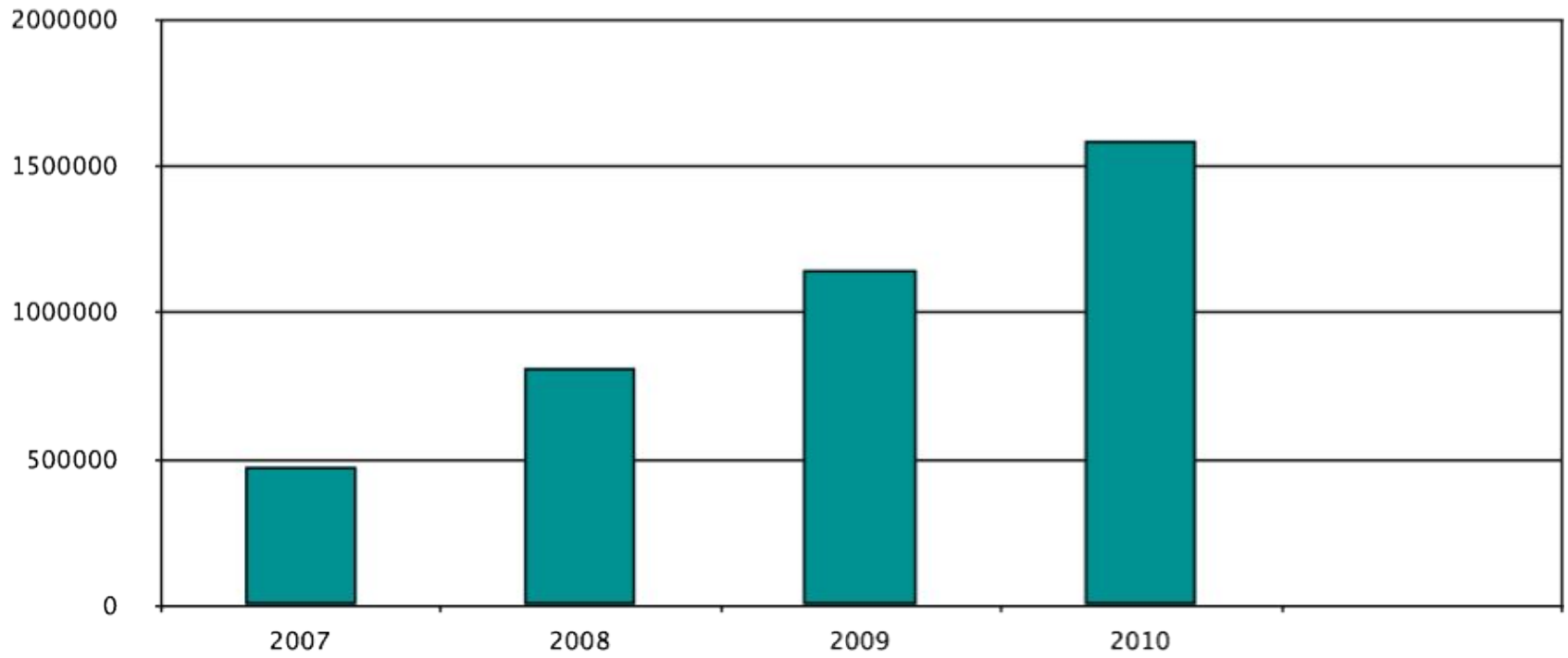
Dr.WEB®
www.drweb.com

Defend what you create

Современные методы обработки и алгоритмы детектирования вредоносного программного обеспечения. Краткий обзор угроз для мобильной платформы Android

Dr.WEB®
www.drweb.com

Количество добавленных угроз в вирусные базы

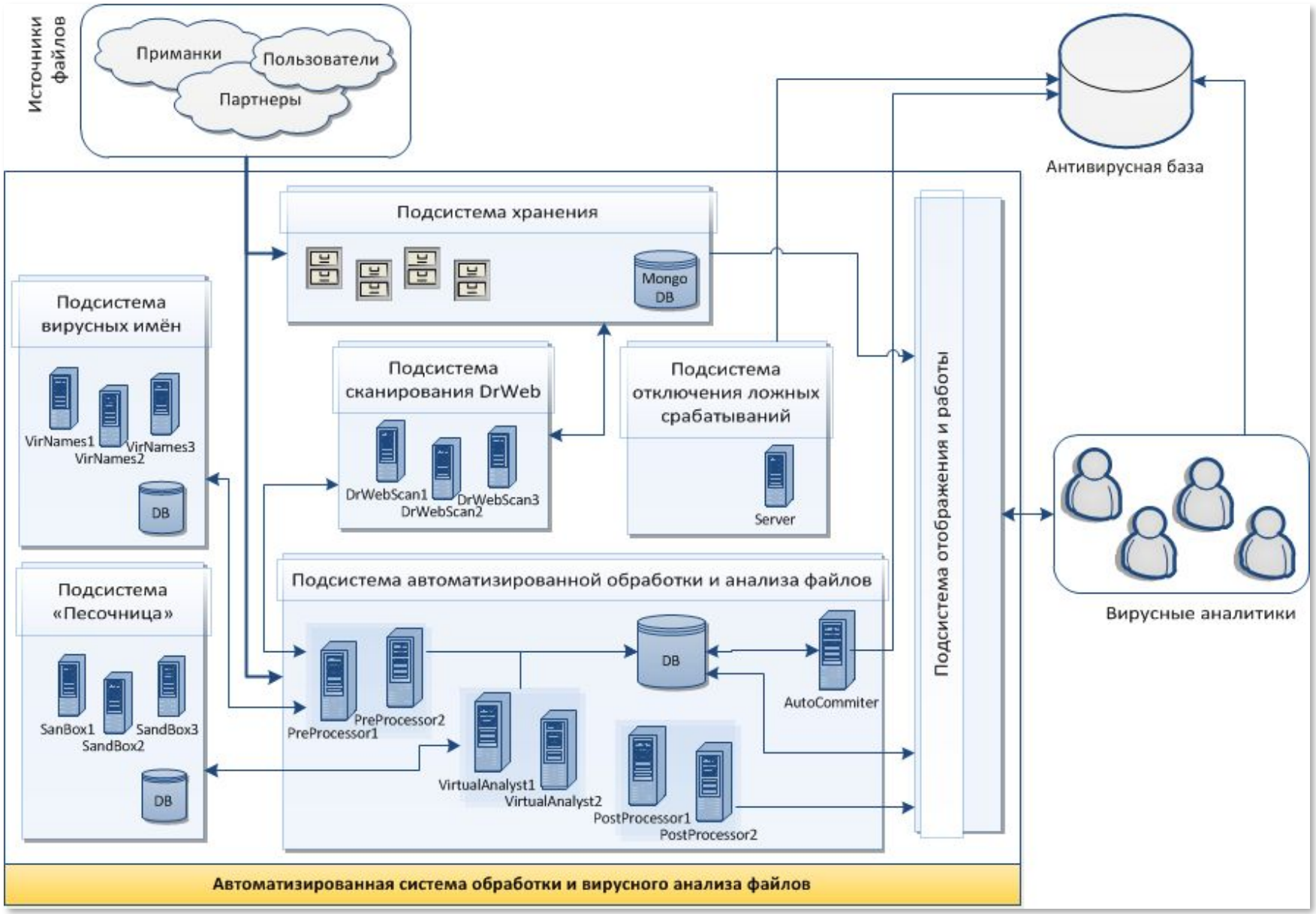


Dr.WEB®
www.drweb.com

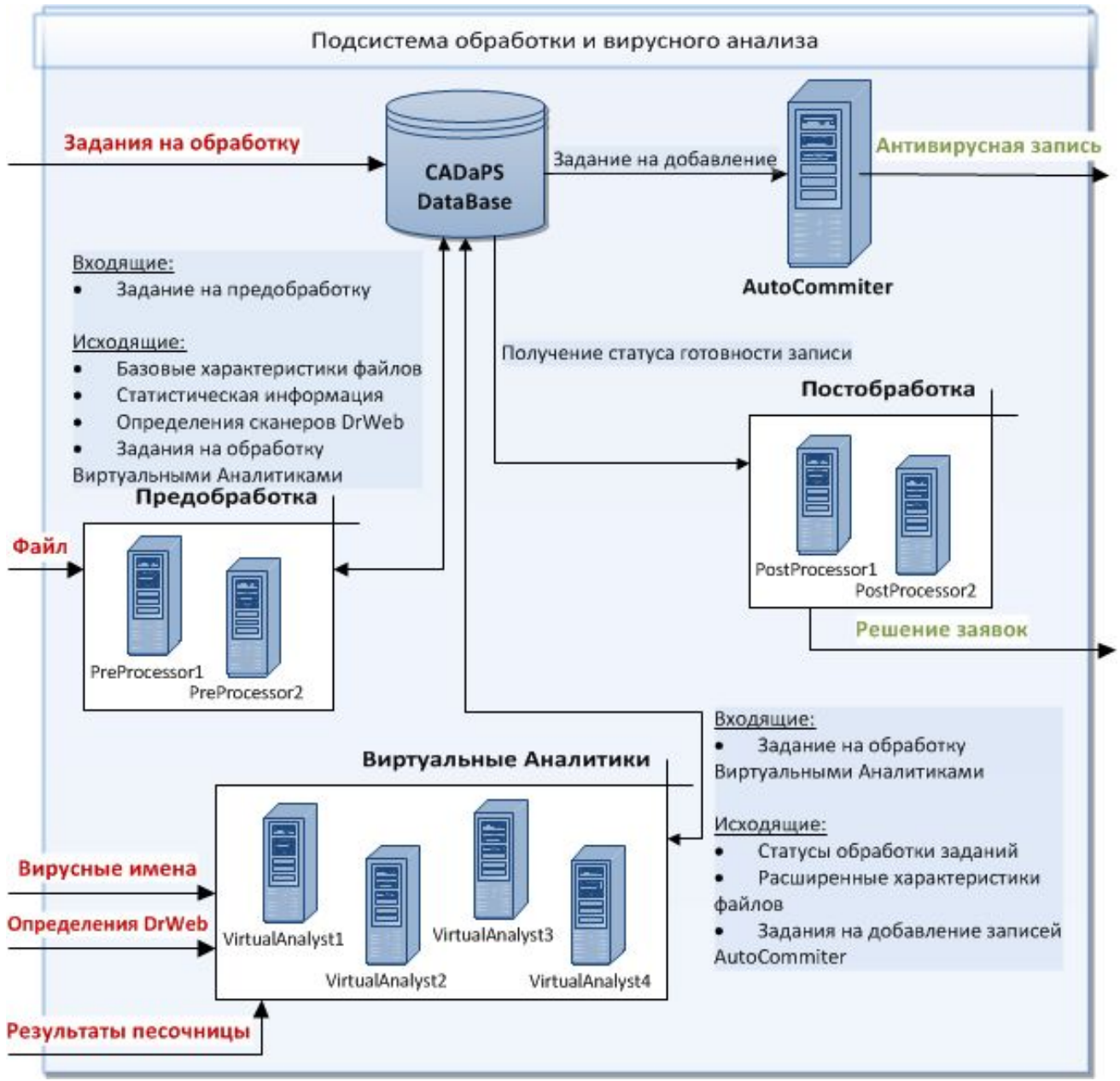
Источники вирусов

- Система регистрации вирусных заявок
  - Пользователи
  - Партнеры лицензирующие модуль поиска вирусов
- Система мониторинга вредоносных ссылок
- Система honeypot’ов
- Системы мульти-сканеров (virustotal, jotti, virscan..)
- Ежедневный обмен среди антивирусных вендоров)

Dr.WEB®
www.drweb.com



Dr.WEB®
www.drweb.com



Dr.WEB®
www.drweb.com

Алгоритмы детектирования вредоносных программ

- Оценка похожести файлов на основе вейвлет анализа
- Оценка похожести файла на основе анализа графа передачи управления (Origin Tracing, Origin Tracing for Android)

Dr.WEB®
www.drweb.com

Оценка похожести файлов на основе вейвлет анализа

- Экспоненциальный рост количества файлов присылаемых в лабораторию. Более 60000 уникальных файлов в день.
- Сложные техники для предотвращения детектирования антивирусами (полиморфиз, обфускация)
  - BackDoor.Tdss.based (TDL3/4) ~2000 в месяц
  - Win32.HLLW.Autoruner (Win32/Rimecud,Palevo) ~3000 в месяц

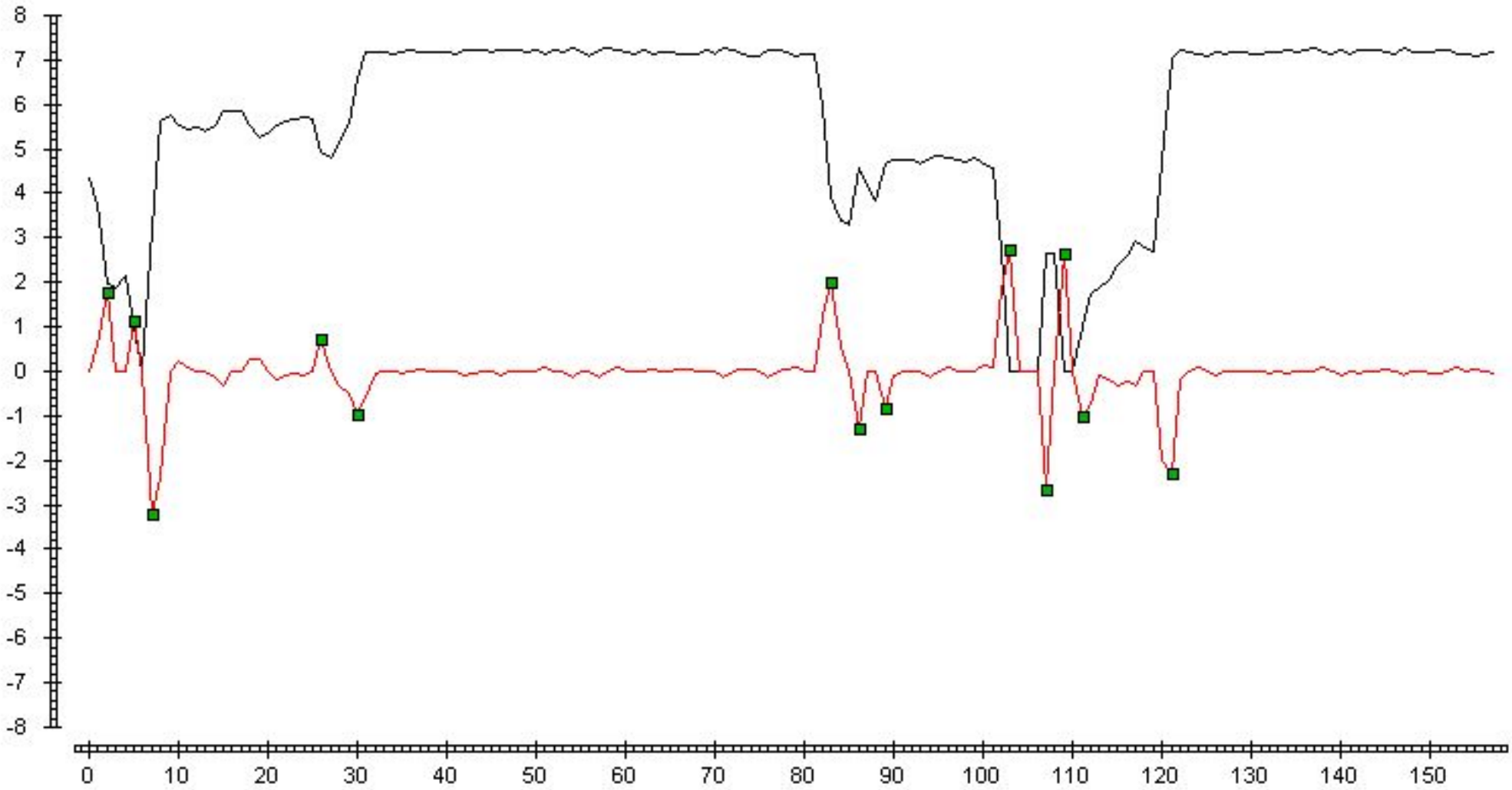
Подсчет энтропии методом скользящего окна

$$Y = \{ y_i : i = 1, \ldots, N \}$$

$$y_i = -\sum_{j=1}^{m} p(j) \log_2 p(j)$$

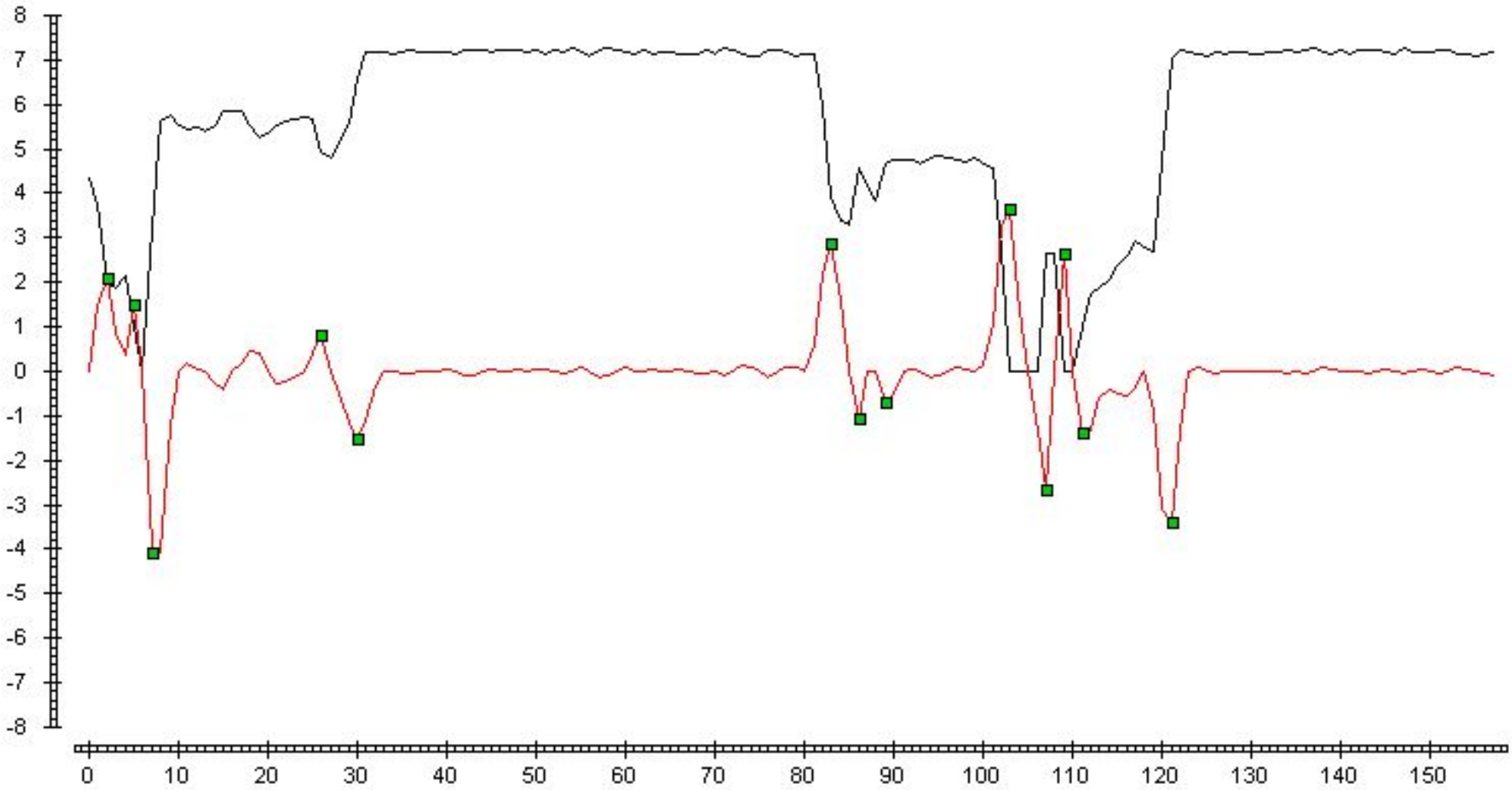
Dr.WEB®
www.drweb.com

Вейвлет анализ



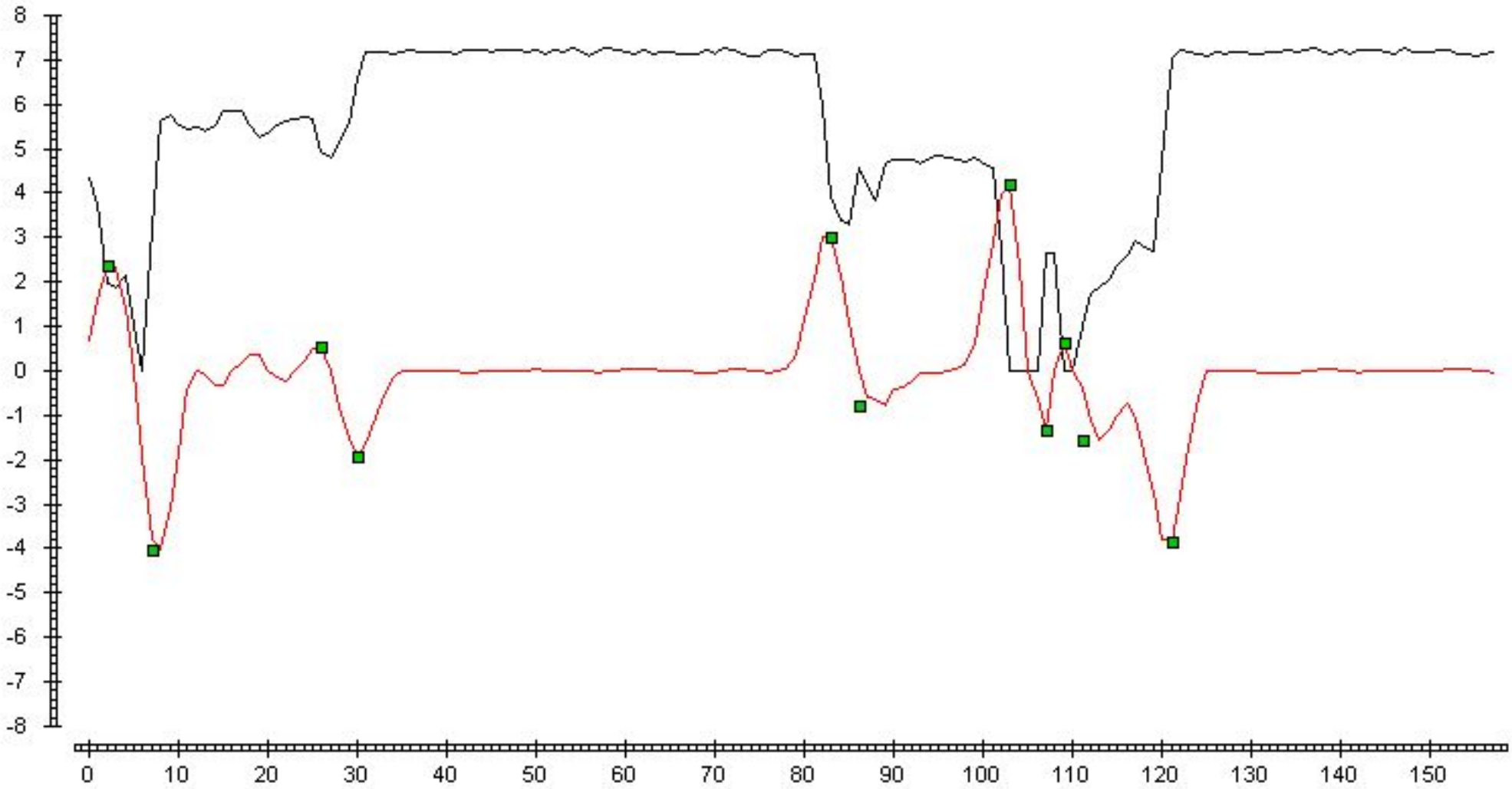
Dr.WEB®
www.drweb.com

Вейвлет анализ



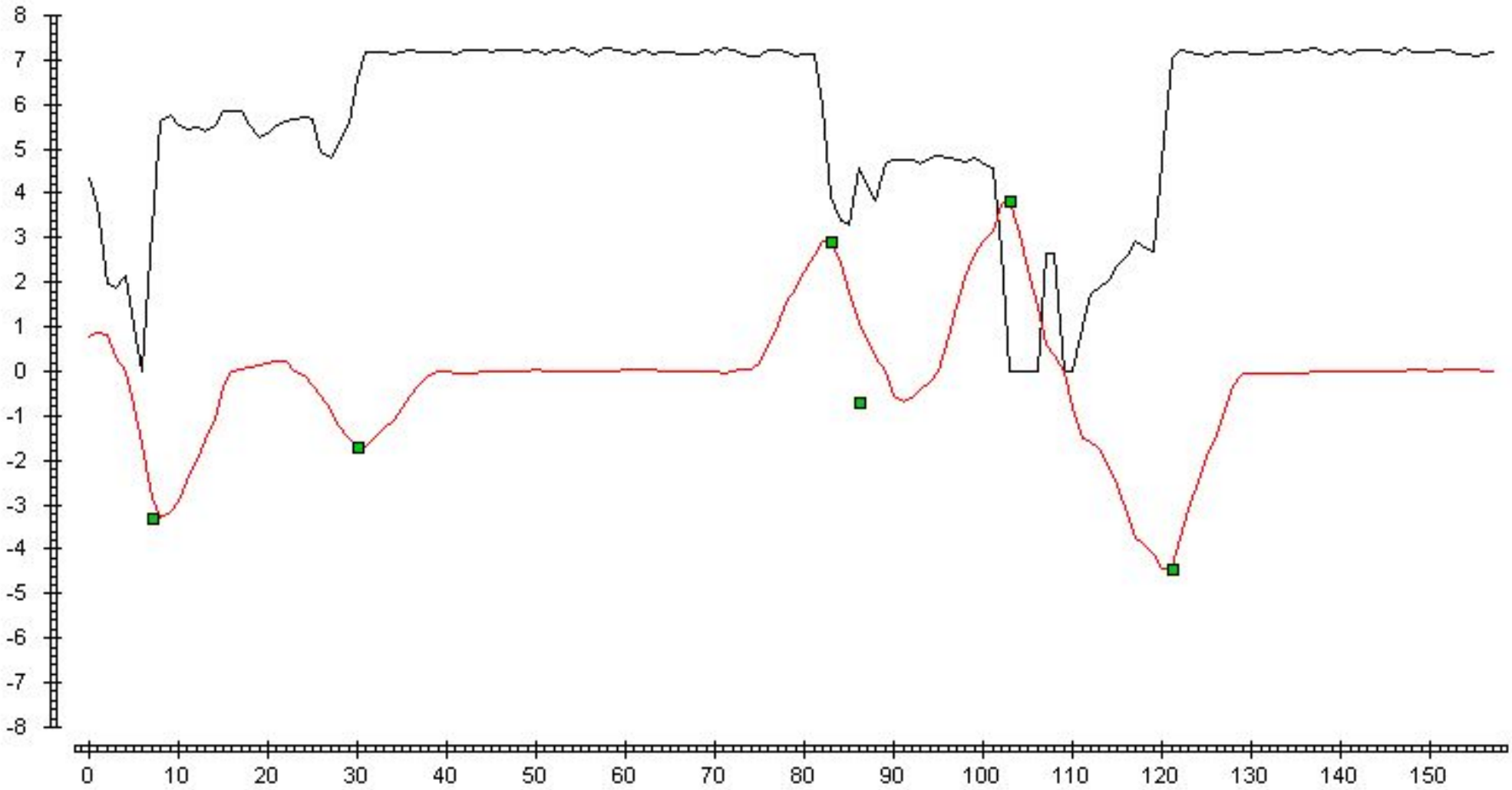
Dr.WEB®
www.drweb.com

Вейвлет анализ



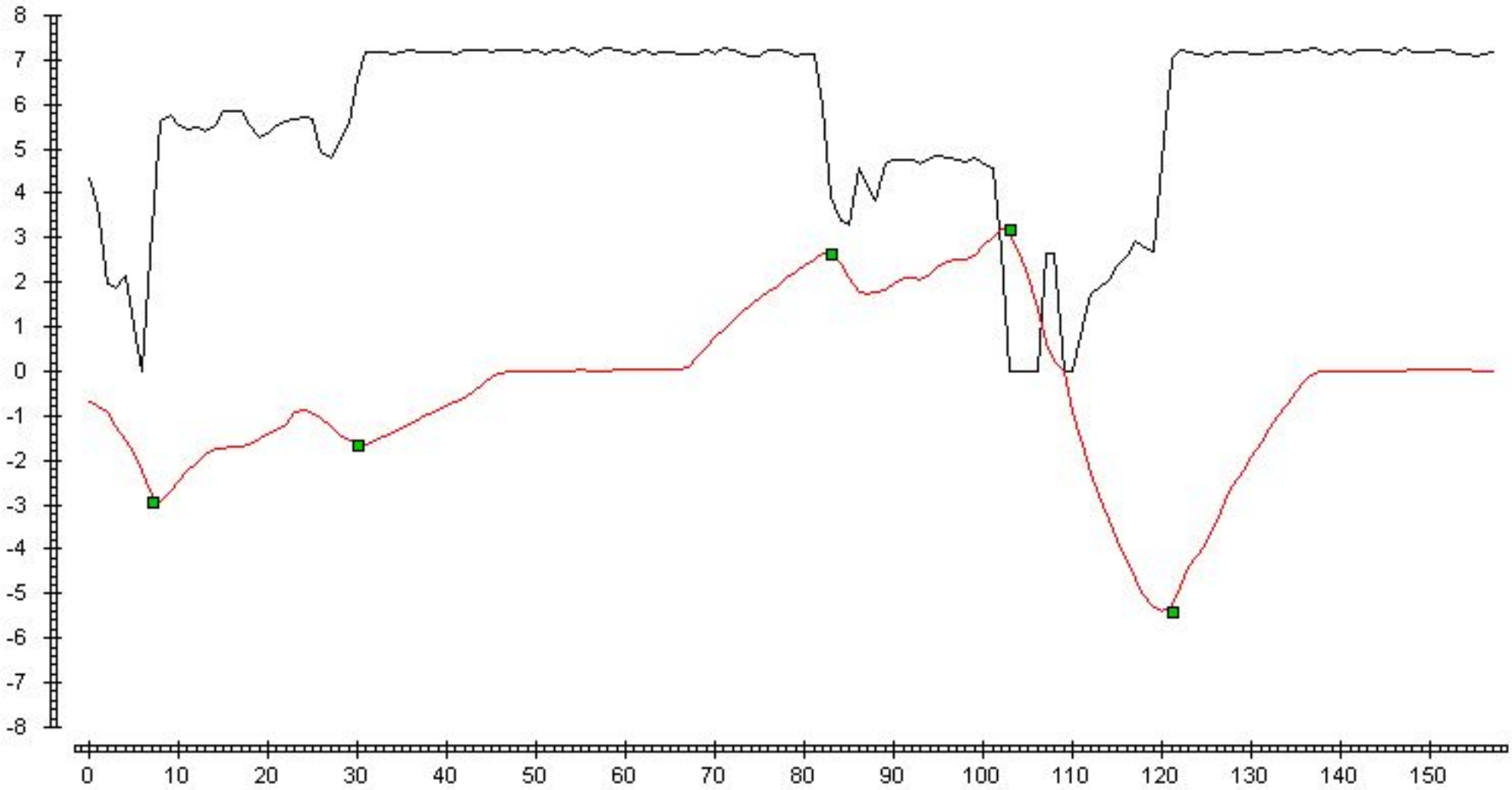
Dr.WEB®
www.drweb.com

Вейвлет анализ



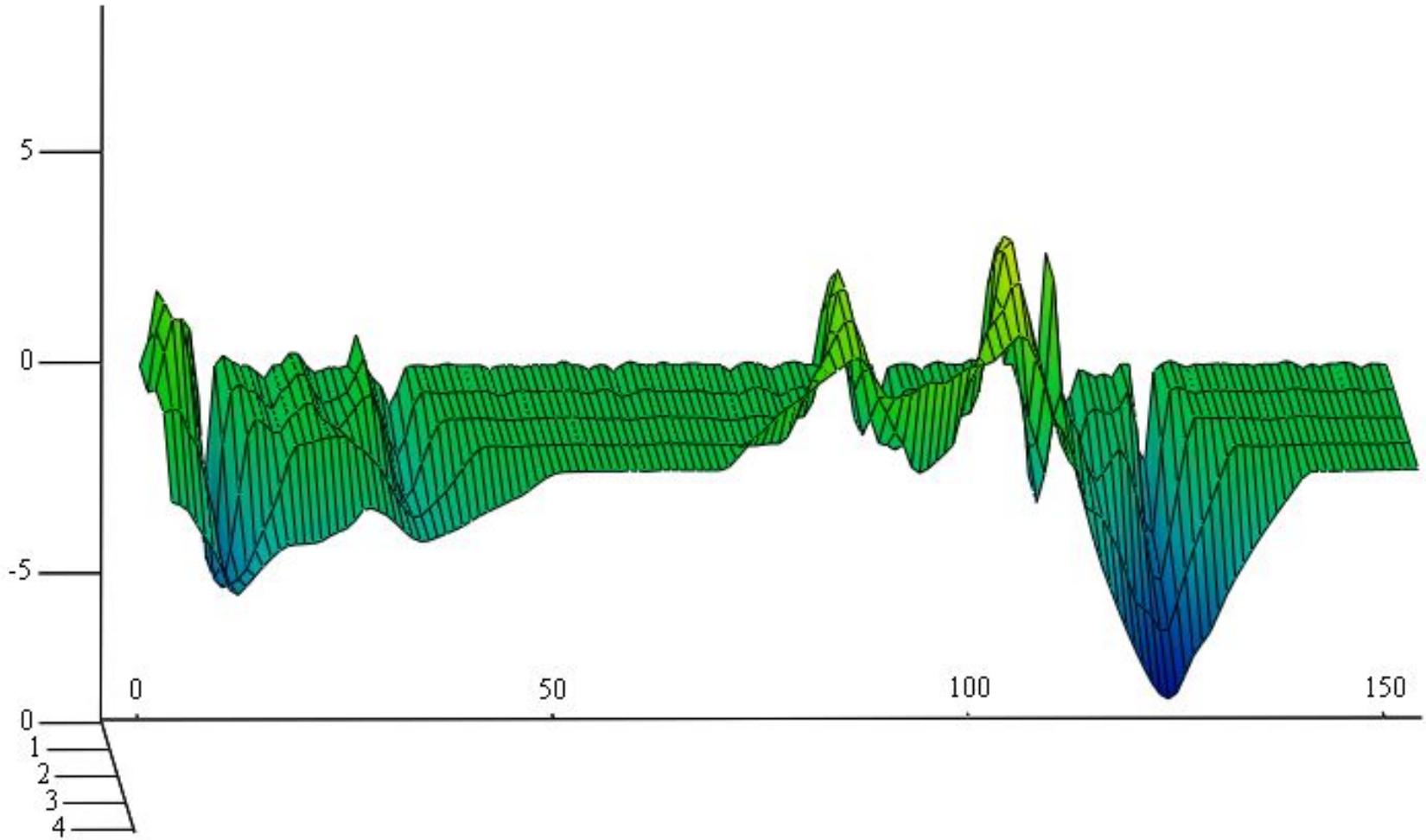
Dr.WEB®
www.drweb.com

Вейвлет анализ



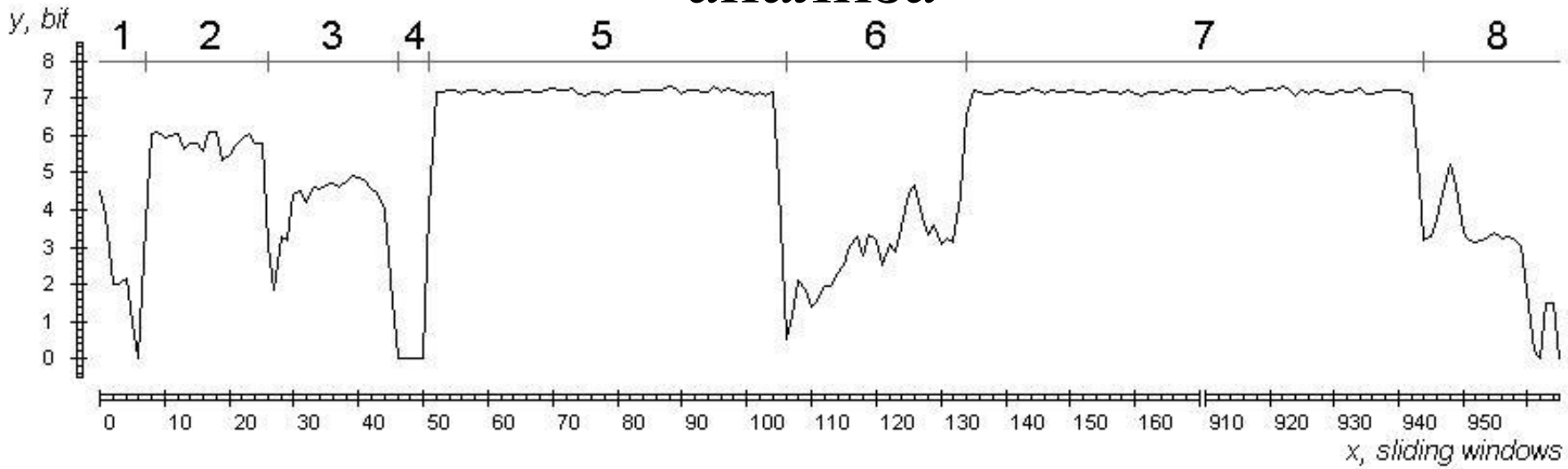
Dr.WEB®
www.drweb.com

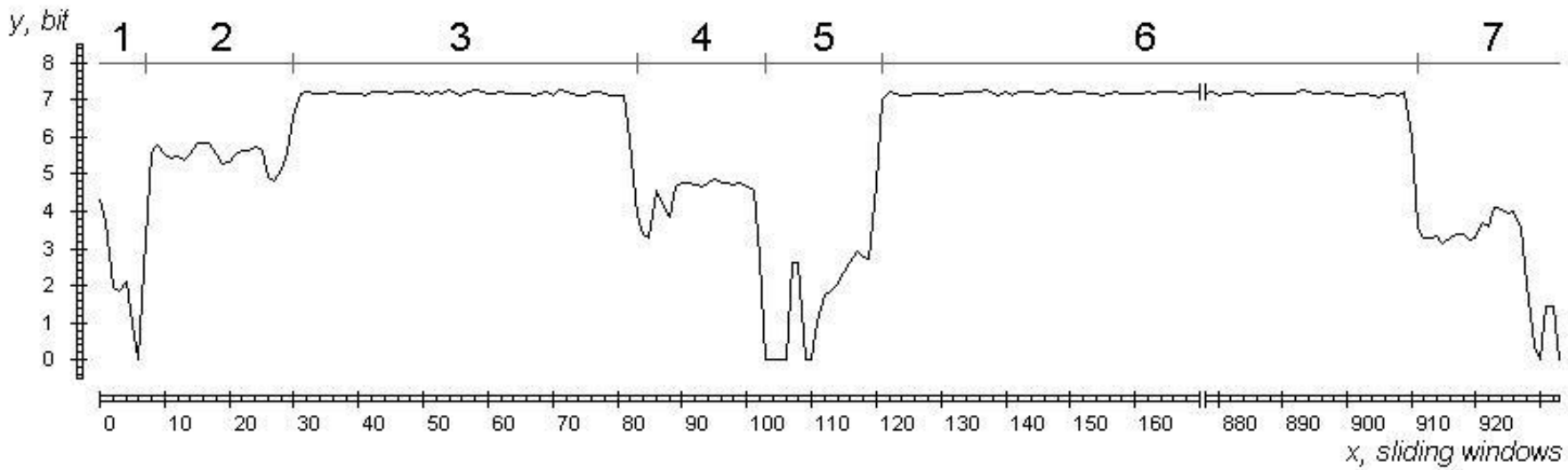
Оценка похожести файла на основе вейвлет анализа



Dr.WEB®
www.drweb.com

Оценка похожести файла на основе вейвлет анализа





Dr.WEB®
www.drweb.com

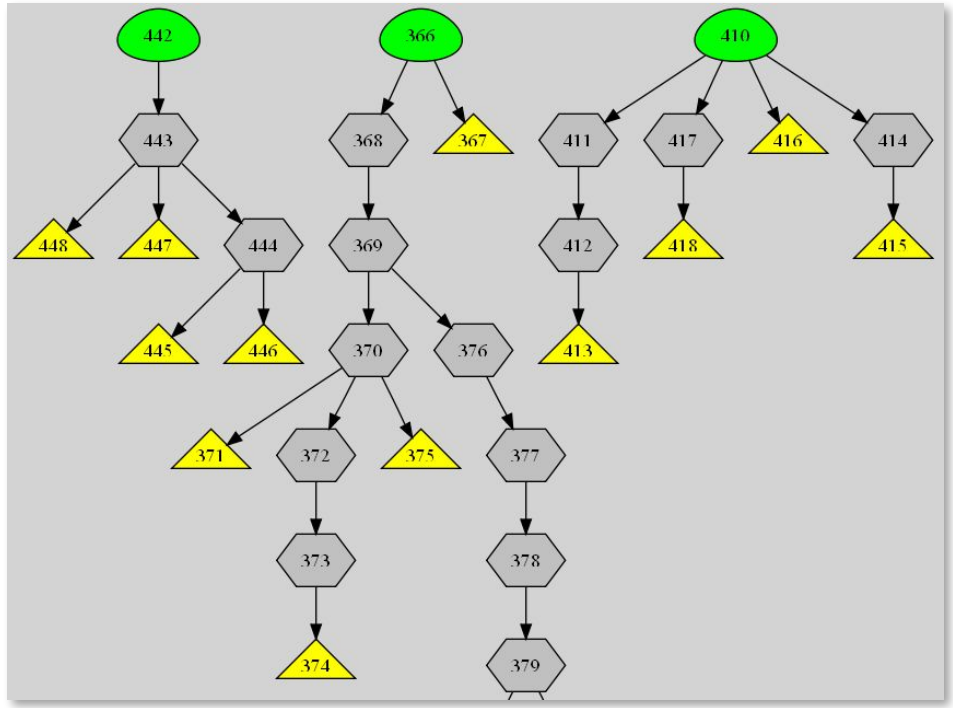
Оценка похожести файлов на основе вейвлет анализа

- Быстрый алгоритм не требующий больших вычислительных ресурсов (эмуляция файла, дизассемблирование)
- Компактная запись для вирусной базы

Dr.WEB®
www.drweb.com

Технология Origin Tracing

- Статический анализ кода
- Построение графа управления программы
- Выделение подозрительных вершин графа
- Составление записи детектирования вредоносного семейства

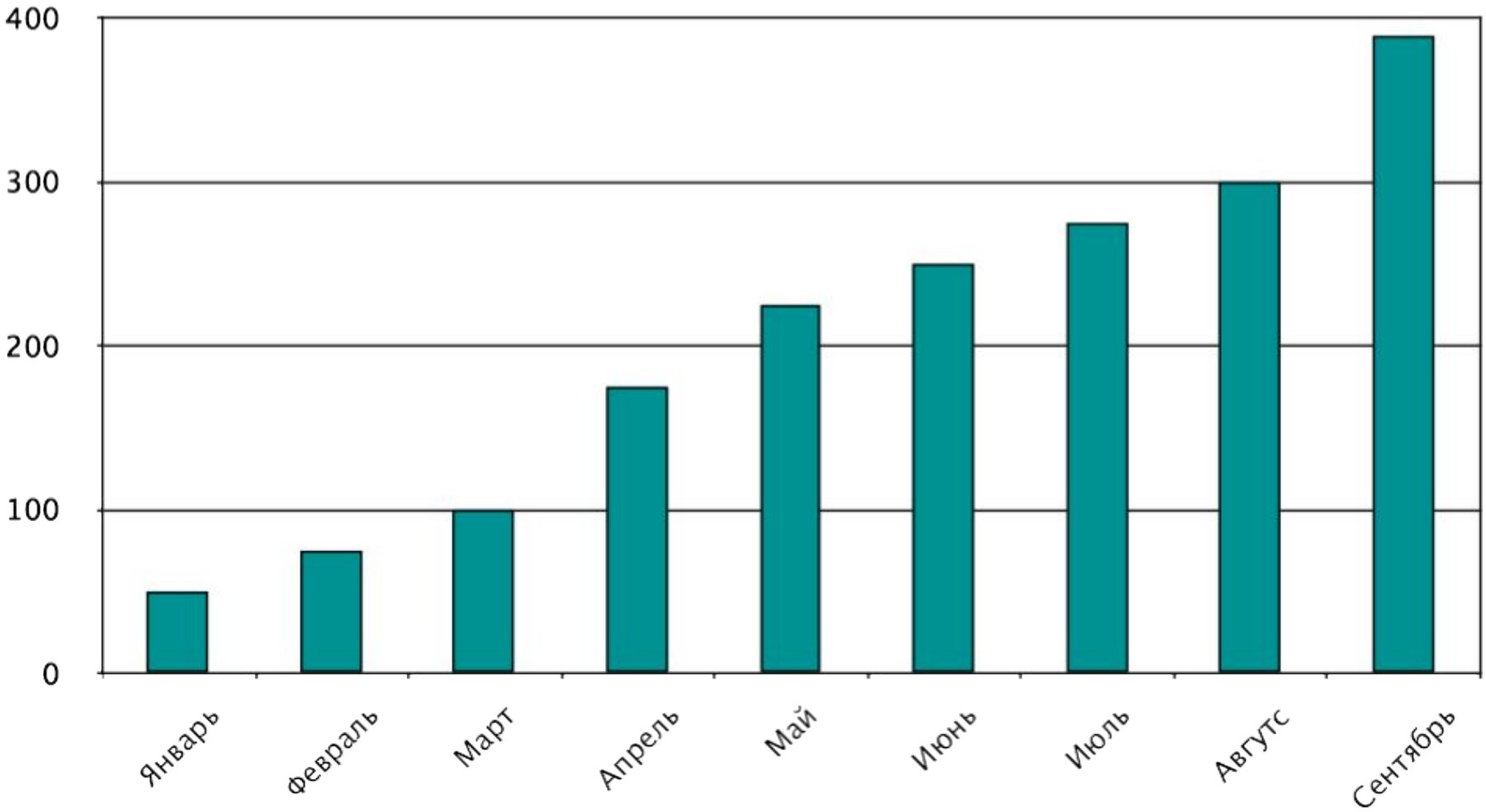


Dr.WEB®
www.drweb.com

Мобильные угрозы для Android OS

Dr.WEB®
www.drweb.com

Рост количества угроз



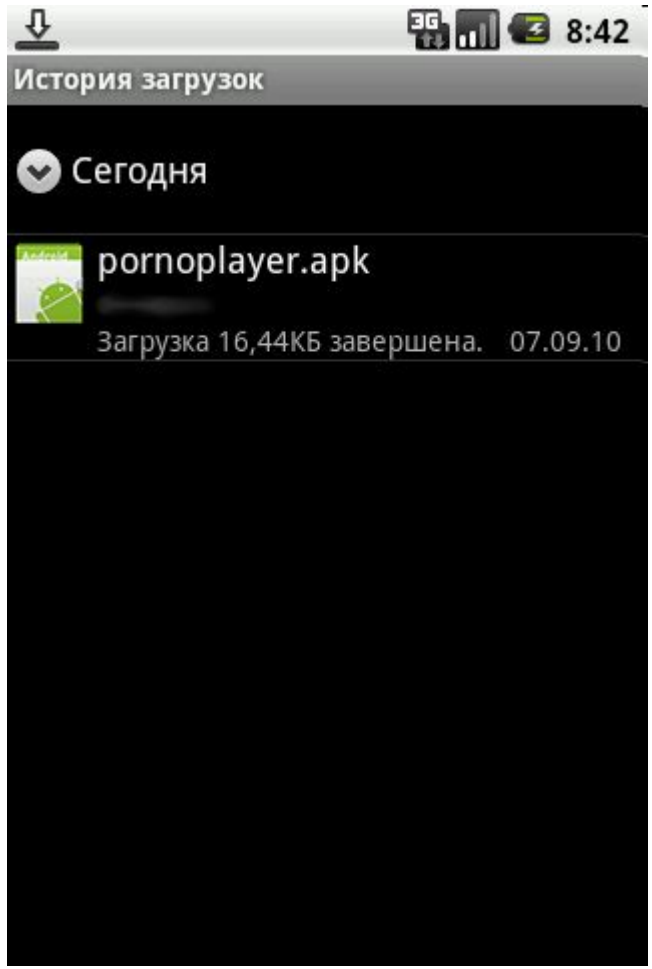
Dr.WEB®
www.drweb.com

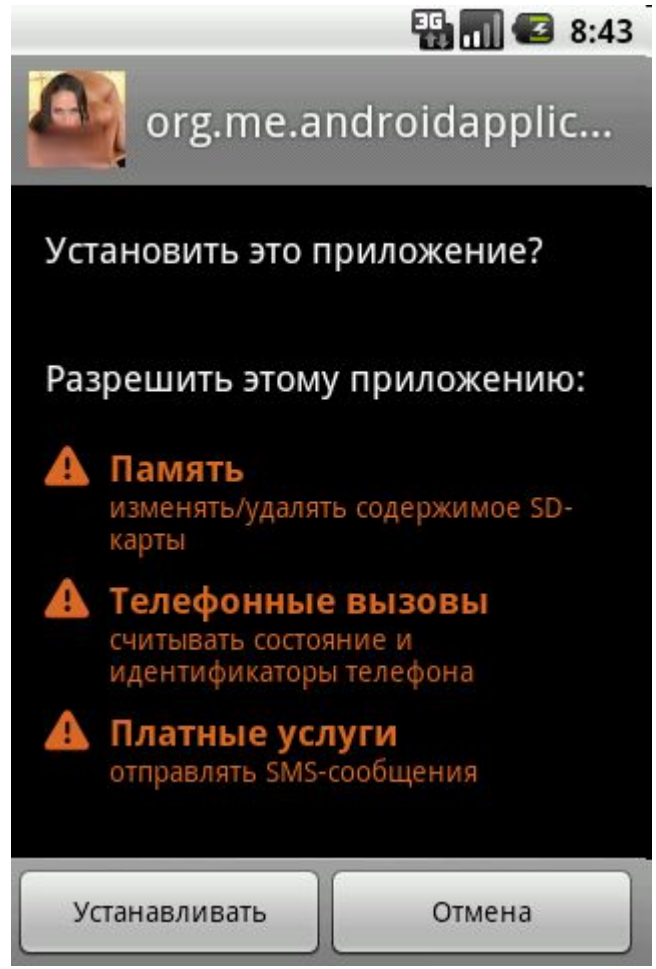
Типы угроз

- Вредоносные приложения не несущие полезной нагрузки
  - Android.SmsSend
  - Android.SpyEye.1
- Платные шпионские программы
  - Flexispy, Mobile Spy, Mobistealth
- Легитимные инфицированные приложения распространяющиеся на сторонних маркетах
  - Android.Plankton
  - Android.Gongfu (Android.DreamExploid)

Dr.WEB®
www.drweb.com

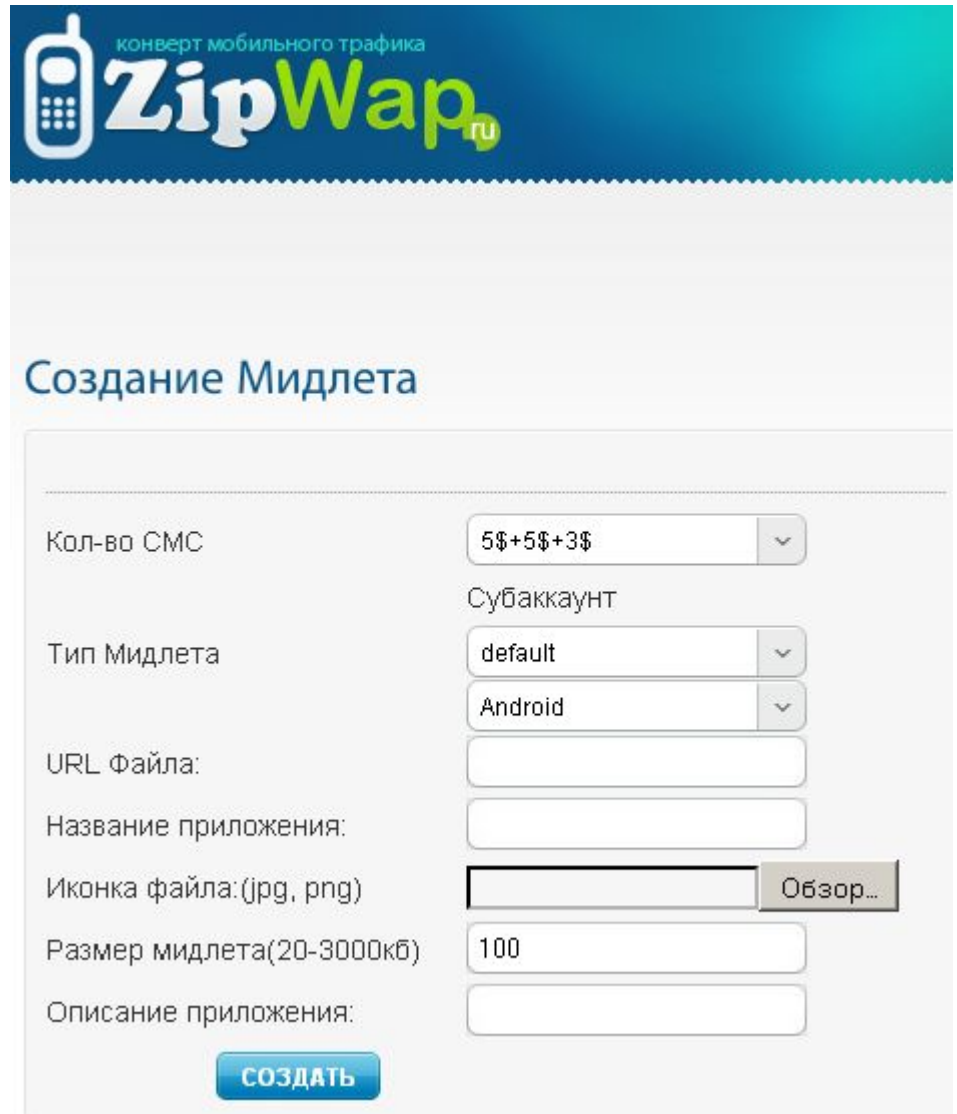
Android.SmsSend





Dr.WEB®
www.drweb.com

Пример схемы мошенничества



Dr.WEB®
www.drweb.com

Пример схемы мошенничества

Список мидлетов

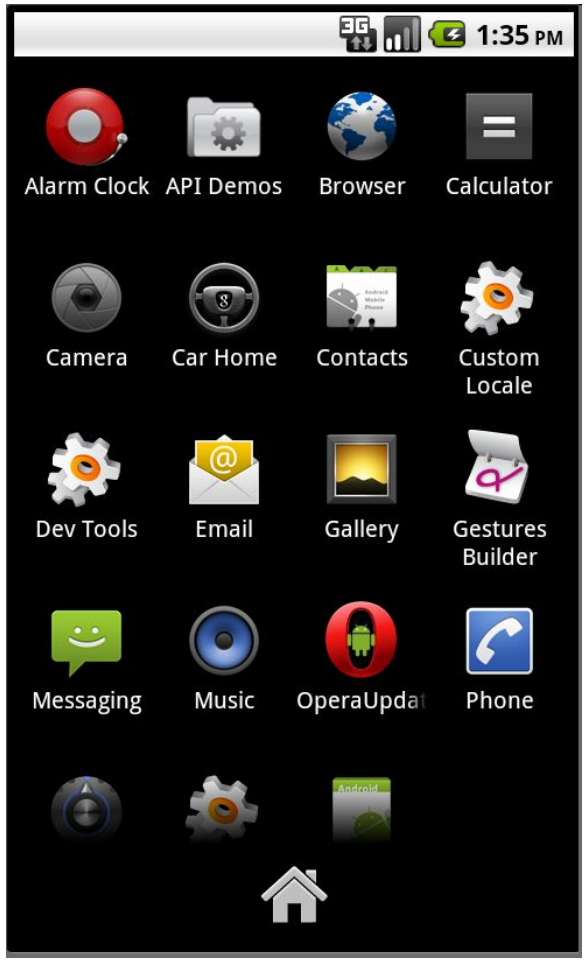
Тип	Схема Активации	Название	URL	Ссылка
	10$+5$+5$	drwebantivirus	http://company.drweb.com/ca...	http://newmobifile.ru/getfile.php?dtype=pp&r=834-2
	5$+5$+3$	20years	http://www.f-secure.com/web...	http://newmobifile.ru/getfile.php?dtype=pp&r=834-1

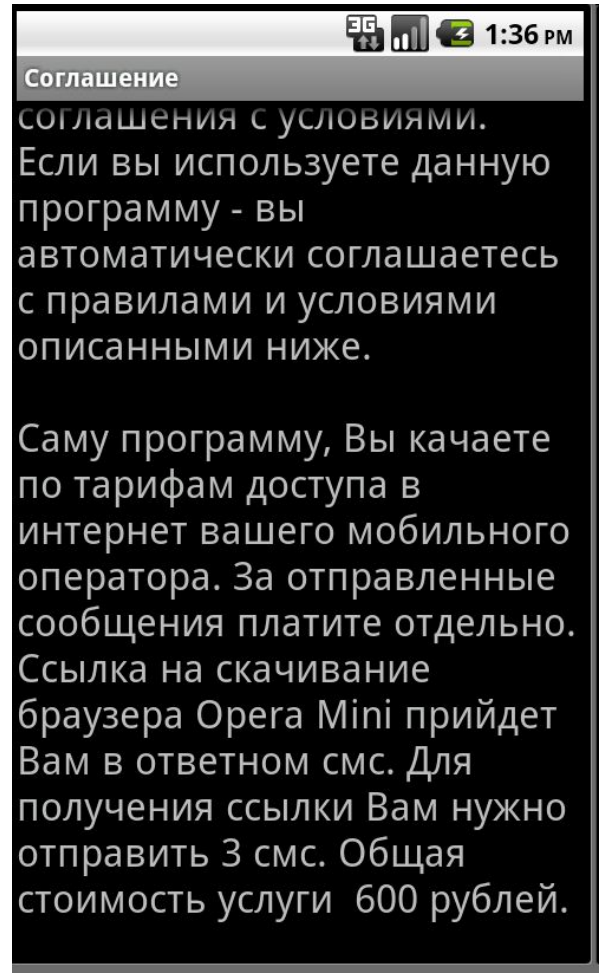
Dr.WEB®
www.drweb.com

Пример схемы мошенничества

Dr.WEB®
www.drweb.com

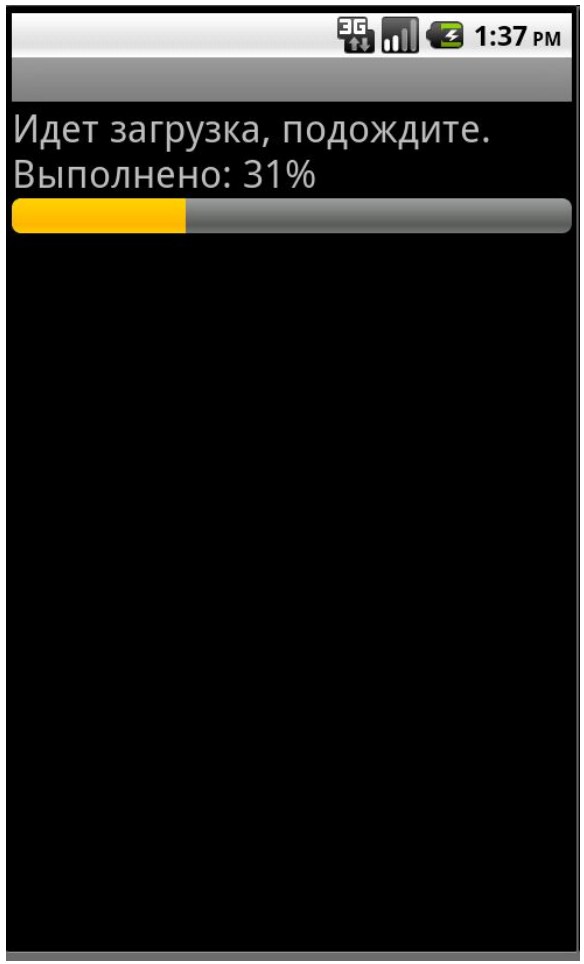
Пример схемы мошенничества

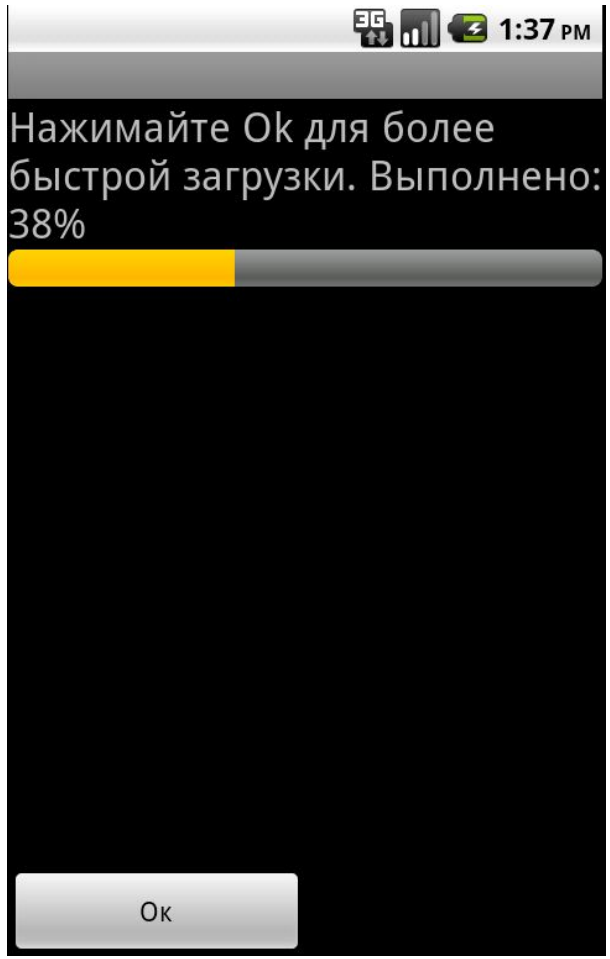


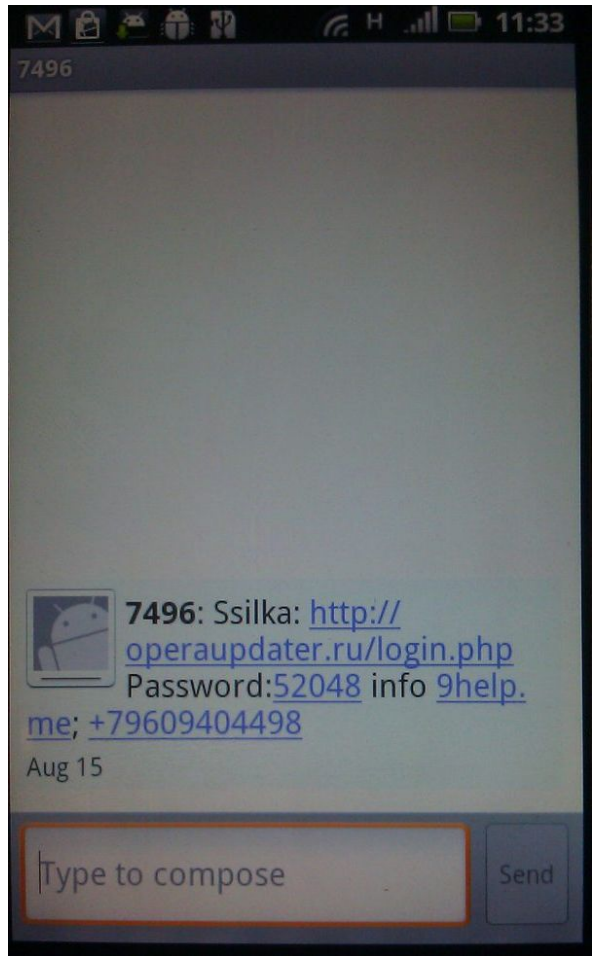


Dr.WEB®
www.drweb.com

Пример схемы мошенничества

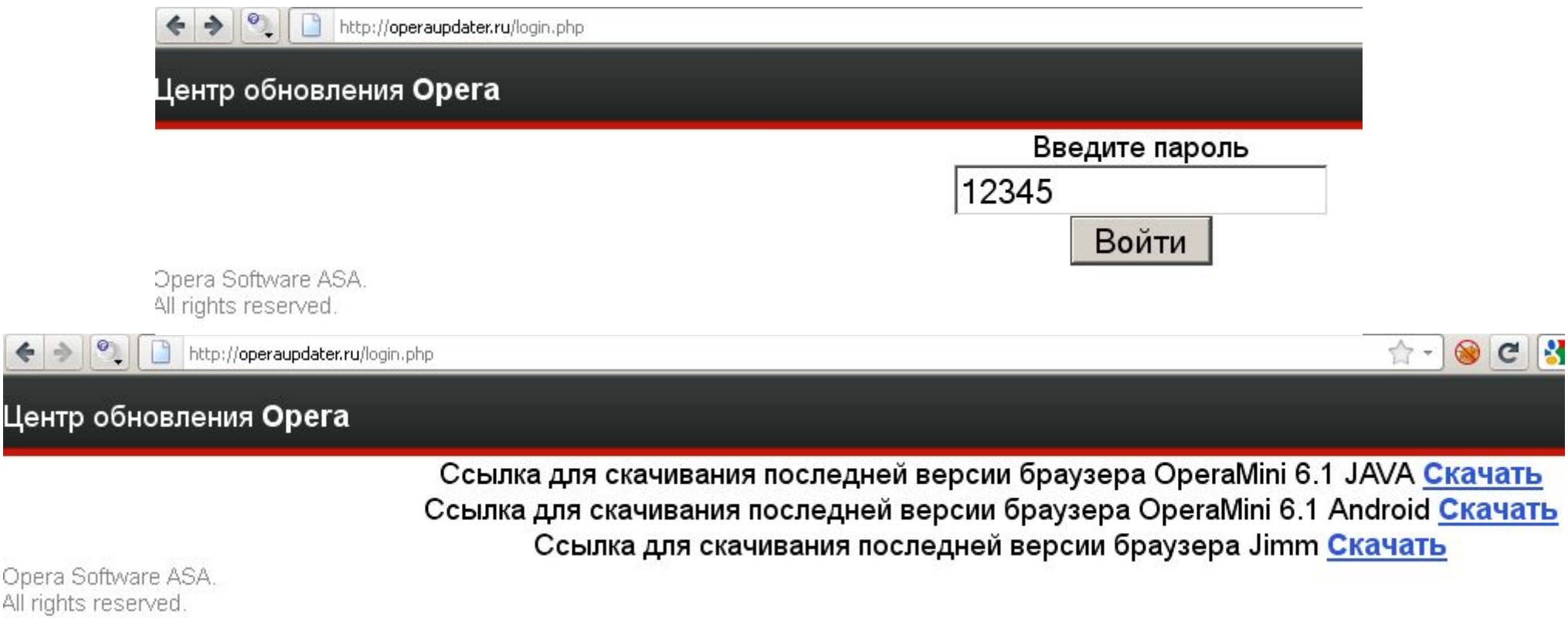






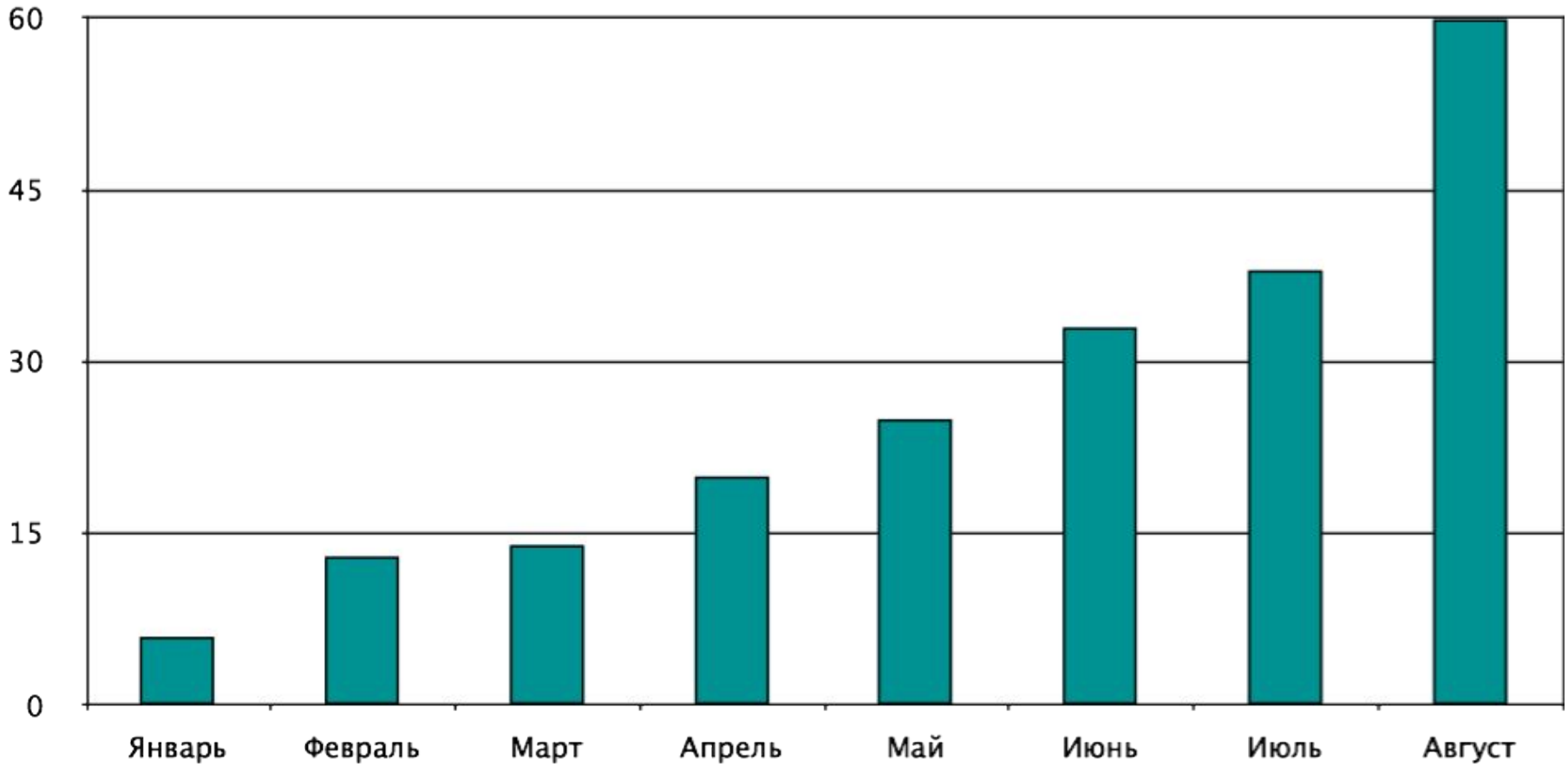
Dr.WEB®
www.drweb.com

Пример схемы мошенничества



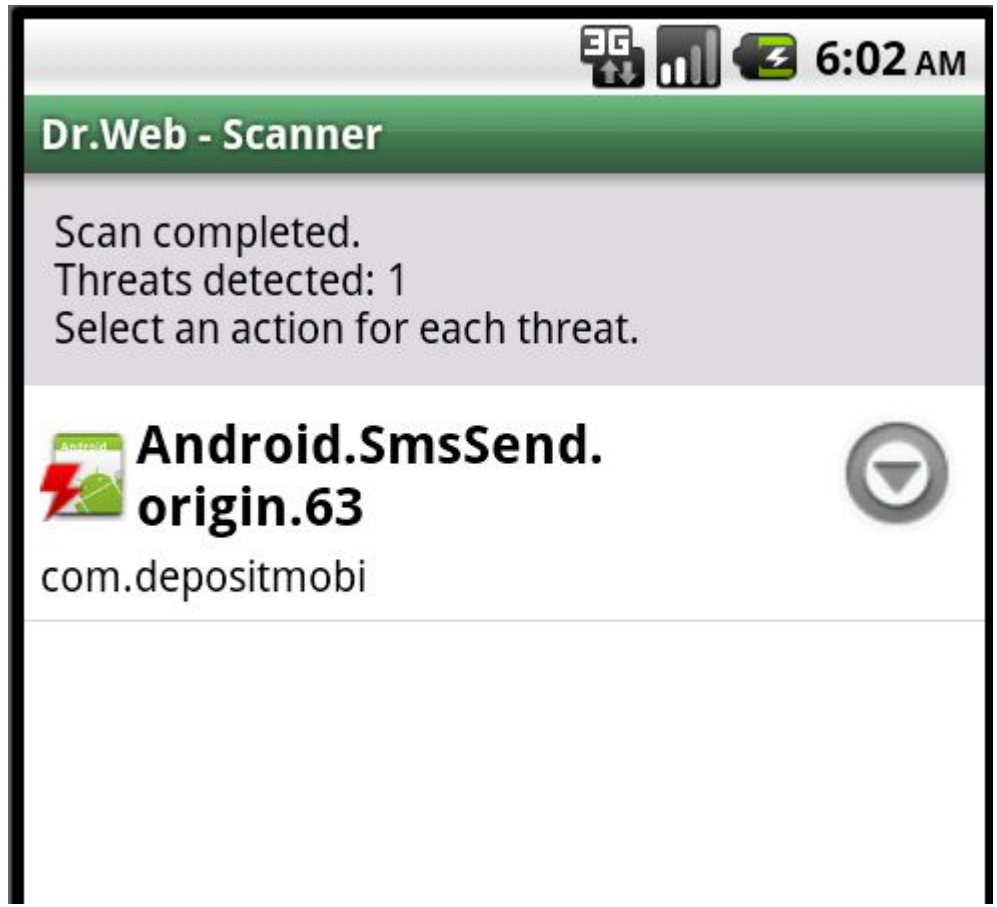
Dr.WEB®
www.drweb.com

Количество модификаций Android.SmsSend



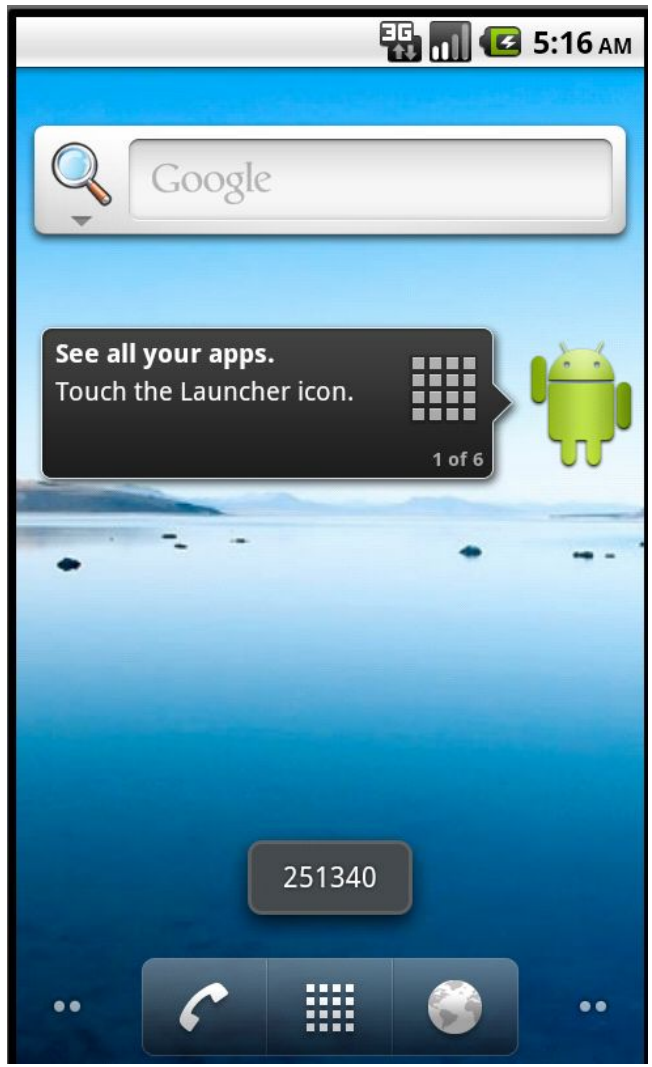
Dr.WEB®
www.drweb.com

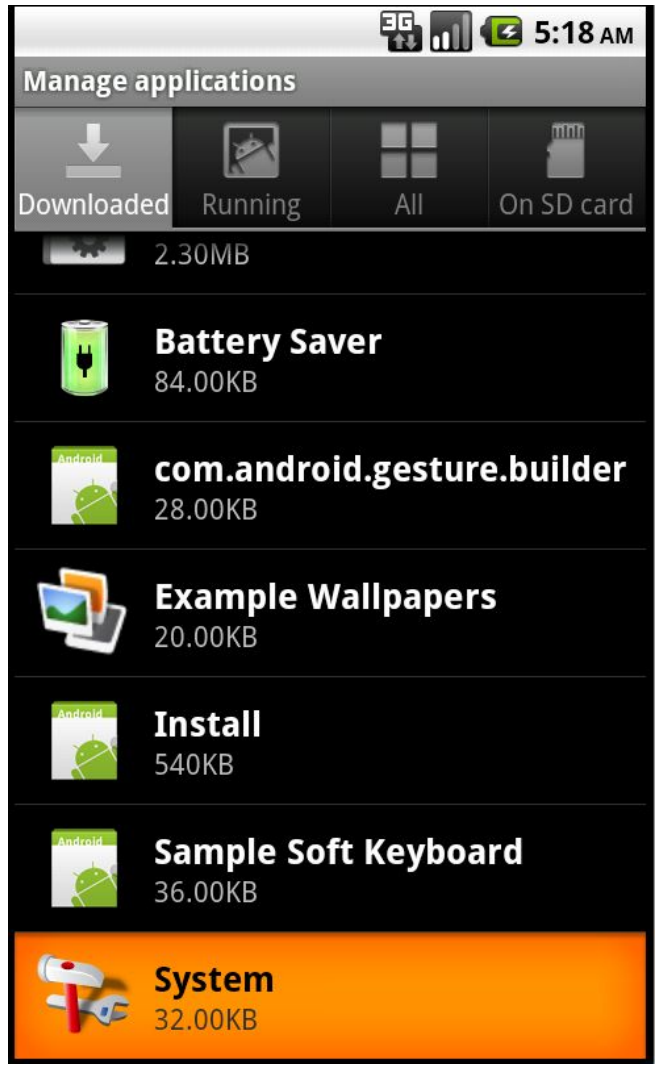
Детектирования новых угроз с помощью технологии Origin Tracing



Dr.WEB®
www.drweb.com

Android.SpyEye.1





Dr.WEB®
www.drweb.com

Android.SpyEye.1

```
<?xml version="1.0" encoding="UTF-8"?>
<settings>
<send value="1"/>
<telephone value="123"/>
<http>
<addr value="http://124ffsaf.com/sms/gate.php"/>
<addr value="http://124ff42.com/sms/gate.php"/>
<addr value="http://124ffdfsaf.com/sms/gate.php"/>
<addr value="http://124sfafsaffa.com/sms/gate.php"/>
</http>
<tels>
</tels>
</settings>
```

Dr.WEB®
www.drweb.com

Dr.WEB®
www.drweb.com

Home | Features | Phones | Buy Online | Stealth Club | Demo | Affiliates

MobiStealth.com

keep an eye on cheat...
monitor your kids...

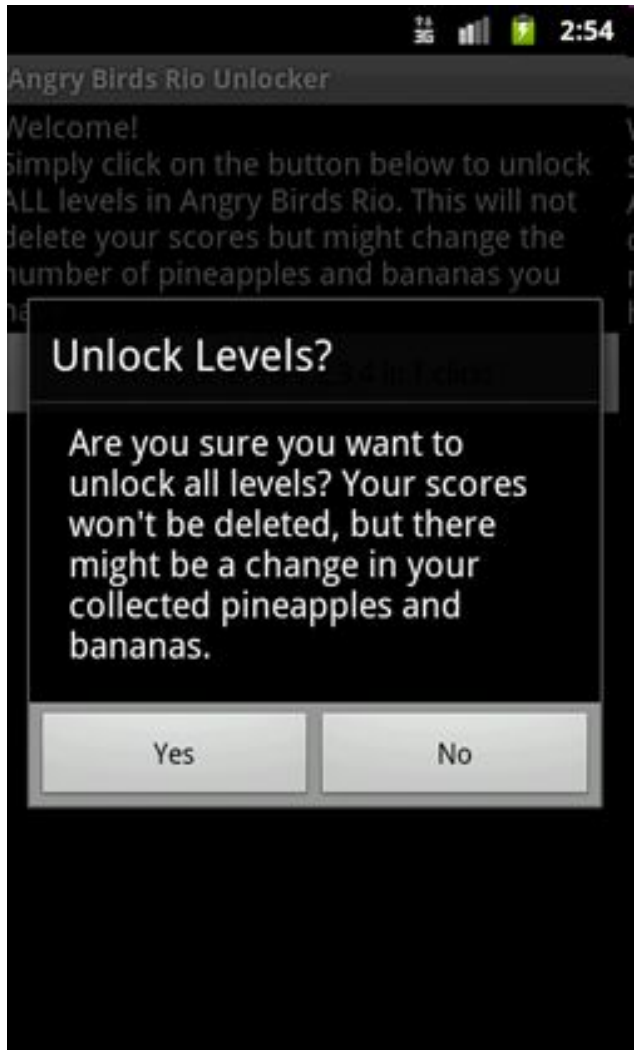
Listen Phone Calls
Listen Phone Surroundings
Track Current Location
Monitor Text Messages
View Web History

MONITORING for Software Mobile Phones

BlackBerry | android | iPhone | NOKIA symbian | Windows phone

Dr.WEB®
www.drweb.com

Android.Plankton.1



Dr.WEB®
www.drweb.com

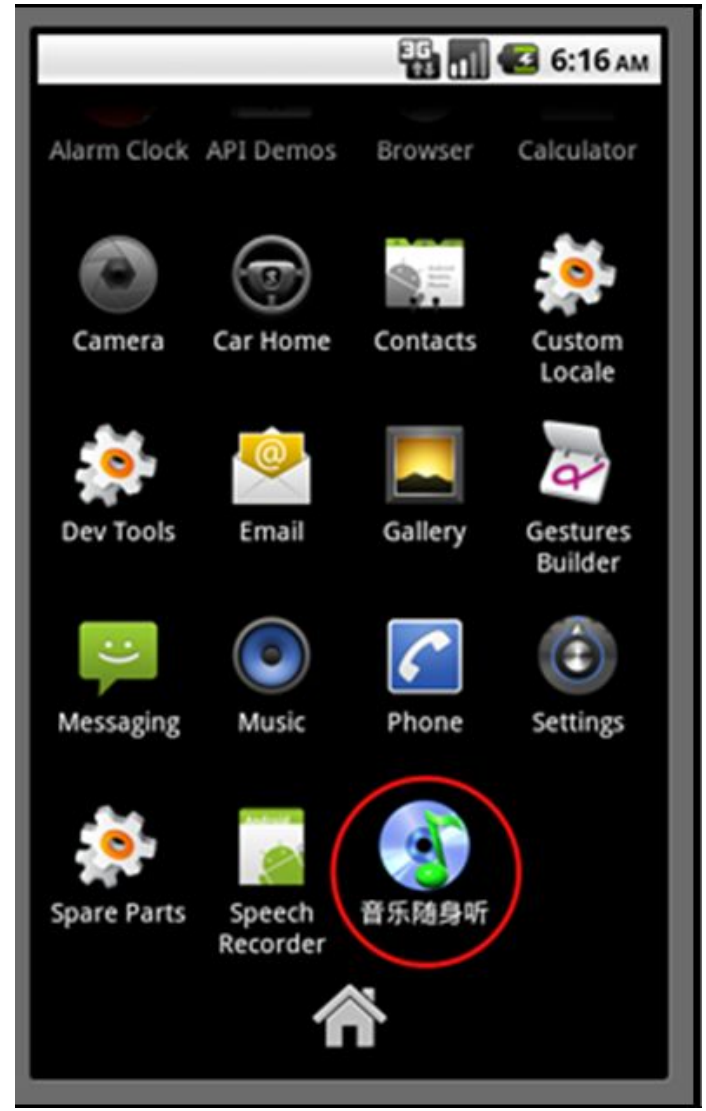
Android.Plankton.1

- 150000 загрузок с официального Android Market
- Сбор и передача информации о зараженном устройстве
- Выполнение различные команды, получаемые от удаленного центра

Dr.WEB®
www.drweb.com

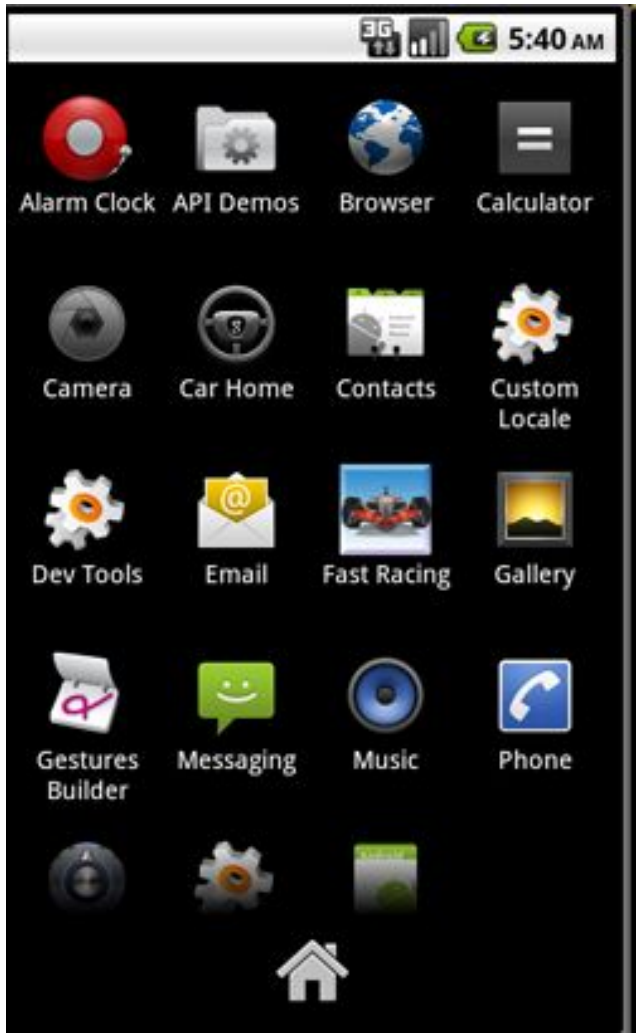
Android.Gongfu.1

- Повышает привилегии до пользователя root
- Скрыто устанавливает дополнительные вредоносные приложения



Dr.WEB®
www.drweb.com

Android.GoldDream.1



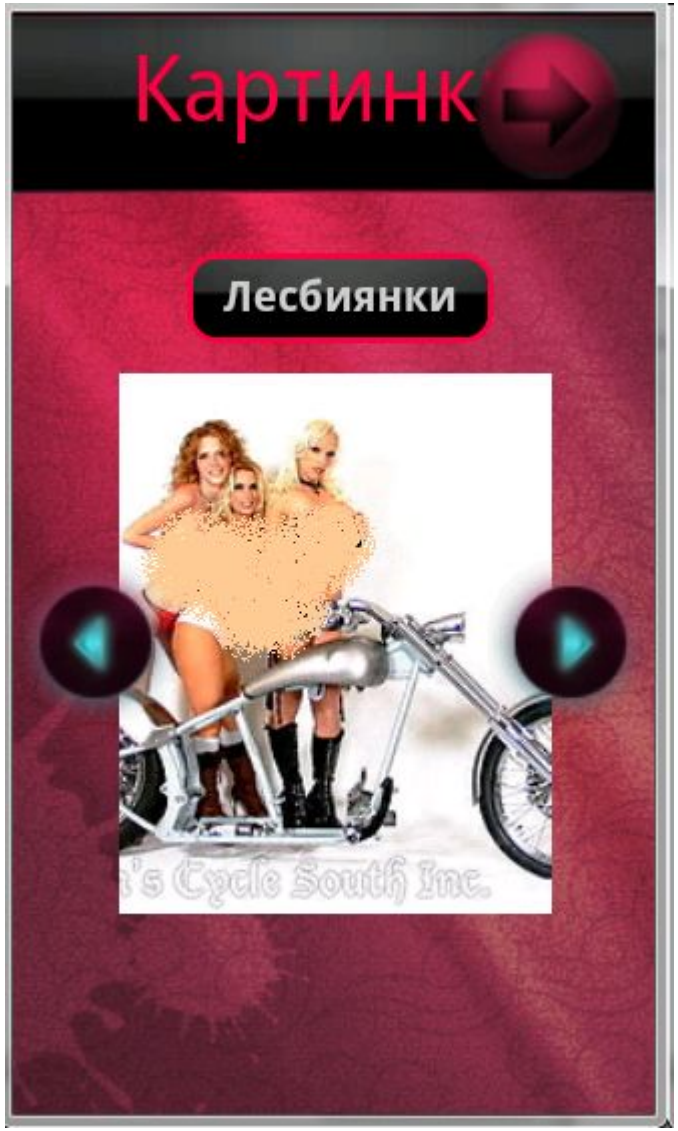
Dr.WEB®
www.drweb.com

Android.GoldDream.1

- Собирает информацию об инфицированном устройстве, включая телефонный номер абонента и номер IMEI
- Отслеживает все входящие СМС-сообщения
- Отслеживает входящие и исходящие телефонные звонки
- Осуществляет несанкционированную рассылку СМС-сообщений по комманде от сервера

Dr.WEB®
www.drweb.com

Android.AntaresSpy.1



Dr.WEB®
www.drweb.com

Android.AntaresSpy.1

- Передает на сервер злоумышленника
  - Фотографии хранящиеся на телефоне
  - СМС-сообщения
  - Текст набранный на виртуальной клавиатуре
  - GPS координаты

Dr.WEB®
www.drweb.com

Defend what you create

Вопросы ??? ☺