Mobile threats landscape

2013 Summary and 2014 Predictions

Yukihiro Okutomi
Mobile Malware Researcher

November 28, 2013

SAFE NEVER SLEEPS™

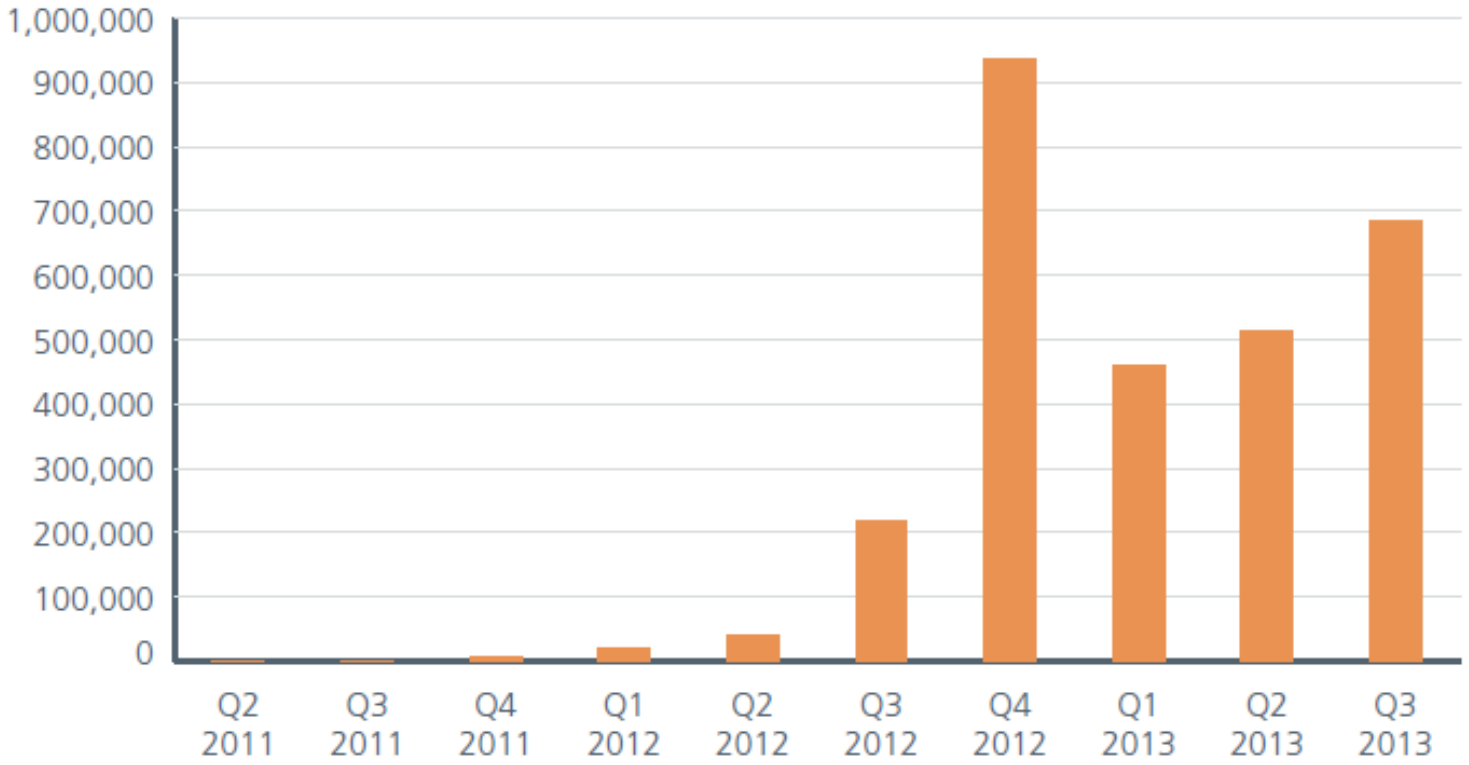
トピック

- 2013年サマリー
  - Androidマルウェアの統計
  - デバイス管理者権限を悪用したランサムウェア
  - モバイルバンキングマルウェア
  - 日本のユーザを狙ったマルウェア

- 2014年予測
  - デジタルウォレットがターゲットに
  - 狙われる生体認証
  - 第3のモバイルOSに注目

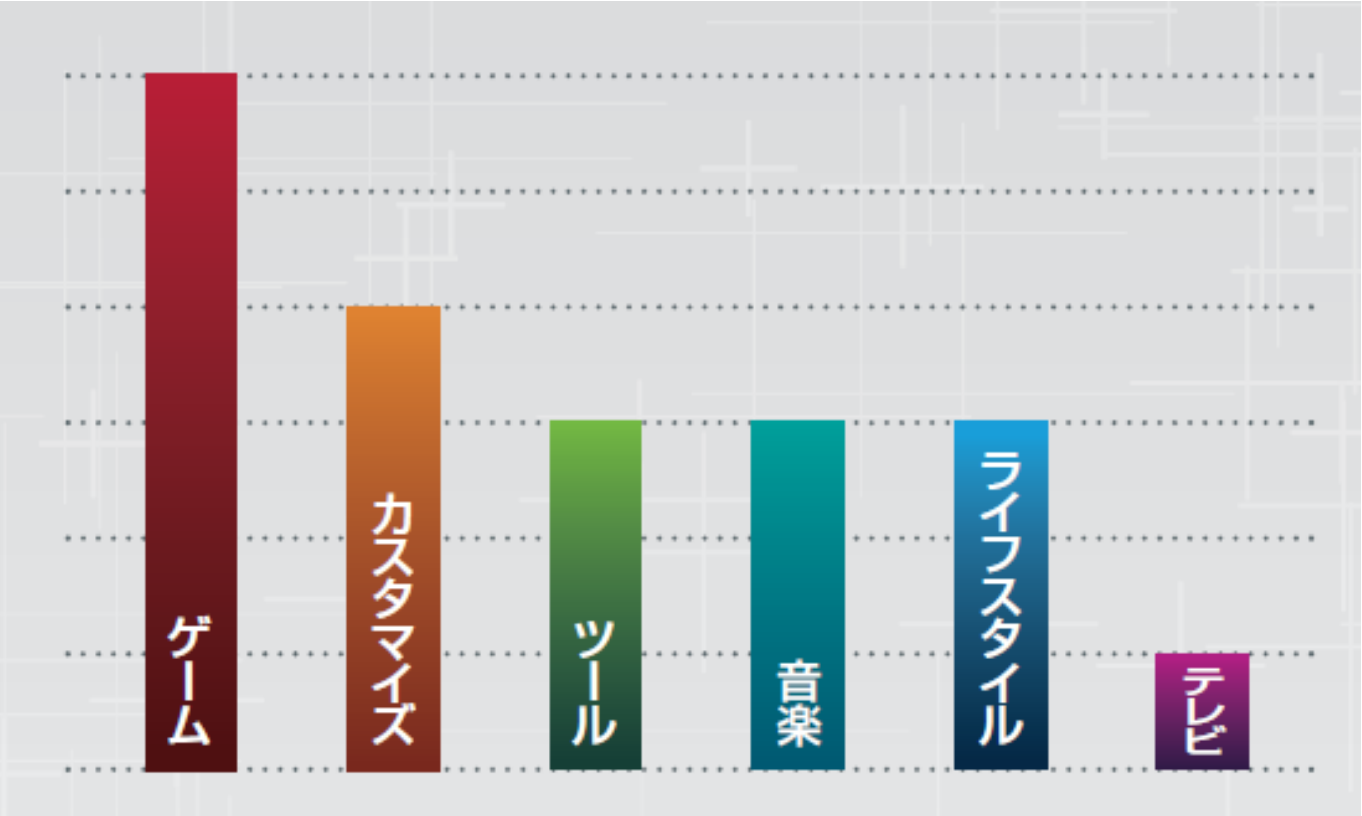
Androidマルウェアの統計

- モバイルマルウェアといえば、Androidマルウェアといっても過言ではないぐらいAndroidがマルウェアのターゲットとなっています。
- 2013年Q3では、68万件のマルウェアが発見され、今年は一定した増加傾向がみられています。



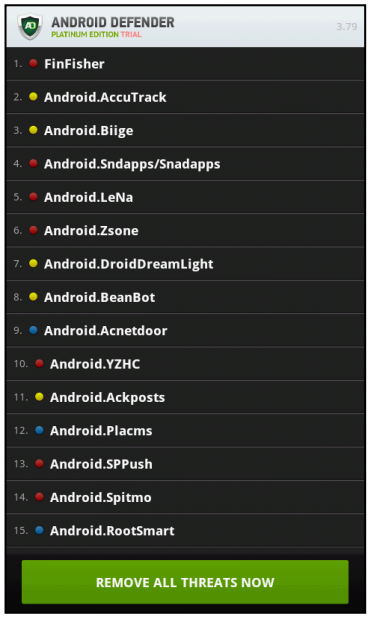
悪質なアプリのカテゴリ TOP20
ゲームとカスタマイズ

- マルウェアに感染したアプリのダウンロードトップ20のカテゴリとして、最も多かったのが「ゲーム」で、次が「カスタマイズ」。以下同順位で、「ツール」、「音楽」、「ライフスタイル（アダルトコンテンツ）」でした。

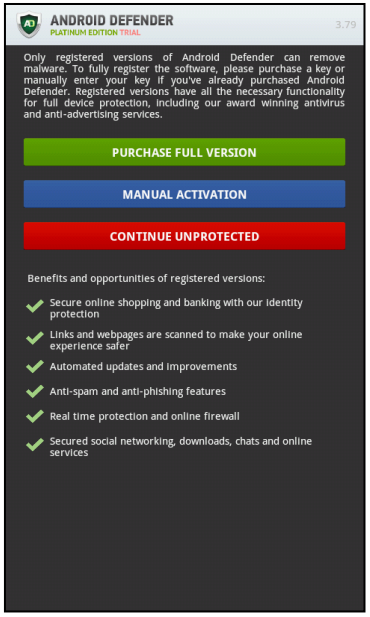


デバイス管理者権限を悪用したランサムウェア Android/Fakedefender

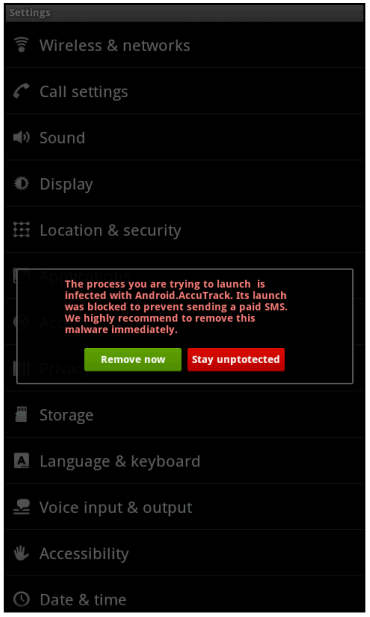
- マルウェアの特徴:
  - デバイス管理者権限を要求する
  - 有料版を購入させるため偽の感染結果を表示する
  - アンインストールを妨害するため設定画面を表示できなくする



偽の検出結果



有料版購入

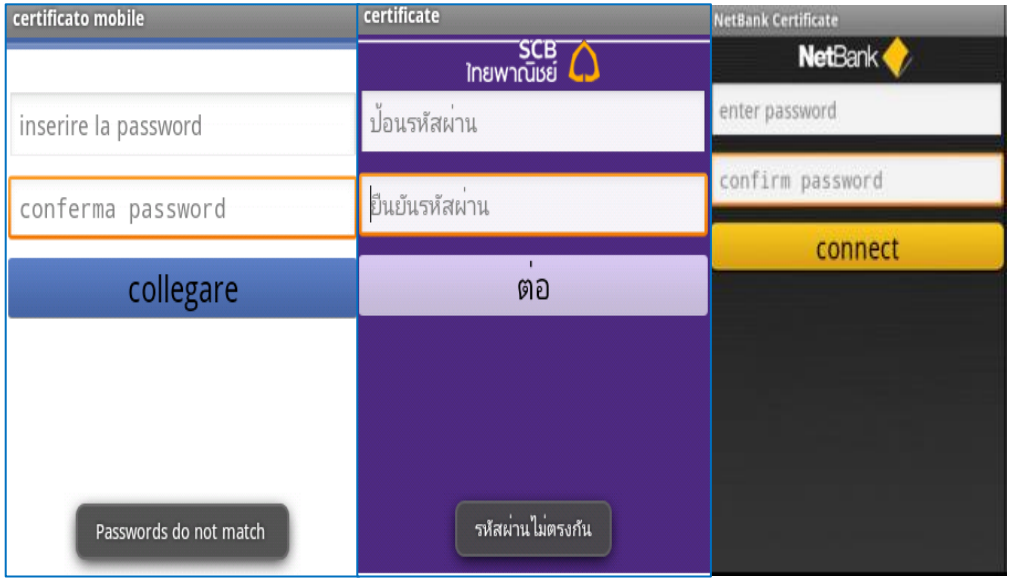


アンインストール操作を妨害

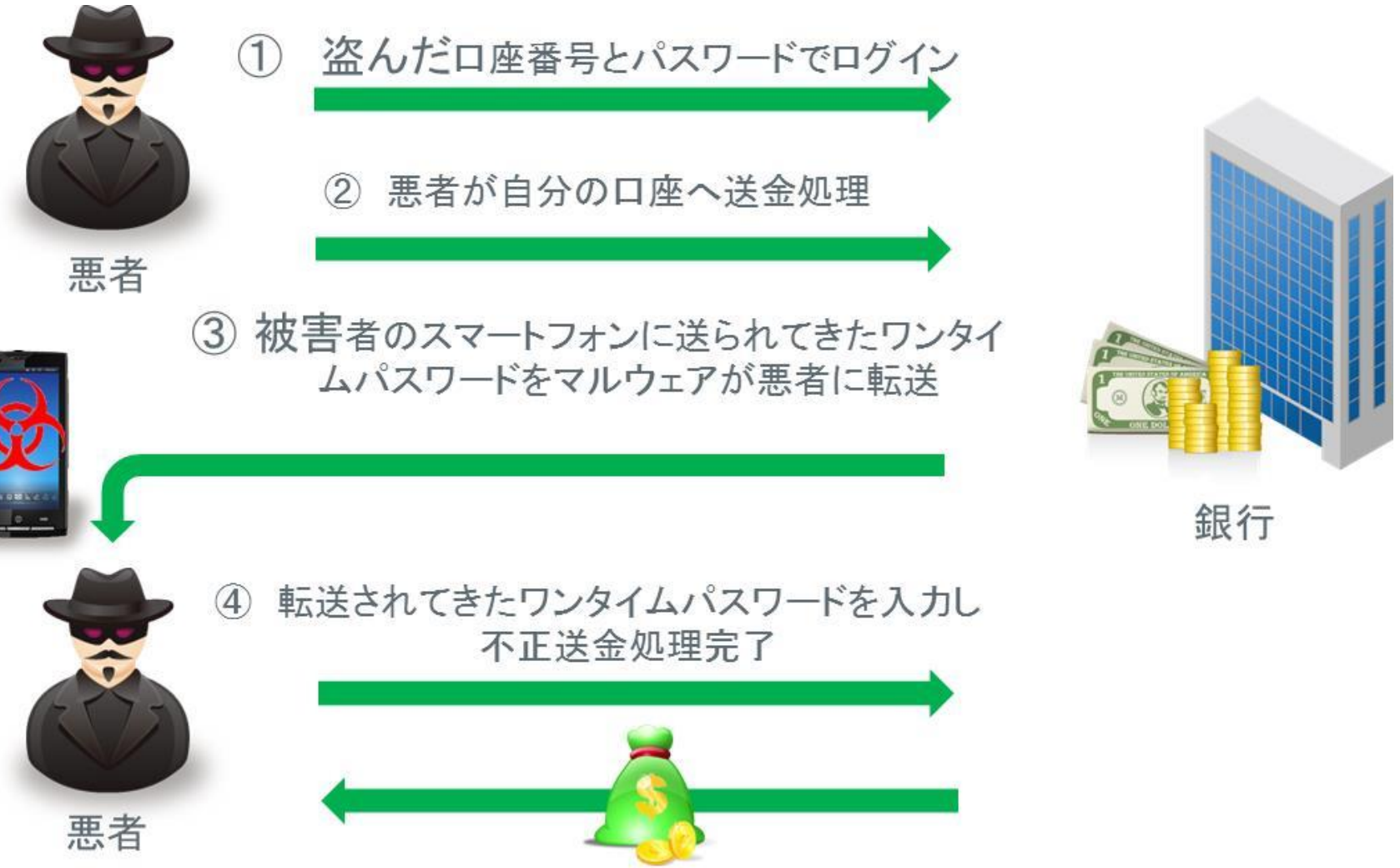
デバイス管理者権限を悪用したランサムウェア Android/Fakedefender

モバイルバンキングマルウェア
Android/FakeBank, Android/FkSite

- マルウェアの特徴
  - イタリア、タイ、オーストラリア、韓国など多くの国で発見された
  - 正規のモバイルバンキングアプリやセキュリティトークン生成アプリを装い、ユーザが入力したアカウントやパスワードを攻撃者のサーバに送信する
  - SMS経由で送られてくるモバイル取引認証番号（mTAN）と呼ばれるワンタイムパスワードを攻撃者のサーバに送信する



モバイルバンキングマルウェアを使用した不正送金の流れ



モバイルバンキングマルウェア
Android/FakeBank

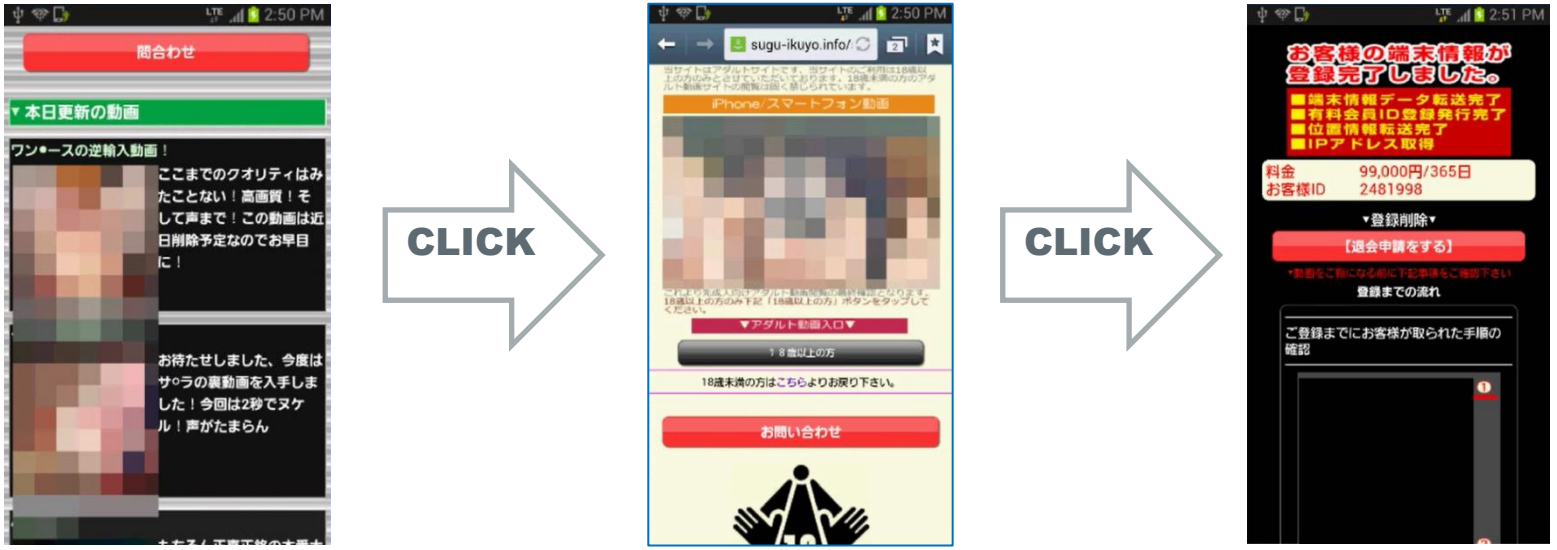
日本のユーザを狙った個人情報窃盗
Android/Uracto

- マルウェアの特徴:
  - 配布サイトのリンクがSMS経由して送信されてくる
  - 「服が透けるアプリ」や「日刊アンドロイド」等のアプリ名称を使用
  - 電話帳の内容を外部サーバに送信する

日本のユーザを狙った個人情報窃盗
Android/Uracto

日本のユーザを狙ったワンクリック詐欺 Android/OneClickFraud

- マルウェアの特徴:
  - Google Playストアにて配布されていた
  - ユーザによる年齢認証や同意画面を経由させる
  - ユーザーがアプリを操作しない限り 詐欺がすぐに判明しないようにアプリを技術的に「2クリック詐欺」または「3クリック詐欺」とし、自動スクリーニングやスキャンのプロセスを難しくしている



コンテンツ表示　年齢認証　架空請求

悪質なアダルト出会い系アプリ
Android/DeaiFraud

- マルウェアの特徴:
  - Web上の悪質な出会い系サイトへユーザーを誘導する
- 悪質な出会い系サイトの特徴:
  - 登録するためにメールアドレスを要求し、いったんサービスに登録するとすぐに、サクラと思われるユーザからのスパムメールが届く。
  - サービス登録直後は無料でメール閲覧や返信などができますが、いざ待ち合わせの約束をするという段階で突如無料期間が終了し、料金の支払いを要求される。

2013年のモバイル脅威のサマリー

- デバイス管理者権限を悪用したマルウェアが登場しました。デバイス管理者権限はとても強力であり、端末紛失時のリモートロックやリモートワイプといった端末を操作させないための機能を提供している反面、悪用されると端末が一切操作できなくなってしまいます。
- 世界各国で、モバイルバンキングを狙ったマルウェアが発見されました。正規のバンキングアプリ、セキュリティトークン生成アプリ、SSL証明書などのアプリを装い、ユーザの銀行口座を狙っています。
- 日本では、2012年から引き続いて、電話帳や電話番号といった個人情報を搾取するマルウェアが発見されました。これらのマルウェアは、SMSやスパムメールを経由して配布され、限定的な個人にのみ送信することで発見を遅らせることをしています。
- また、ワンクリック詐欺、出会い系詐欺などユーザを詐欺サイトに誘導するマルウェアがGoogle Playストア上で多く発見されています。公開されたアプリの削除と登録のいたちごっこは今もなお続いています。金銭被害に発展するケースもあるためユーザ自身も騙されないよう気を付けなければなりません。

2014年のモバイル脅威予測 (1)
デジタルウォレットがターゲットに

- 「モバイルペイメントプログラム」や「デジタルウォレット」に用いられるタップ＆ペイ型の近距離通信（NFC）技術がターゲットになるでしょう。
- 近接していることを利用して（いわゆる「bump and infect（ぶつかった相手に感染）」手法で）繁殖するワームを伴う可能性があります。
- この配布経路では、エレベーターや列車といった密接した状態を介してマルウェアが拡散します。

2014年の脅威予測 (2)
狙われる生体認証

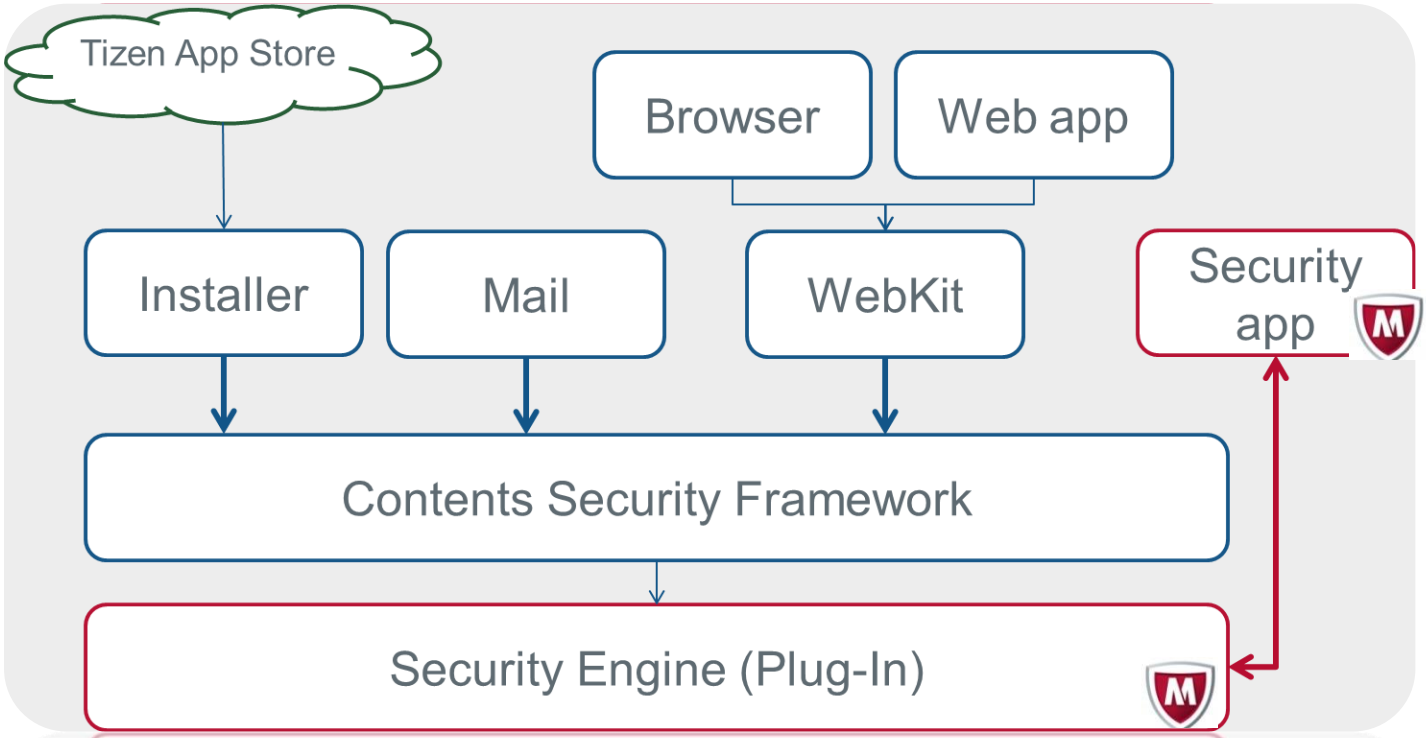
- 指紋認証、光彩認証、顔認証といった生体認証について研究が進みます。
- カメラや指紋センサーなど生体認証に必要なセンサーはすでにスマートデバイスには搭載されており、生体認証が端末ロックやモバイルペイメントで使用される兆しを見せています。
- スパイ映画さながらに、ドアノブから指紋を採取され、端末ロックが解除される日もそう遠くありません。

2014年の脅威予測 (3)
注目される第3のモバイルOS

- Apple iOS　/ Google Androidに続き、新しいWeb技術ベースのモバイルプラットフォーム「Tizen OS」や「Firefox OS」に注目が集まります。
- アプリマーケットにはFacebook, Lineといったアプリが並び、ユーザは思いのほか気軽にこの第3のモバイルOSを利用することができるでしょう。
- 一方、Web技術を悪用し、これらのOSを狙ったフィッシングサイトやJavaScriptマルウェアもまた出現し始めます。私たちは、これらのモバイル脅威が近い将来さらに増加するリスクに私たちは備えなければなりません。

TizenOSのセキュリティ機構について
Contents Security Framework

- 怪しいマーケットアプリは、インストールする前にスキャンされる
- 怪しいメール添付ファイルも、開く前にスキャンされる
- 怪しいサイトも、ブラウザでアクセスする前にスキャンされる
- ユーザが好きなセキュリティアプリを選択できる



TizenOSのアプリ開発のしやすさ

- アプリ公開にかかる費用はいまのところ無料で、参入障壁は低い
- アプリ審査では、自動評価に加えて、手動評価が行われる。
- ストア外のアプリは許可されるものの使用できるパーミッションに制限がある。

	Android	iOS	Tizen
登録費用	¥2500	¥8400 / year	無料?
アプリ審査	自動評価	自動評価 手動評価	自動評価 手動評価
ストア外のアプリ	OK	NG	OK (制限付)


McAfee®
An Intel Company