RSA CONFERENCE ASIA PACIFIC 2013

Security in knowledge

MOBILE WEB REPUTATION: TRACING BAD TERRITORIES ON YOUR SMARTPHONE

Myla V. Pilao

Director Core Technology Trend Micro

Session ID: MBS-T04

Session Classification: Intermediate

2.7B
Internet Users[1]

1 Trillion+ URLs
indexed
by Google[2]

665M
Web Sites[3]

54%
of Facebook
Access is via
Mobile[6]

300M
Mobile Financial Users[4]

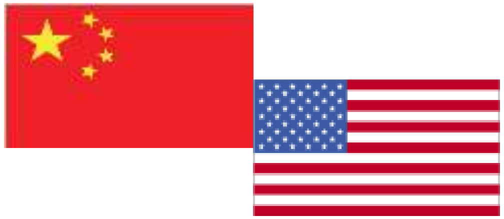
1B
Smart Phones in
use[5]

Sources – 1: ITU ; 2: Google, 2008; 3: NetCraft Site Data, July 2012;
4: Junifer, Oct 2012; 5: mobiThinking; 6: SocialBakers, May 2012;

Mobile Users

96%

246M



194%

Ave adoption rate

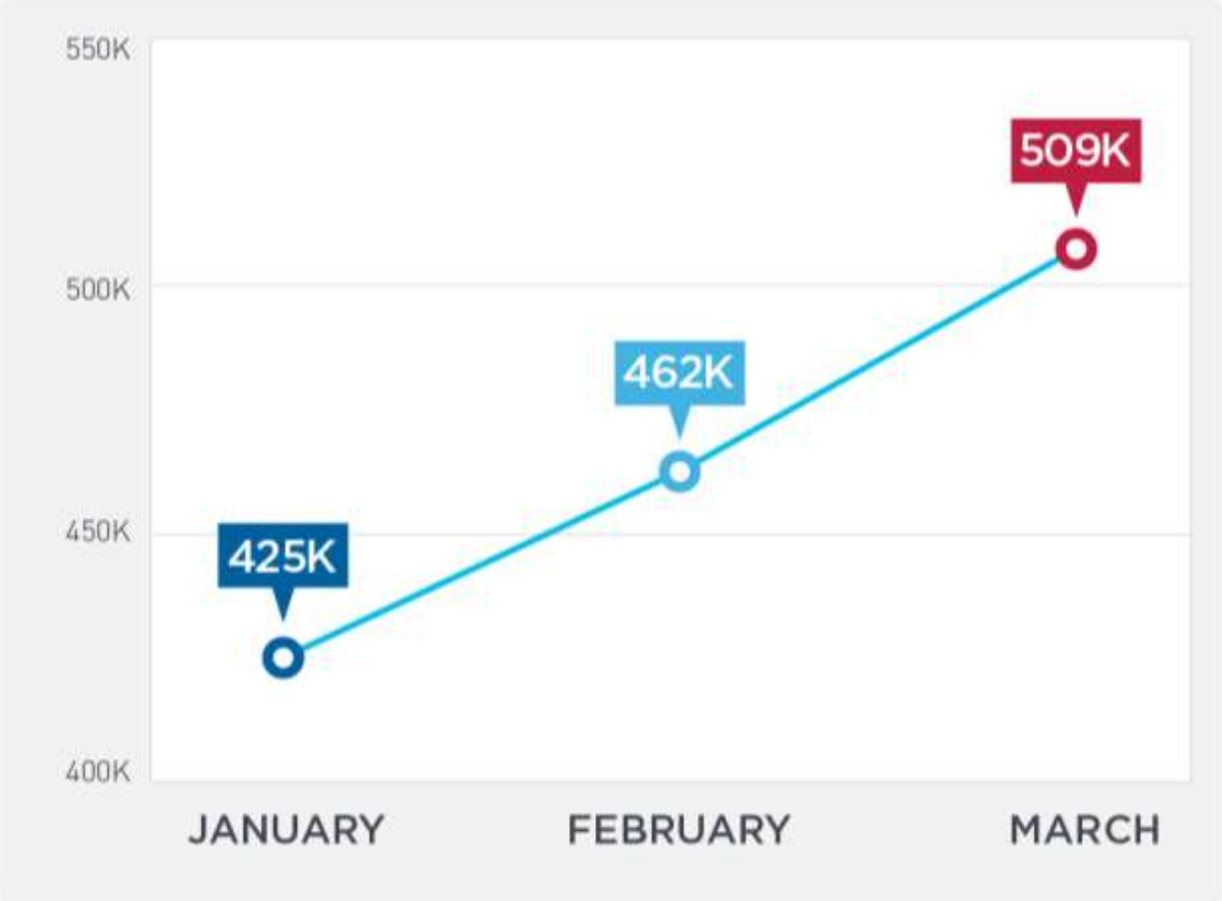
RSA CONFERENCE ASIA PACIFIC 2013

Everything's Coming Up Mobile

File emphasis is a fallacy

Mobile Threats on the Rise

Android Threat Volume Growth, Q1 2013

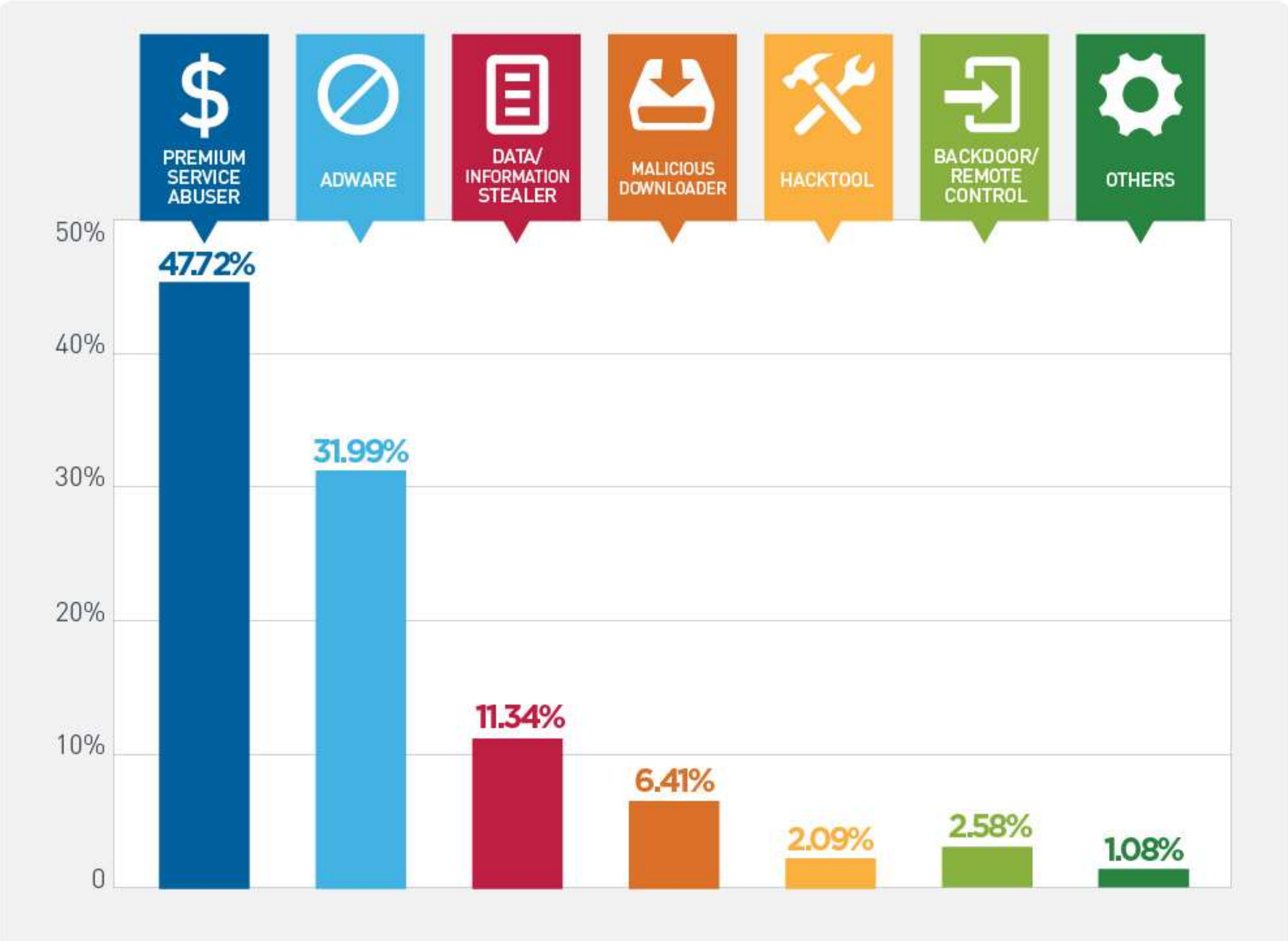


The Android threat volume has reached the halfway mark to our predicted 1M threats

Distribution of Android Threat Types, Q1 2013

Premium service abusers register users to **overpriced services**

Adware aggressively push ads and may even **collect personal information**

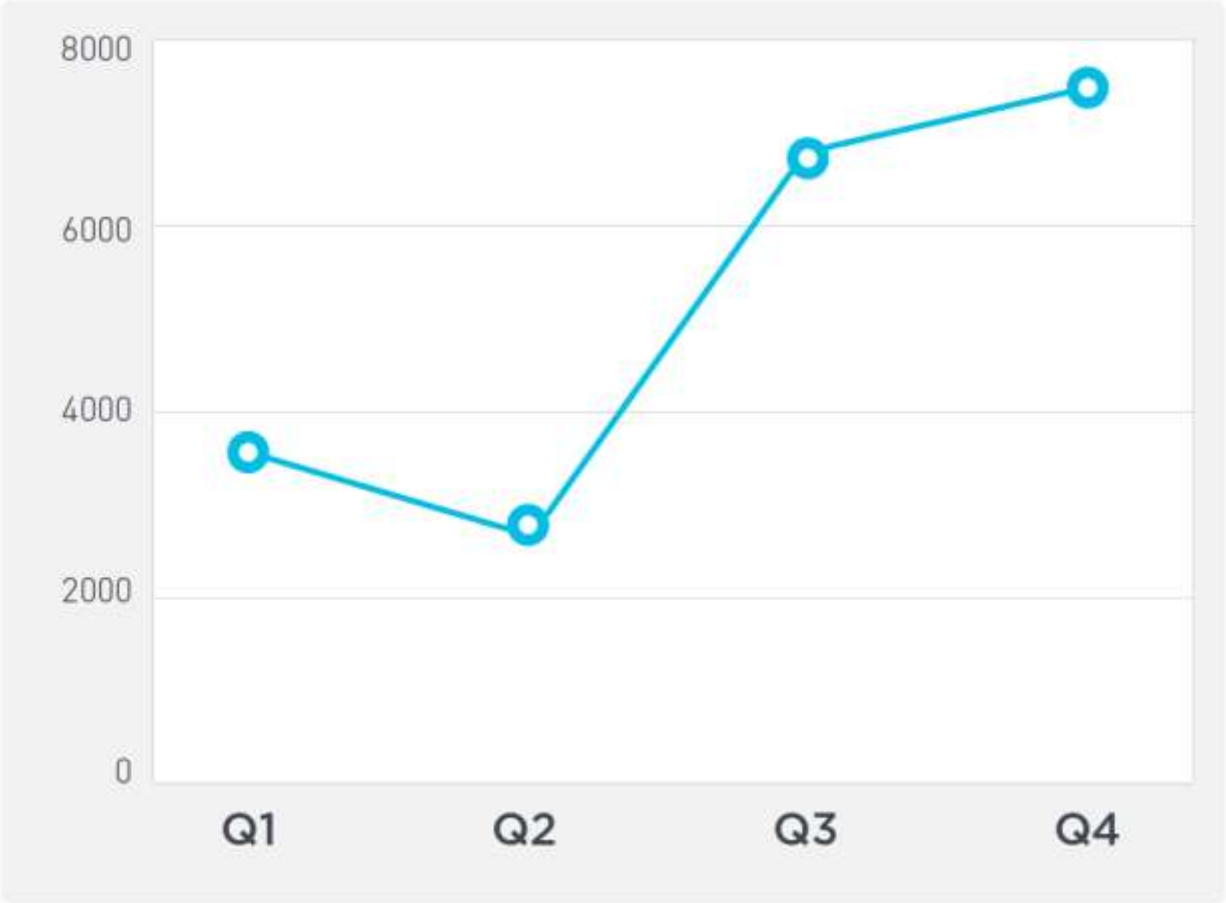


Malicious apps are just one piece of the puzzle.

RSA CONFERENCE ASIA PACIFIC 2013

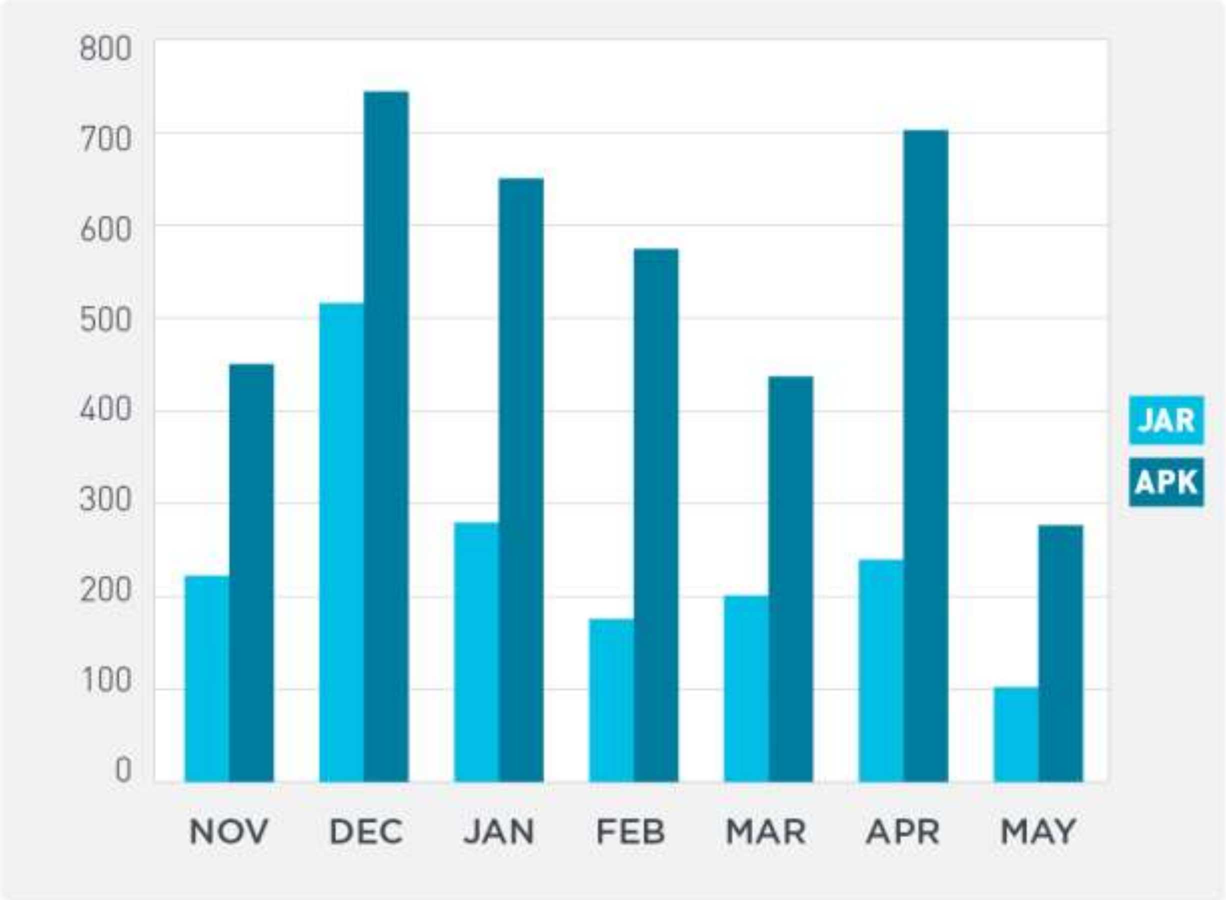
Malicious Domains: What Goes In

Malicious Domains in 2012



- Malicious domain count related to Android apps in 2012

Number of Visited Download Sites



The Role of Social Engineering

- Majority of the monitored URLs contain keywords related to browser updates, gaming apps, and Android rooters.
  - “Flash Player” was one of the top keywords used

- Forums, blog posts, and emails are also used to spread bad apps

The Great Migration: From China to Russia

- China
  - third-party app stores became popular, partly due to limited access to Google Play
  - possible lack of resources required to maintain effective levels of monitoring and testing
  - stricter rules about domain registration was implemented in 2010

- Russia
  - lax laws concerning domain registration
  - lax premium SMS regulations

Perils of Popularity

- Cut the Rope
- 17 domains

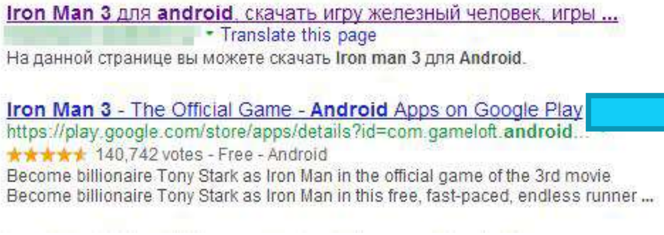
- Asphalt 6:Adrenaline
- 9 domains

- Where’s My Water?
- 8 domains

as of July 2012

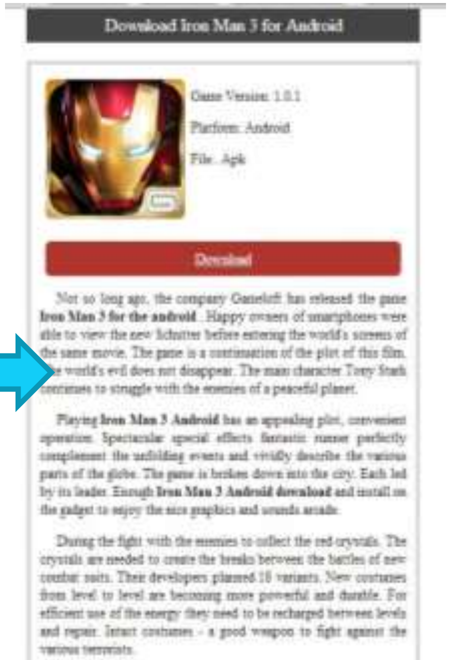
Image Source: Google Play

A Sequence of Redirections



Iron Man 3 для android, скачать игру железный человек, игры ...
[redacted] ▾ Translate this page
На данной странице вы можете скачать **Iron man 3** для **Android**.

Iron Man 3 - The Official Game - **Android** Apps on Google Play
https://play.google.com/store/apps/details?id=com.gameloft.**android**...
★★★★★ 140,742 votes - Free - Android
Become billionaire Tony Stark as Iron Man in the official game of the 3rd movie
Become billionaire Tony Stark as Iron Man in this free, fast-paced, endless runner ...



Download Iron Man 3 for Android

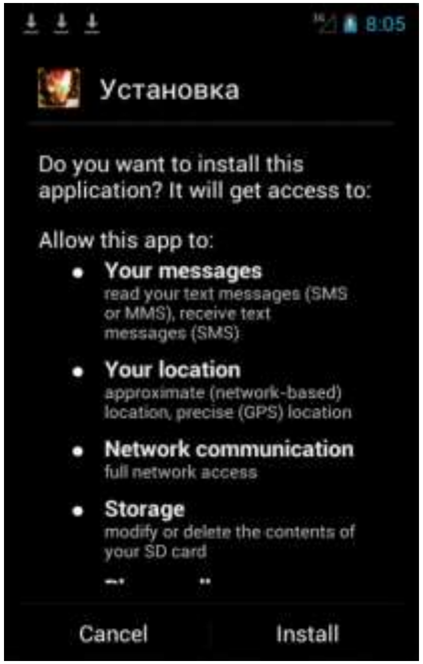
Game Version: 1.0.1
Platform: Android
File: Apk

Download

Not so long ago, the company Gameloft has released the game **Iron Man 3 for the android**. Happy owners of smartphones were able to view the new blockbuster before entering the world's screens of the same movie. The game is a continuation of the plot of this film. The world's evil does not disappear. The main character Tony Stark continues to struggle with the enemies of a peaceful planet.

Playing **Iron Man 3 Android** has an appealing plot, convenient operation. Spectacular special effects fantastic runner perfectly complement the unfolding events and vividly describe the various parts of the globe. The game is broken down into the city. Each led by its leader. Enough **Iron Man 3 Android download** and install on the gadget to enjoy the nice graphics and sounds arcade.

During the fight with the enemies to collect the red crystals. The crystals are needed to create the breaks between the battles of new combat suits. Their developers planned 16 variants. New costumes from level to level are becoming more powerful and durable. For efficient use of the energy they need to be recharged between levels and repair. Intact costumes - a good weapon to fight against the various terrorists.



Установка

Do you want to install this application? It will get access to:

Allow this app to:

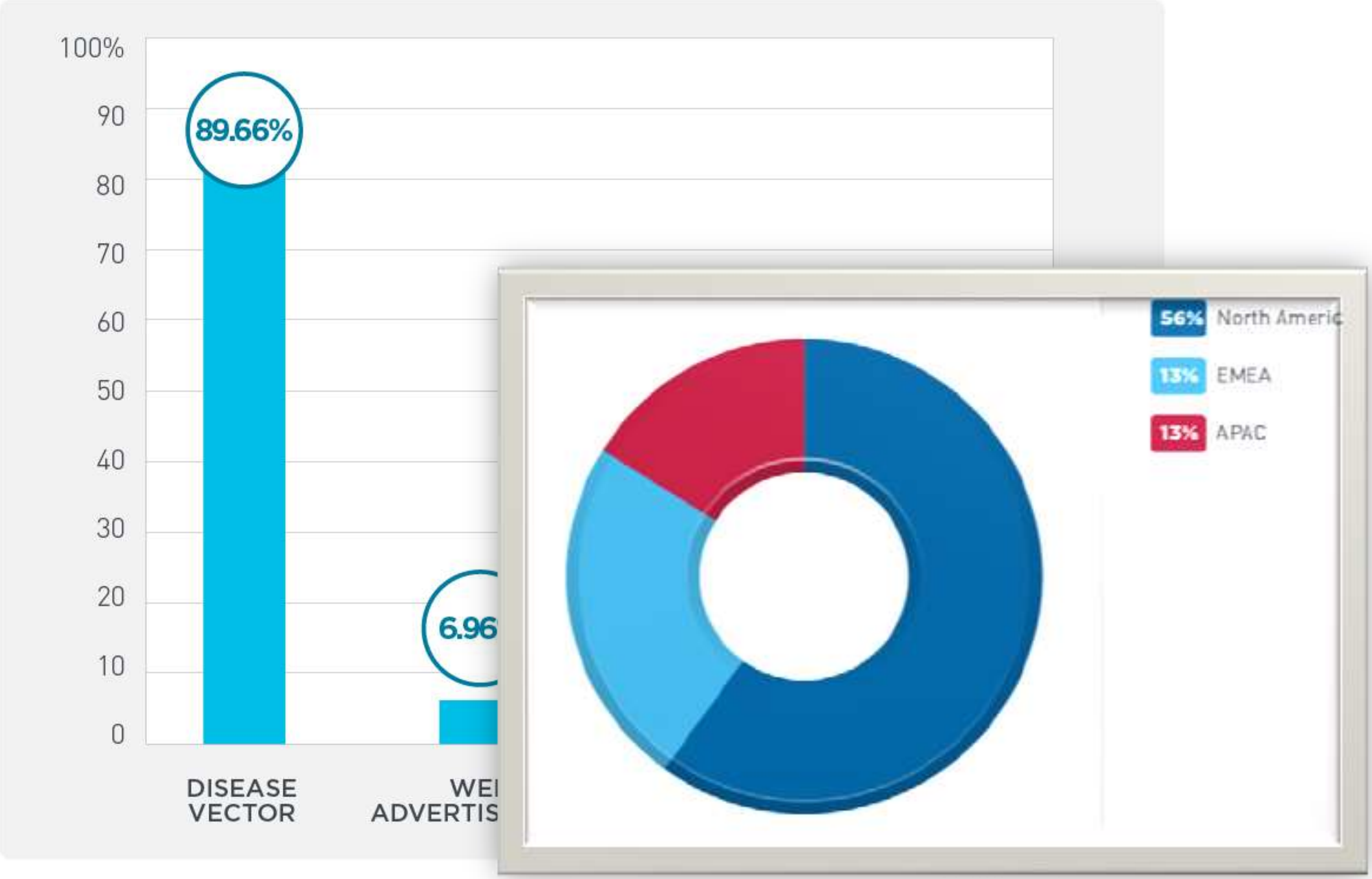
- **Your messages**
  read your text messages (SMS or MMS), receive text messages (SMS)
- **Your location**
  approximate (network-based) location, precise (GPS) location
- **Network communication**
  full network access
- **Storage**
  modify or delete the contents of your SD card

http://{BLOCKED}n3-android.ru/download.php

http://{BLOCKED}andex.com/…/iron_man_3_installer.apkoid.ru/download.php

- Users visit a website to download an app. Clicking the “download” button redirects them (unknowingly) to a different URL where the malicious app is hosted

Classification of Embedded URLs in Malicious Apps



- 90% of embedded URLs are categorized as “disease vectors.”

RSA CONFERENCE ASIA PACIFIC 2013

Implication of Malicious URLs

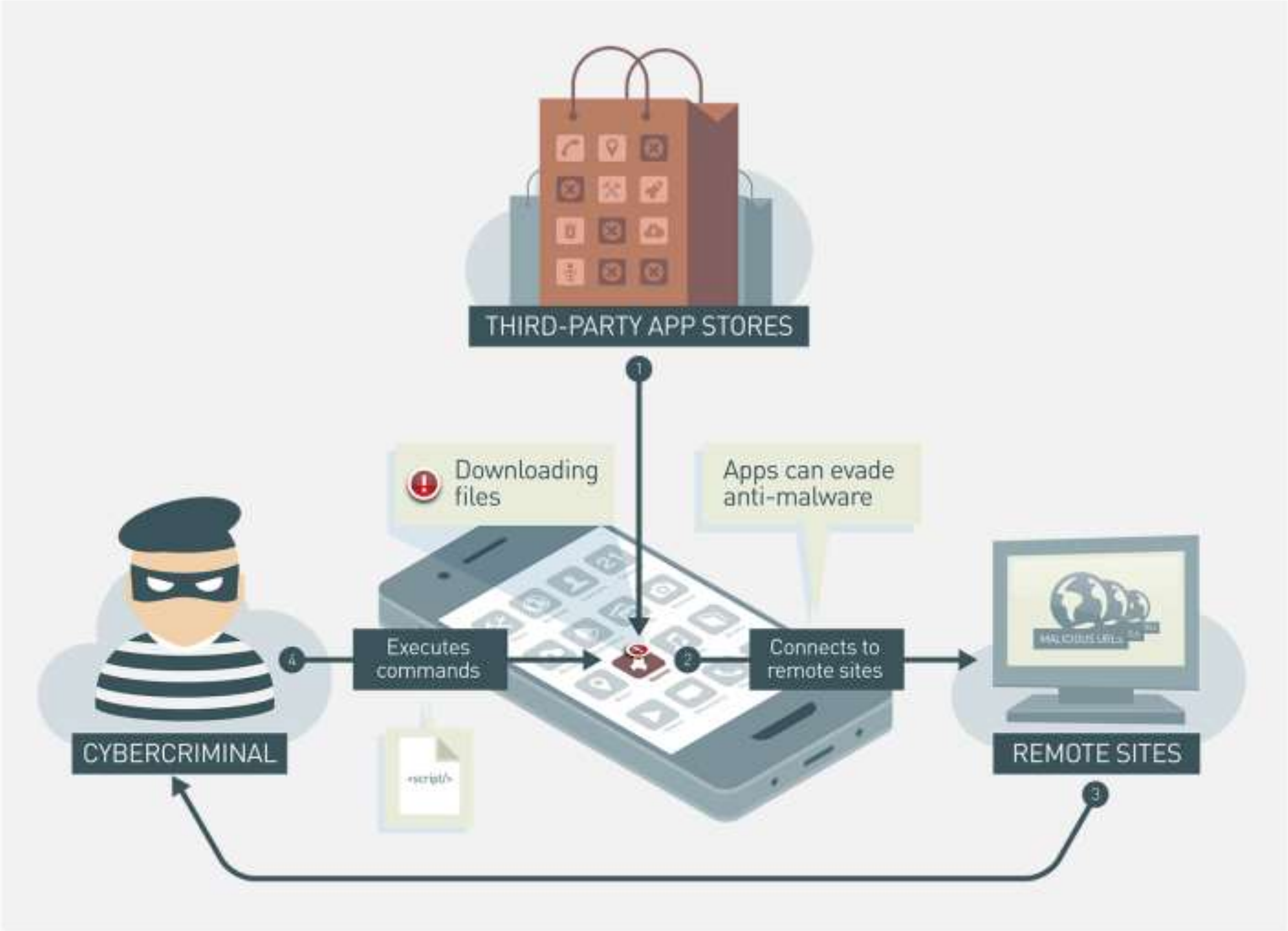
Threats are transitioning from PC to mobile with help from malicious URLs

Backdoors and Remote Servers

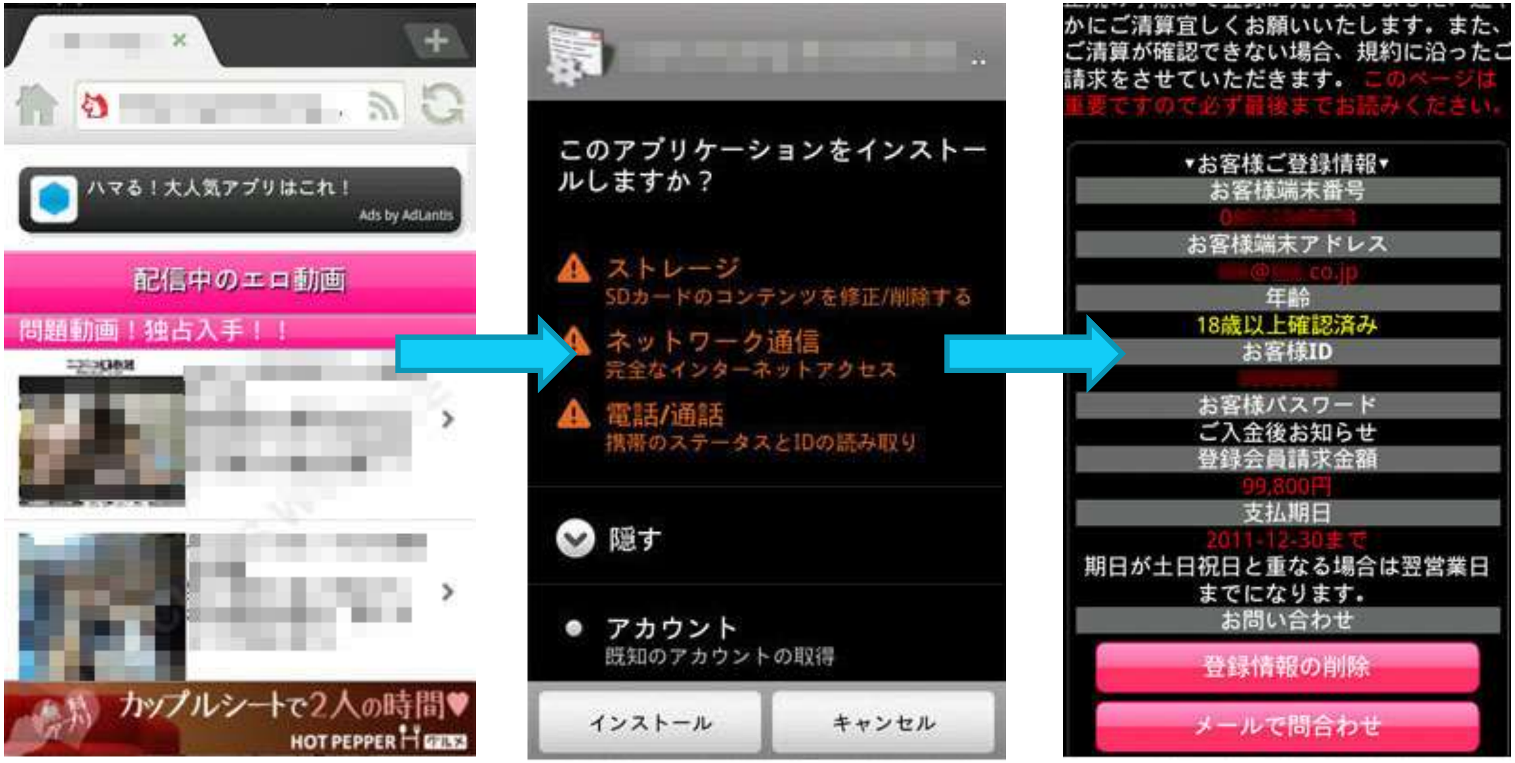
- ANDROIDOS_ ADVINST
  - polls its C&C server every four hours for new instructions
  - pushes several pieces of sensitive information including the device's phone number and its serial number (IMEI) up to the server

- ANDROIDOS_CHULI.A
  - used to attack Tibetan and Uyghur minorities
  - receives commands through SMS messages
  - opens a backdoor and sends stolen information to one remote location URL

Botnets on Your Mobile



One-Click Billing Fraud Goes Mobile 2



[redacted]

ハマる！大人気アプリはこれ！

Ads by AdLantis

配信中のエロ動画

問題動画！独占入手！！

[redacted]

カップルシートで2人の時間♥

HOT PEPPER

[redacted]

このアプリケーションをインストールしますか？

ストレージ
SDカードのコンテンツを修正/削除する

ネットワーク通信
完全なインターネットアクセス

電話/通話
携帯のステータスとIDの読み取り

隠す

● アカウント
既知のアカウントの取得

インストール | キャンセル

かにご清算宜しくお願いいたします。また、ご清算が確認できない場合、規約に沿ったご請求をさせていただきます。このページは重要ですので必ず最後までお読みください。

▾お客様ご登録情報▾

お客様端末番号
[redacted]

お客様端末アドレス
[redacted]@[redacted].co.jp

年齢
18歳以上確認済み

お客様ID
[redacted]

お客様パスワード

ご入金後お知らせ

登録会員請求金額
99,800円

支払期日
2011-12-30まで

期日が土日祝日と重なる場合は翌営業日までになります。

お問い合わせ

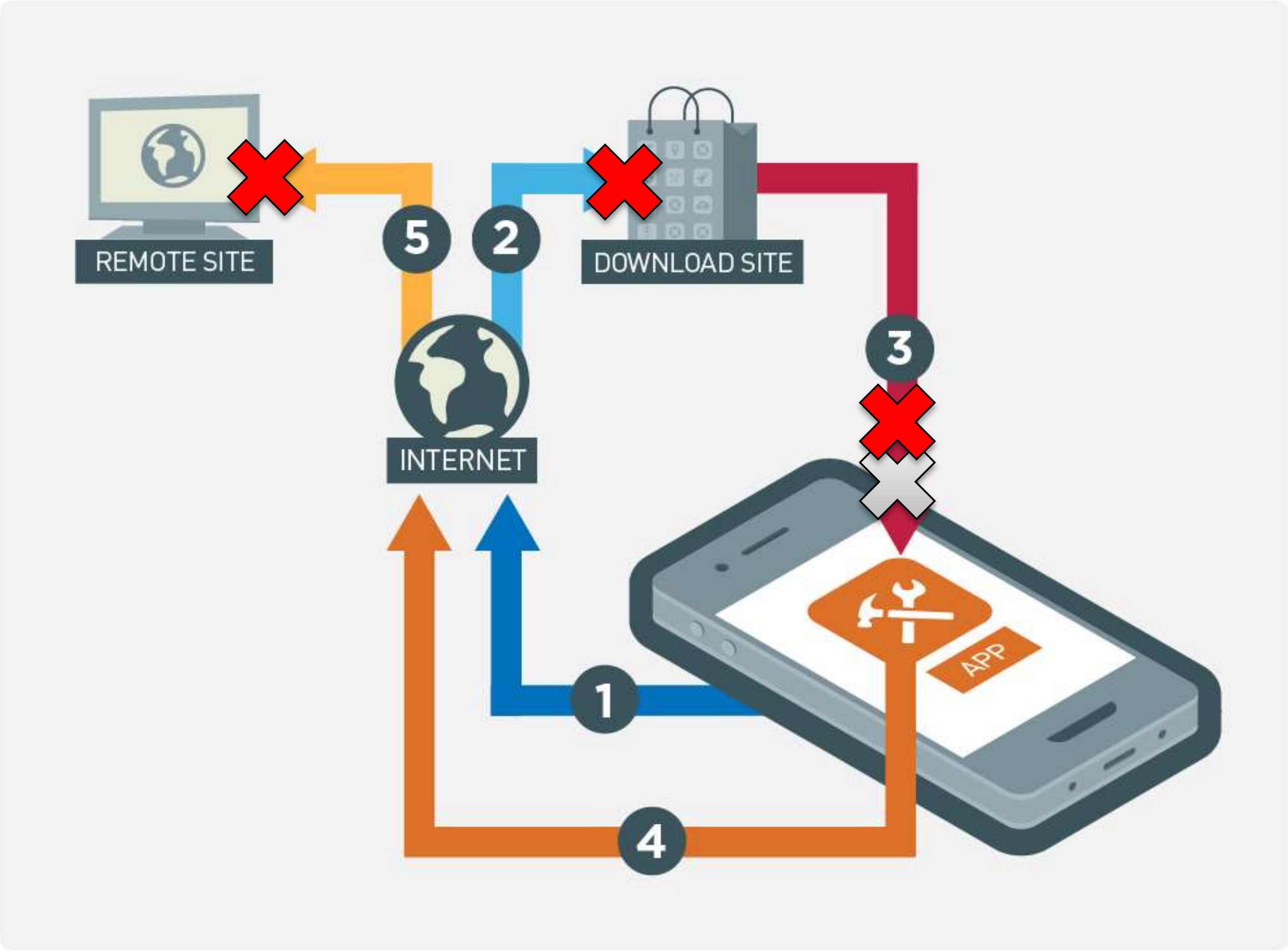
登録情報の削除

メールで問合わせ

- Users are asked to download a malicious app after visiting a blog site. This app asks users to pay a certain amount

Addressing Malicious URLs

Addressing the Issue at the Exposure Layer



next big thing

Next “Big” Things

- Continuous growth web attacks
- More financial-related fraud
- Shortened URLs and DDNS
- Traffic monetization
- Privacy loss and identity theft
- Advanced Persistent Threats (APTs) on Android

Thank you

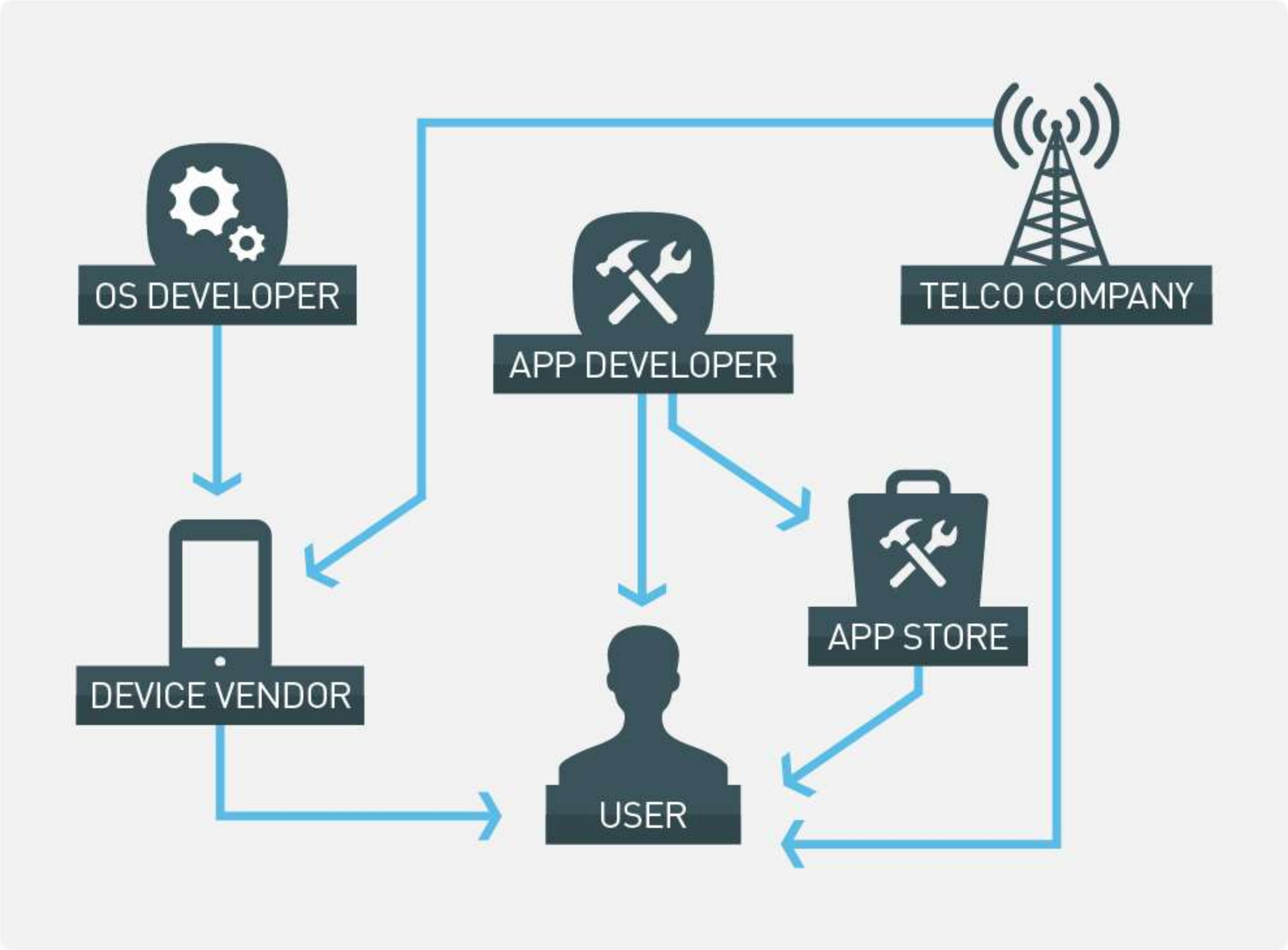
Myla V. Pilao

myla_pilao@trendmicro.com

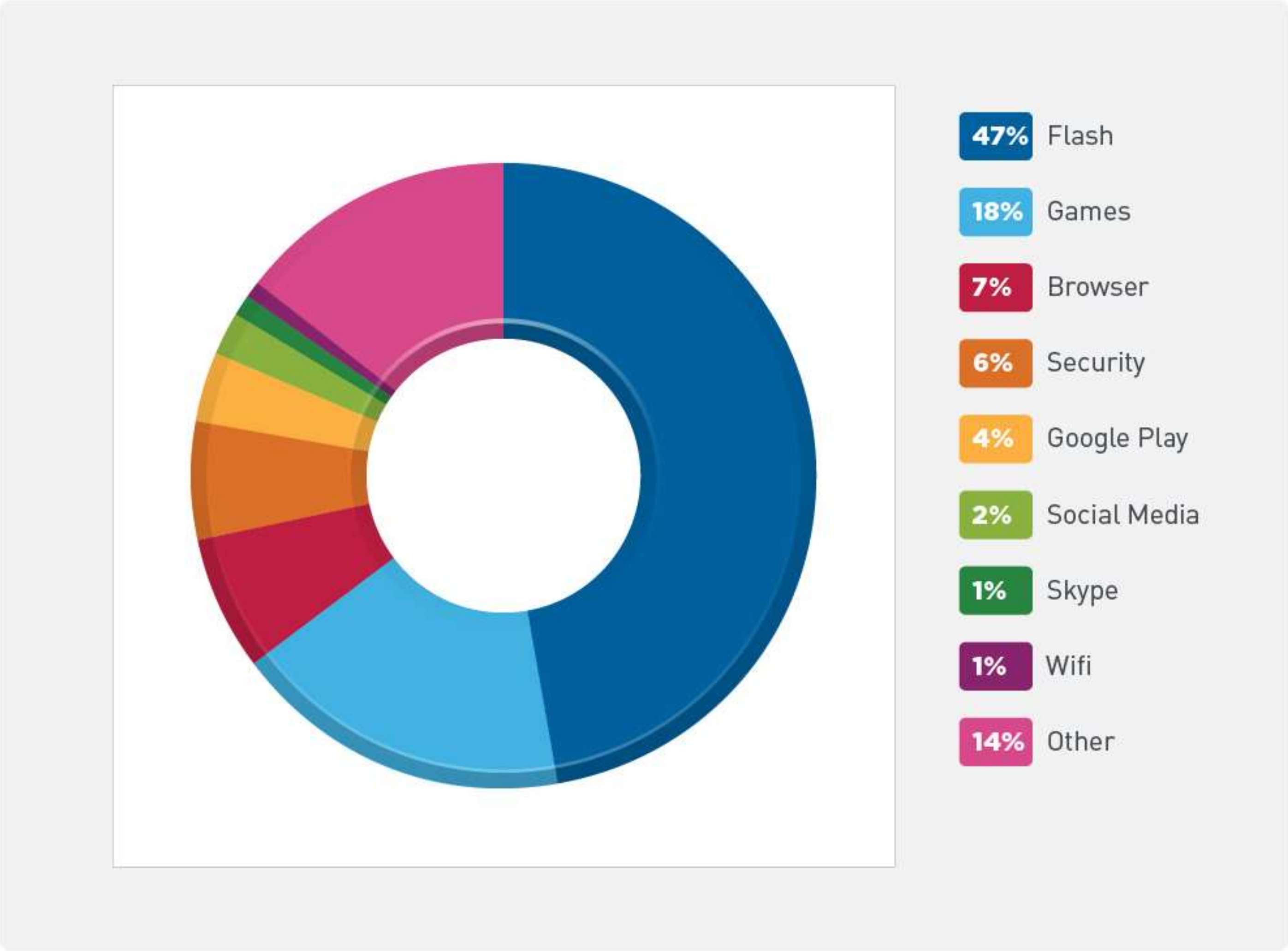
RSA CONFERENCE ASIA PACIFIC 2013

Backup Slides

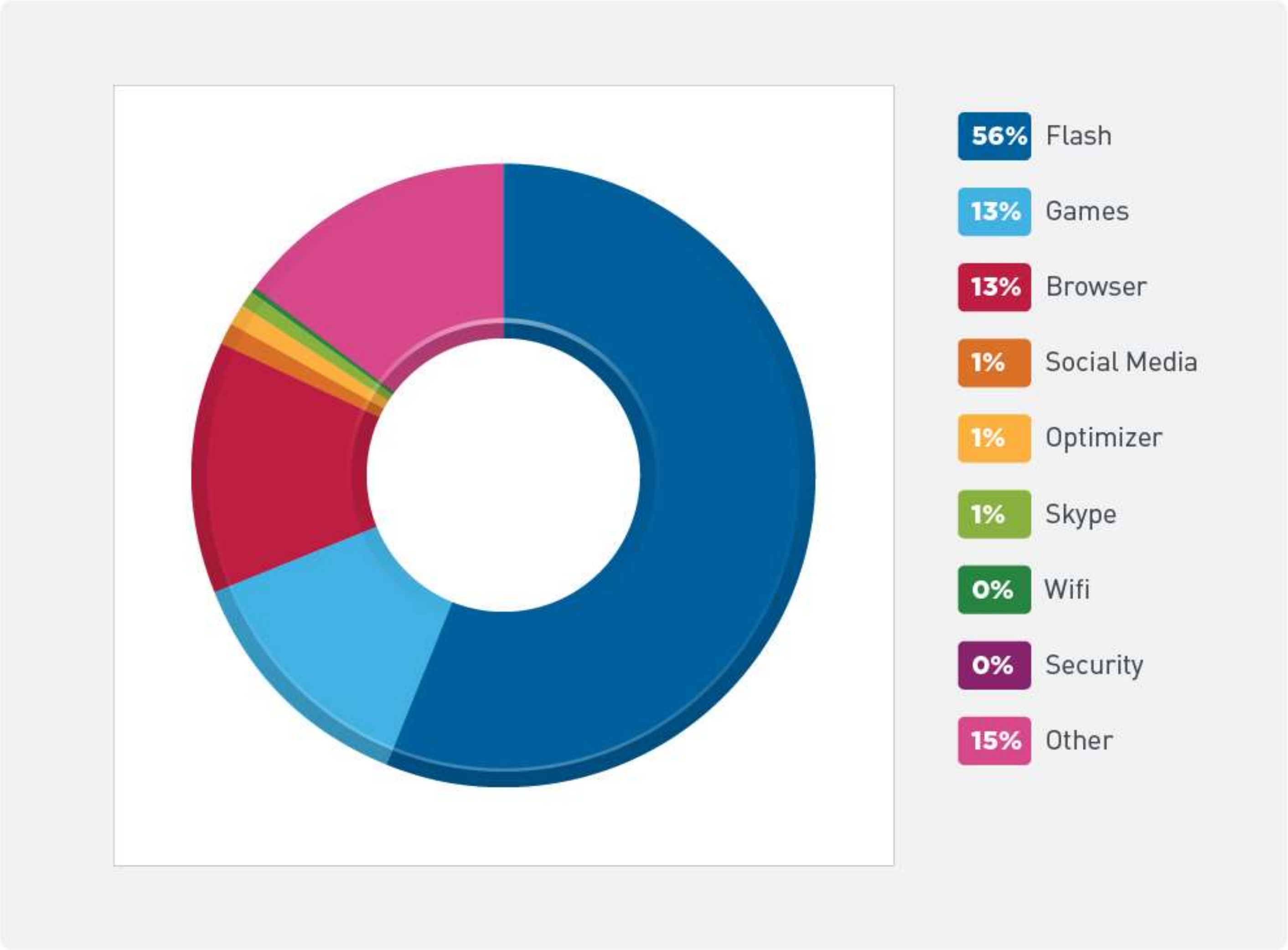
Solutions Within The Mobile Eco-system



Most Downloaded Android App Types



Most Downloaded J2ME App Types



90% CREATED IN THE LAST 2 YEARS

2.5 QUINTILLION BYTES OF DATA/DAY!

Source: IBM

Identify trends

Understand customer behavior

INFORMATION HAS BECOME *YOUR MOST* STRATEGIC ASSET

Analyze opportunities

Discover efficiencies