



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  
サブリーダー  
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)



[ホーム](#) > [マルウェア情報](#)

## マルウェア情報

### ANDROIDOS\_FAKETOKEN.A

情報提供: [トレンドマイクロ](#) 更新日: March 16, 2012, 12:00 am

感染経路: インターネットからのダウンロードトレンドマイクロは、このスパイウェアをNoteworthy (要注意) に分類しました。スパイウェアは、偽のトークン・ジェネレータを装うことにより、モバイルバンキングのユーザをターゲットにします。実行中に、スパイウェアはユーザのパスワードを要求し、偽のトークンを生成します。さらに、ユーザの個人情報を特定の電話番号やバックグラウンドの不正なリモートサーバに送信します。スパイウェアは、特定の銀行からのトークン・ジェネレータを装ったアプリケーションです。ユーザ…

### ANDROIDOS\_SMSBOXER.AB

情報提供: [トレンドマイクロ](#) 更新日: March 14, 2012, 12:00 am

感染経路: インターネットからのダウンロードトレンドマイクロは、このマルウェアをNoteworthy (要注意) に分類しました。マルウェアは、以前はAndroidマーケットとして知られていた「Google Play」を装った偽のWebサイトからダウンロードされます。マルウェアは、SMSのメッセージ (以下、テキストメッセージ) を送信する機能を備えています。マルウェアは、感染したデバイス機器の国番号とオペレータコードを確認します。テキストメッセージを送信後、特定のWebサイトを開きま

## 情報提供

[アンラボ](#)

[エフセキュア](#)

[カスペルスキー](#)

[キャノン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](#)



ホーム > マルウェア情報 > ANDROIDOS\_FAKETOKEN.A

## ANDROIDOS\_FAKETOKEN.A

発見日: March 16, 2012, 12:00 am

情報公開日: March 26, 2012, 10:23 am

情報更新日: March 26, 2012, 10:23 am

### 概要

感染経路: インターネットからのダウンロードトレンドマイクロは、このスパイウェアをNoteworthy (要注意) に分類しました。スパイウェアは、偽のトークン・ジェネレータを装うことにより、モバイルバンキングのユーザをターゲットにします。実行中に、スパイウェアはユーザのパスワードを要求し、偽のトークンを生成します。さらに、ユーザの個人情報を特定の電話番号やバックグラウンドの不正なリモートサーバに送信します。スパイウェアは、特定の銀行からのトークン・ジェネレータを装ったアプリケーションです。ユーザはパスワードの入力を要求され、入力しない場合は、エラーメッセージが表示されます。ユーザが"Generar"をクリックすると、スパイウェアは偽のトークンを生成し、バックグラウンドで不正なコードを実行します。スパイウェアは、悪意あるWebサイトからユーザが誤ってダウンロードすることにより、コンピュータに侵入します。スパイウェアは、ユーザの手動インストールにより、コンピュータに侵入します。

### 感染経路

### 活動

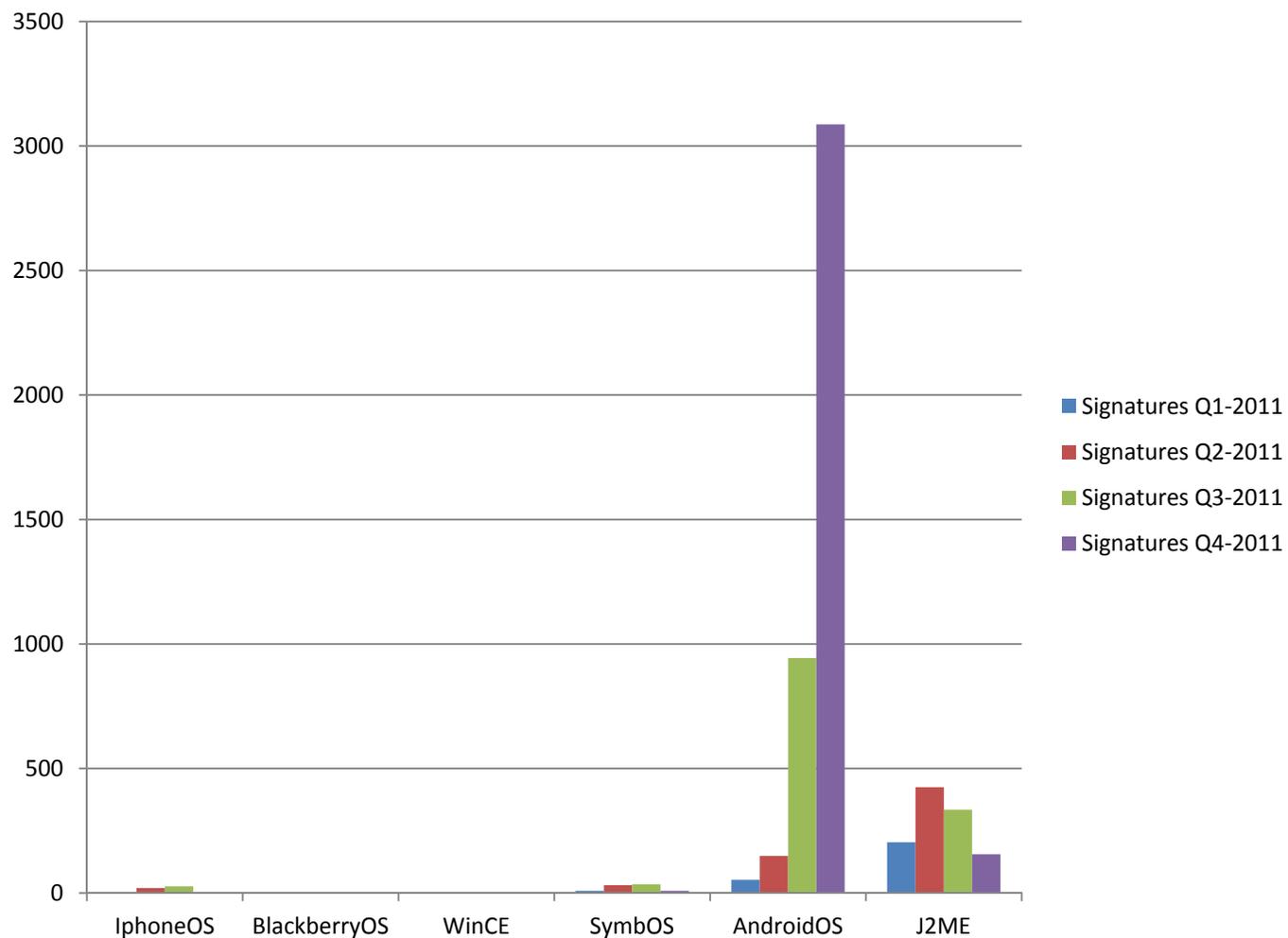
情報提供

トレンドマイクロ

# マルウェアの傾向

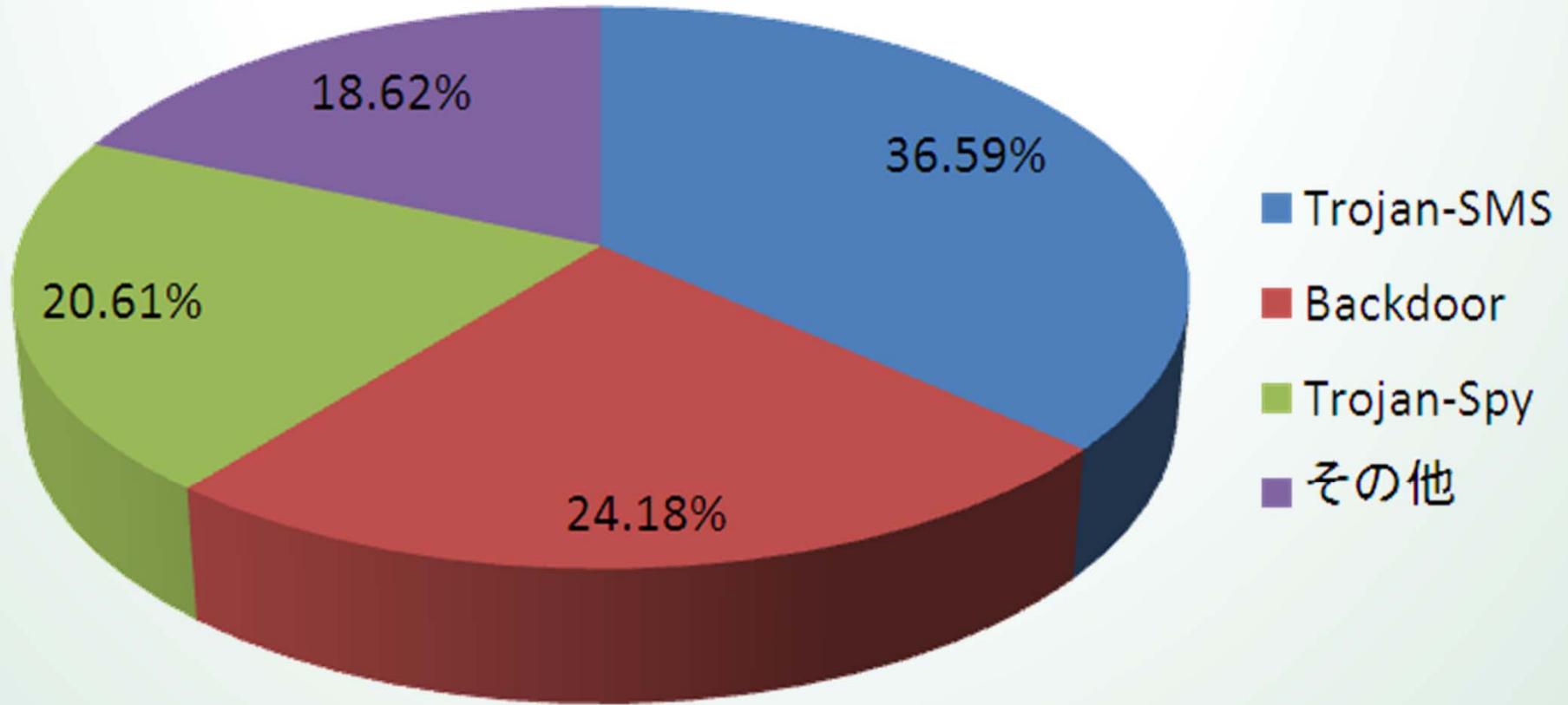


# モバイルOS向けマルウェア数



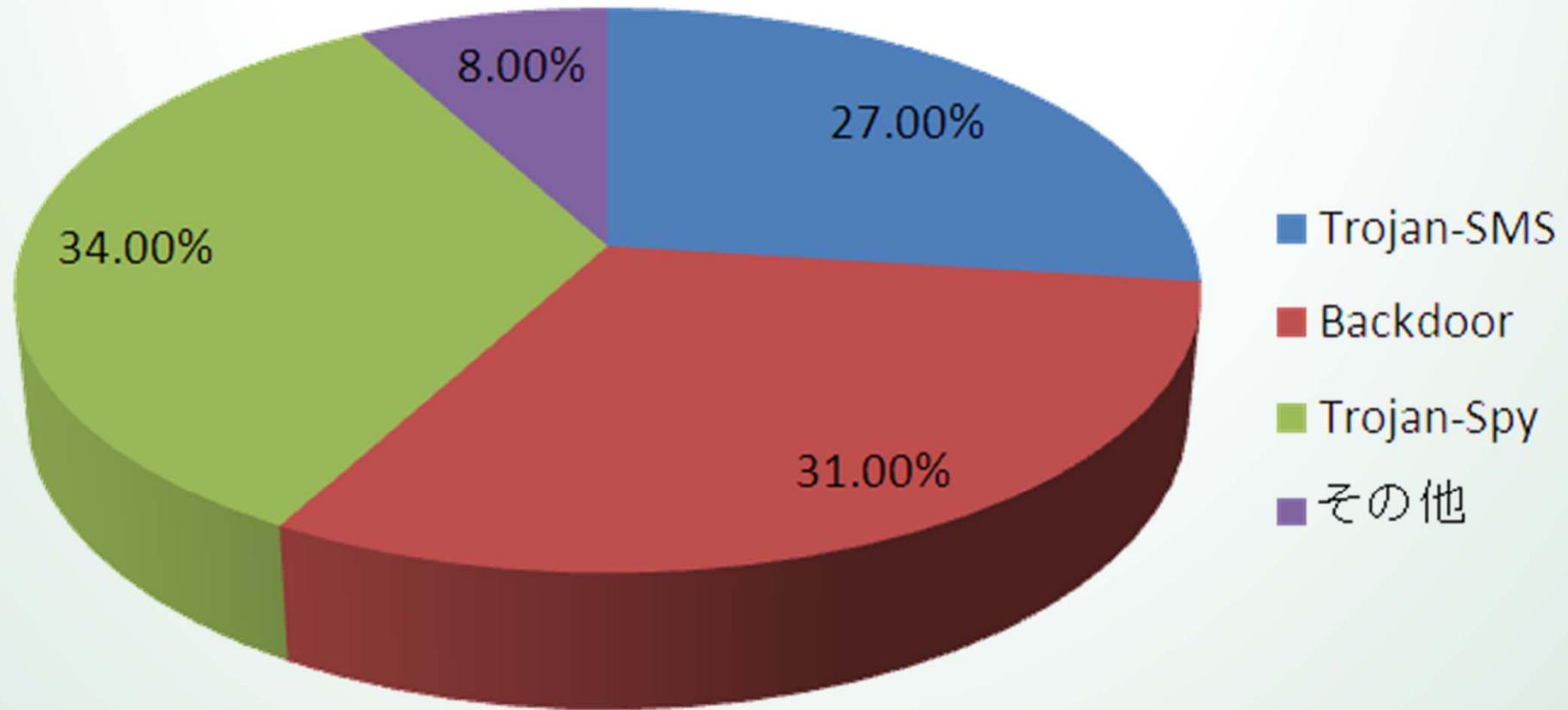
出典  
Kaspersky Lab

# 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

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

03-1234-5678

お客様端末アドレス

■■@■■.co.jp

年齢

18歳以上確認済み

お客様ID

■■■■■■■■■■

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

メールで問い合わせ

# 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



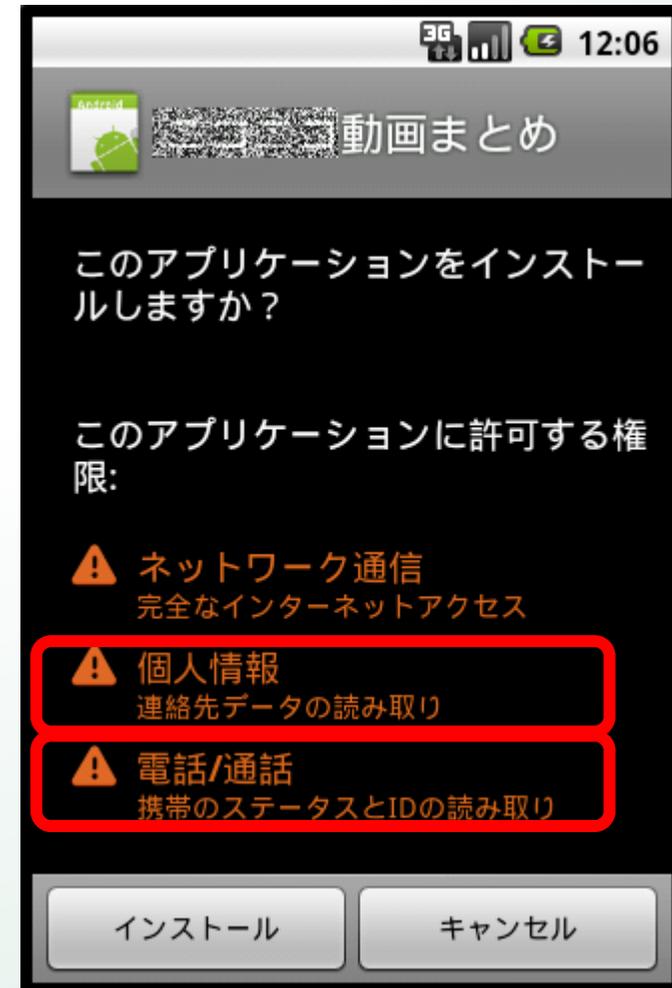
# 日本語アプリのマルウェア(2)

- 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



# 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



JSSEC成果発表会2012  
(2012年5月24日 @東京電機大学)