資料３

TREND MICRO
Securing Your Journey to the Cloud

スマートフォンのプライバシー保護に関する取り組み

トレンドマイクロ株式会社
セキュリティエキスパート本部

櫻井 勉

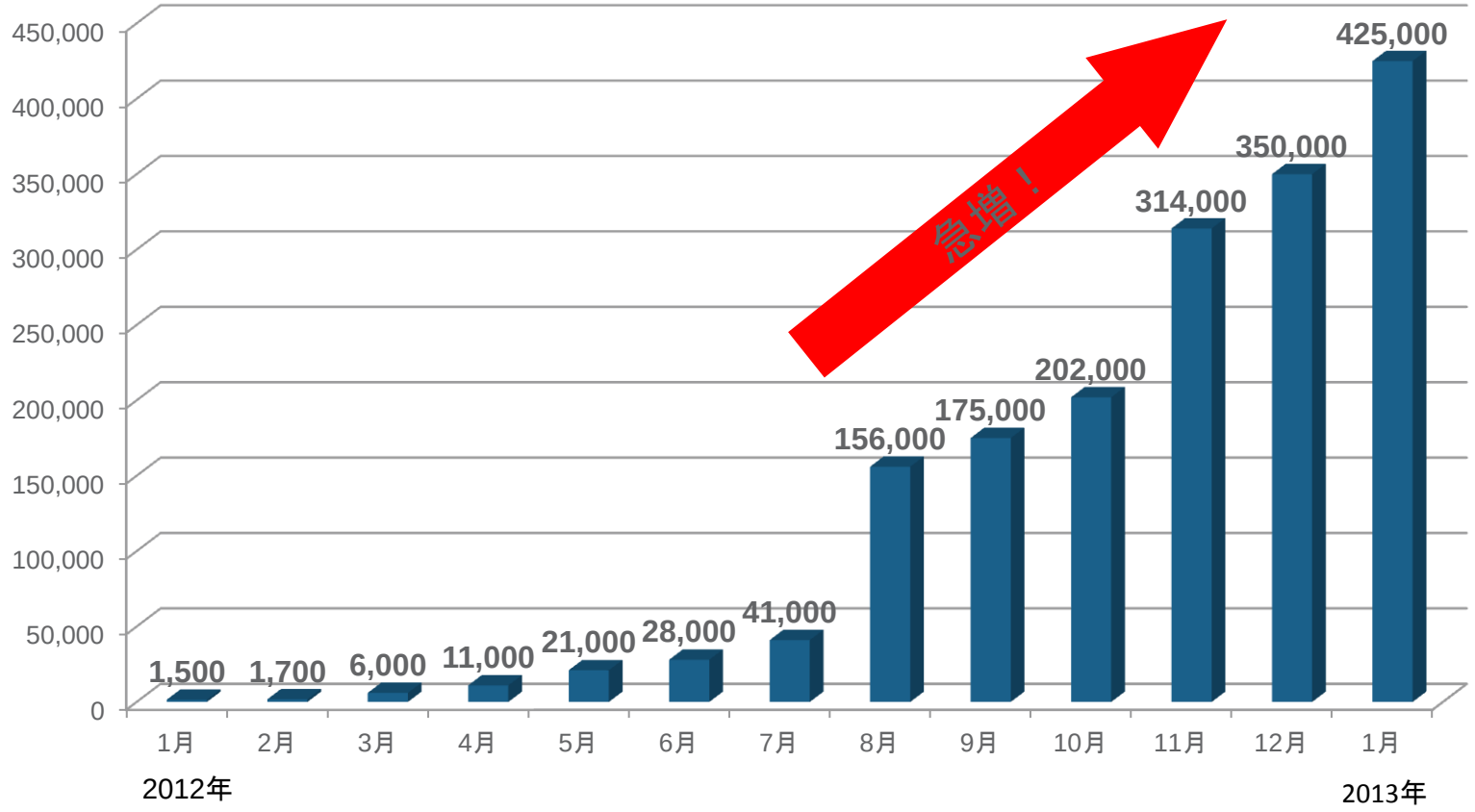
2013年2月25日

どのようなことがおきているか？

モバイル端末の脅威動向

モバイル環境の脅威：不正アプリの急増

「不正かつ危険度の高いAndroid向け不正アプリの数」

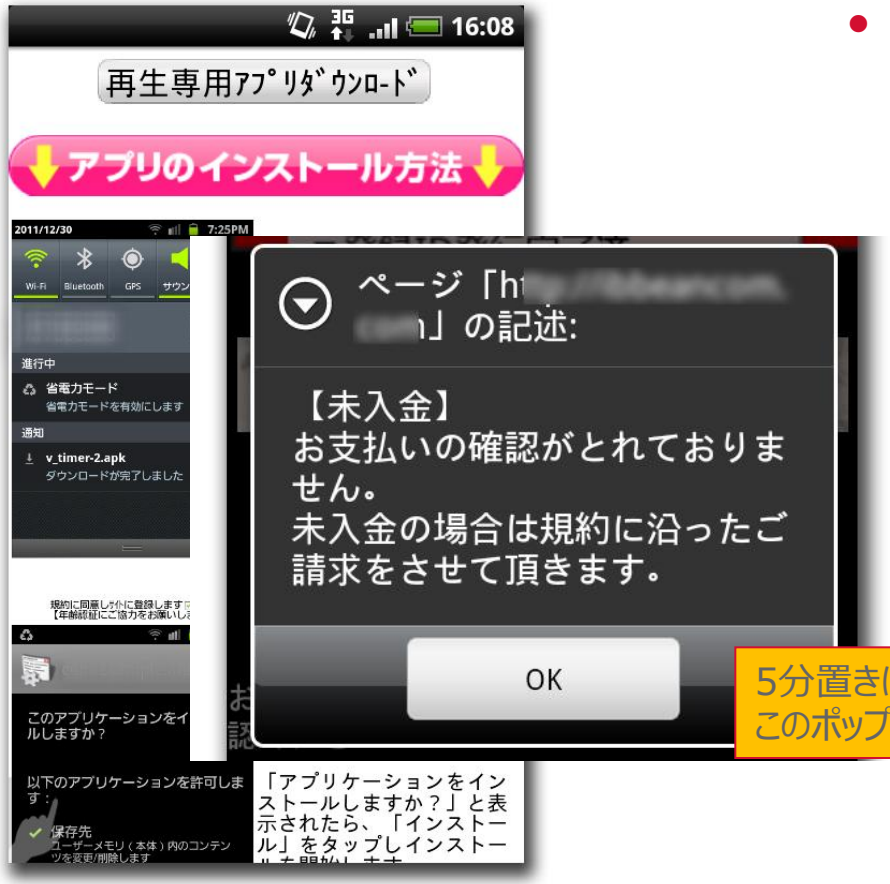


※1　2012年7月26日公開の第2四半期のセキュリティラウンドアップの作成時におけるAndroidのアプリの集計方法から変更があり、6月末の不正アプリ数を公開時の2万5千から2万8千に修正しています。

出典：2012年第3四半期セキュリティラウンドアップ、2012年第2四半期セキュリティラウンドアップ他
http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012q3.pdf
http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012q2.pdf

2012年確認されたAndroid向け不正アプリ①:
通称「ワンクリ（ワンクリック詐欺）アプリ」

検出名：「 ANDROIDOS_FAKETIMER.A 」ファミリ、「ANDROIDOS_FAKETIMER.SM」ファミリ等



- 主に成人向けコンテンツの閲覧を装い「登録する」といったボタンをクリックすると利用料金と称し、金銭振込を要求されてしまう「ワンクリック詐欺」の手口を利用
  - PCの場合と異なるのは、ユーザの電話番号がインストール時に読み取られ、実際にアプリ開発者に渡っている可能性がある点
  - 位置情報を取得したり、請求画面の表示時にカメラのシャッター音やバイブ機能の鳴動をするものも

5分置きにアプリからの命令により
このポップアップ画面が立ち上がる

金銭搾取目的

http://blog.trendmicro.co.jp/archives/4714

2012年確認された不正アプリ②:
通称「The Movieウイルス」

検出名：「ANDROIDOS_DOUGALEK」ファミリ

- 動画再生アプリにみせかけインストールを促す
  - 電話番号だけでなく、アドレス帳に登録した連絡先の読み取りを行い、読み取ったアドレス帳データを外部に送信

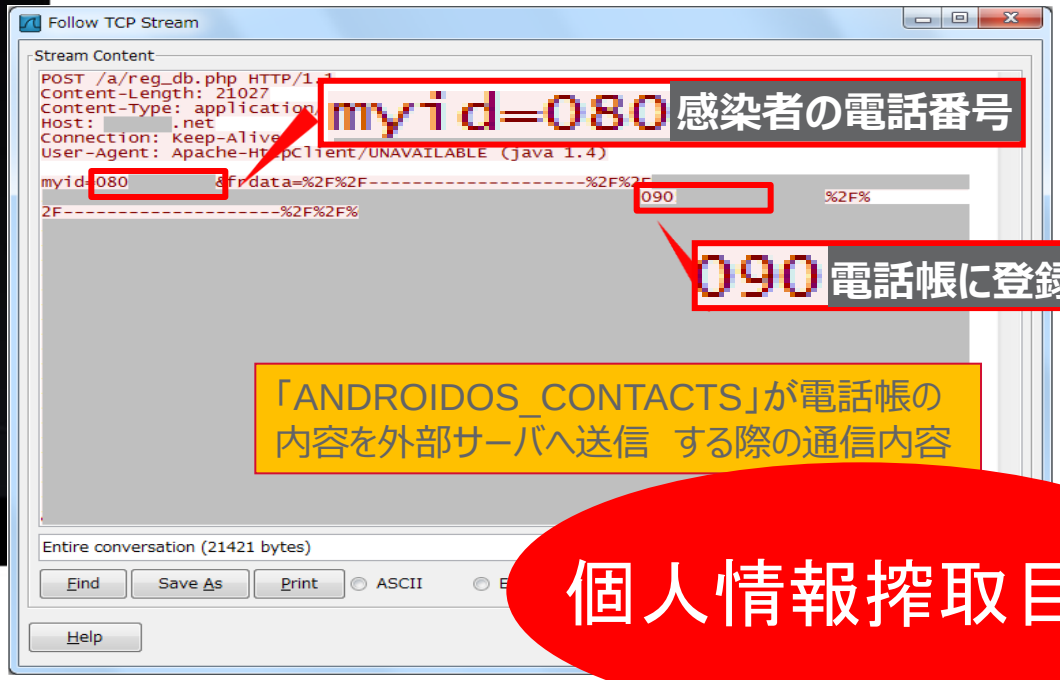
個人情報搾取目的

http://blog.trendmicro.co.jp/archives/6194

2012年確認された不正アプリ③:
通称「電池長持ちアプリ」、「電波改善アプリ」・・・

検出名：「 ANDROIDOS_CONTACTS.E 」ファミリ

- バッテリー長持ち、太陽光発電アプリ等にみせかけインストールを促す
  - 電話番号だけでなく、アドレス帳に登録した連絡先の読み取りを行い、読み取ったアドレス帳データを外部に送信

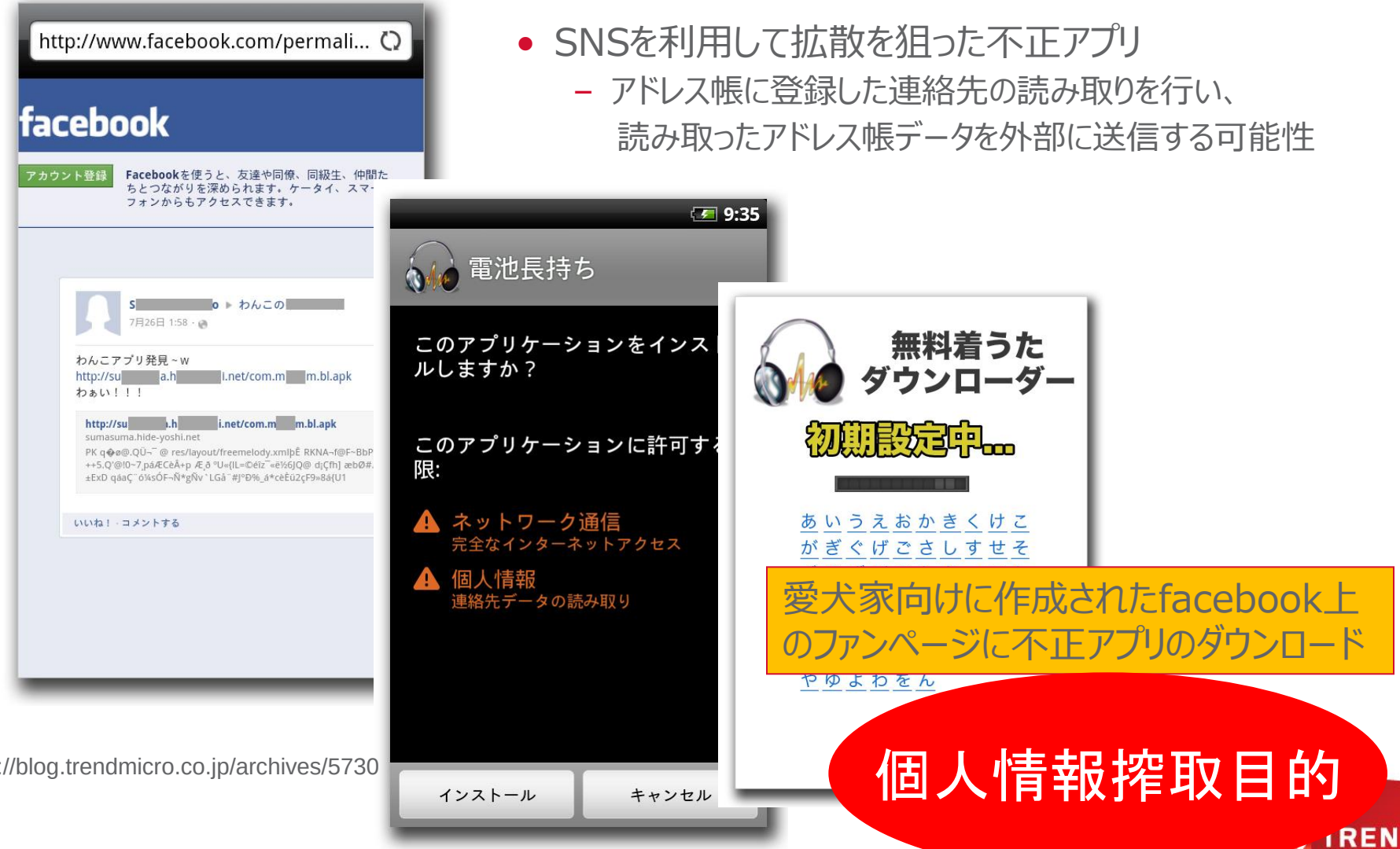


個人情報搾取目的

http://blog.trendmicro.co.jp/archives/6194

2012年確認された不正アプリ④:
通称「わんこアプリ」

検出名：「ANDROIDOS_FAKEBATTSAVE.A」ファミリ

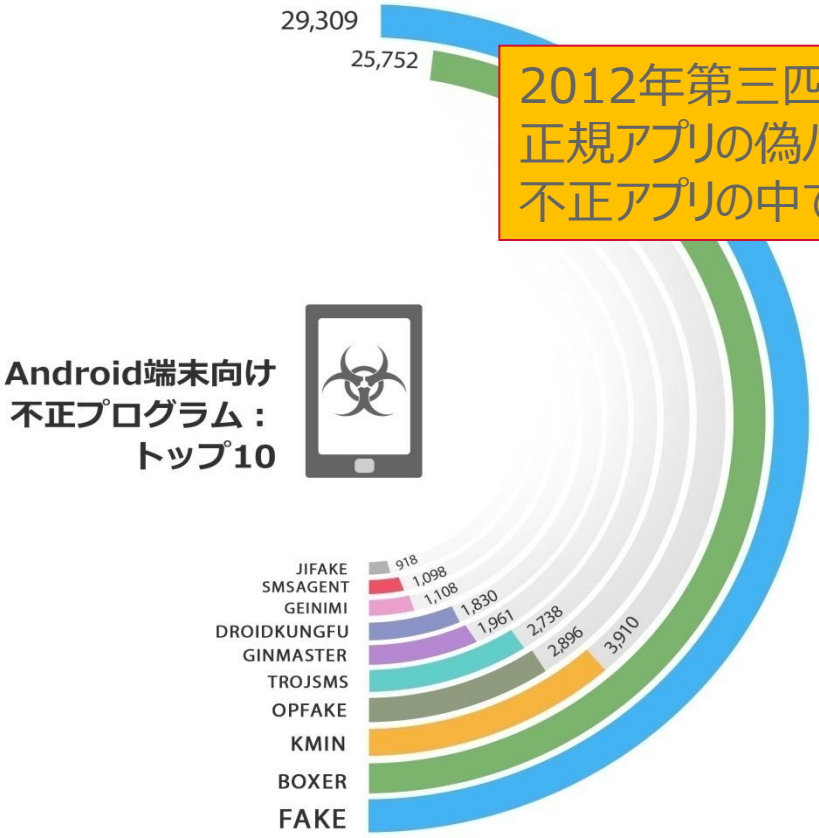


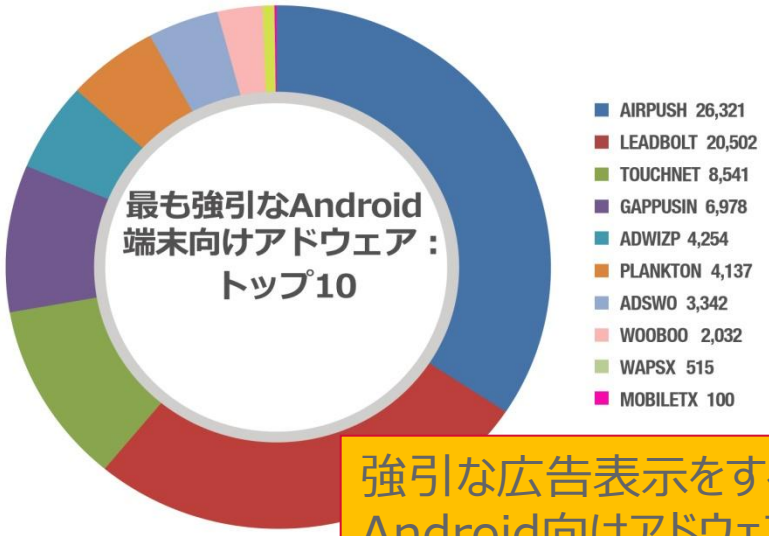
- SNSを利用して拡散を狙った不正アプリ
  - アドレス帳に登録した連絡先の読み取りを行い、読み取ったアドレス帳データを外部に送信する可能性

http://blog.trendmicro.co.jp/archives/5730

モバイル環境の脅威:「エゴアプリ」の脅威が拡大

2012年第三四半期の調査では、
正規アプリの偽バージョンがAndroid向け
不正アプリの中でもっとも多く存在





強引な広告表示をする
Android向けアドウェアが
多く存在

※図表の数値には、2012年第3四半期だけでなく、
確認したすべての期間中の情報も含まれています。

出典：2012年第3四半期セキュリティラウンドアップ
http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012q3.pdf

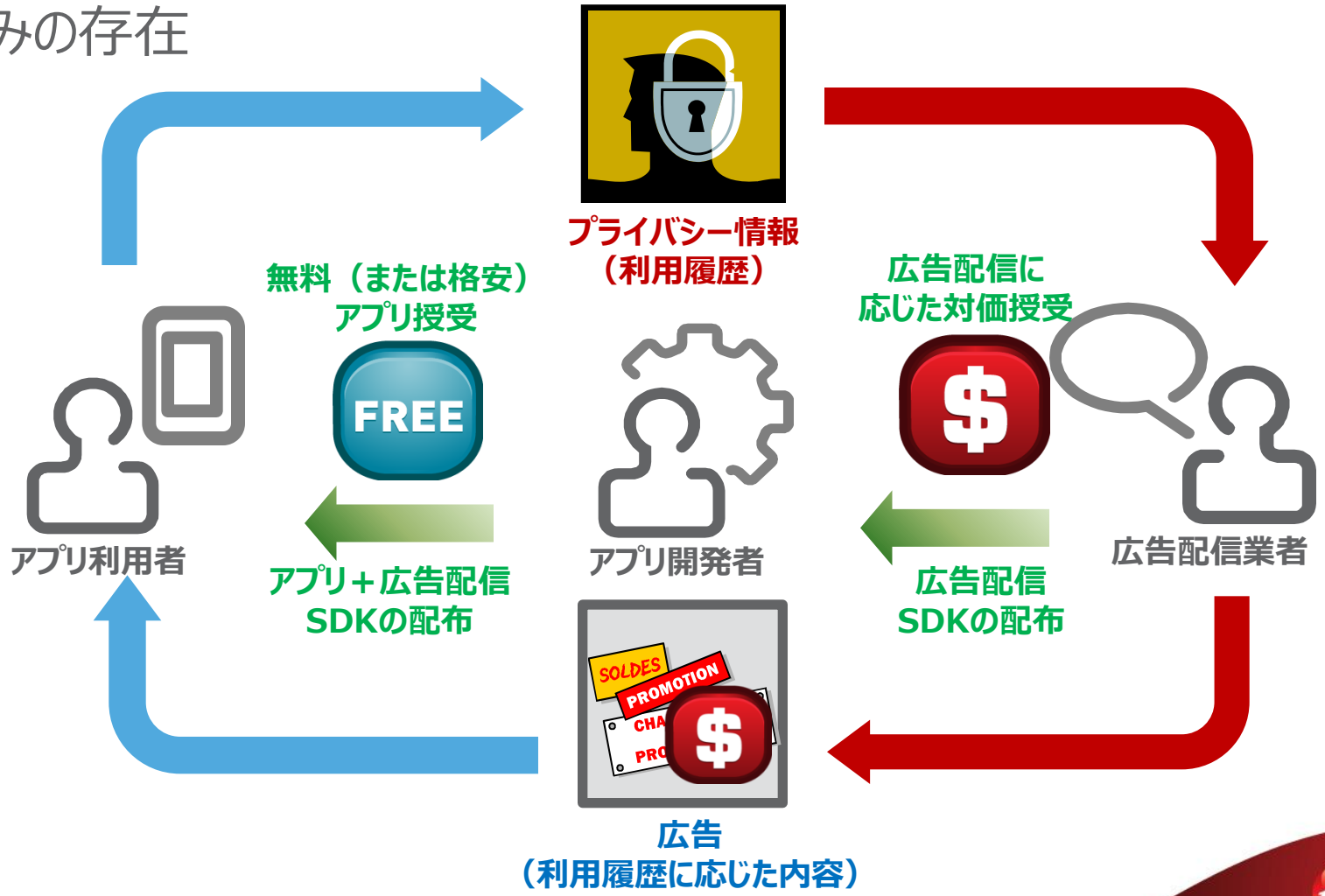
エゴアプリとは

- 利用者が潜在的に望まない「利己的な＝エゴな」挙動をするアプリ
  - ユーザが認知していない状態でプライバシー情報を勝手に利用するアプリ
  - ユーザの許諾を得ずに広告を強制表示するようなアプリ
  - 端末のシステムリソースを過剰に消費するようなアプリ

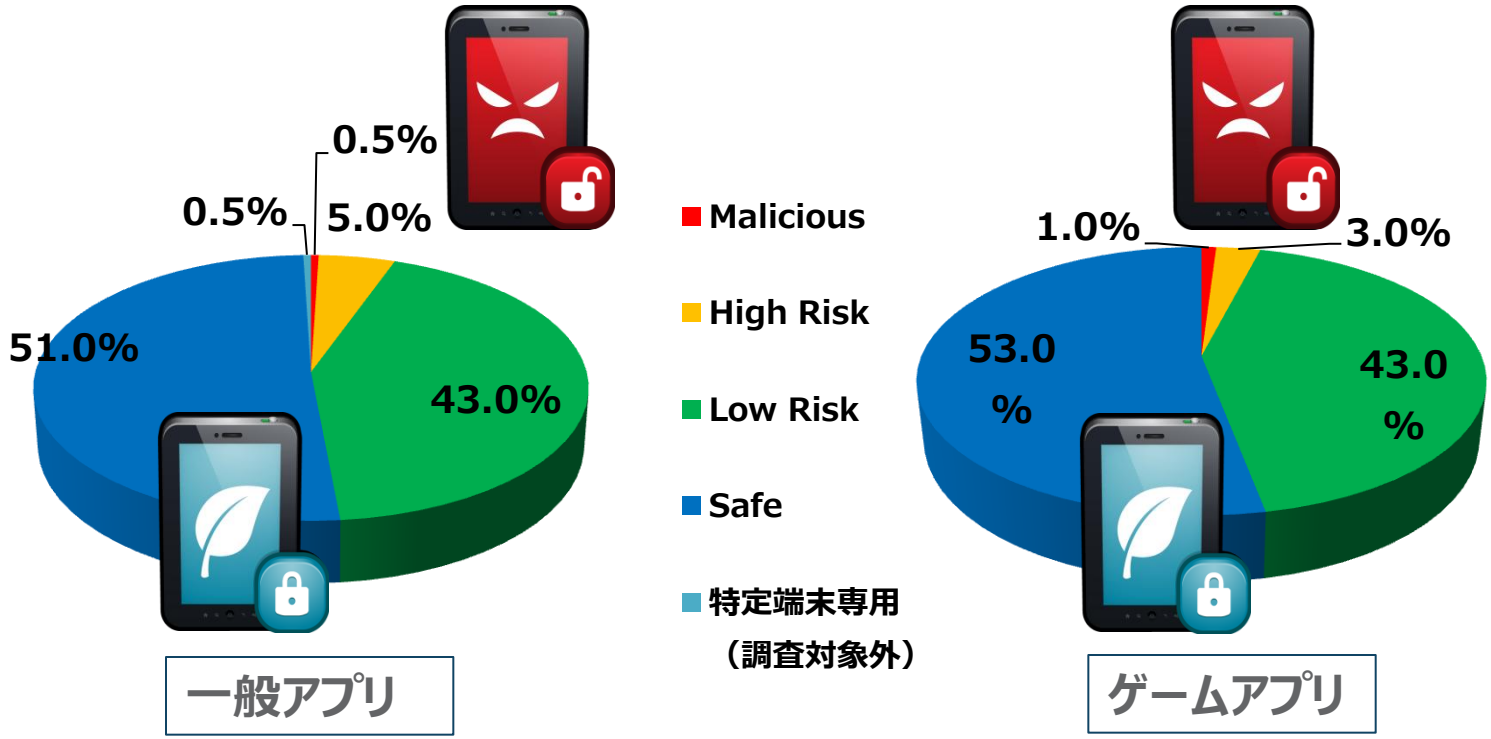
エゴアプリの中で悪質なものが、
「不正アプリ」、すなわち
「不正プログラム」、「ウイルス」と
呼ばれるものです

「無料」に潜むエゴアプリの脅威

- モバイル端末上での広告配信の流通におけるエコサイクルによって、無料でアプリを入手する代わりにプライバシー情報を提供する枠組みの存在



国内無料アプリの実態：プライバシー情報流出リスク
~Google Play上でTop200の無料アプリを評価（※）~



Google Play上の一般アプリTop200、ゲームアプリ Top200内に不正な広告配信とプライバシー情報の送出を組み合わせた挙動をする不正アプリを計3件確認

※2012年8月31日付Google社の発表した対象日のランキングにおける一般アプリの上位200とゲームアプリの上位200にランクインしたアプリをTrend Micro Mobile App Reputationを使って評価

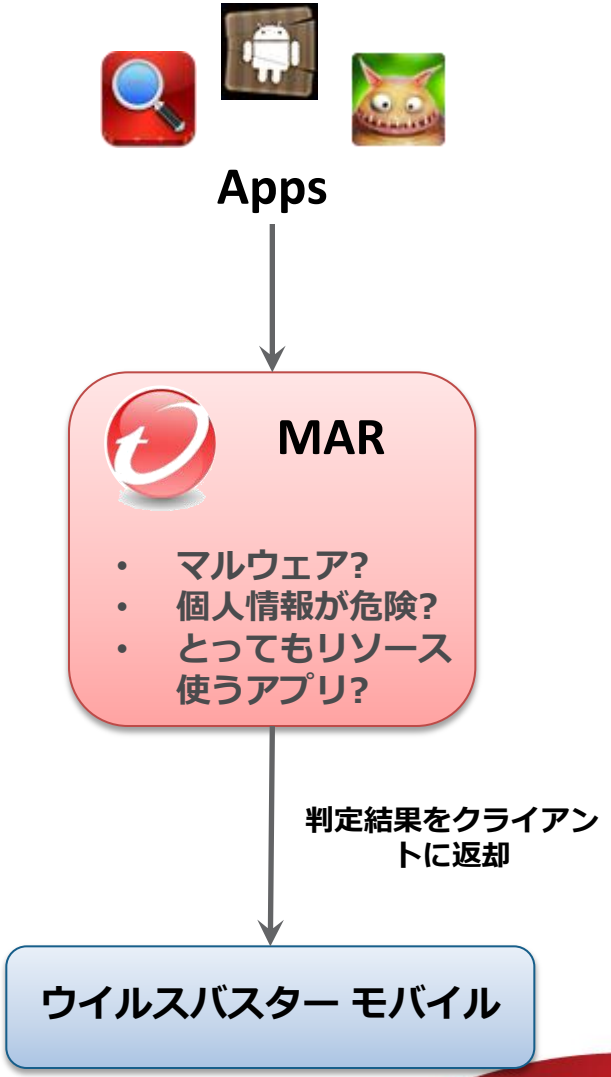
安全なアプリを配布できる環境

モバイルアプリケーション評価システム
MAR (Mobile App Reputation)

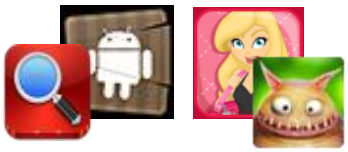
MAR (Mobile App Reputation)

概要

- MARは脅威のあるアプリを自動的に特定する高度なクラウドベースのソリューション
  - 例えば、デバイスのリソースを浪費するようなアプリや、個人情報を悪用するようなマルウェアを全て検知
- 最新の脅威に即時対応
- サービスプロバイダのアプリストアとシームレスに統合可能

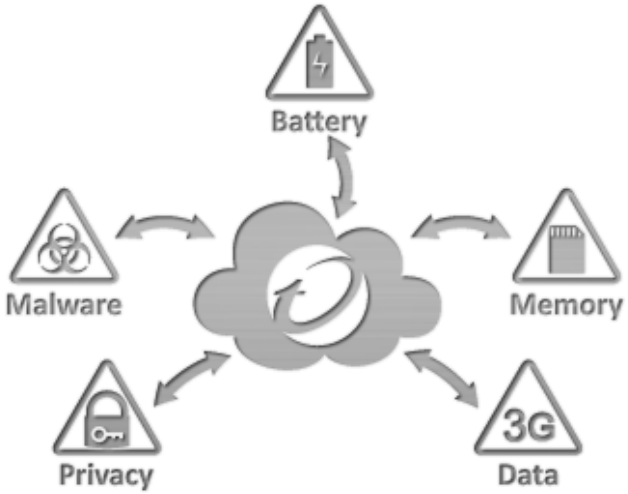


静的解析と動的解析



1

クラウド上でAppを収集し、それらを検索



3

Smart Protection Networkを使ってWeb Reputationとも連携

2

静的解析:
外観から判断できる情報(ハッシュ値など)とリバースエンジニアリング

4

動的解析:
Appを実機上で動作させ実際の行動を分析

MARは
レピュテーションスコアと
詳細なレポートを生成

生成されたレポートの例

TREND MICRO | Mobile App Reputation Close

Basic Information	
Sha1	8704D4848867DE63CB4364E64B62B102C3C97C48
Package Name	com.bzyg.bideyuanli
App Label	Peter Principle
Size	1329374 Bytes
Version	1.0
SDK	3

Scan Information	
Scan Time	2012-08-21 21: 13: 00

Security Check	
Scan Result	Malicious
Virus Name	AndroidOS_TROJTouchnet.HRY
Reason	
API Security	Dangerous API Called
Data Leak	IMEI send out by HTTP_GET (URLEncoder)
Data Leak	IMEI send out by HTTP_GET (Uri)
Data Leak	SIM_SN send out by HTTP_GET (URLEncoder)
Data Leak	IMSI send out by HTTP_GET (URLEncoder)
Data Leak	LOCATION send out by HTTP_GET (URLEncoder)
Data Leak	LOCATION send out by HTTP_GET (HttpGet)

Resource Usage	
Battery Consumption	Average
Internet Data	Low
Memory	Average

Permission
android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_LOGS
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_WIFI_STATE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.ACCESS_NETWORK_STATE

Certification	
Owner	
Common Name	bzyg
Organization Unit	bzyg
Organization	bsoft
Location	xian
State	shanxi
Country	cn
Serial Number	4d293940
Valid Date	from: Sun Jan 09 12:27:44 CST 2011 until: Mon Dec 16 12:27:44 CST 2109
Signer	
Common Name	bzyg
Organization Unit	bsoft
Organization	bsoft
Location	xian
State	shanxi
Country	cn
Date/Time Signed	Jun 25 2011

現状のMARデータベース

- 不正な挙動の分析
  - ✓ アプリケーションが不正な振る舞い（データリークなど）を行うか分析・評価
  - ✓ 不正な署名情報による改造アプリや海賊アプリの分析・評価
- プライバシーリスク
  - ✓ 外部に送信しようとするプライバシー情報に関するリスク分析・評価
- システムリソースの消費
  - ✓ アプリケーションが使用するバッテリー、メモリ、インターネット回線の使用帯域、CPU使用率の分析・評価

プライバシーリスクの検出

MARは、「Data Leak」挙動（プライバシーリスク）の積極的な検出に力をいれており、特に以下の情報の出力に対しては厳格に評価しています。

- IMEI / IMSI / SIM_SN等の端末識別情報
- 位置情報
- DATABASE情報
- 電話番号
- 利用者がインプットした情報
- 連絡先情報

上記情報の出力状況を独自のアルゴリズムで点数化し、4段階評価

- ✓ Normal
- ✓ Low Risk
- ✓ High Risk
- ✓ Malicious

活用の可能性

スマートフォン利用者情報取扱指針:各論①

2 各論①:アプリ提供者、情報収集モジュール提供者等による取組み

1 プライバシーポリシーの作成

下記の事項について明示するプライバシーポリシーを作成し、利用者が容易に参照できる場所に掲示またはリンクを張る（また、スマートフォンの画面上で容易に理解できるように、分かりやすい概要版を作成し掲示する）。

①情報を取得するアプリケーション提供者等の氏名または名称:アプリケーション提供者等の名称、連絡先等を記載する。

②取得される情報の項目:取得される利用者情報の項目・内容を列挙する。

③取得方法:利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか示す

④利用目的の特定・明示
利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤通知・公表または同意取得の方法、利用者関与の方法
通知・公表の方法、同意取得の方法:プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。利用者関与の方法:利用者情報の利用を中止する方法等を記載する。

⑥外部送信・第三者提供・情報収集モジュールの有無
外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦問合せ窓口
問合せ窓口の連絡先等(電話番号、メールアドレス等)を記載する。

⑧プライバシーポリシーの変更を行う場合の手続き
プライバシーポリシーの変更を行った場合の通知方法等を記載する。(同意の範囲が変更される場合改めて同意取得)

2 適切な安全管理措置

3 情報収集モジュール提供者に関する特記事項：アプリ提供者へ取得する情報項目や目的等を通知

4 広告配信事業者に関する特記事項：アプリ提供者や情報収集モジュール提供者となる場合の対応、配慮原則等

事例:アンドロイダー

アンドロイダーとトレンドマイクロの協業により
アプリ開発者支援体制を強化
～アプリの事前検査に、トレンドマイクロの評価システム※1を
業界初採用※2～

アンドロイダー株式会社(本社:東京都渋谷区、代表取締役:池田 武史)は、Android™アプリ情報サイト「アンドロイダー」(http://androider.jp/)において、Androidアプリの国内レビューサイトとして初めて、トレンドマイクロ株式会社(本社:東京都渋谷区、代表取締役社長兼CEO:エバ・チェン、以下、トレンドマイクロ)のモバイルアプリ評価システム(Trend Micro Mobile App Reputation、以下、Mobile App Reputation)でアプリを事前に検査し不正な挙動が認められた際にアプリ開発者(以下、デベロッパー)への適切なフィードバックを行うと共に、不正アプリが広がることを防止します。

http://jp.trendmicro.com/jp/about/news/pr/article/20120920033611.html

- AppをWebに公開する前にMARでチェックして「安全」なものだけを公開

ダウンロードしたアプリが安全とわかる

ウイルスバスター for モバイル

製品概要

情報漏えい対策

紛失したAndroid端末を遠隔操作でロックしたり、GPS機能で端末の場所の特定も可能。プライバシースキャン機能も加わり、大切な個人情報を守ります。

Web脅威対策

Webレピュテーション
怪しいサイトへのアクセスをブロック。

ペアレンタルコントロール
未成年者に不適切なWebサイトへのアクセスを制御。

不正アプリ対策

インストール時にファイルをスキャンして、不正なアプリケーションがインストールされるのを防ぎます。

着信フィルタ/SMSフィルタ

迷惑電話、迷惑SMSをブロックします。

Android端末おまかせサポート

Android端末の「困った！」も解決！

Android端末のサポートを365日ご提供。
〈メールでも〉〈チャットでも〉〈電話でも〉

プライバシースキャン

- アプリが個人情報を漏洩する可能性のある場合に警告を表示します
  - リアルタイム検索
    - アプリのインストール時にファイルをスキャンし、不正なアプリがインストールされるのを防ぎます
  - 手動検索
    - インストール済みアプリを手動検索可能です
- SDカード内のAPKファイルも検索します
- 検索対象となる個人情報

個人情報
IMEI, IMSI, ICCID
電話番号, アカウント
位置情報
写真・動画（カメラ機能）
着信履歴, 連絡先
SMS, 音楽ファイル, マイク（ボイスレコード）, ファイル転送, ユーザが入力する　データ

プライバシースキャン<フロー>

個人情報の送信内容を確認の上、
該当するアプリを削除する事ができます。

サポート

- ユーザ同士のコミュニティの場所を提供
- メール、電話の相談窓口

トレンドマイクロが考える課題

1. 善意の開発者が開発したアプリが不正アプリとなってしまい評判が下がる
   - 利用者側のセキュリティ対策が進んでおり、開発者よりも利用者環境で先に検出される
   - 一部の広告配信SDKが適正なプライバシー情報の取り扱いをしていない
2. 利用者が不正アプリに気付き、どのように対応していいかわからない
   - 適切な相談窓口がない。難しい単語が多い。
   - 不正な活動が既におきたかどうかを知りたい（意図しない加害者になりたくない）
3. ルールがない場所には不正アプリが自由における
   - マーケット以外の場所からも自由にアプリ(野良アプリ）がダウンロードできる

まとめ

- アプリ提供者
  - スマートフォン利用者情報取扱指針の理解とプライバシーポリシーの作成・順守
- マーケット事業者
  - 危険なアプリの排除
  - エコアプリの推奨
- 利用者
  - アプリの性質を理解できるセキュリティ対策ソフトの導入
  - 優良マーケット事業者の選択
  - 迷った、困ったときは窓口に相談