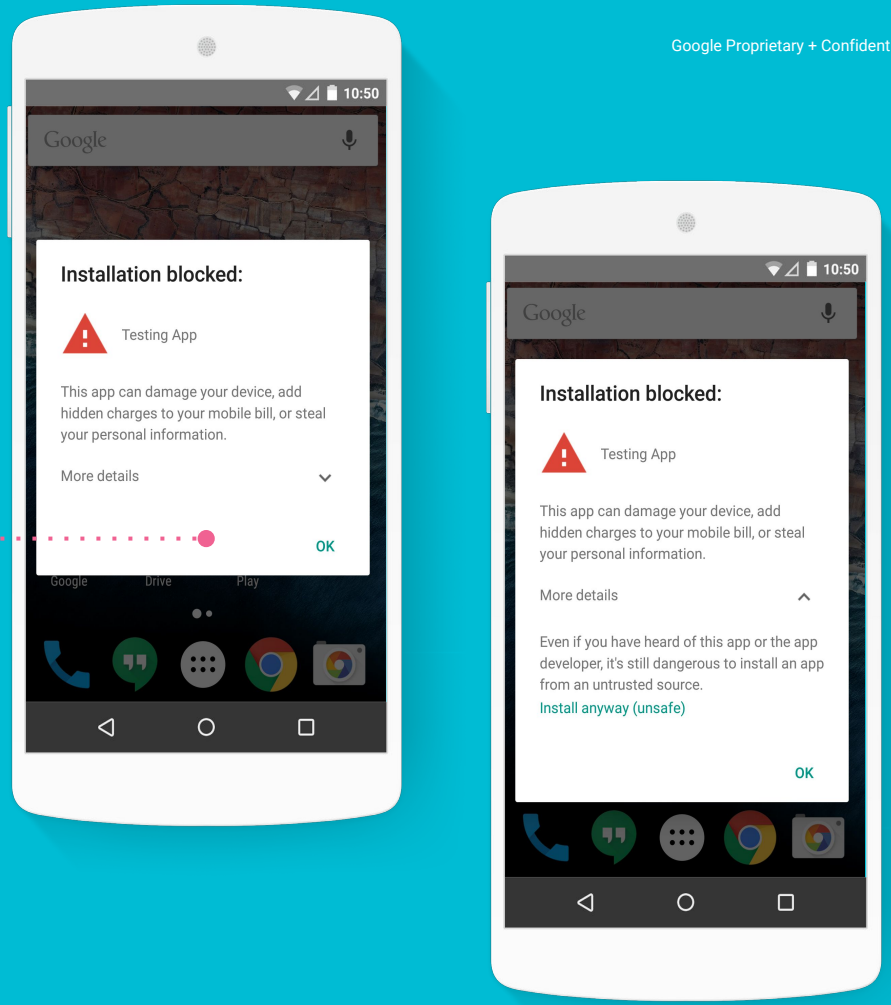
Verify Apps

Verify Apps

Continually scans all installed and sideloaded apps.

Warns, blocks, or automatically removes harmful apps.

Opinionated design increases cognitive load to install or keep the harmful app.



android

UX makes a difference

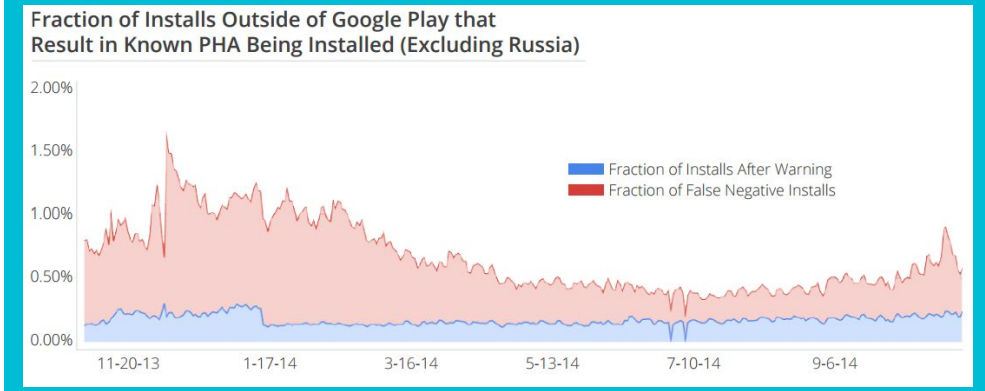
Two ways to install harmful apps:

- User clicks through warning dialog
- We incorrectly assume the app is safe (false negative)

User clickthroughs account for a large fraction of harmful app installs.

Clickthroughs before UX change 20.7%
Clickthroughs after UX change 10.4%

50% fewer installs of known harmful apps

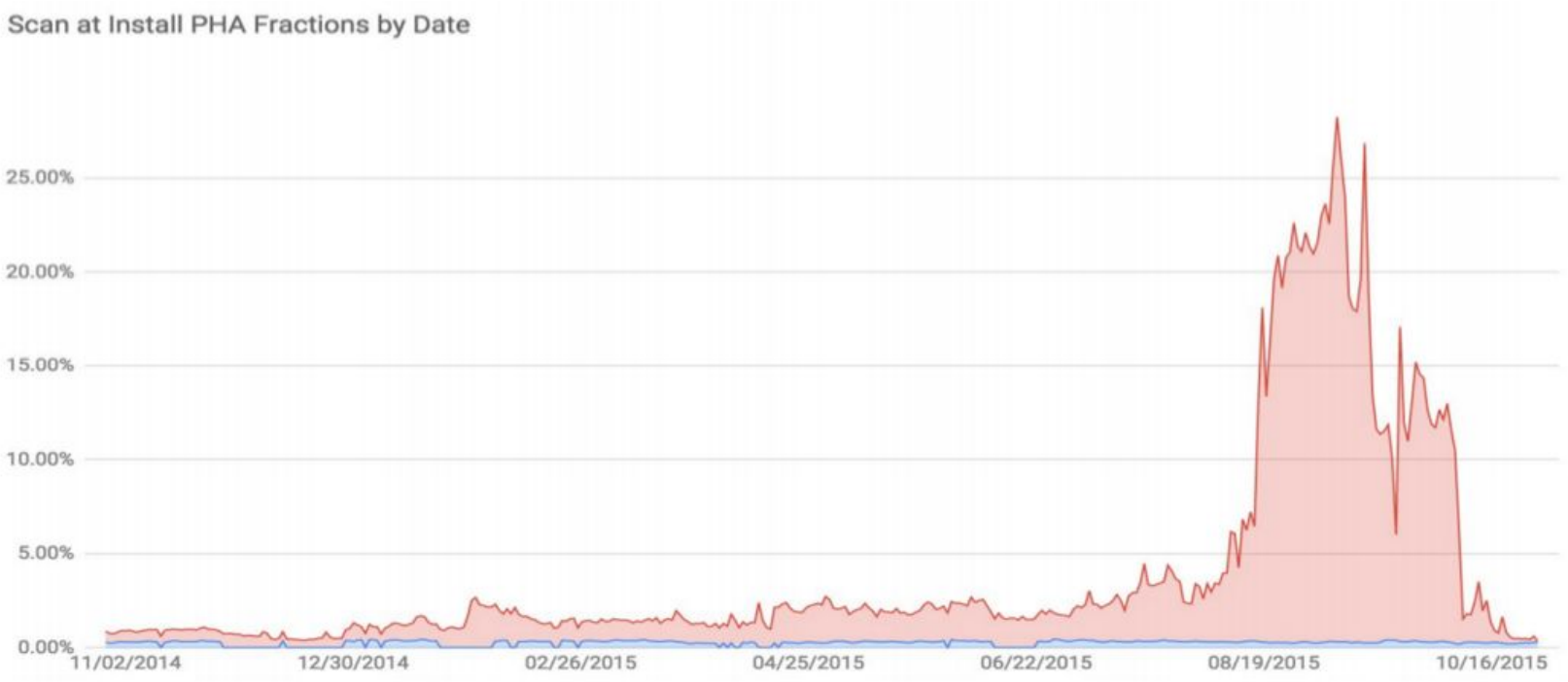


Source: https://source.android.com/devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf

Pre-installed apps are the next

major security risk.

Pre-installed apps installing malware



Ability to remove all apps

DevicePolicyManager

Ability to remove apps that evade removal through DevicePolicyManager. First used to protect against a large fraud campaign against a Russian bank.

System apps

Ability to disable system apps. We've seen massive growth in compromise of devices via pre-installed apps in the last 4 months.

Key metrics

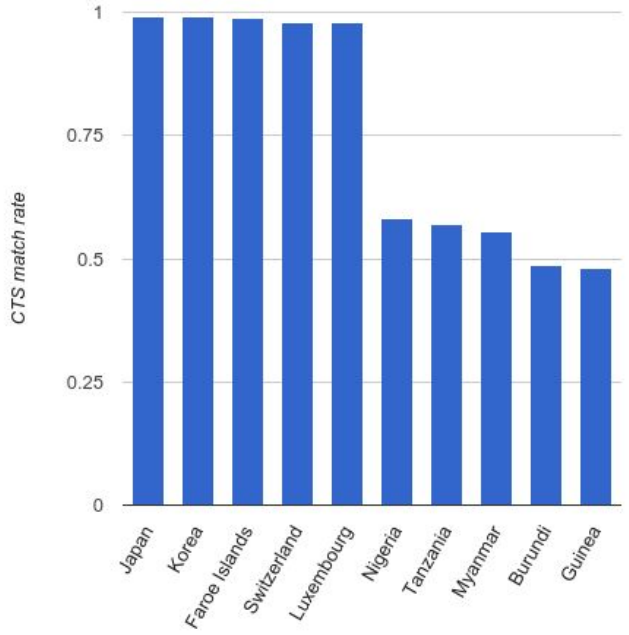
1.4B	Users
100%	Play apps are reviewed
99.5%	Devices have no known malware installed

SafetyNet APIs

Is this device CTS compatible?

Checking Device Compatibility with SafetyNet Attest

- Detects CTS state despite advanced tampering
- Can be used for app servers to identify apps communicating with them
- 10 major applications (including Android Pay, Snapchat, and Shopkick)



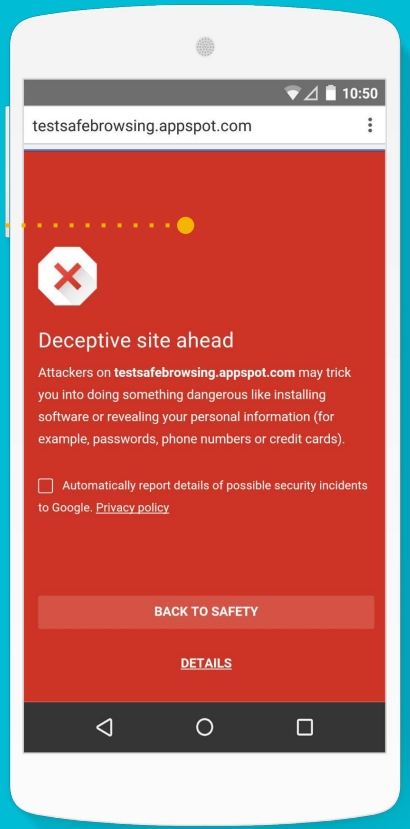
Resources: http://developer.android.com/training/safetynet

Is this website harmful?

Safe browsing launched in Chrome

Alerts on phishing, malware, and social engineering attacks

3P API and WebView integration coming in 2016



Sensor network

Tracking attempted exploits

Vulnerability Logging

- Instrument security patches to log when an exploit is attempted on a patched device
- Used to identify rooting attempts and SSL exploits
- All new security fixes to the platform require vulnerability logging

Android Device Manager

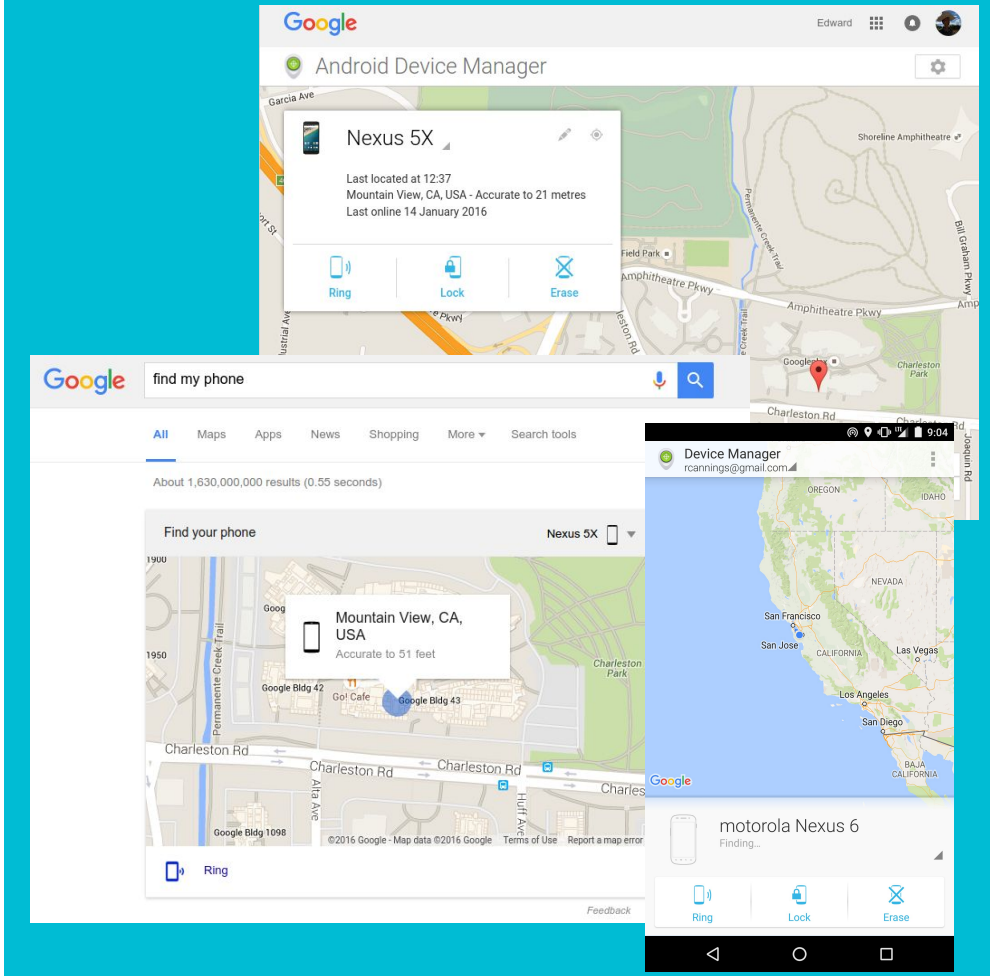
android

Where is my phone?

1M devices located per day

Features

- Part of Google Play Services
- Web app
- Android app
- Search integration: “find my phone”



android

Do devices need security apps?

No

Enjoy. It’s safe out there.

THANK YOU