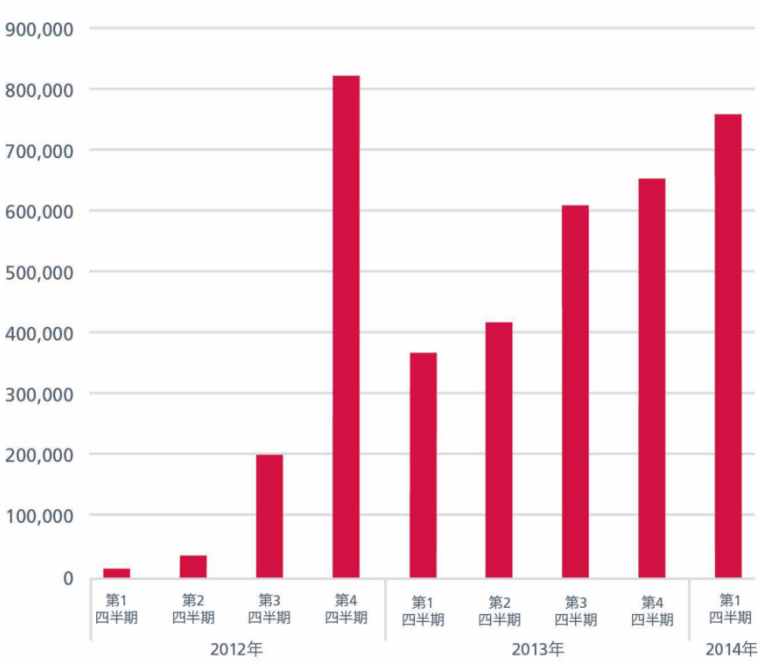
最新モバイル脅威レポート

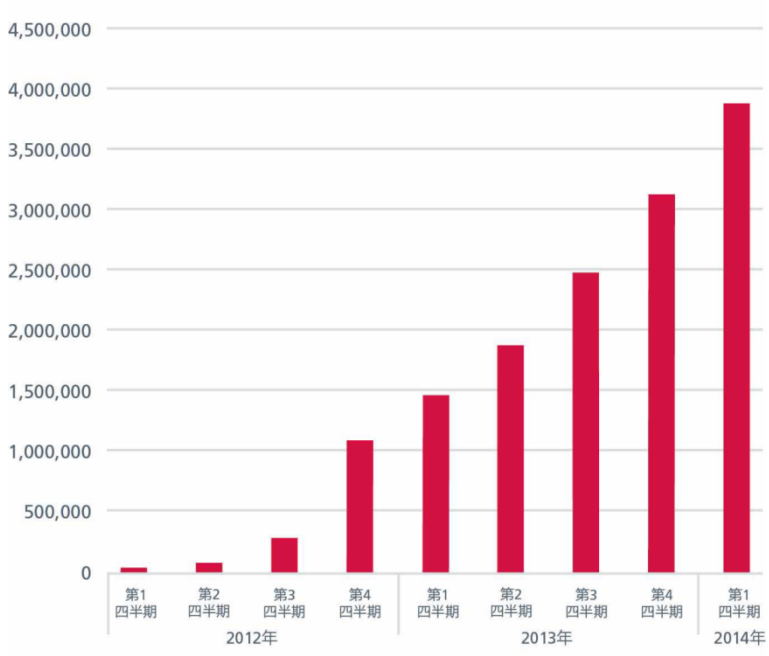
August 1, 2014

Yukihiro Okutomi | Mobile Malware Researcher

モバイルマルウェア数の統計

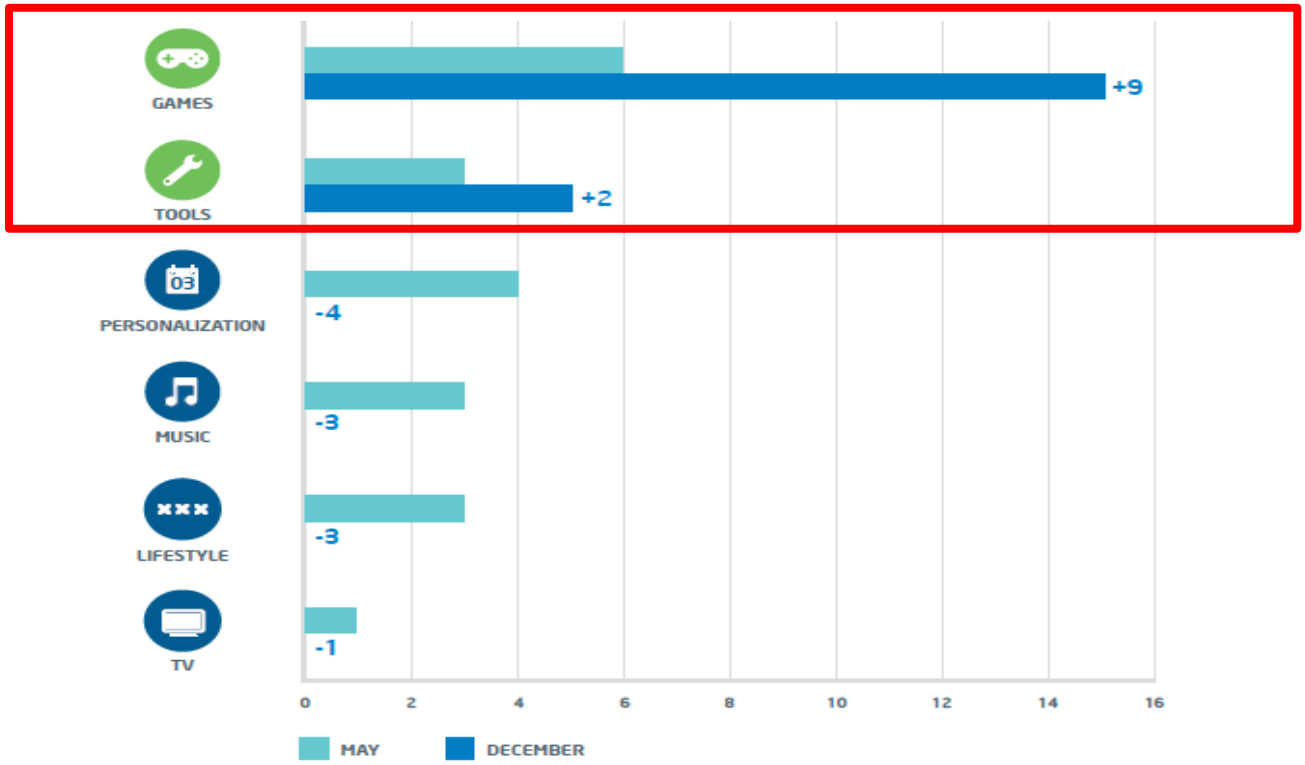
依然として増加傾向



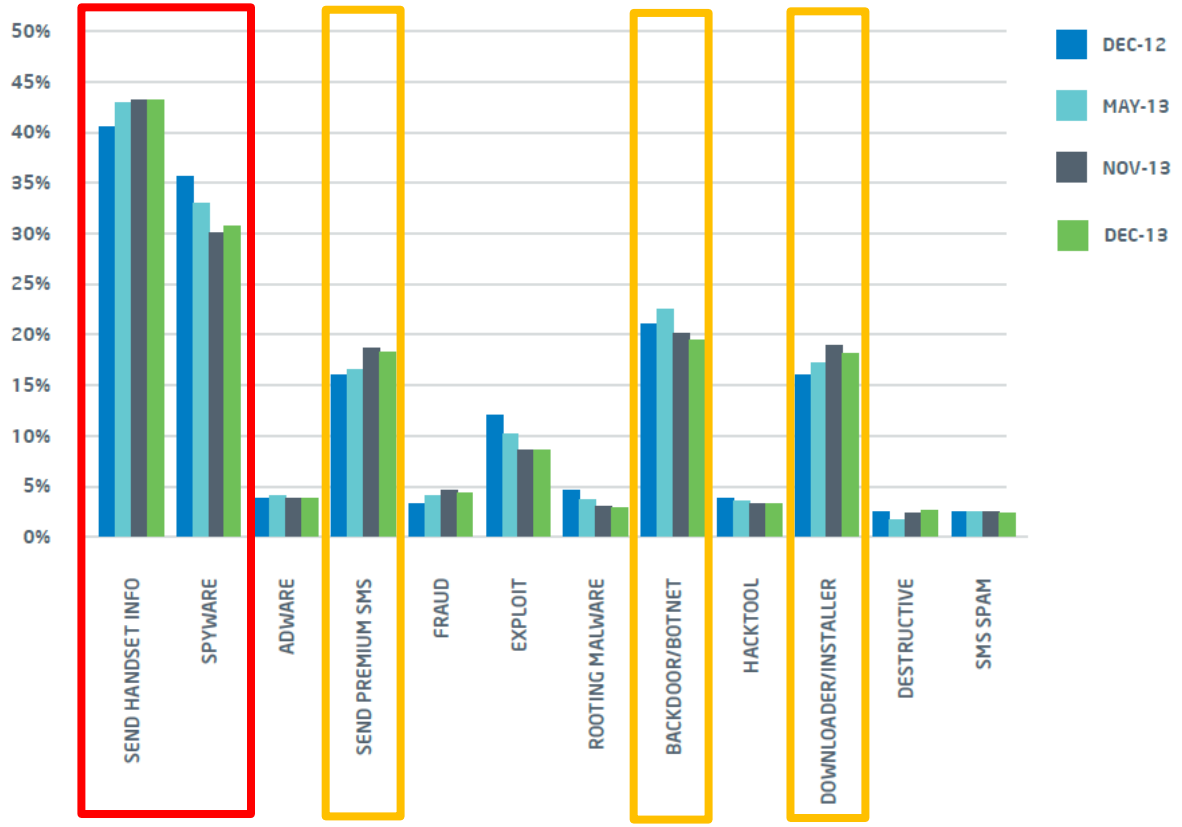


マルウェアが悪用するカテゴリ

ゲームとツールに集約

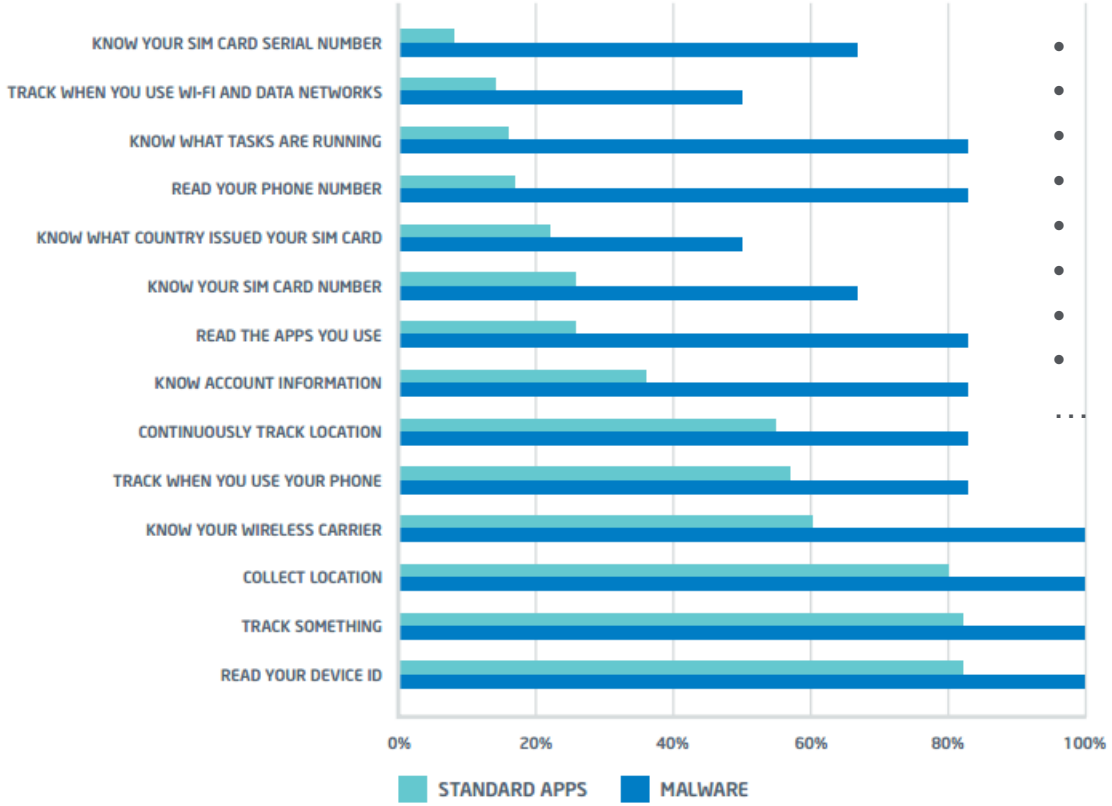


マルウェアの機能


50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
SEND HANDSET INFO
SPYWARE
ADWARE
SEND PREMIUM SMS
FRAUD
EXPLOIT
ROOTING MALWARE
BACKDOOR/BOTNET
HACKTOOL
DOWNLOADER/INSTALLER
DESTRUCTIVE
SMS SPAM
DEC-12
MAY-13
NOV-13
DEC-13

アプリの端末情報・ユーザ情報の収集

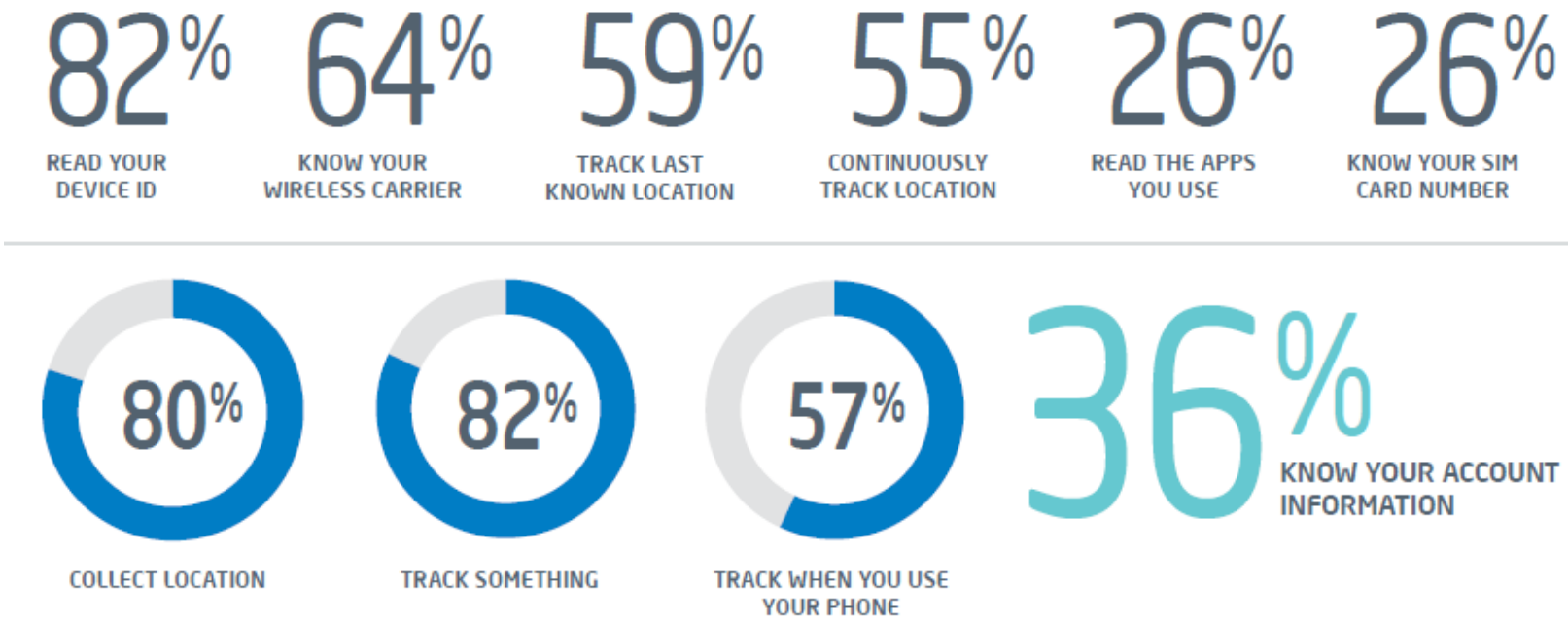
マルウェアと正規アプリのギャップ



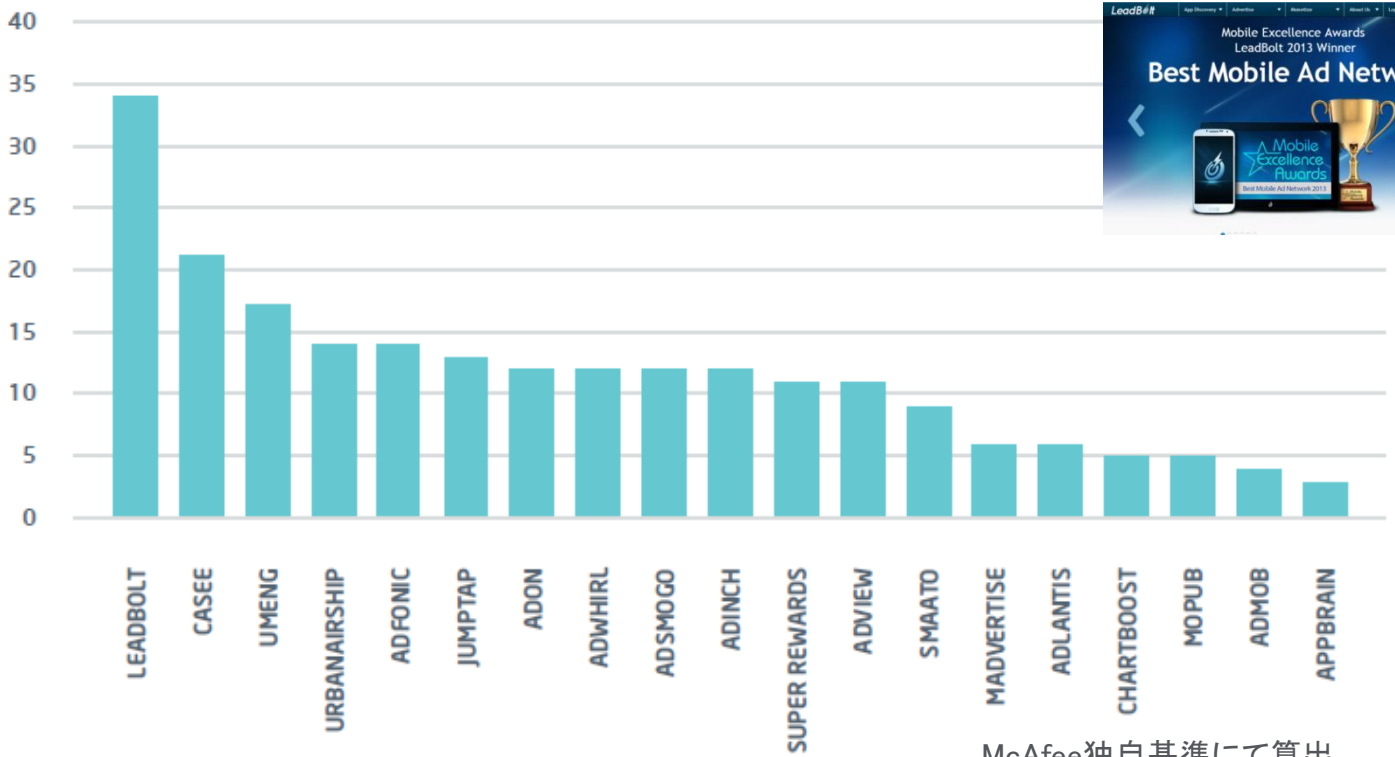
- SIMのシリアル番号
- 通信利用状況
- 実行中のタスク
- 電話番号
- SIMの国情報
- SIMカード番号
- インストールアプリ
- アカウント情報
- …

アプリの端末情報・ユーザ情報の収集

正規アプリに関するデータ



広告モジュールのプライバシースコア



McAfee独自基準にて算出

Android threats

有名アプリを狙った脅威

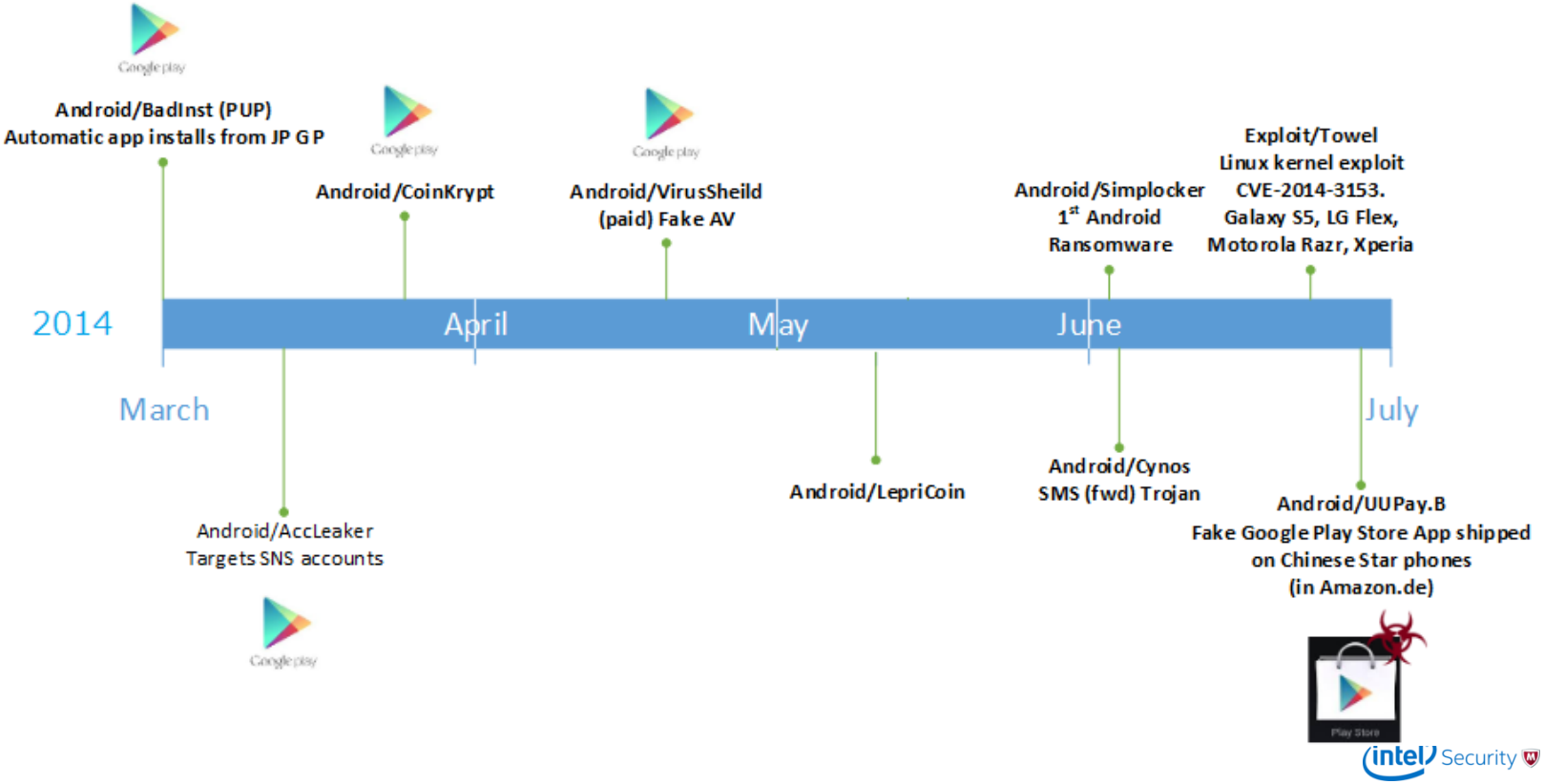
- Android/FakeInstaller
  - FacebookやWhatsAppアプリのインストーラを装う
- Android/BalloonPopper.A
  - バルーンポップゲームアプリを装う
  - WhatsAppのチャットログや画像を盗む
- Android/PinFwd
  - WhatsAppやChatOnアプリのアカウント情報を盗む
- Android/Waller.A
  - Adobe Flash Playerを装う
  - Visa QIWI WalletアプリのSMS認証を模倣し、送金を実施する

Flappy Birdの偽物による攻撃

- 開発者が今年2月に人気ゲームFlappyBirdを、突然アプリマーケットから削除した
- それと同時に悪意のある偽物が出現し始める
- SMS送信、通話発信、デバイスやユーザ情報の抜き取りといった悪意のあるコードが追加されていた

時系列でみるマルウェアの脅威

2014年3月～6月



Google Playストアからの自動インストール

Android/BadInst (PUP)

発見日：2014年3月

ターゲット：日本

特徴：

- ダウンロードベースのリワード広告
- 非公式な方法で自動インストールを実現していた
  - Googleアカウントに関連したサービスを利用するためにSID とLSID の権限を要求
  - AccountManager.getAccountsByType() や AccountMangaer.getAuthToken()を使用
- マルウェアの自動インストールに悪用される可能性がある

McAfee Blog: http://blogs.mcafee.com/mcafee-labs/automatic-app-installation-google-play-store-poses-big-risk

SNSアカウントを狙った脅威

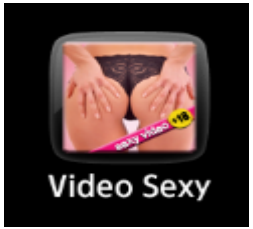
Android/AccLeaker

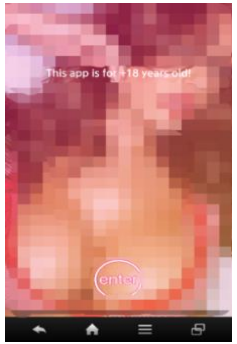
発見日：2014年3月

ターゲット：グローバル

特徴：

- Google PlayストアにてアダルトHD動画プレーヤーとして配布されていた
- 外部サーバにGoogle/Facebook/TwitterといったSNSアカウント情報を送信する





McAfee Blog: http://blogs.mcafee.com/mcafee-labs/suspicious-mobile-app-finds-gmail-facebook-twitter-accounts

有料の偽アンチウィルスアプリ

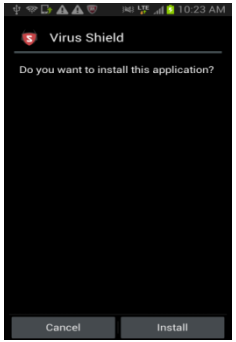
Android/VirusSheild

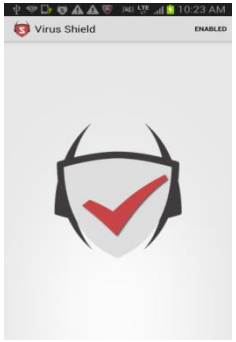
発見日：2014年4月

ターゲット：グローバル

特徴：

- 有料アプリとしてGoogle Playストアにて販売されていた
- 偽のウイルス対策ソフト
- マルウェアをスキャンする機能は一切ない





仮想通貨採掘マルウェア

Android/CoinKrypt, Android/LepriCoin

発見日：2014年3, 5月

ターゲット：グローバル

特徴：

- 音楽ファイルのダウンローダーやカレンダーアプリとして配布されていた
- 仮想通貨（BitCoin/Litecoin/Dogecoin）の採掘をバックグラウンドで実行
- バッテリーレベルやスクリーンのオンオフ状態を監視し、バッテリーが十分にある状態や、スクリーンがオフ状態であるときのみ動作するようになっていた

ユーザファイルの暗号化を行う初のランサムウェア

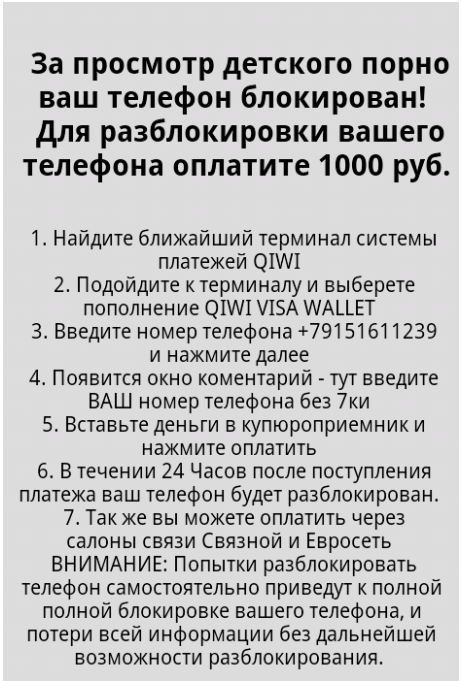
Android/Simplocker

発見日：2014年6月

ターゲット：ロシア、ウクライナ

特徴：

- ポルノアプリ、ゲームとして配布されていた
- これまでのランサムウェアは画面ロックや架空請求画面によってユーザを脅迫するだけであった
- SDカード上の画像やドキュメントを暗号化し、暗号化を解除するために、金銭を要求する
- 外部サーバとの通信には匿名通信技術(Tor)が使用されていた



ワンクリックルート化ツール

Exploit/Towel

発見日：2014年6月

ターゲット：グローバル

特徴：

- Linuxカーネルの脆弱性（CVE-2014-3153）を突き ルート権限を奪取
- 6月3日以前にビルドされたLinuxカーネルを持つ AndroidOS4.4(KitKat)がこの脆弱性の影響を受ける
- 脆弱性を受けるデバイスとして、Samsung Galaxy S5, LG G Flex, Motorola Razr, Sony Xperiaが含まれている

プリインアプリとして出荷されたマルウェア

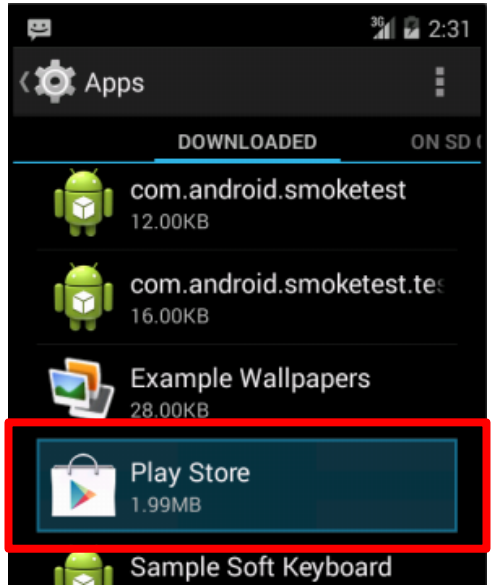
Android/UUPay.B

発見日：2014年6月

ターゲット：グローバル

特徴：

- 中国製デバイスにGoogle Playアプリとしてプリインされていた
- デバイスはドイツのアマゾンで販売されていた
- UIがないサービスアプリケーション、
  ホーム画面にはアイコンは表示されない
- デバイス情報やユーザ情報を収集し、外部サーバに送信する



SMSを転送するトロイの木馬

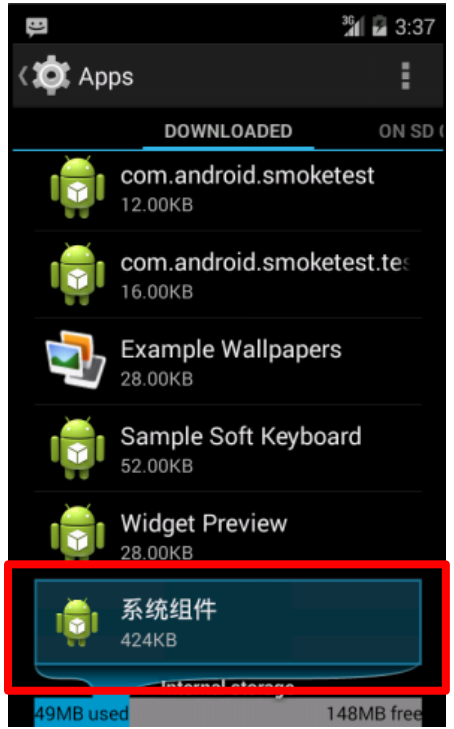
Android/Cynos

発見日：2014年6月

ターゲット：中国

特徴：

- システムコンポーネントとしてインストールされる
- UIがないサービスアプリケーション
- 特定の番号からのSMSをブロックしたり、
  特定のキーワードが含まれるSMSをブロックする
- 受信SMSを特定の番号に転送する



iOS threats

Jailbreakされた端末に潜んでいたダウンローダー

発見日：2014年3月

特徴：

- 設定ファイルと実行ファイルの2つで構成
- /System/Library/LaunchDaemons/com.archive.plist
  - 設定ファイル
  - 2時間おきに、/bin/uvdatesrv（ダウンローダープログラム）を実行する
- /bin/updatesrv
  - 実行ファイル（ダウンローダー）
  - ドメイン “www.jb-app.com” から別のプログラムをダウンロードする
  - ダウンロードしたプログラムを実行後、痕跡を隠すためにそのプログラムを削除する

News: http://weicdsq.lofter.com/post/20a5c5_13cc45e

遠隔ロックを悪用した身代金要求

発生日：2014年5月

- ユーザの端末は遠隔ロックされ、ロックを解除するためには、50ドルを特定のPayPalアカウントに支払う必要があるという身代金の要求のメッセージが端末に表示された
- 端末紛失時にリモートから遠隔ロックや端末の位置情報を把握する「Find My iPhone」という機能が悪用された事件で、オーストラリアで多く報告された

事象：

- iCloudのパスワードがハックされた
- ユーザデバイスがロックされた
- OpenSSLのHeartBleed脆弱性が関連か
  - Apple社のサーバーはOpenSSLの脆弱性の影響は受けないので、おそらく、攻撃者は他のWebサイトからパスワードを盗んだのであろう

News: http://mashable.com/2014/05/27/australian-hackers-ios-ransom/

Web threats

インターネット検索で最も危険な有名人

- 1位：リリー・コリンズ
- 2位：アヴリル・ラヴィーン
- 3位：サンドラ・ブロック
- 4位：キャシー・グリフィン
- 5位：ゾーイ・サルダナ
- 6位：ケイティ・ペリー
- 7位：ブリトニー・スピアーズ
- 8位：ジョン・ハム
- 9位：アドリアナ・リマ
- 10位：エマ・ロバーツ

McAfee Blog: http://promos.mcafee.com/offer.aspx?id=541880&cid=127364

インターネット検索で最も危険なスーパーヒーロー

- 1位：スーパーマン
- 2位：マイティー・ソー
- 3位：ワンダーウーマン
- 4位：ウルヴァリン
- 5位：スパイダーマン
- 6位：バットマン
- 7位：ブラック・ウィドウ
- 8位：キャプテン・アメリカ
- 9位：グリーン・ランタン
- 10位：ゴーストライダー

McAfee Blog:: http://blogs.mcafee.jp/mcafeeblog/2014/07/post-6992.html


intel
Security