Android Malware is on the Rise

Timothy Armstrong, Researcher, Kaspersky Lab

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

06.10.2011, Virus Bulletin Conference, Barcelona, Spain

Agenda

- **Arrival**
- **Statistics**
- **Variety** of **malware**
- **Malware sources**
- **Evolution** of **affiliate networks**

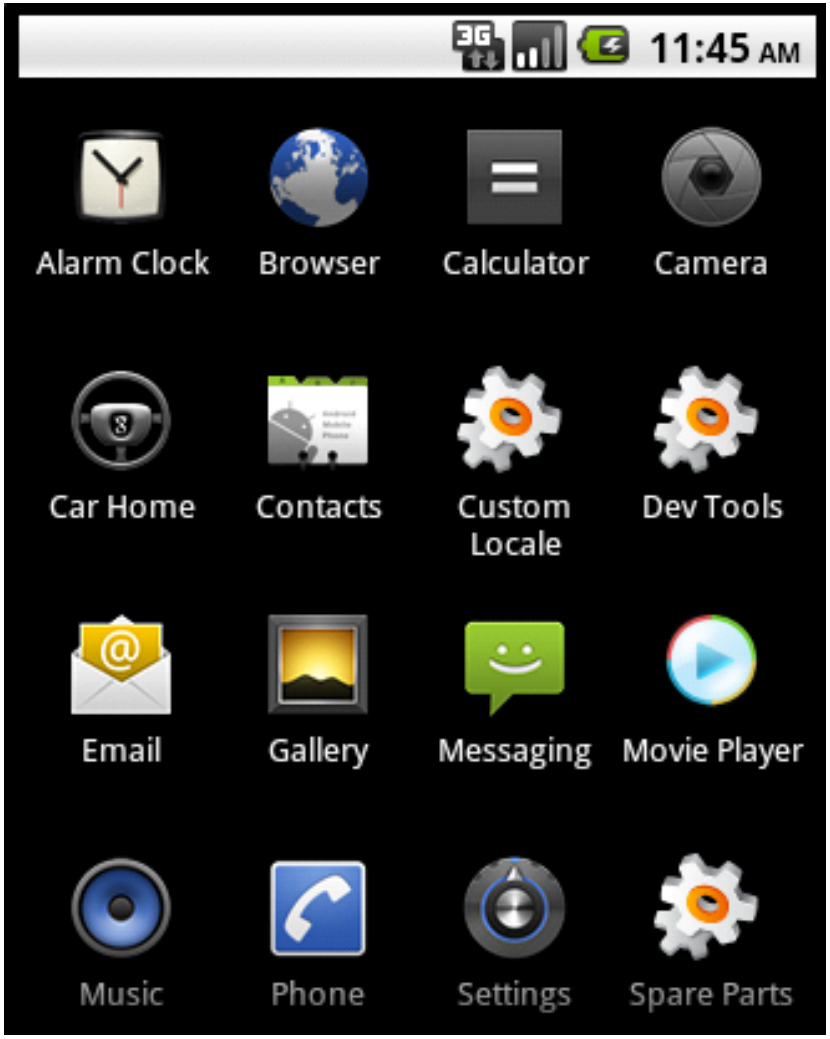
Arrival

KASPERSKY lab

Arrival

FakePlayer

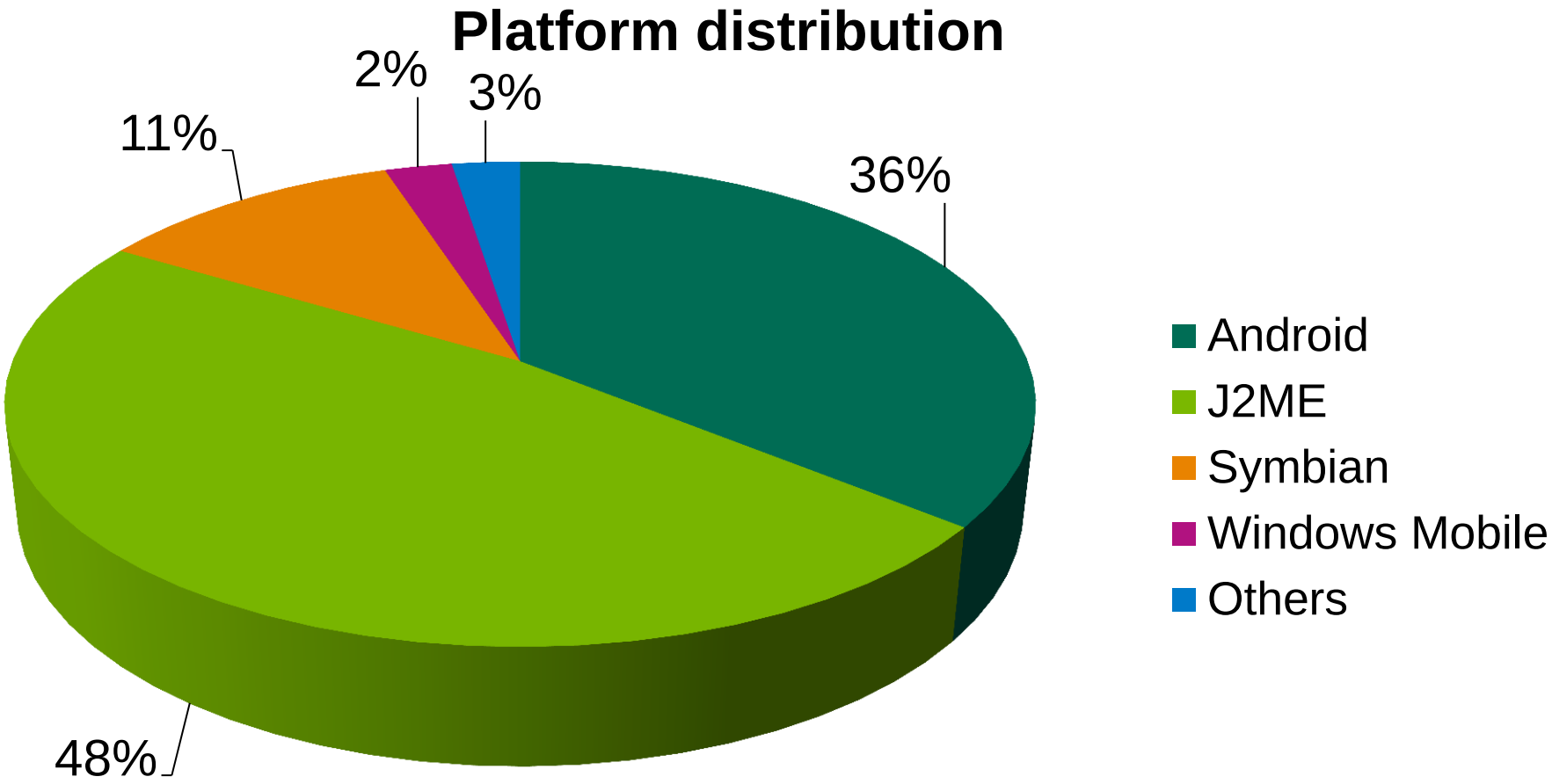
- **Found** in **August 2010**
- **‘Legitimate’** app: **Movie Player**
- **Simple SMS Trojan**
- Used a **black SEO** for delivery



Statistics

Statistics

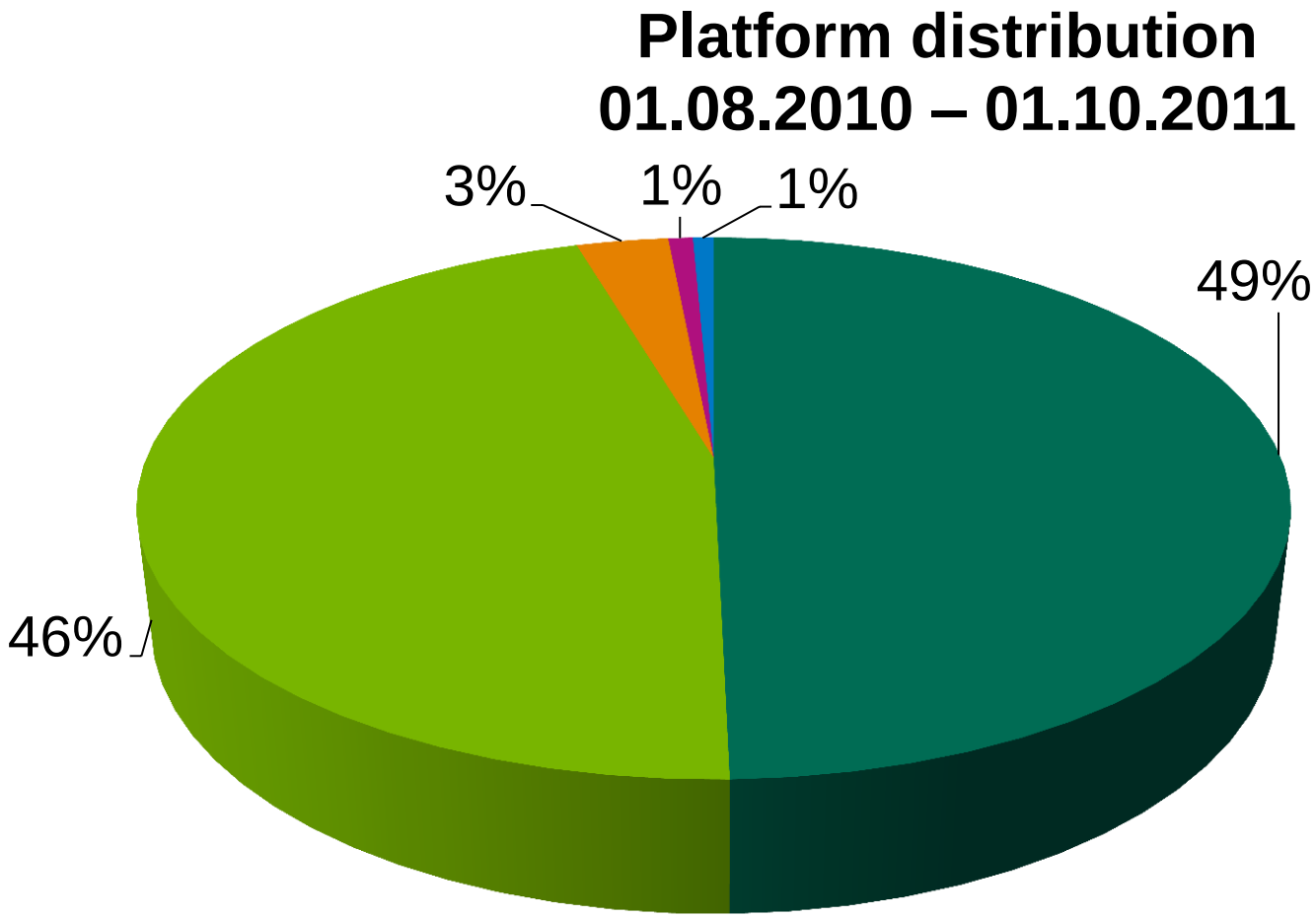
Mobile malware



Total	**3194 modifications**	**273 families**

Statistics

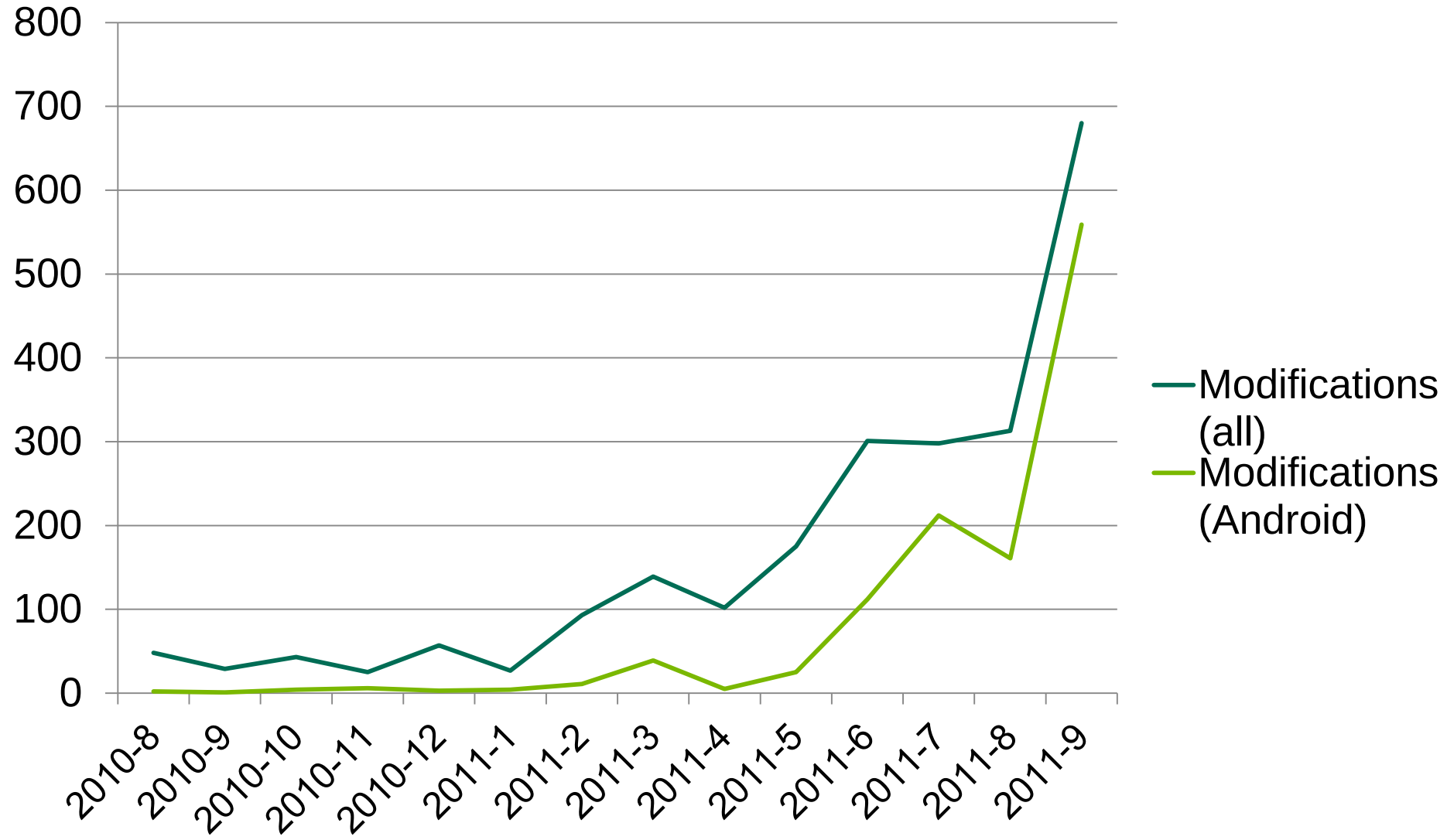
14 months



Android	**1144**
J2ME	**1055**

Statistics

Android vs. All



Variety of malware

Premium rate SMS

- **Send expensive SMS messages**
- **Popular** in **Russia, China**
- **Requests permission** to send **SMS**

Data Theft

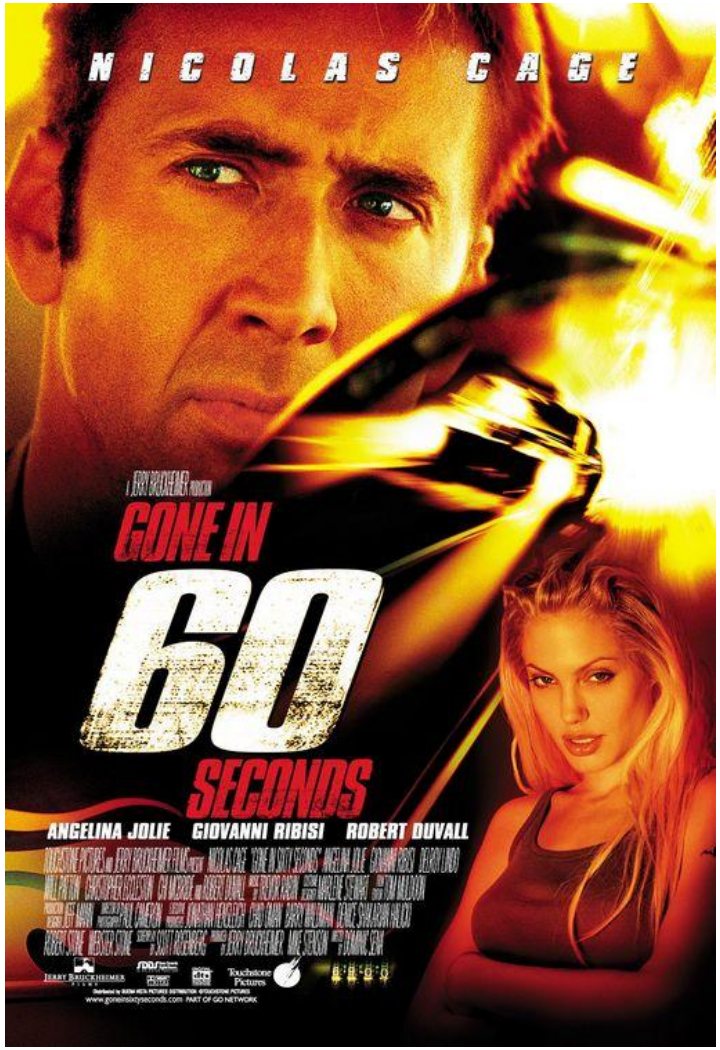
- **Steals** multiple types of **personal information**
  - **IMEI**
  - **IMSI**
  - **Language**
  - **Country**
  - **SMS messages**
  - **Call logs**
  - **Contacts**
  - **…**
- **Uploads** to a **remote server**

DroidDream

- **March 2011: DroidDream Trojan arrives in Android Market**
- **More than 50** different **apps in Android Market**
- **Complex malware with:**
  - **data theft functionality**
  - **root exploits**
  - **botnet-like** capabilities
- **Tens of thousands** of **infected users**

Spyware

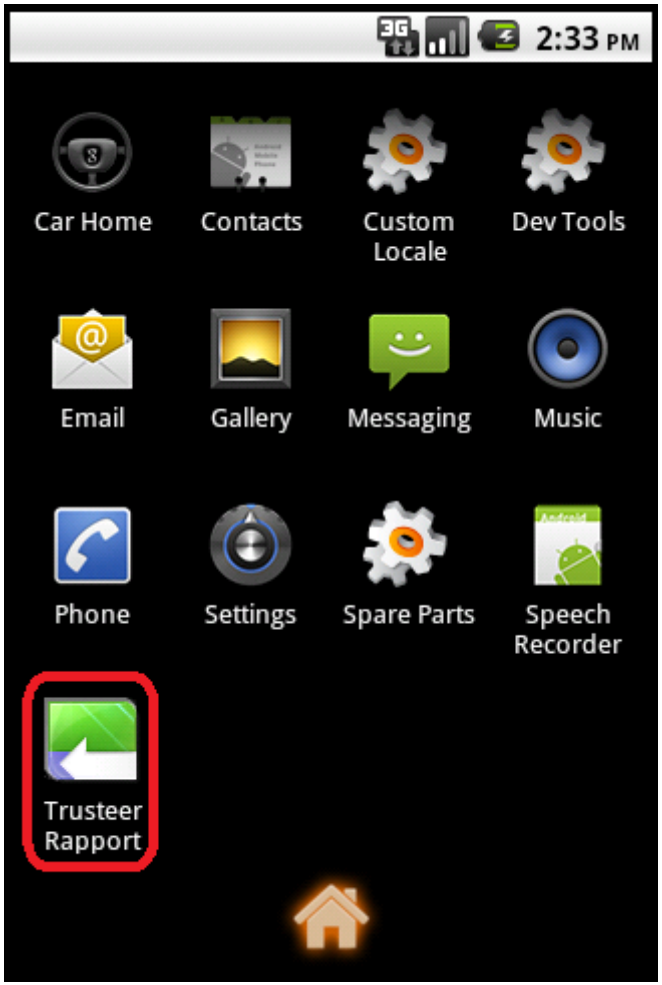
- **Spying tools** created for **‘educational purposes’**
- **Usually are not very expensive**
- **Often require physical access** to **target phone**



Man-in-the-Mobile

- **ZitMo: ZeuS-in-the-Mobile**
- **SpitMo: SpyEye-in-the-Mobile**
- **Target: mTANs**
- **Malware incarcerated**

  for **specific purposes**



Three pillars

Money

- SMS Trojans (or dialers)

Data

- ‘Steal-everything’ malware
- Spyware

Target

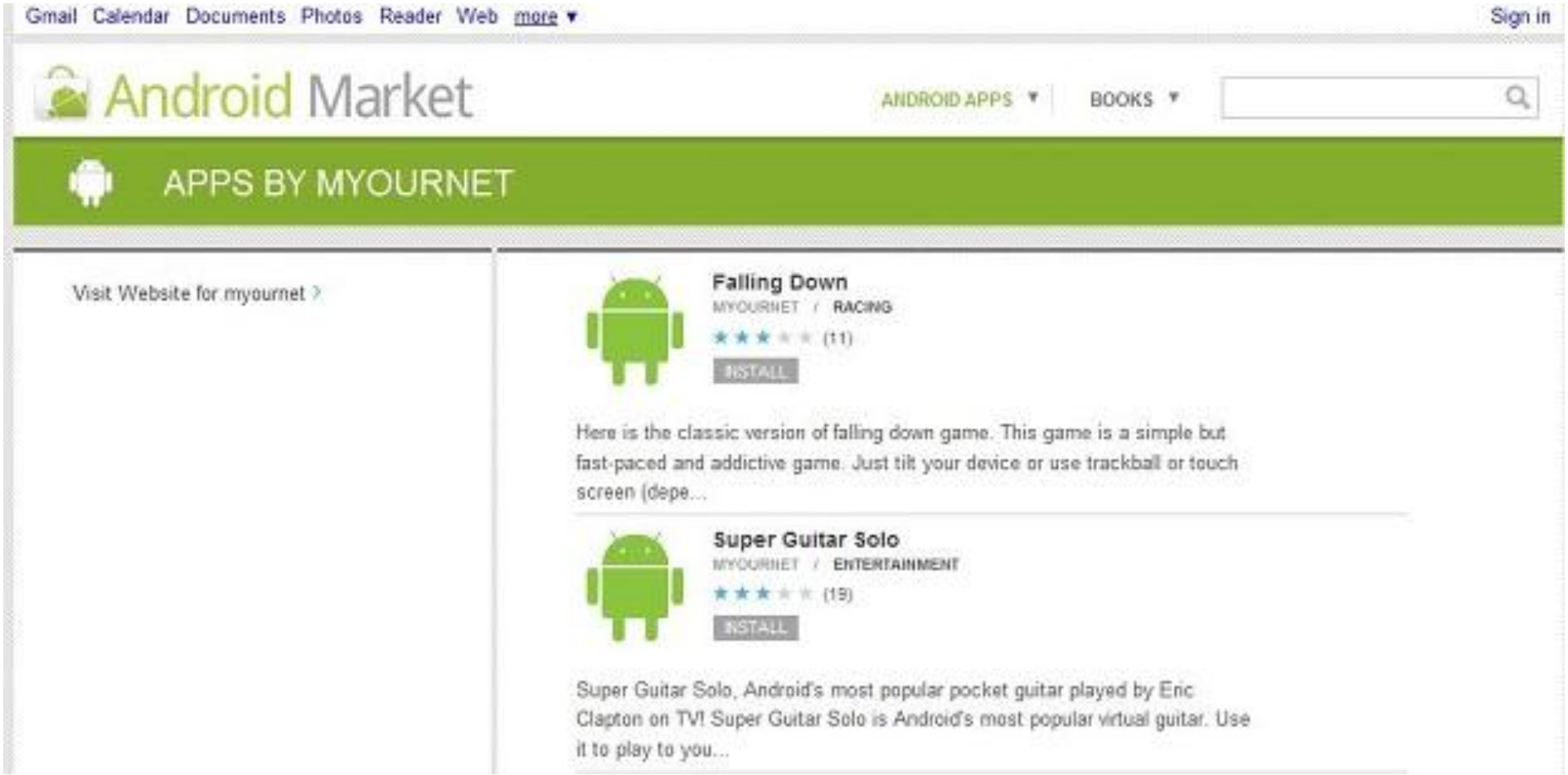
- ‘Targeted’ malware

Malware sources

Malicious websites

Malicious websites

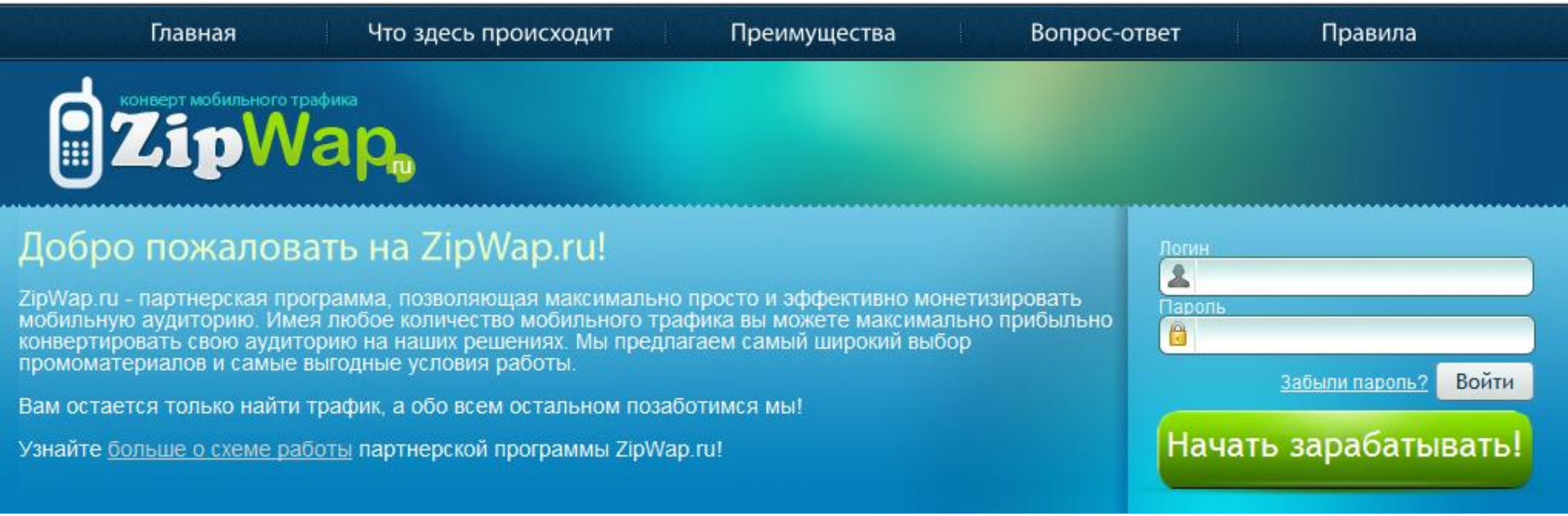
Android Market



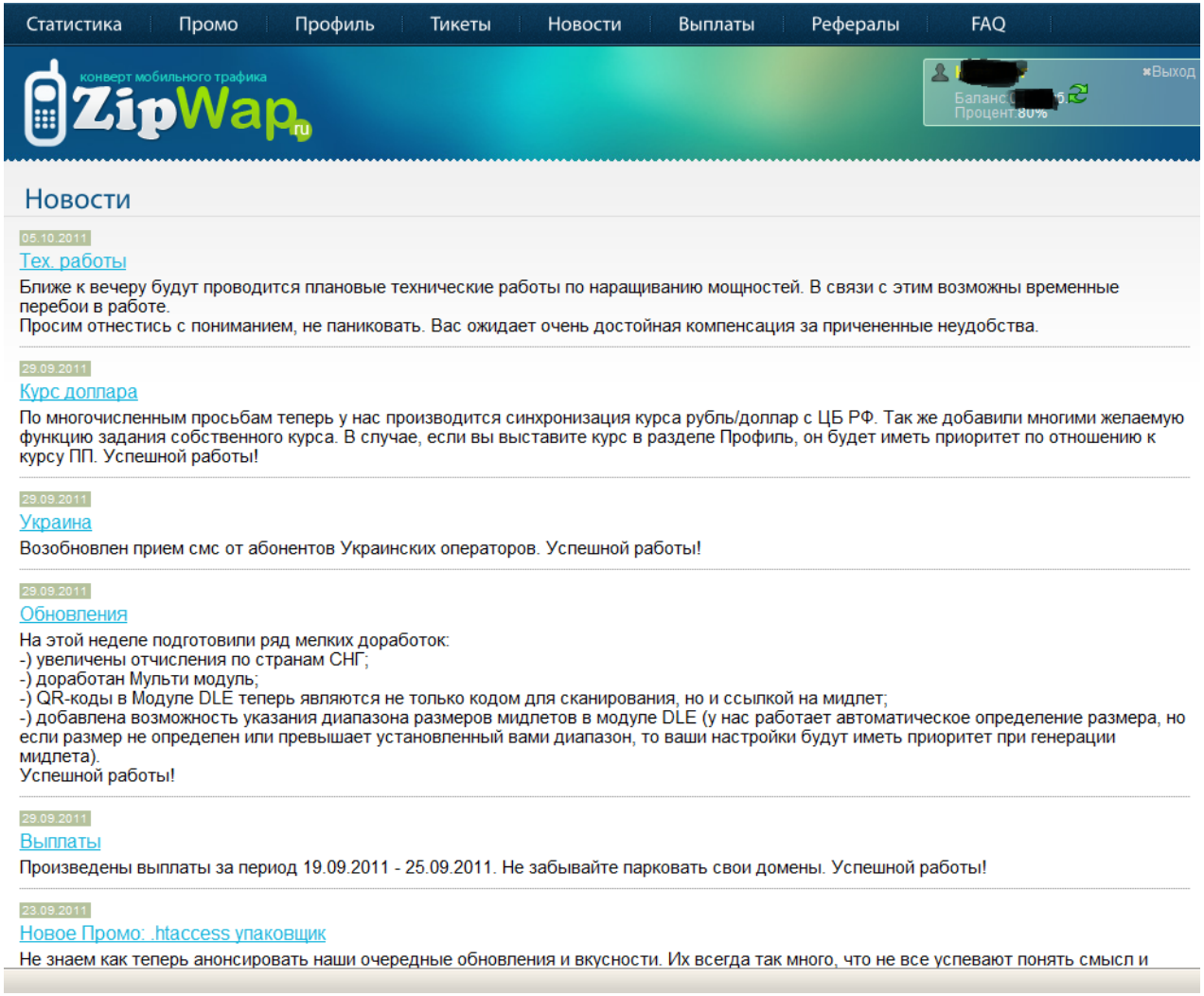
Alternative Chinese app markets

Evolution of affiliate networks

Current state



News feed


Статистика
Промо
Профиль
Тикеты
Новости
Выплаты
Рефералы
FAQ
конверт мобильного трафика
ZipWap.ru
Выход
Процент:80%
Новости
05.10.2011
Тех. работы
Ближе к вечеру будут проводится плановые технические работы по наращиванию мощностей. В связи с этим возможны временные перебои в работе.
Просим отнестись с пониманием, не паниковать. Вас ожидает очень достойная компенсация за причененные неудобства.
29.09.2011
Курс доллара
По многочисленным просьбам теперь у нас производится синхронизация курса рубль/доллар с ЦБ РФ. Так же добавили многими желаемую функцию задания собственного курса. В случае, если вы выставите курс в разделе Профиль, он будет иметь приоритет по отношению к курсу ПП. Успешной работы!
29.09.2011
Украина
Возобновлен прием смс от абонентов Украинских операторов. Успешной работы!
29.09.2011
Обновления
На этой неделе подготовили ряд мелких доработок:
-) увеличены отчисления по странам СНГ;
-) доработан Мульти модуль;
-) QR-коды в Модуле DLE теперь являются не только кодом для сканирования, но и ссылкой на мидлет;
-) добавлена возможность указания диапазона размеров мидлетов в модуле DLE (у нас работает автоматическое определение размера, но если размер не определен или превышает установленный вами диапазон, то ваши настройки будут иметь приоритет при генерации мидлета).
Успешной работы!
29.09.2011
Выплаты
Произведены выплаты за период 19.09.2011 - 25.09.2011. Не забывайте парковать свои домены. Успешной работы!
23.09.2011
Новое Промо: .htaccess упаковщик
Не знаем как теперь анонсировать наши очередные обновления и вкусности. Их всегда так много, что не все успевают понять смысл и

Malware generator

- **Number** and **cost** of **SMS**
  - From **$1** to **$10+$5+$5**
- **Type**
- **Name**
- **Icon**
- **Size** (20 – 3000 kB)

CMS for websites

- **Own CMS**
  - **Based** on **legitimate ‘DataLife Engine’**

CMS for websites

- **Own CMS**
  - **Based** on **legitimate ‘DataLife Engine’**
- **QR module** was added on **August 25**

25.08.2011

Обновление модуля DLE: QR-коды

Традиционно спешим обрадовать партнеров свеженьким функционалом. Обновлен модуль DLE. Новая фишка - QR-коды, которые сейчас приобретают все большую популярность за счет простоты передачи данных и простоты взаимодействия с пользователем, а так же благодаря продвижению данной технологии со стороны разработчиков Android.
Данная надстройка позволяет выводить под обычными ссылками на контент изображения QR-кодов. Пользователь, наведя камеру своего телефона на изображение получает ссылку на мидлет. Тем самым частично решается проблема с AB и увеличивается конверсия, потому что юзеру не нужно сначало скачивать мидлет на компьютер, а затем переносить на свой аппарат, он будет скачиваться прямо с телефона.
Для работы QR-кодов необходимо обновить модуль DLE, а так же выполнить новый шаг (8) из инструкции по настройке модуля.
Успешной работы!

- **Based** on **Google Chart Tools**

Google Chart Tools: Infographics

You can create a QR code on the fly with a URL GET request.

```
config['show_qr_code']) {
$width = $zw_config['qr_code_width'];
$height = $zw_config['qr_code_height'];
$qr_code .= "<div><br />QR-ъюф фы  {$row['name']}:<br /><a href=\"/zw/r.php?s={$url}\"><img src=\"http://chart.apis.google.com/chart?cht=qr&ch
```

Malicious QR code

Просто введите во встроенный браузер своего телефона ссылку:

http://[redacted].ru/jimm.apk

$$$

Дата	Скачивания	Смс	Ратио смс	руб/1К	Реф.	Сумма
22.07.2011	4350	245	1:17	3203.11 р.	0.00 р.	13933.55 р.
23.07.2011	4385	243	1:18	3180.05 р.	0.00 р.	13944.50 р.
24.07.2011	4634	221	1:20	2910.50 р.	0.00 р.	13487.25 р.
25.07.2011	4982	406	1:12	3400.21 р.	0.00 р.	16939.85 р.
26.07.2011	2568	212	1:12	3385.48 р.	0.00 р.	8693.92 р.
Итого	20919	1327	1:15	3202.79 р.	0 р.	66999.07 р.

Дата	Скачивания	Смс	Ратио смс	руб/1К	Реф.	Сумма
22.07.2011	16234	835	1:19	2922.09 р.	0.00 р.	47437.23 р.
23.07.2011	11982	627	1:19	2746.36 р.	0.00 р.	32906.93 р.
24.07.2011	10378	572	1:18	2969.34 р.	0.00 р.	30815.86 р.
25.07.2011	18017	998	1:18	2570.04 р.	0.00 р.	46304.34 р.
26.07.2011	7370	329	1:22	2175.71 р.	0.00 р.	16035.01 р.
Итого	63981	3361	1:19	2711.73 р.	0.00 р.	173499.37 р.

$$$

Дата	Скачивания	Смс	Ратио смс	руб/1K	Реф.	Сумма
22.07.2011	4350				0.00 р.	13933.55 р.
23.07.2011	4385				0.00 р.	13944.50 р.
24.07.2011	4634				0.00 р.	13487.25 р.
25.07.2011	4982				0.00 р.	16939.85 р.
26.07.2011	2568				0.00 р.	8693.92 р.
Итого	20919	1327	1:15	3202.79 р.	0 р.	66999.07 р.

~$2200/5 days

Дата	Скачивания	Смс	Ратио смс	руб/1K	Реф.	Сумма
22.07.2011	16234				0.00 р.	47437.23 р.
23.07.2011	11982				0.00 р.	32906.93 р.
24.07.2011	10378				0.00 р.	30815.86 р.
25.07.2011	18017				0.00 р.	46304.34 р.
26.07.2011	7370				0.00 р.	16035.01 р.
Итого	63981	3361	1:19	2711.73 р.	0.00 р.	173499.37 р.

~$5800/5 days

Conclusions

Conclusions

- **In terms** of **numbers**
  - **Android** has already **beaten Symbian**
  - **Android will beat J2ME very soon…**
    - …at least **till the end of 2011**
- **In terms of complexity**
  - **More complicated examples**
  - **More simple examples**
- **Number** of **malware sources** can be **reduced**

Conclusions

- **In terms** of **numbers**
  - **Android** has already **beaten Symbian**
  - **Android will beat J2ME very soon…**
    - …at least **till the end of 2011**
- **In terms of complexity**
  - **More complicated examples**
  - **More simple examples**
- **Number** of **malware sources** can be **reduced**
- **It's time for…**

Thank You

Android Malware is on the Rise

Timothy Armstrong, Researcher, Kaspersky Lab
Timothy.Armstrong@kaspersky.com
Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab
Denis.Maslennikov@kaspersky.com, @hEx63
07.10.2011, Virus Bulletin Conference, Barcelona, Spain

KASPERSKY lab