Kaspersky®

SECURITY
ANALYST
SUMMIT

Protecting Android users against harmful apps

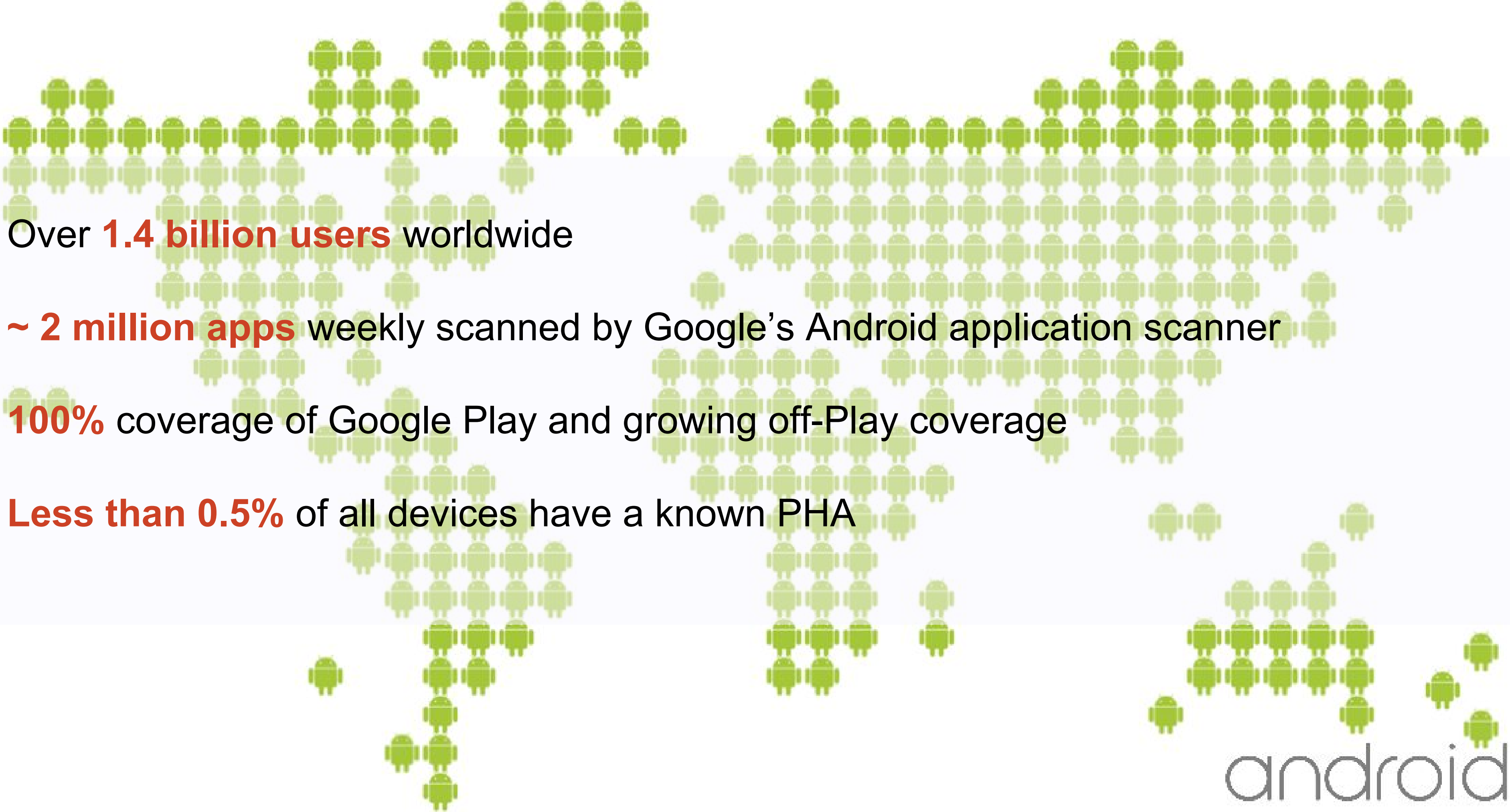
Elena Kovakina
Android Security

kovakina@google.com

Before I start - some terminology

Potentially Harmful App (PHA) - Our own term meaning apps that might be harmful to user or device

Term both wider and narrower than “Malware”. Together with universally harmful categories (trojans, ransomware, billing fraud), it includes non-malicious rooting, which is intentional yet still harmful.



Over **1.4 billion users** worldwide

~ 2 million apps weekly scanned by Google's Android application scanner

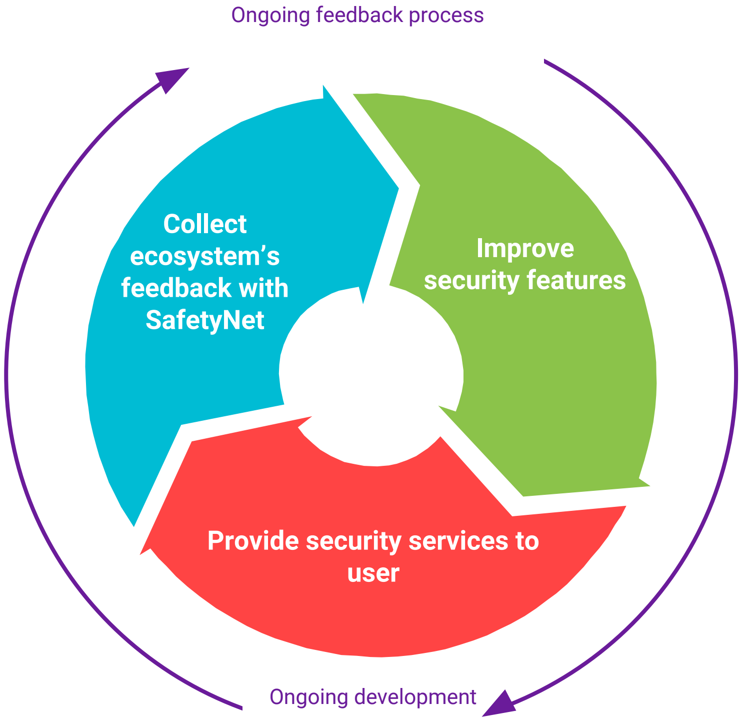
100% coverage of Google Play and growing off-Play coverage

Less than 0.5% of all devices have a known PHA

android

Building a feedback loop

- Security settings
- Feature use
- Warnings and prompts
- Granting privileged access
- PHA removal


Ongoing feedback process
Collect ecosystem's feedback with SafetyNet
Improve security features
Provide security services to user
Ongoing development

Protecting Android users against harmful apps

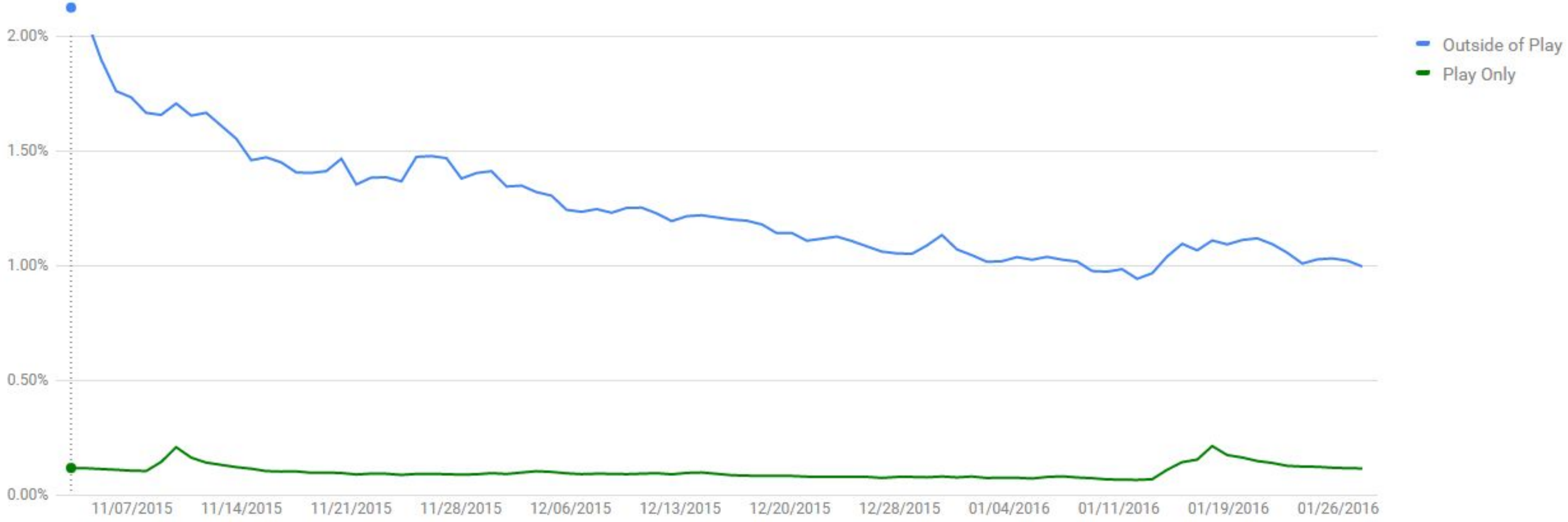
Billions of choices

android

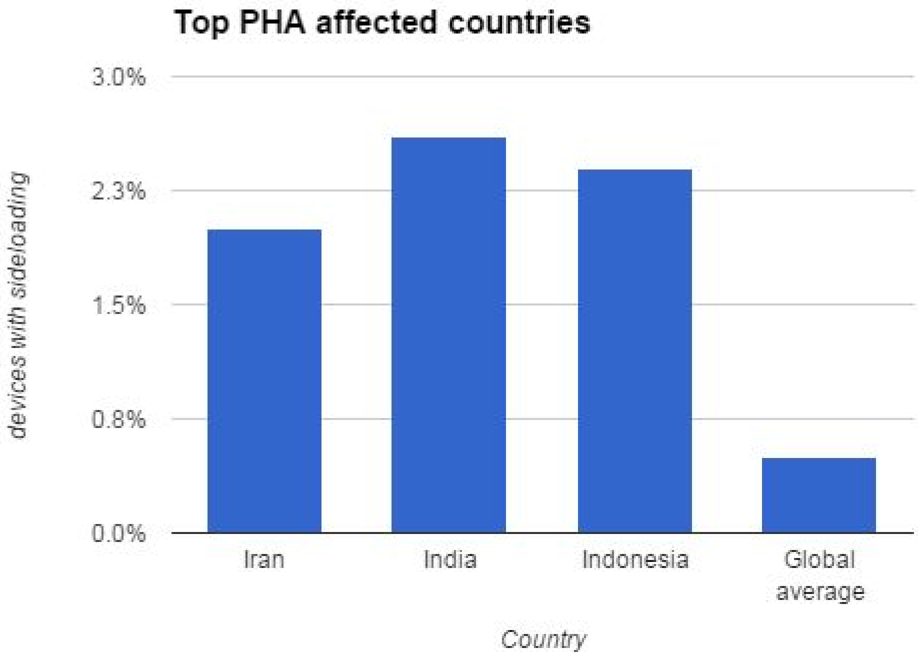
Choice #1 : To Play or not to Play?

Choosing Google Play is 10x safer

Daily % of devices with known PHAs (except non-malicious rooting) for past 3 months



Countries with most devices with known PHAs



Based on data from second half of 2015:

Iran: 2%

India: 2.6%

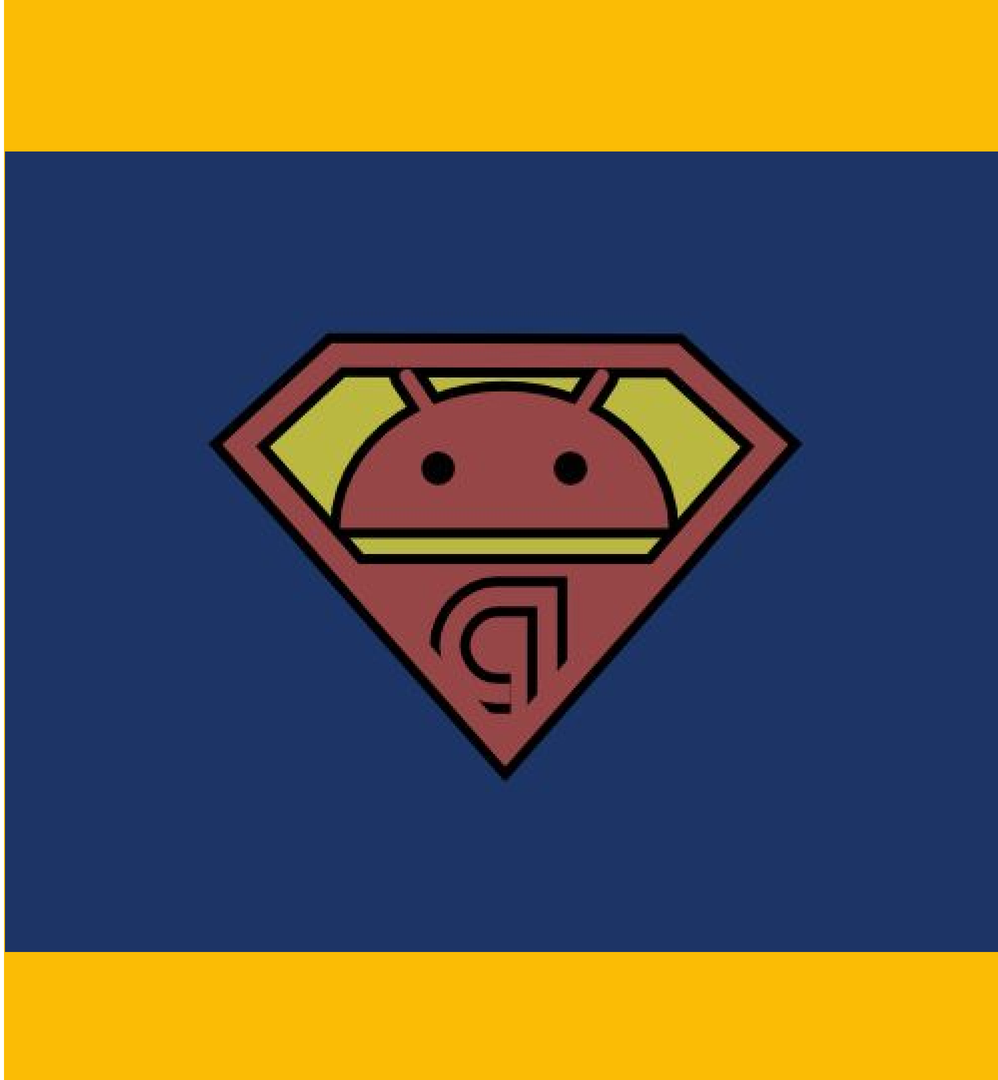
Indonesia: 2.4%

Global average: **less than 0.5%**

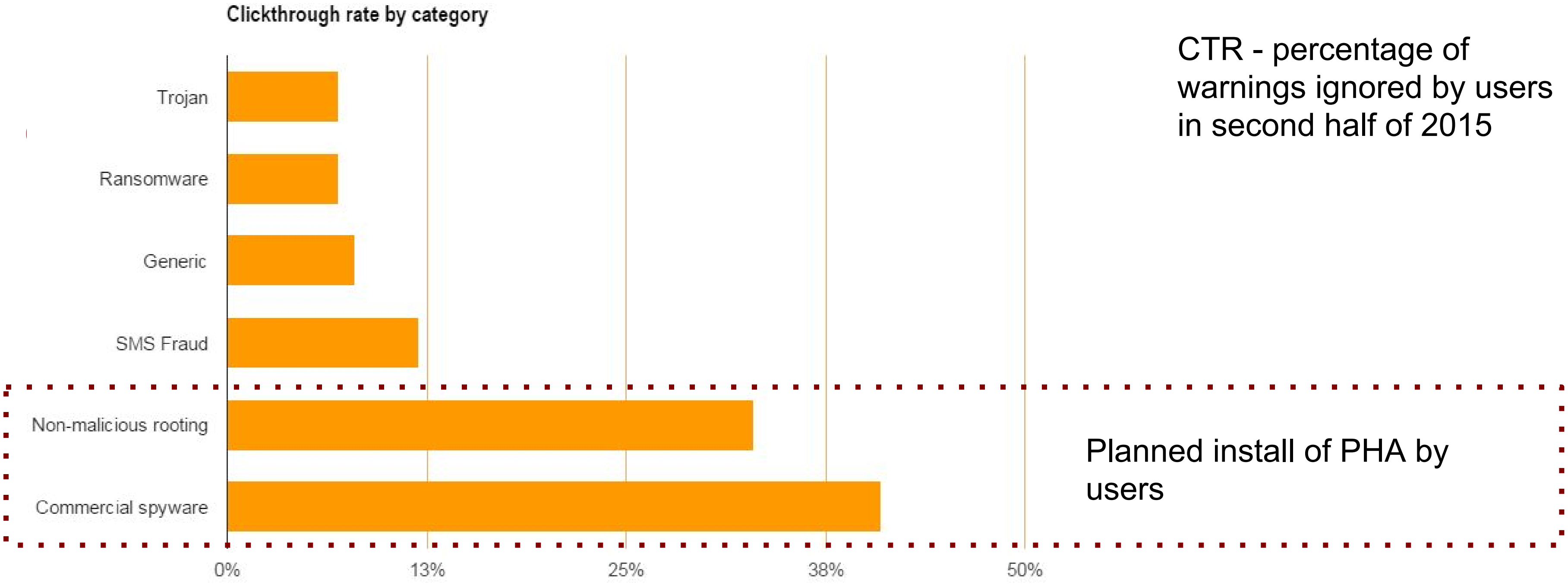
Choice #2: Stay safe in the wild

Verify Apps

- Has been available since 2011
- Same scanning backend as Play
- 1.4 billion users enrolled (by consent)
- Able to block install



High and low clickthrough rates by category



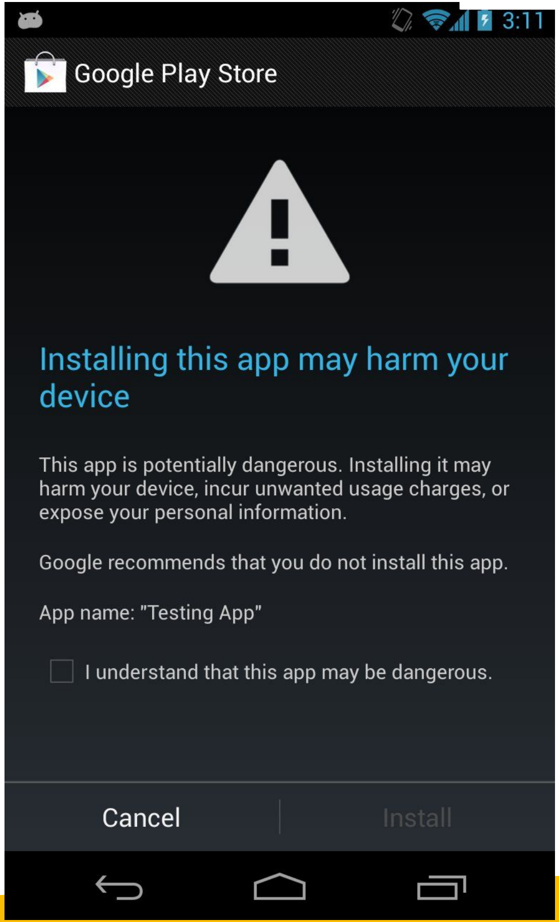
CTR - percentage of warnings ignored by users in second half of 2015

Planned install of PHA by users

Google

Verify Apps UX improvement

Previously warnings required extra click to verify user is aware the app is dangerous to activate “Install” option



Installing this app may harm your device

This app is potentially dangerous. Installing it may harm your device, incur unwanted usage charges, or expose your personal information.

Google recommends that you do not install this app.

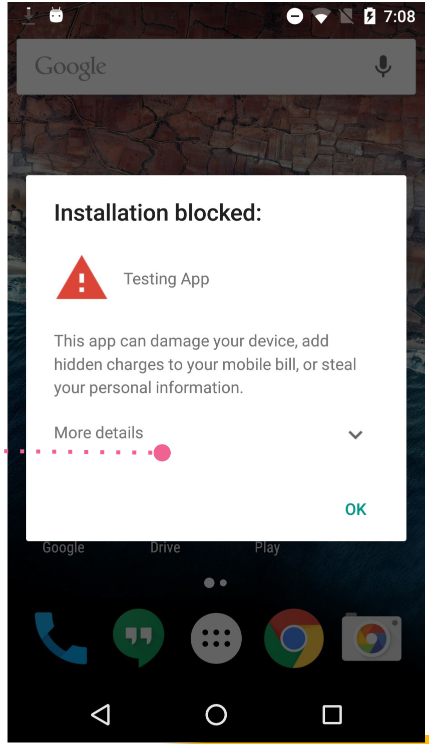
App name: "Testing App"

□ I understand that this app may be dangerous.

Verify Apps UX improvement

New warning dialog makes safer choice more intuitive for the user

Up to **50%** less users are installing PHAs when warned with the new dialogs.

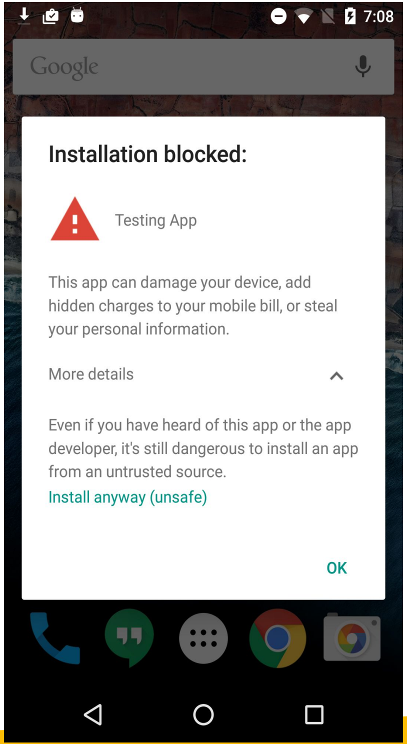


Installation blocked:

Testing App

This app can damage your device, add hidden charges to your mobile bill, or steal your personal information.

More details



Installation blocked:

Testing App

This app can damage your device, add hidden charges to your mobile bill, or steal your personal information.

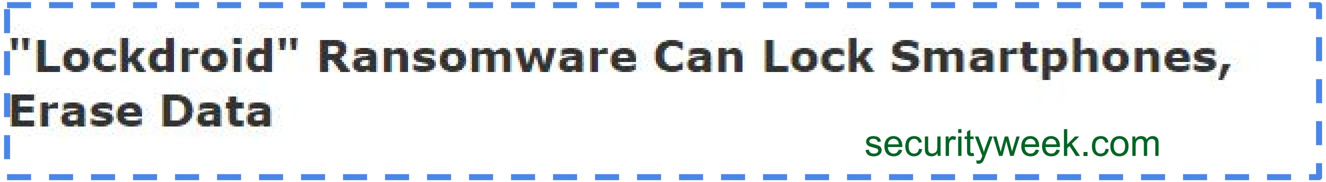
More details

Even if you have heard of this app or the app developer, it's still dangerous to install an app from an untrusted source.

Install anyway (unsafe)

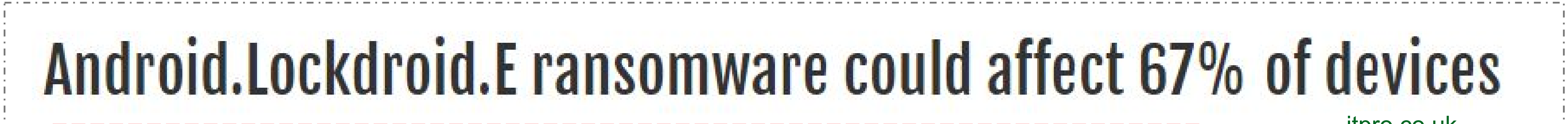
Campaigns as we see them - In actual numbers

News headlines:



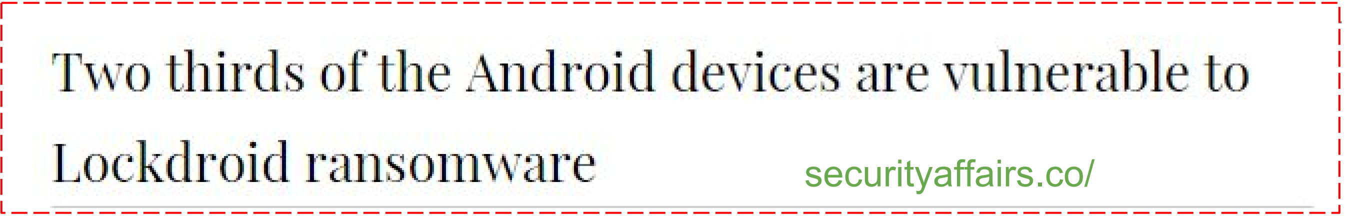
"Lockdroid" Ransomware Can Lock Smartphones, Erase Data

securityweek.com



Android.Lockdroid.E ransomware could affect 67% of devices

itpro.co.uk

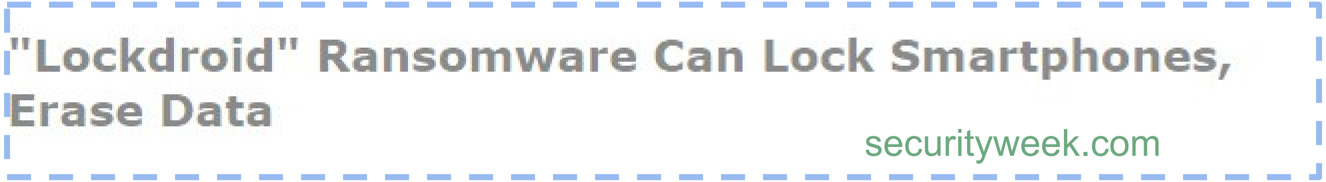


Two thirds of the Android devices are vulnerable to Lockdroid ransomware

securityaffairs.co/

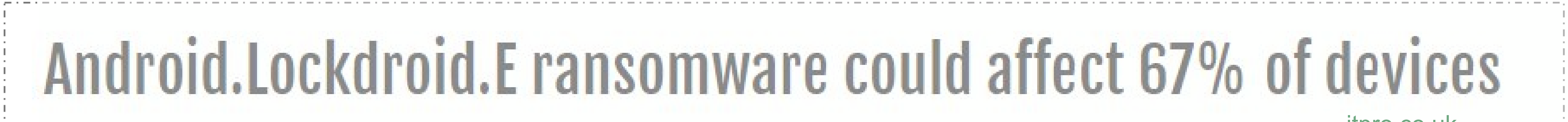
Campaigns as we see them - In actual numbers

News headlines:



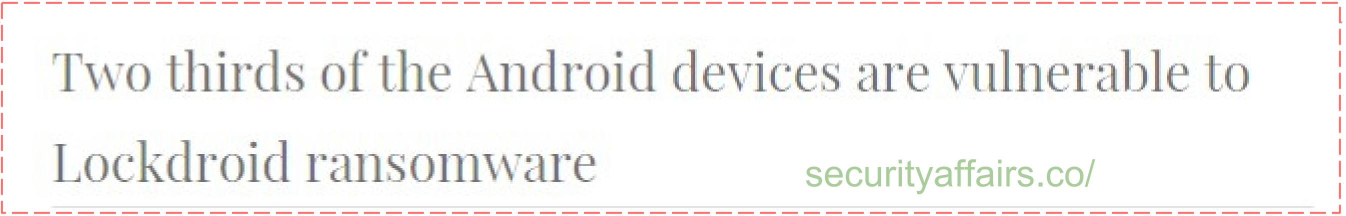
"Lockdroid" Ransomware Can Lock Smartphones, Erase Data

securityweek.com



Android.Lockdroid.E ransomware could affect 67% of devices

itpro.co.uk



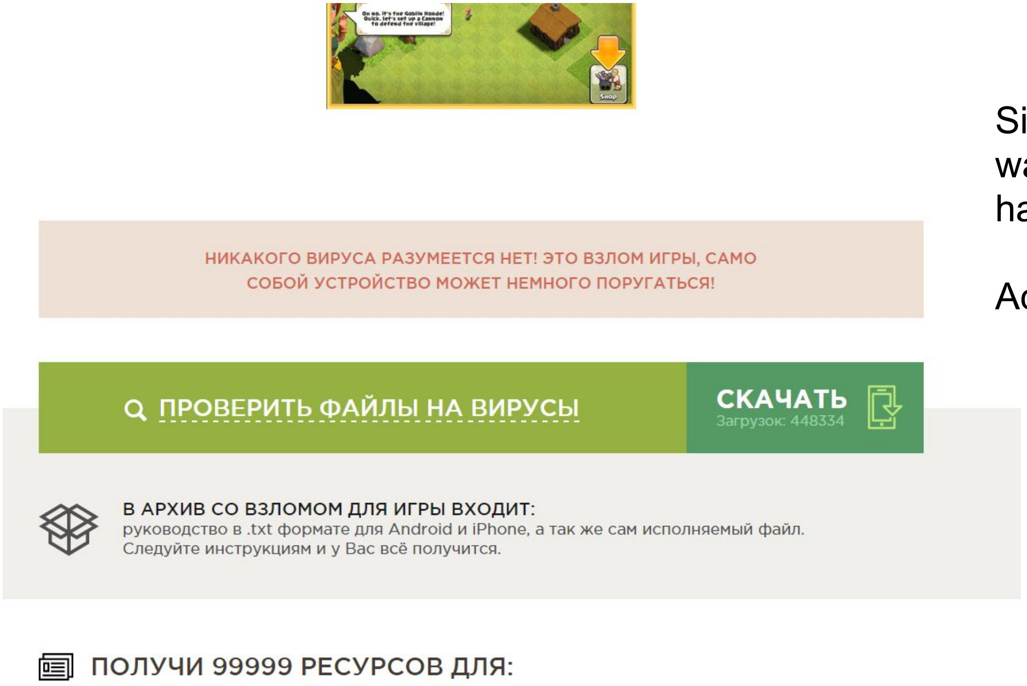
Two thirds of the Android devices are vulnerable to Lockdroid ransomware

securityaffairs.co/

Worldwide downloads: **less than 1000**

Confirmed installs: **None**

Spotting anomalies in the wild:


Oh no, it's the Goblin Horde! Quick, let's set up a Cannon to defend the village!
Shop

НИКАКОГО ВИРУСА РАЗУМЕЕТСЯ НЕТ! ЭТО ВЗЛОМ ИГРЫ, САМО СОБОЙ УСТРОЙСТВО МОЖЕТ НЕМНОГО ПОРУГАТЬСЯ!

ПРОВЕРИТЬ ФАЙЛЫ НА ВИРУСЫ

СКАЧАТЬ
Загрузок: 448334

В АРХИВ СО ВЗЛОМОМ ДЛЯ ИГРЫ ВХОДИТ:
руководство в .txt формате для Android и iPhone, а так же сам исполняемый файл. Следуйте инструкциям и у Вас всё получится.

ПОЛУЧИ 99999 РЕСУРСОВ ДЛЯ:

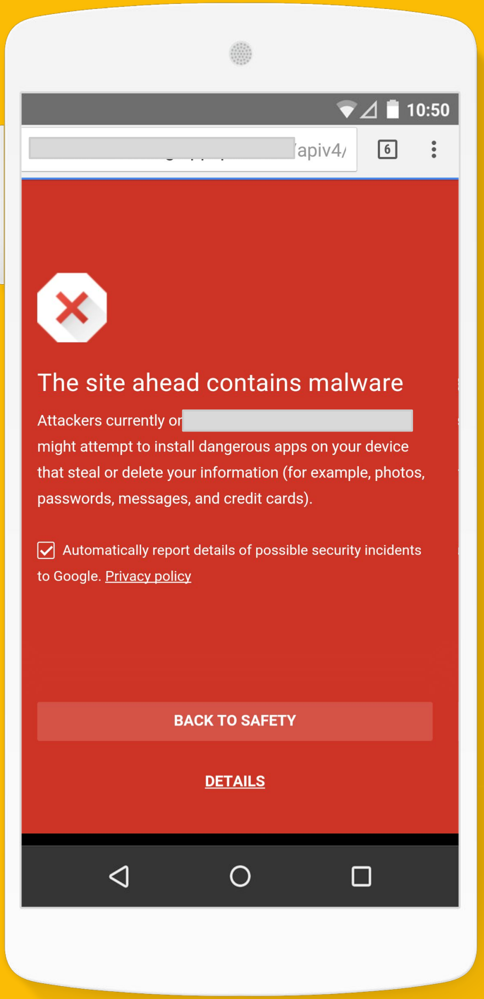
Site claiming users should ignore security warnings (and disable AVs) because “It’s hacked software”

Actually distributes bank phishing trojan

Safe Browsing on mobile Chrome:

- Adding extra layer of protection against potentially dangerous downloads

- Also protects against browser-based phishing and social engineering



10:50

[redacted]apiv4/

The site ahead contains malware

Attackers currently on [redacted] might attempt to install dangerous apps on your device that steal or delete your information (for example, photos, passwords, messages, and credit cards).

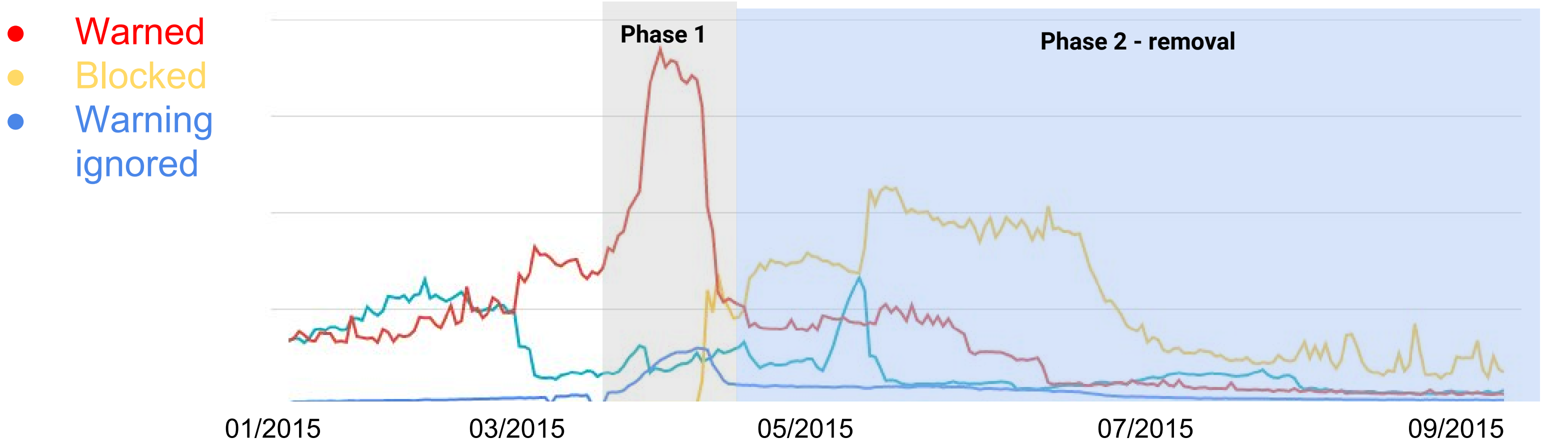
☑ Automatically report details of possible security incidents to Google. Privacy policy

Choice #3: Keep it or remove it?

What uninstall data tells us

- Not all Verify Apps on-device scans result in user uninstalling a malicious app
- Do users really want to keep PHAs, or are there other factors that get in their way?

Example: Bank Phishing in Russia

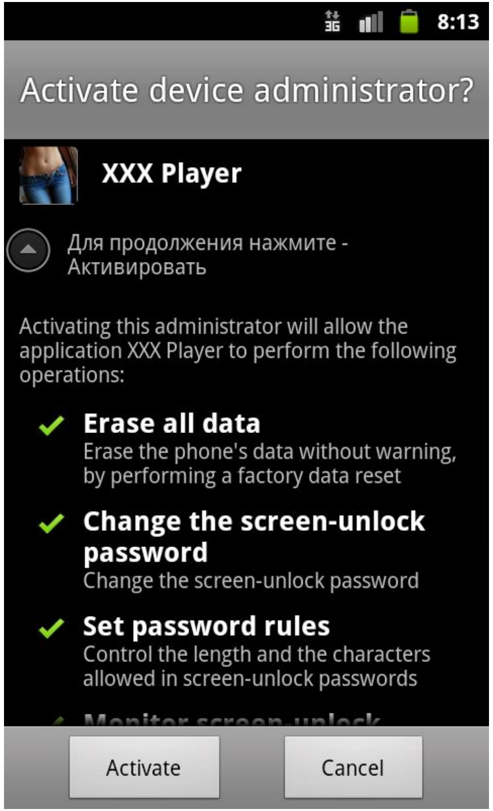


Daily warnings for devices with tracked PHA families between January 1st 2015 and September 1st 2015

Device admin abuse

- PHAs commonly use Device Admin to make uninstall more tricky to user
- In May 2015 we started using Intent Firewall to intercept ACTION_DEVICE_ADMIN_DISABLE_REQUESTED

Impact?



Activate device administrator?

XXX Player

Для продолжения нажмите - Активировать

Activating this administrator will allow the application XXX Player to perform the following operations:

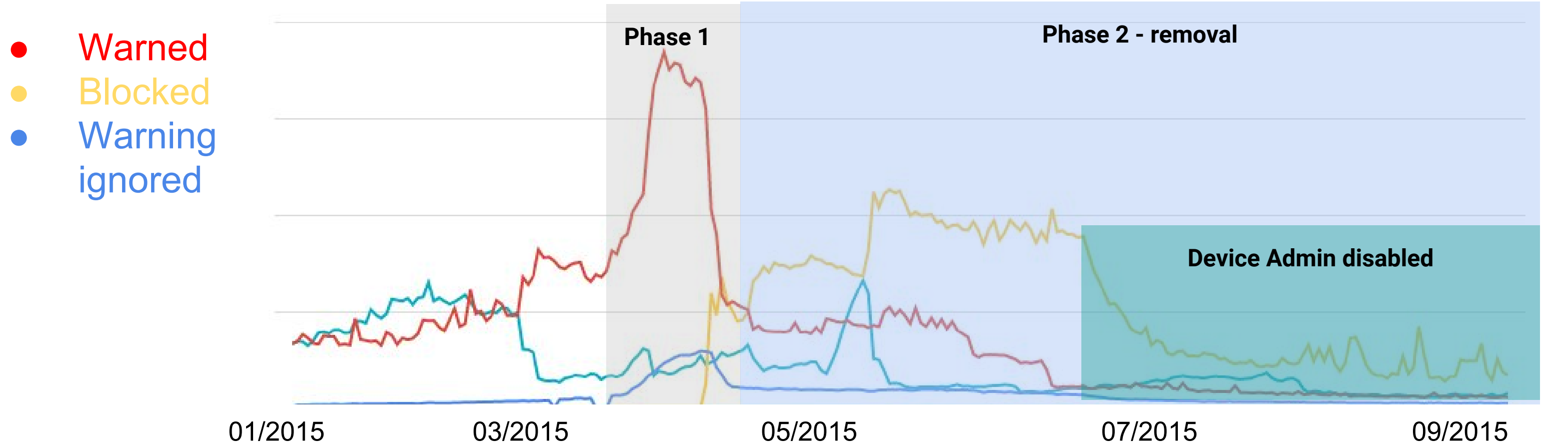
✓ **Erase all data**
Erase the phone's data without warning, by performing a factory data reset

✓ **Change the screen-unlock password**
Change the screen-unlock password

✓ **Set password rules**
Control the length and the characters allowed in screen-unlock passwords

✓ **Monitor screen-unlock**

Example: Bank Phishing in Russia



Daily warnings for devices with tracked PHA families between January 1st 2015 and September 1st 2015

To sum it up:

- Verify Apps can override persistency features of most known PHAs
- We can use auto-removal when user is in danger, but use it sparingly
- Verify Apps allows us to get a bigger perspective and understand ongoing trends in exploitation and abuse

* Estimation based on statistics for PHAs that are blocked. Excludes Ransomware.

Conclusion: Staying aware

Bigger picture

- Potentially Harmful Apps
- Compromised security model (rooting, SELinux status)
- Device protection with lockscreen password
- Device encryption
- Exploitation and abuse attempts (premium SMS, device admin, dynamic permissions)

LET'S TALK?

security@android.com

Learn more:

Android Security State of the Union - https://goo.gl/D7QUm8