JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人日本スマートフォンセキュリティ協会

-スマートフォンを安心して利用出来る社会へ-

日本スマートフォンセキュリティ協会

技術部会

マルウェア対策WG 活動報告

マルウェア対策WG
サブリーダ
前田　典彦
（株式会社カスペルスキー）

JSSEC成果発表会2012
（2012年5月24日 @東京電機大学）

マルウェア対策WG

従来は「アプリケーションWG」として活動
→「マルウェア対策WG」として分離

リーダー	大輪 弘詳（トレンドマイクロ）
サブリーダー	前田 典彦（カスペルスキー）

参加企業（五十音順）

- アンラボ
- エフセキュア
- カスペルスキー
- キヤノンITソリューションズ
- シマンテック
- トレンドマイクロ
- マカフィー

主な活動は、マルウェア情報の提供・注意喚起など。

マルウェア情報提供サイト

- マルウェア情報（XML配信）
  - 発見日、情報掲載日
  - 概要、感染経路、活動、削除方法(記述)

- サンプル特定情報（検討中）
  - 使用するパーミッション
  - ハッシュ

※ 各社公開情報に基づく

情報提供者

- 過去の情報も含め掲載
  - シマンテック
  - トレンドマイクロ
  - マカフィー
- 影響度に応じて随時掲載
  - アンラボ
  - エフセキュア
  - カスペルスキー
  - キヤノンITソリューションズ

公開方法(予定)

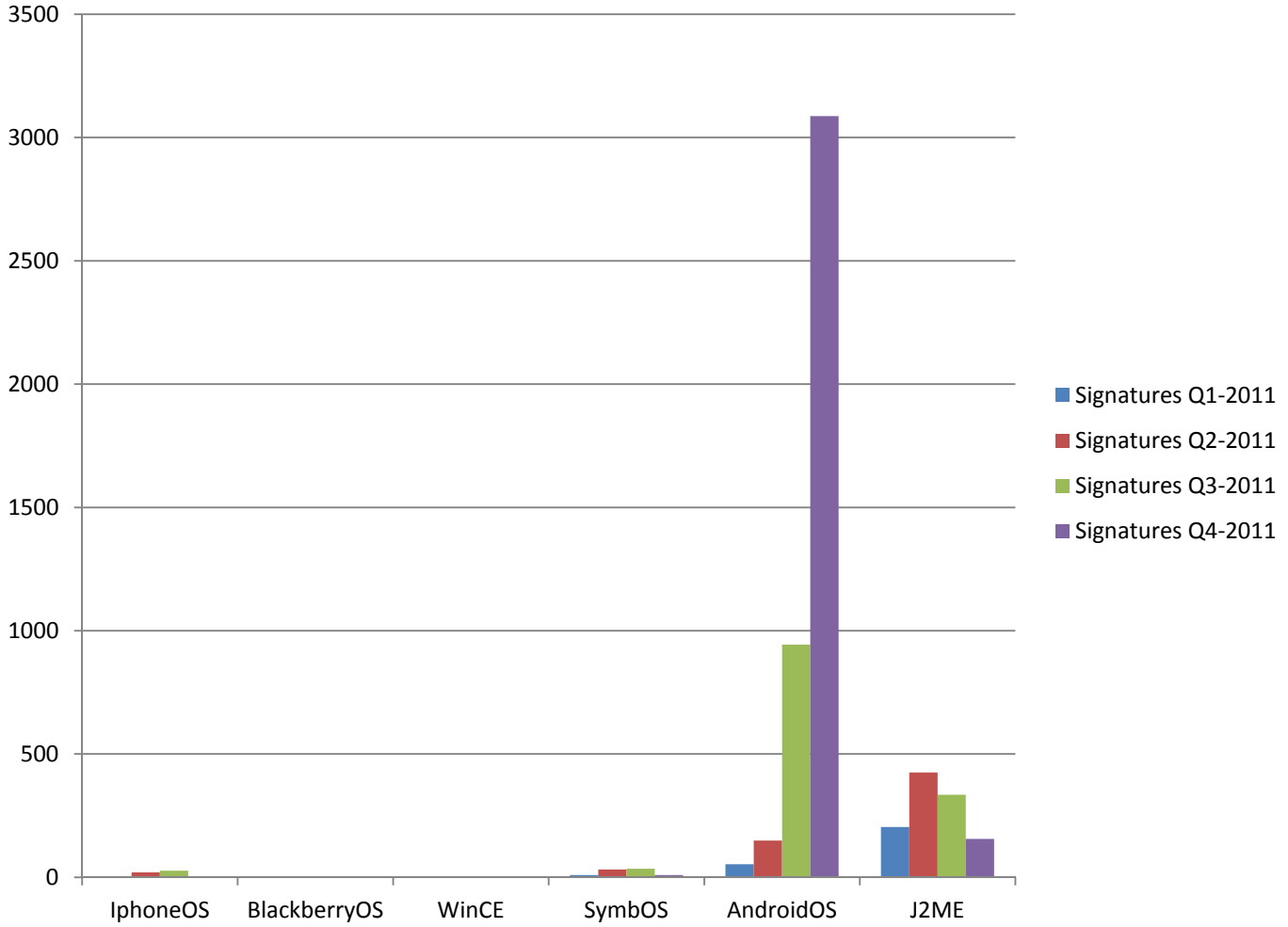
- ウェブサイト

  http://amwg.jssec.org/
- ATOM/RSS フィード
- JSSEC Twitter (@jssec_org)

JAPAN SMARTPHONE SECURITY ASSOCIATION

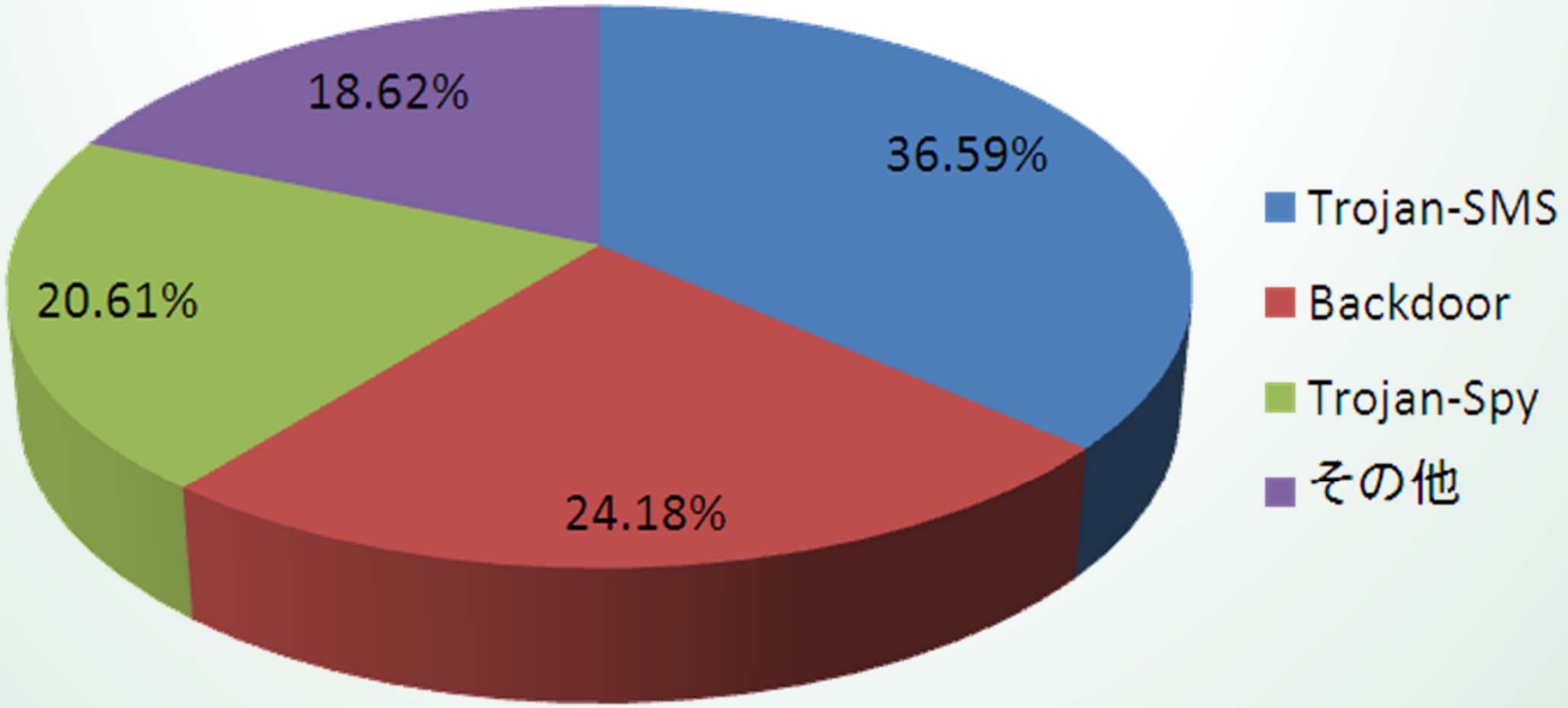
マルウェアの傾向

モバイルOS向けマルウェア数



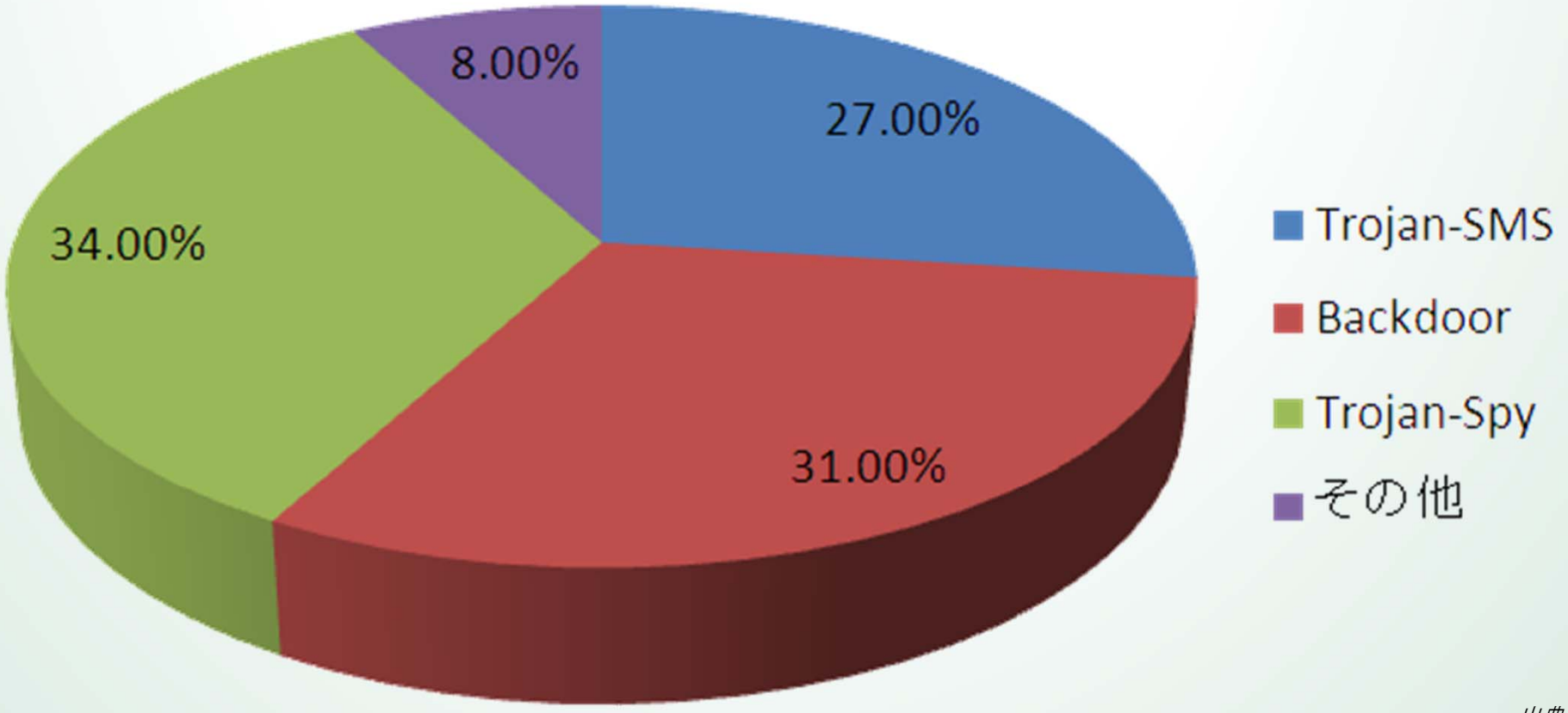
出典
Kaspersky Lab

モバイルOS向けマルウェアの種類



出典
Kaspersky Lab
2011年12月

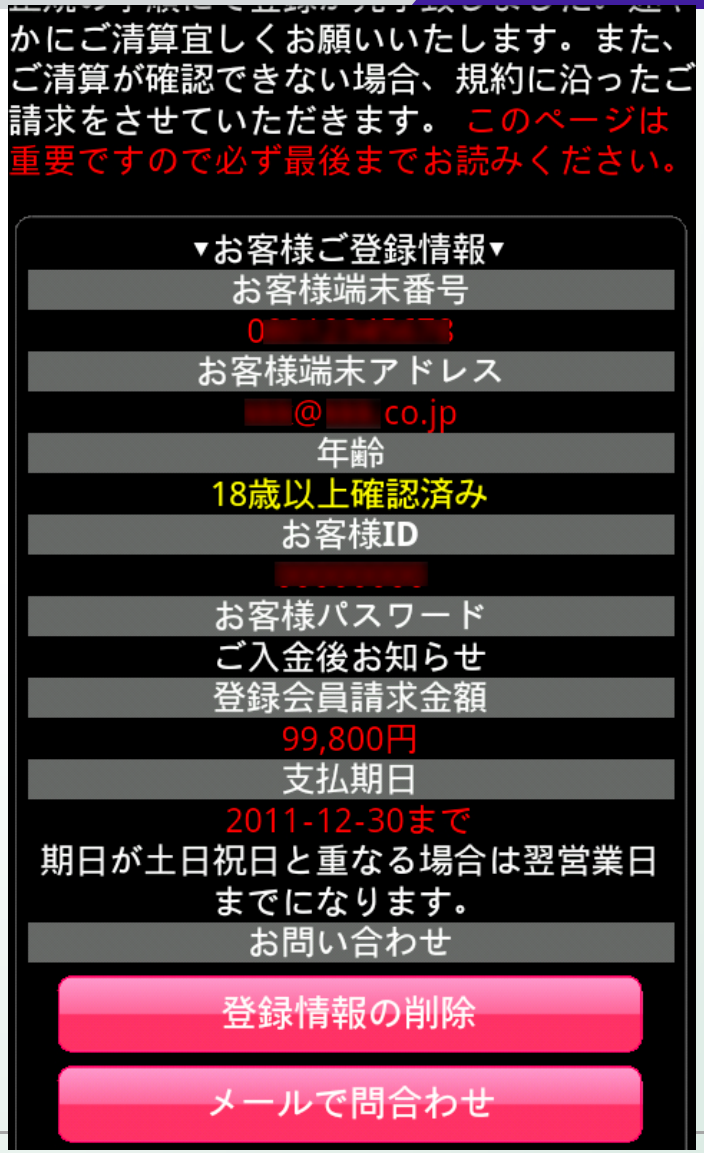
Android向けマルウェアの種類



出典
Kaspersky Lab
2011年12月

日本語アプリのマルウェア(1)

- Trojan.AndroidOS.FakeTimer
- 日本語アダルトサイトで配布された。
- いわゆるワンクリ詐欺のサイト。
- 5分毎に請求ポップアップ



日本語アプリのマルウェア(1)

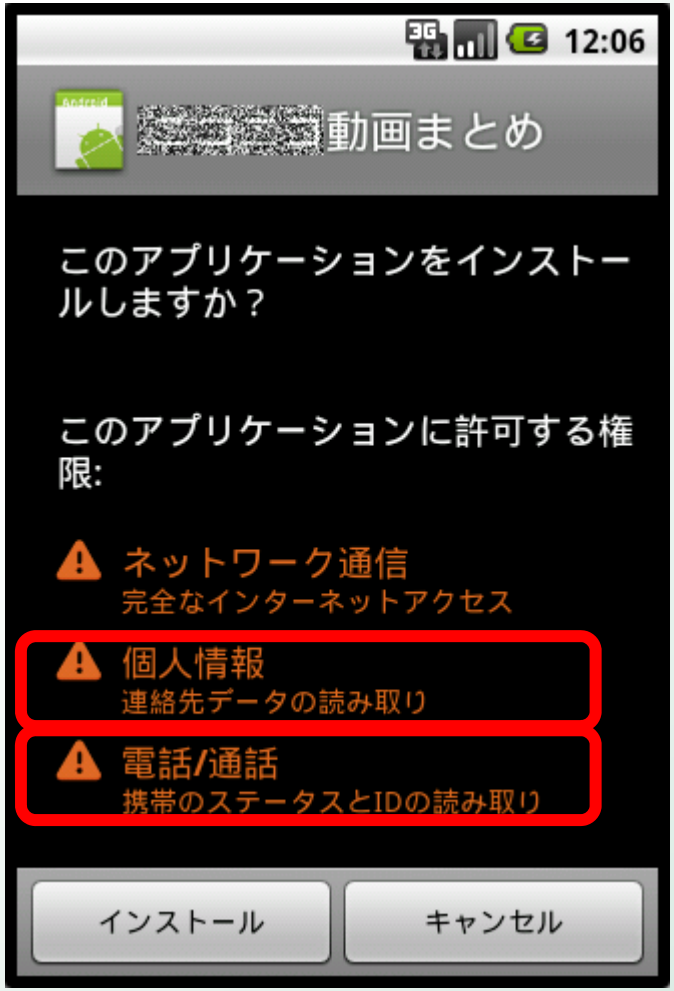
- Trojan.AndroidOS.FakeTimer
- 日本語アダルトサイトで配布された。
- いわゆるワンクリ詐欺のサイト。
- 5分毎に請求ポップアップ

日本語アプリのマルウェア(2)

- Trojan-spy.AndroidOS.Dougalek
- 日本語アプリ
- **Google Play**で配布された。
- コンタクトリスト(電話帳)に登録された情報をリモートサーバに送付

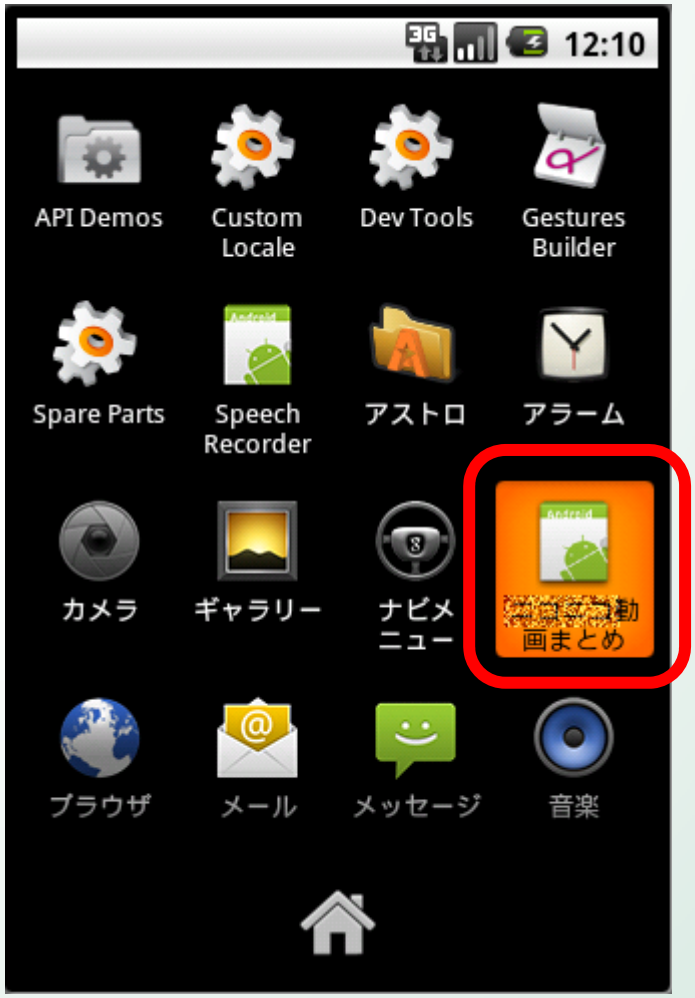
日本語アプリのマルウェア(2)

- Trojan-spy.AndroidOS.Dougalek
- 日本語アプリ
- **Google Play**で配布された。
- コンタクトリスト(電話帳)に登録された情報をリモートサーバに送付



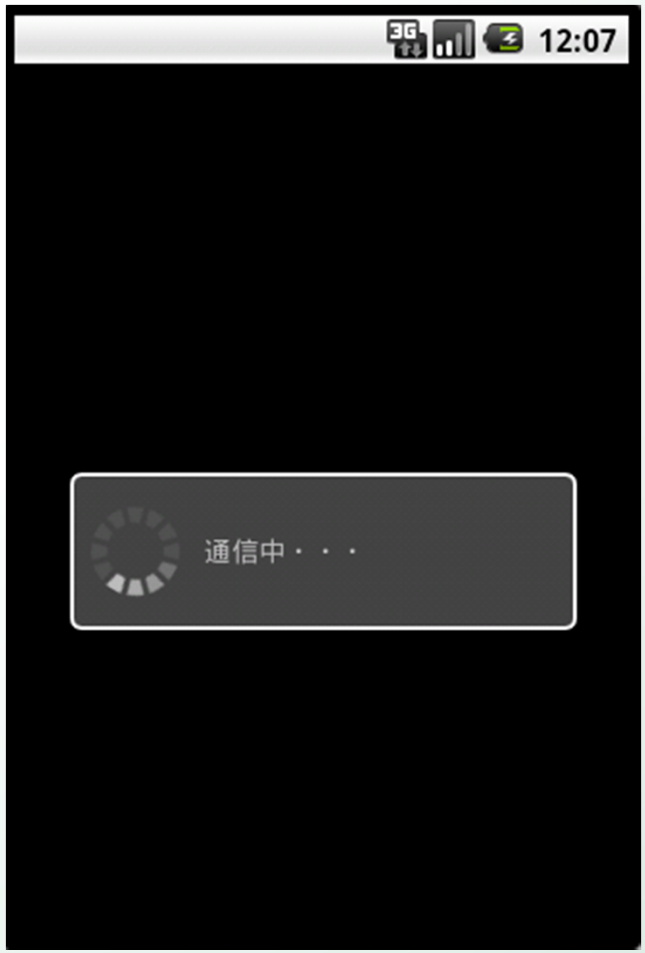
日本語アプリのマルウェア(2)

- Trojan-spy.AndroidOS.Dougalek
- 日本語アプリ
- **Google Play**で配布された。
- コンタクトリスト(電話帳)に登録された情報をリモートサーバに送付



日本語アプリのマルウェア(2)

- Trojan-spy.AndroidOS.Dougalek
- 日本語アプリ
- **Google Play**で配布された。
- コンタクトリスト(電話帳)に登録された情報をリモートサーバに送付



JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

ありがとうございました

一般社団法人日本スマートフォンセキュリティ協会
技術部会
マルウェア対策WG