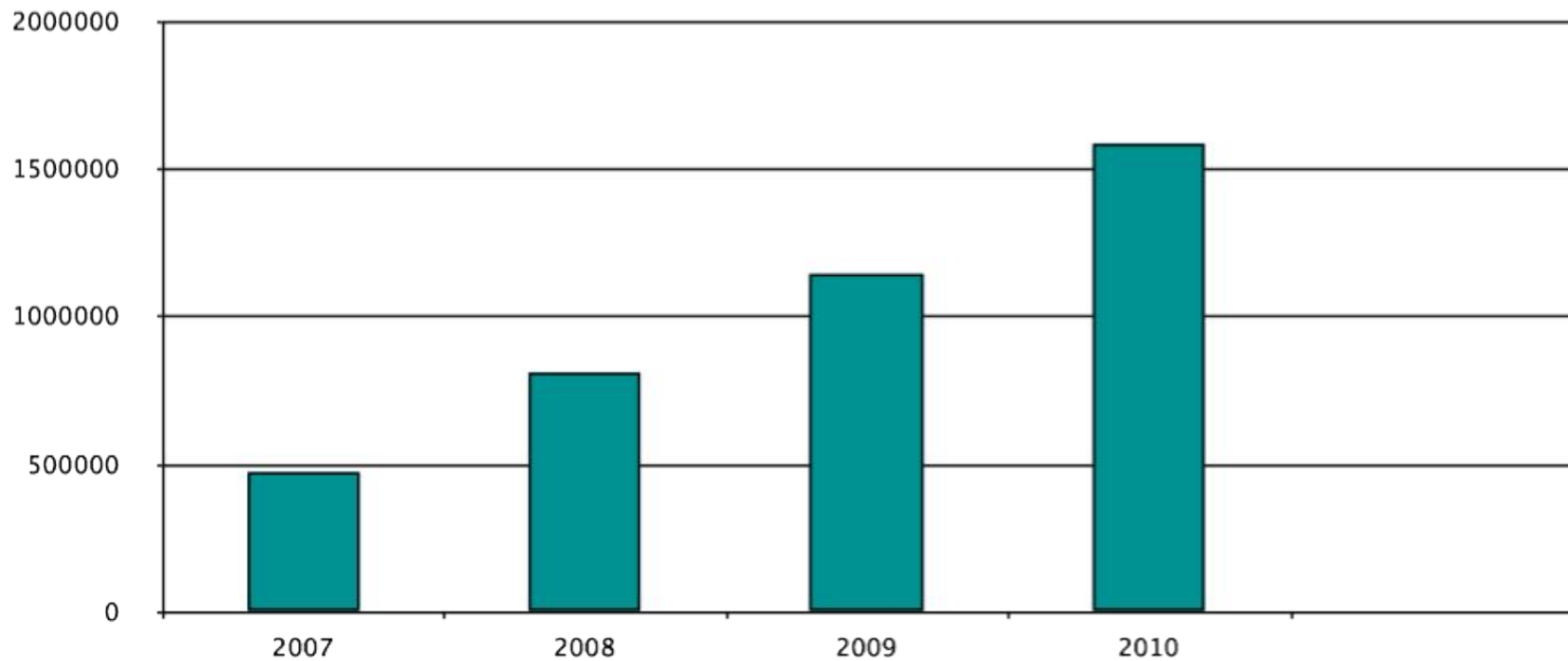


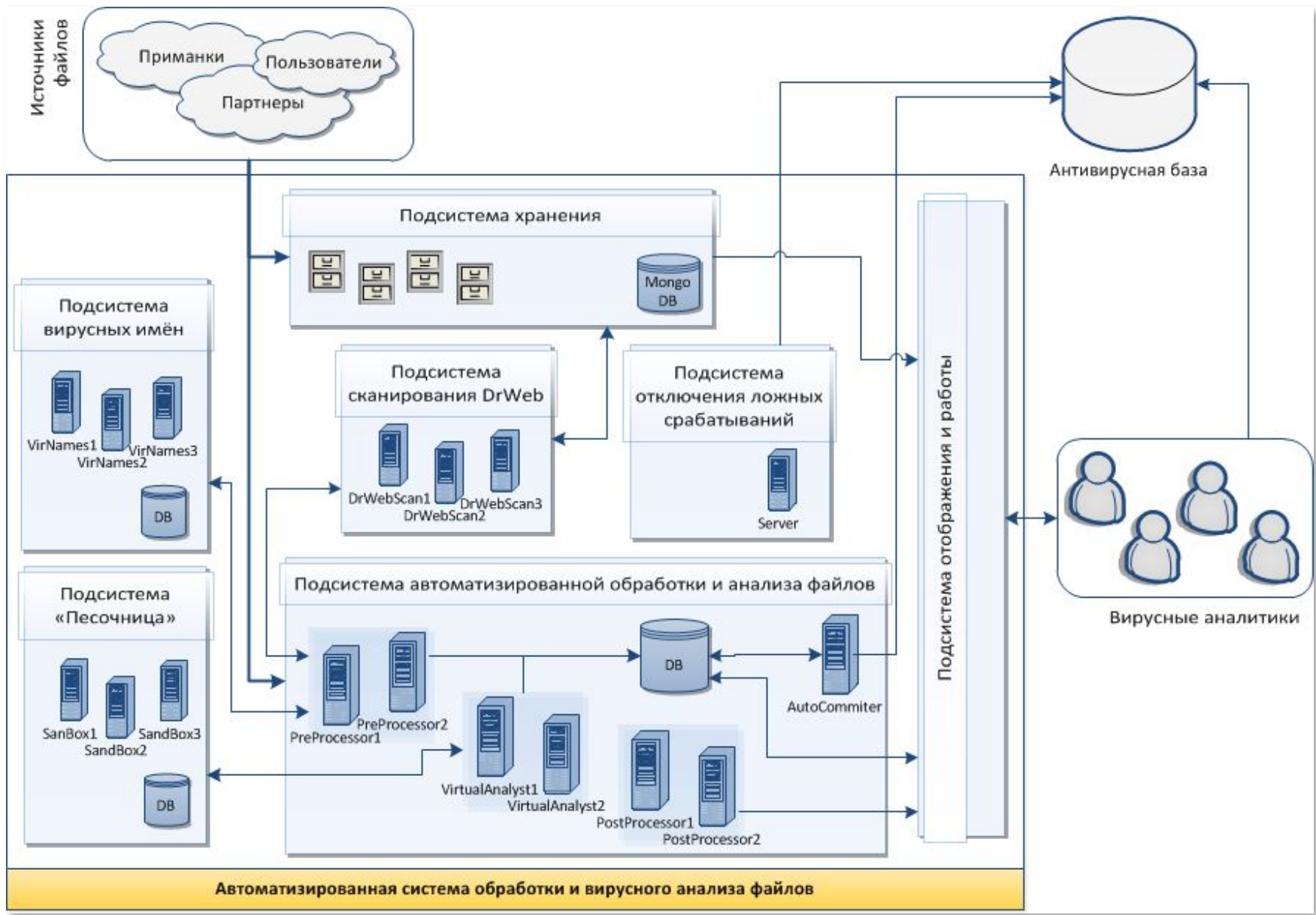
Современные методы  
обработки и алгоритмы  
детектирования вредоносного  
программного обеспечения.  
Краткий обзор угроз для  
мобильной платформы Android

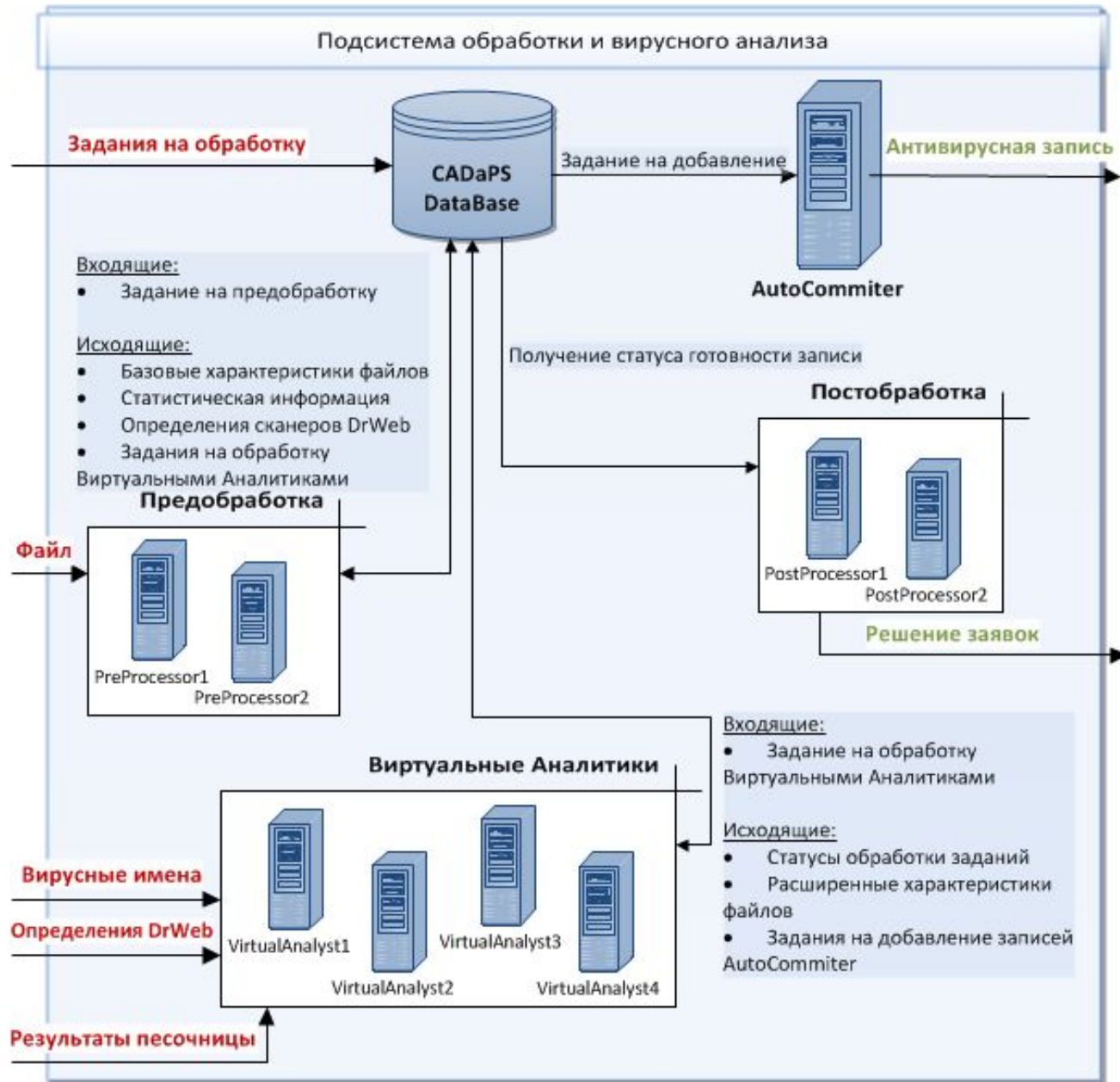
## Количество добавленных угроз в вирусные базы



# 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)





# Алгоритмы детектирования вредоносных программ

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

# Оценка схожести 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

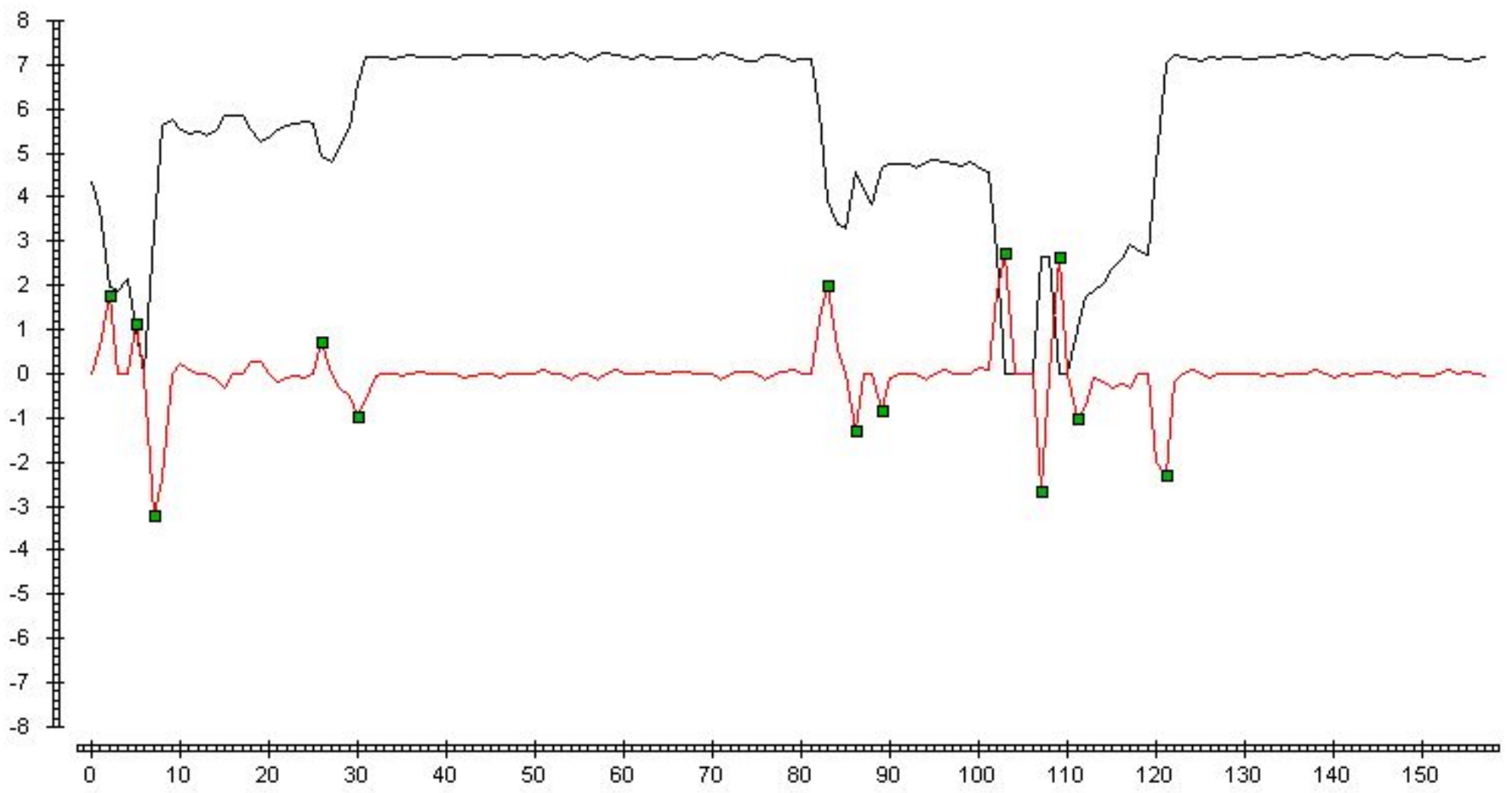
# Подсчет энтропии методом скользящего окна

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

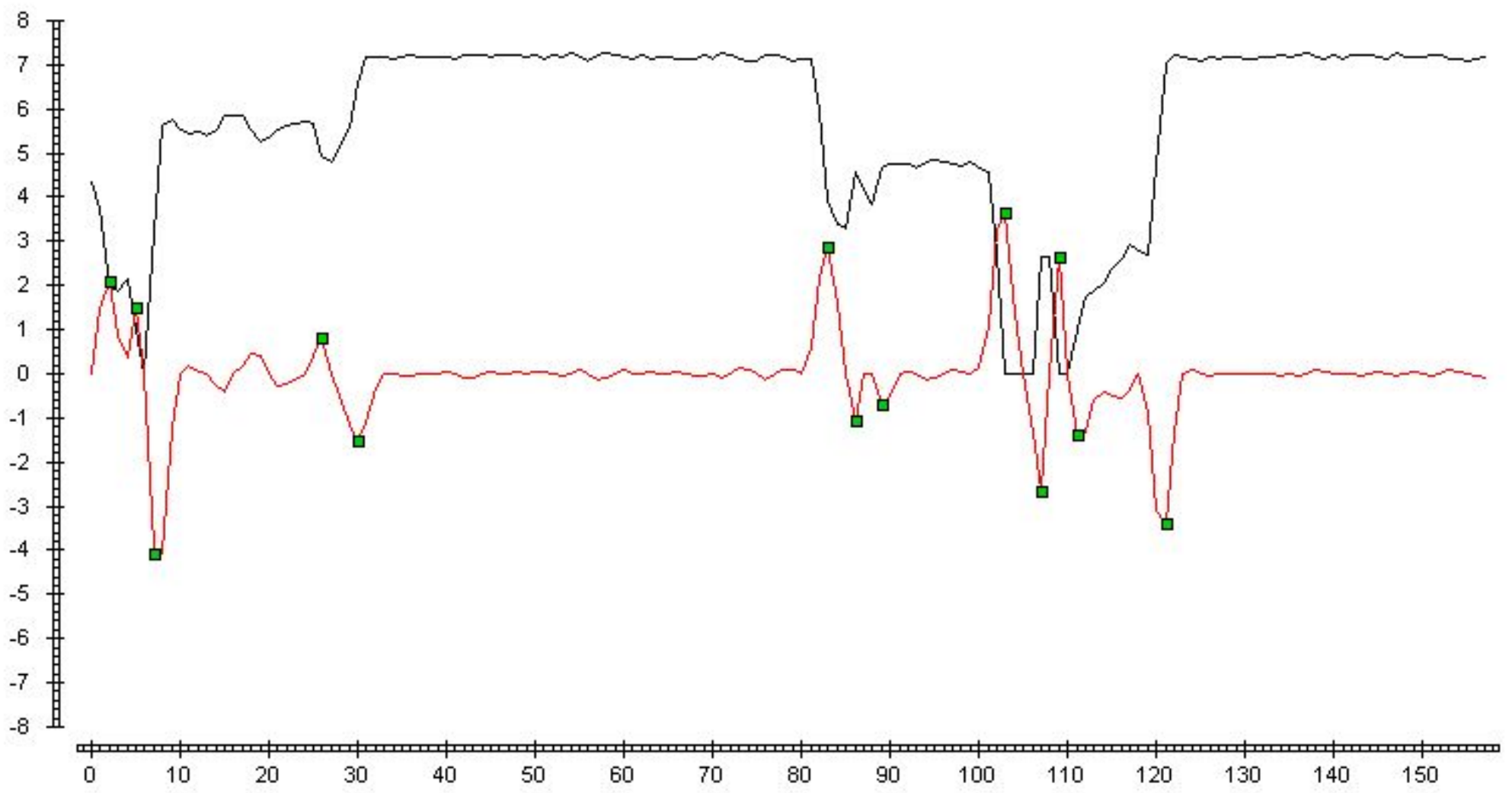
$$y_i = - \sum_{j=1}^m p(j) \log_2 p(j)$$



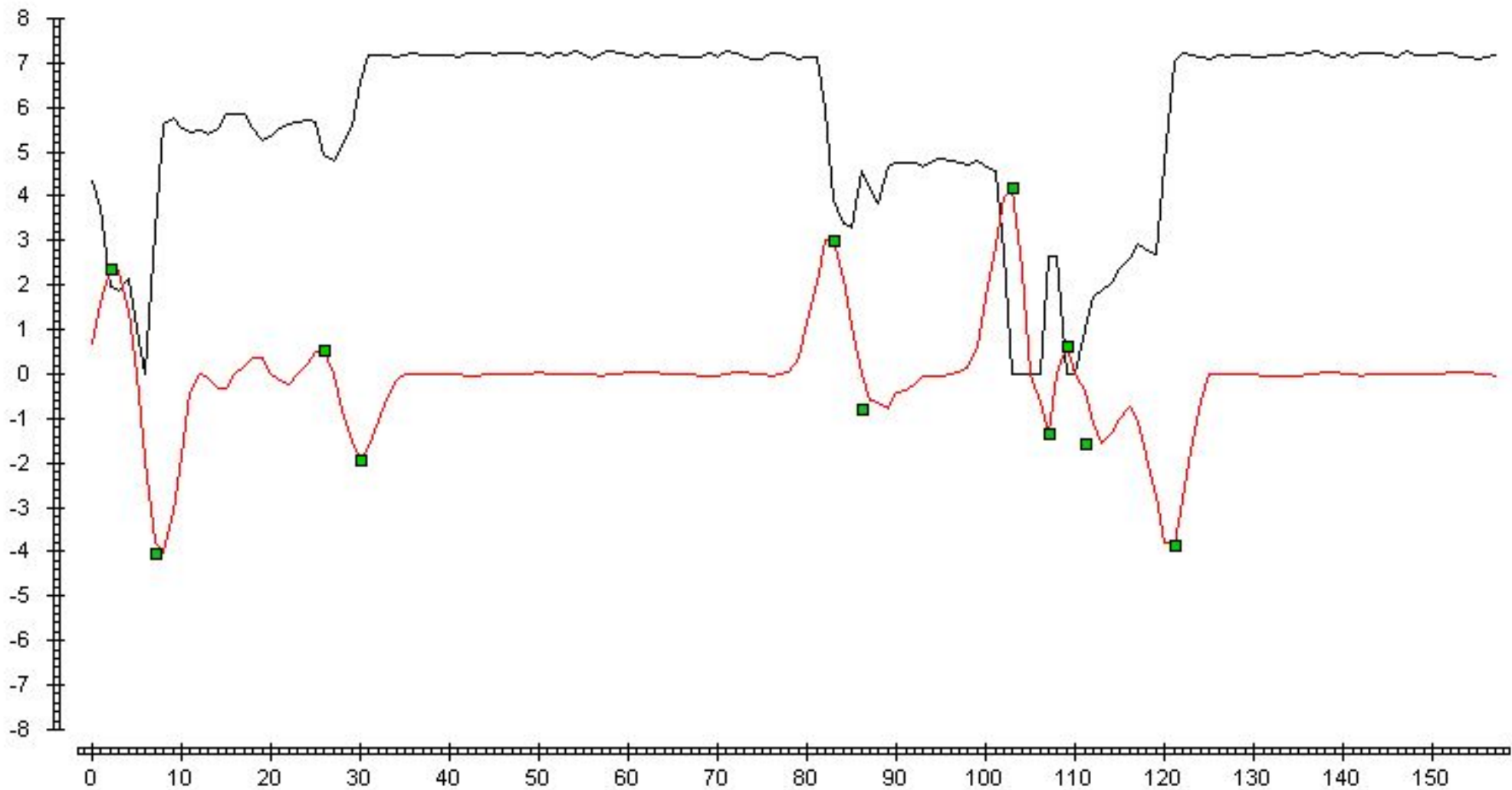
# Вейвлет анализ



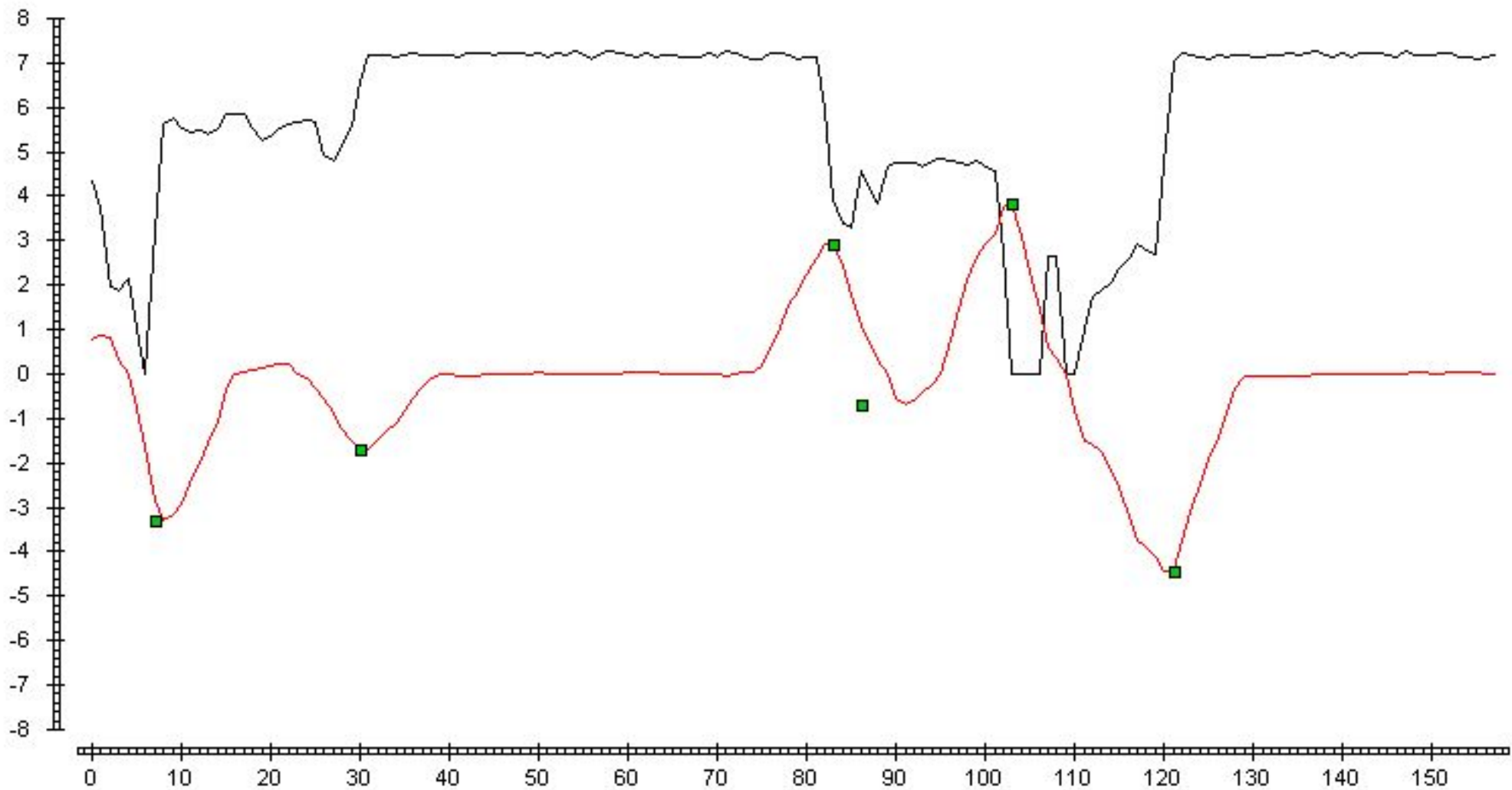
# Вейвлет анализ



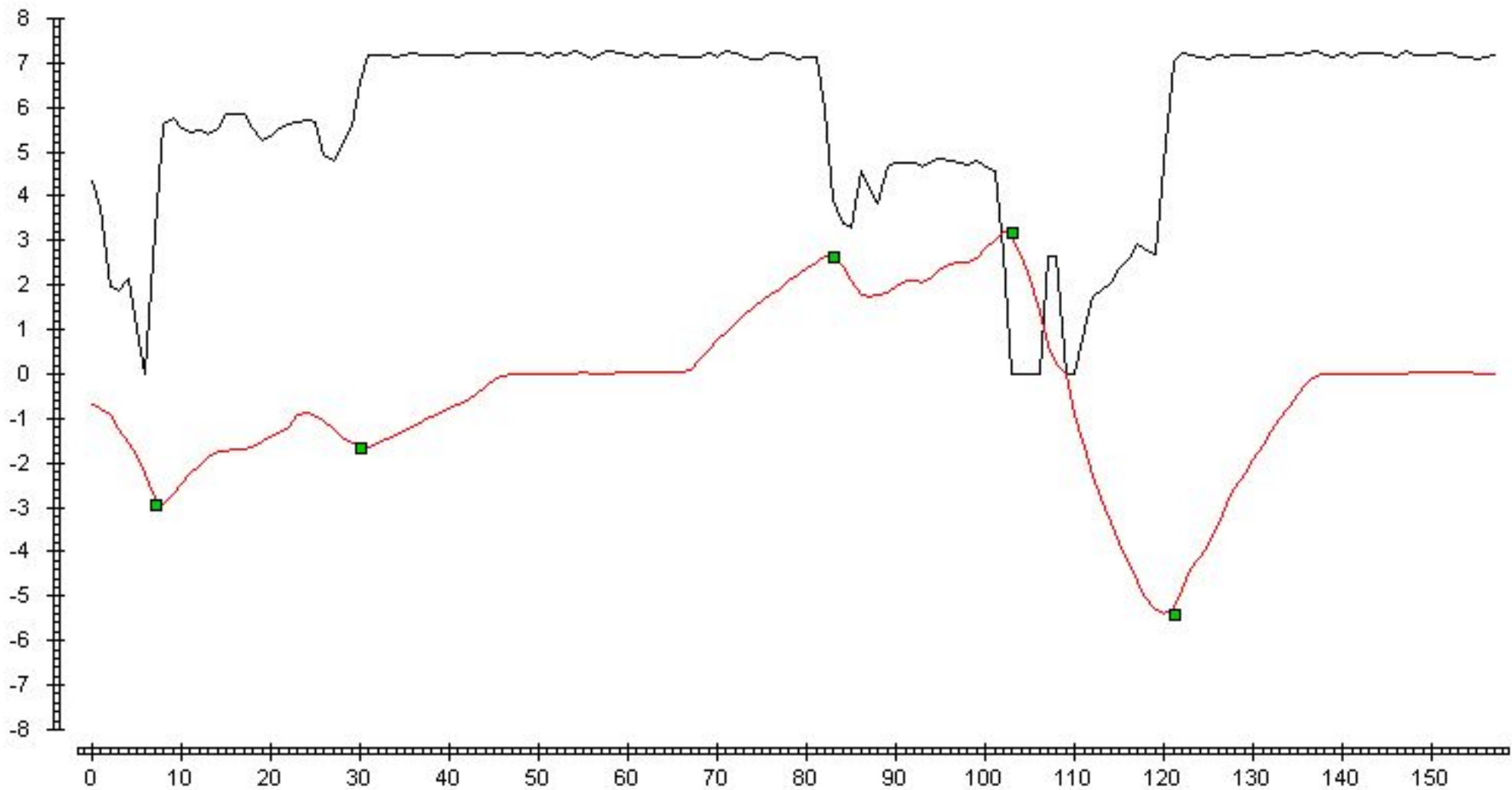
# Вейвлет анализ



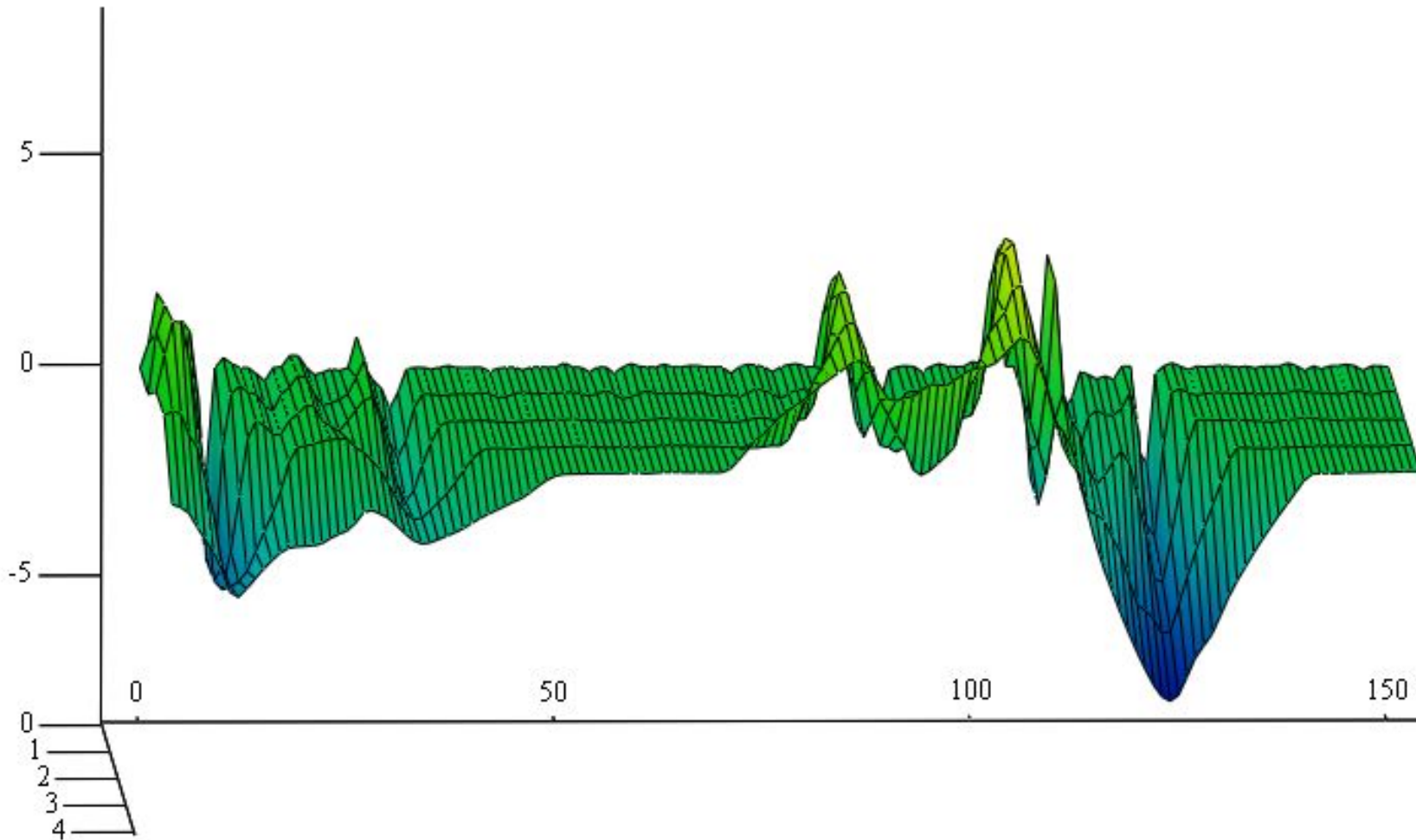
# Вейвлет анализ



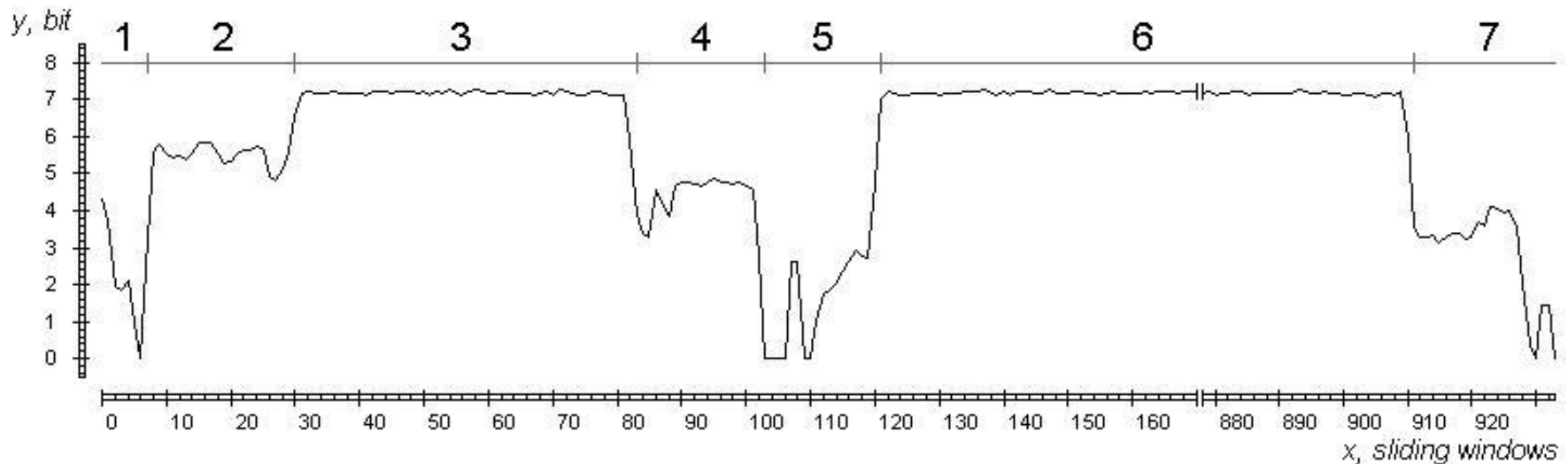
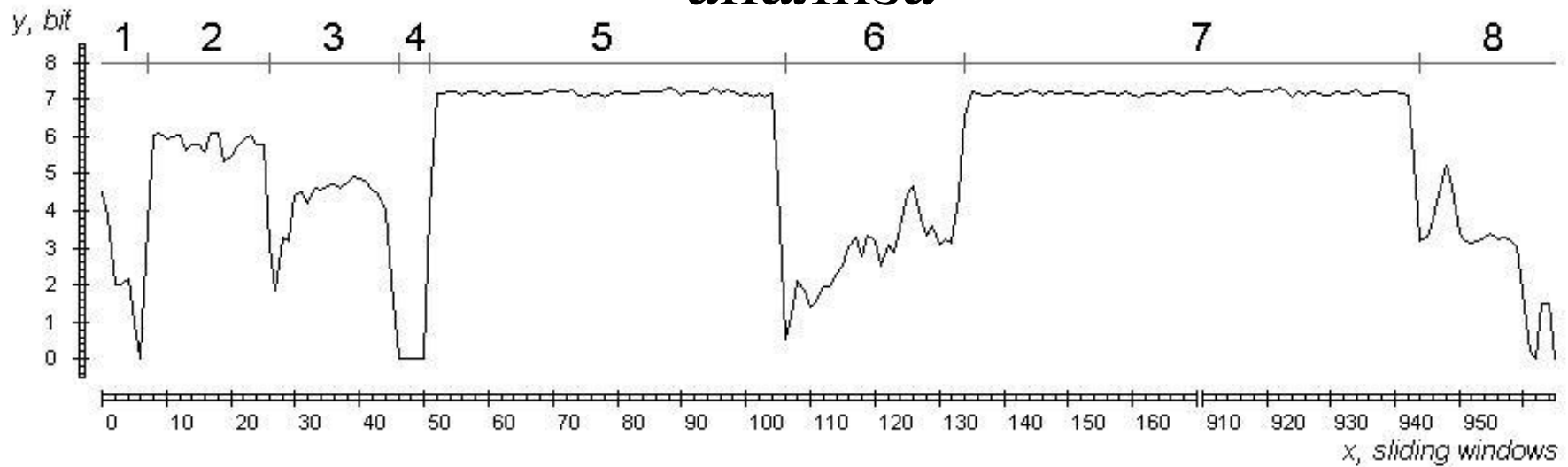
# Вейвлет анализ



# Оценка схожести файла на основе вейвлет анализа



# Оценка схожести файла на основе вейвлет анализа



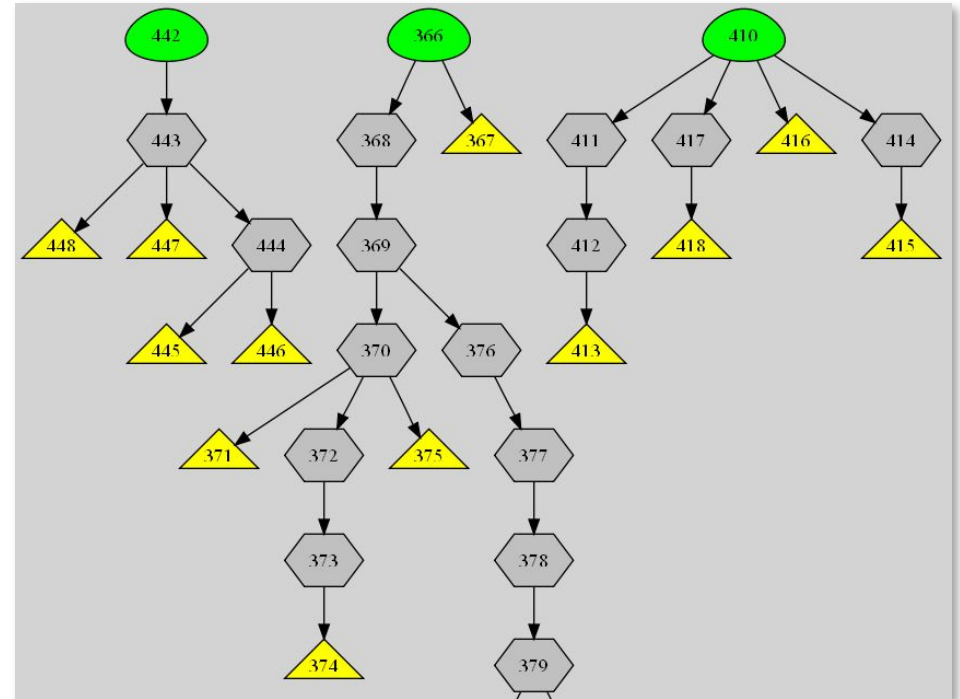
# Оценка похожести файлов на основе вейвлет анализа

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



# Технология Origin Tracing

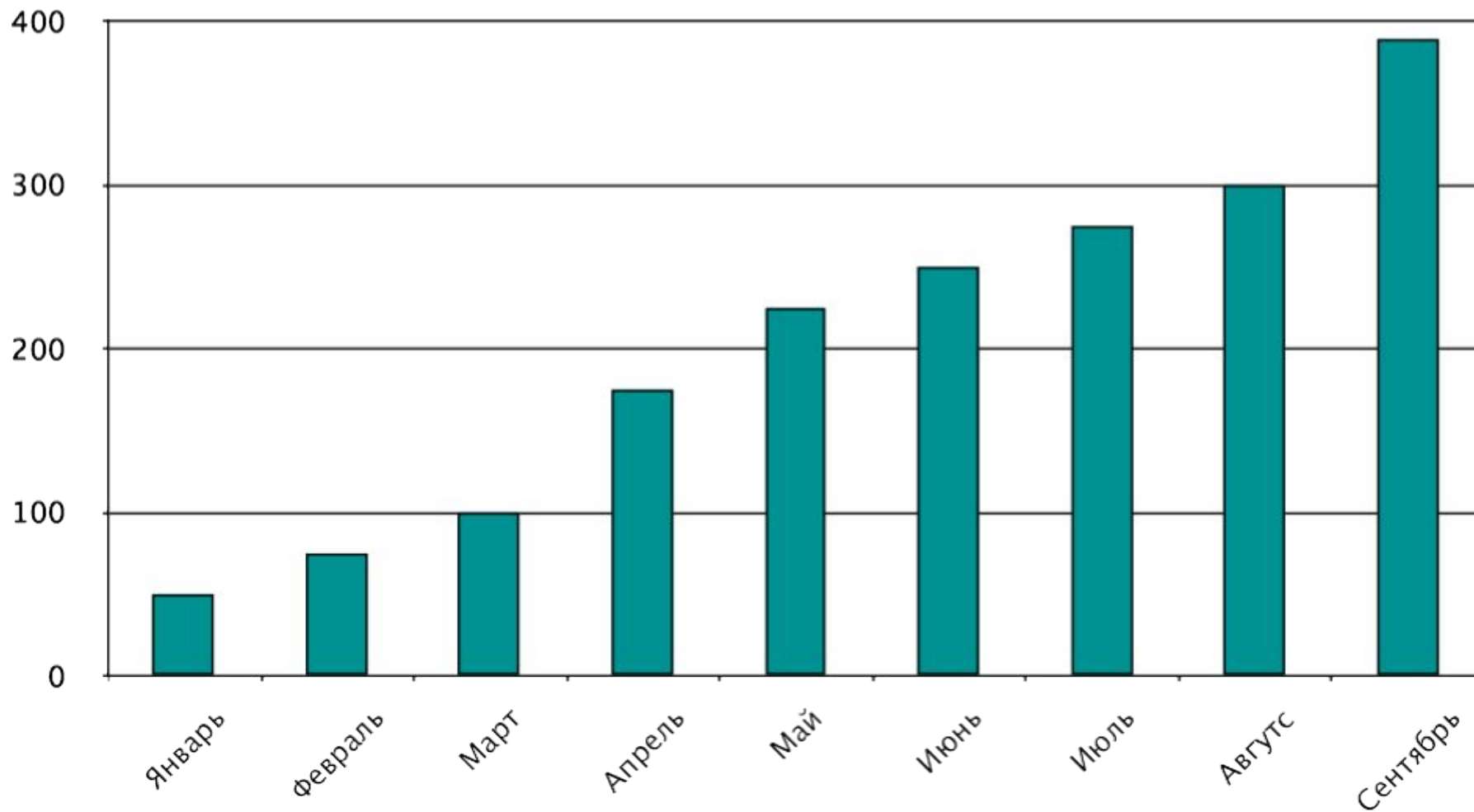
- Статический анализ кода
- Построение графа управления программы
- Выделение подозрительных вершин графа
- Составление записи детектирования вредоносного семейства



# Мобильные угрозы для Android OS



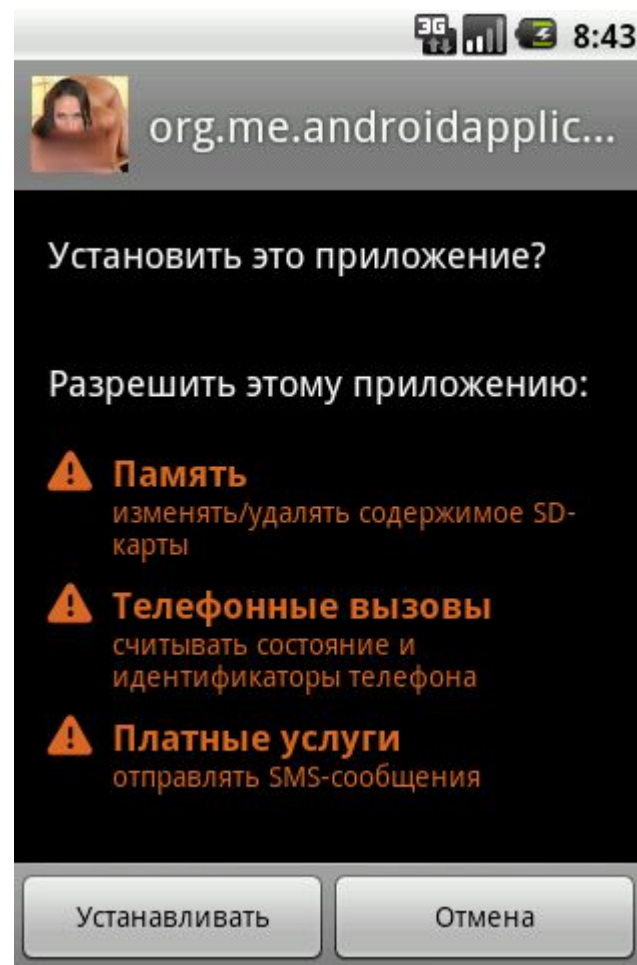
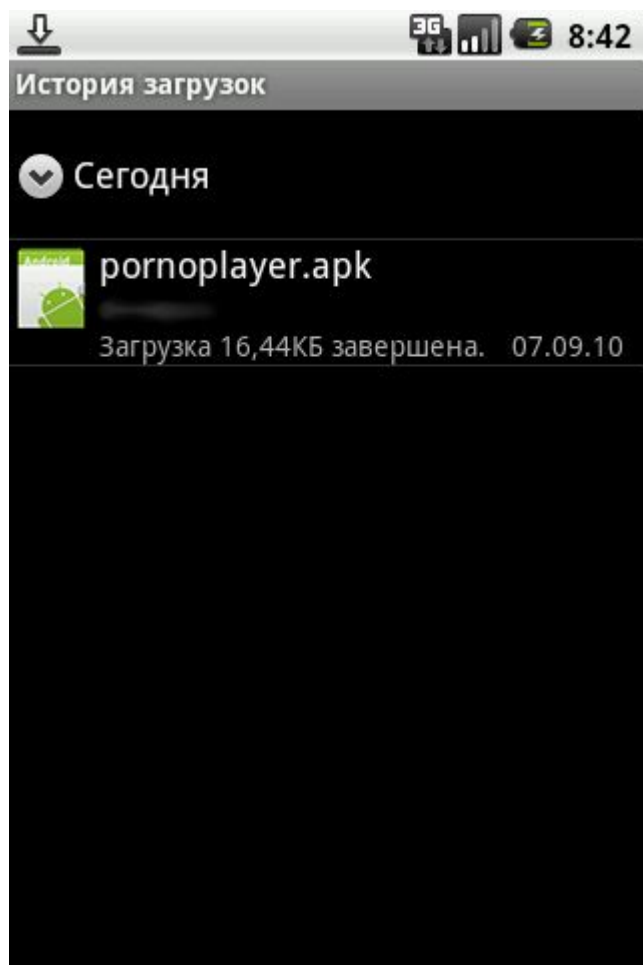
# Рост количества угроз



# 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)

# Android.SmsSend



# Пример схемы мошенничества



 конверт мобильного трафика  
**ZipWar.ru**

## Создание Мидлета

Кол-во СМС	<input type="text" value="5\$+5\$+3\$"/>	▼
Тип Мидлета	<input type="text" value="default"/>	▼
	<input type="text" value="Android"/>	▼
URL Файла:	<input type="text"/>	
Название приложения:	<input type="text"/>	
Иконка файла:(jpg, png)	<input type="text"/>	<input type="button" value="Обзор..."/>
Размер мидлета(20-3000кб)	<input type="text" value="100"/>	
Описание приложения:	<input type="text"/>	

# Пример схемы мошенничества



## Список мидлетов

Тип	Схема Активации	Название	URL	Ссылка	
	10\$+5\$+5\$	drwebantivirus	<a href="http://company.drweb.com/ca...">http://company.drweb.com/ca...</a>	<input type="text" value="http://newmobifile.ru/getfile.php?type=pp&amp;r=834-2"/>	 
	5\$+5\$+3\$	20years	<a href="http://www.f-secure.com/web...">http://www.f-secure.com/web...</a>	<input type="text" value="http://newmobifile.ru/getfile.php?type=pp&amp;r=834-1"/>	 

# Пример схемы мошенничества

---

Сейчас начнется загрузка **срочного** обновления **Орега Мiни 6.1**

Если загрузка не началась автоматически,  
[Обновите Орега Мiни до версии 6.1 вручную.](#)

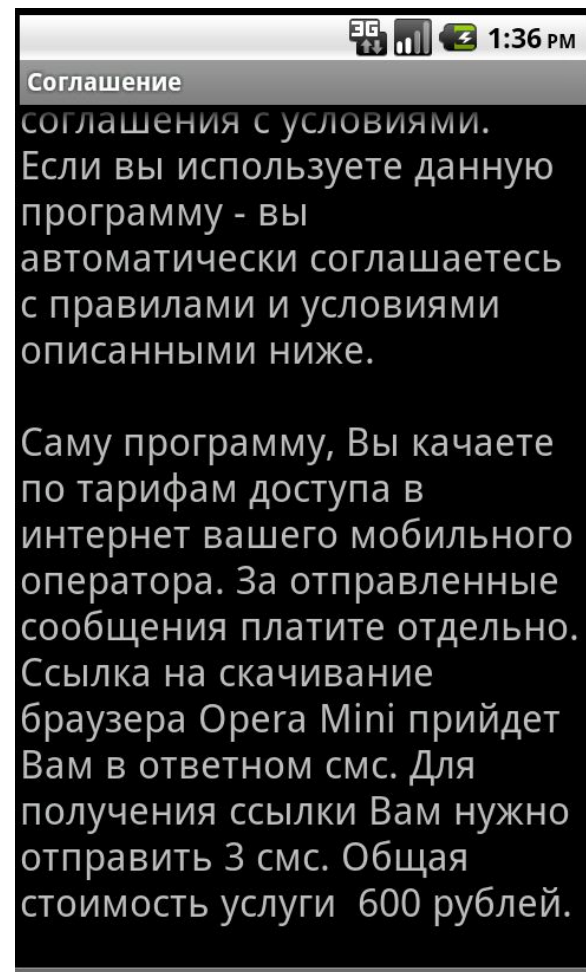
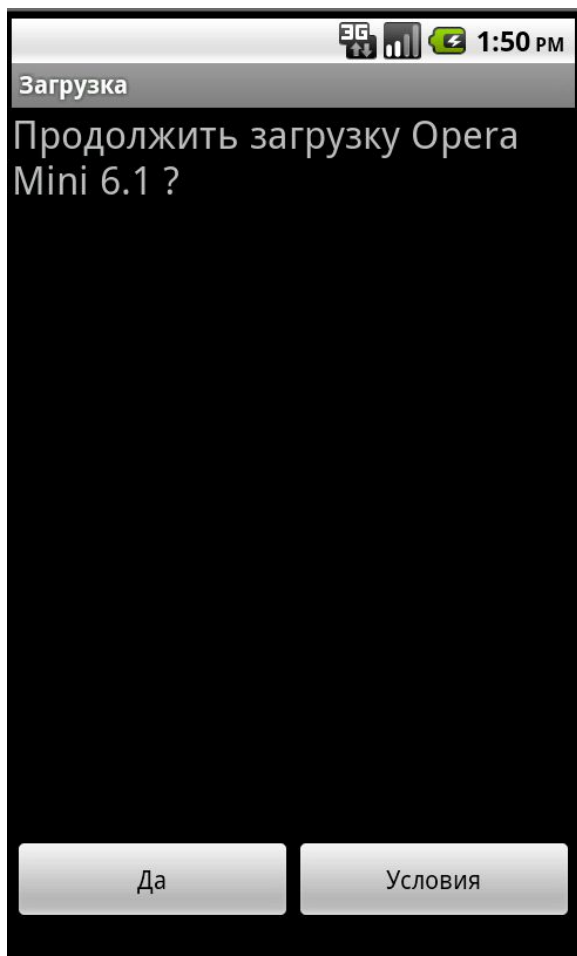
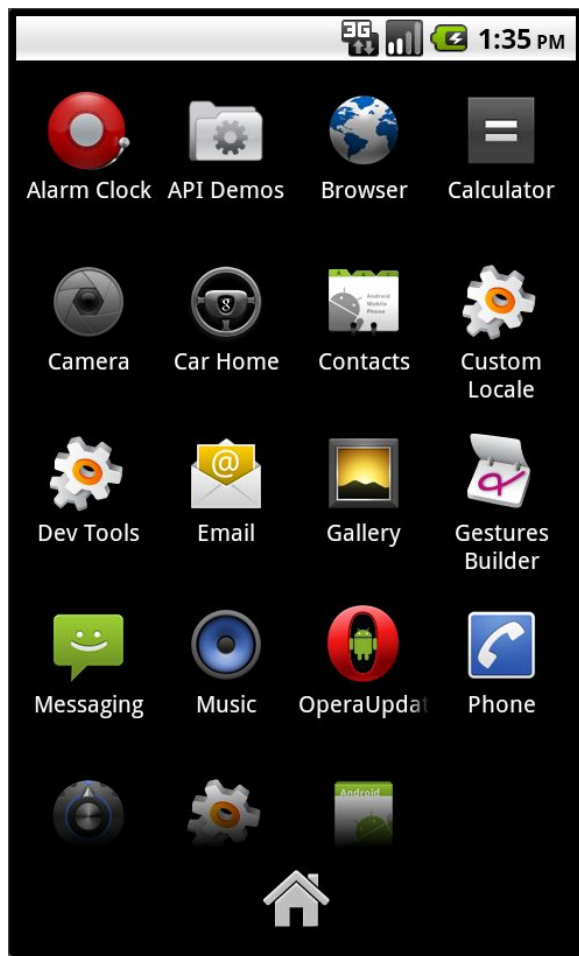


Некорректная работа вашего браузера Орега Мiни подвергает ваш мобильный телефон опасности!  
Браузер необходимо обновить ПРЯМО СЕЙЧАС — нажмите на ссылку [«Обновить Орега Мiни 6.1»!](#)

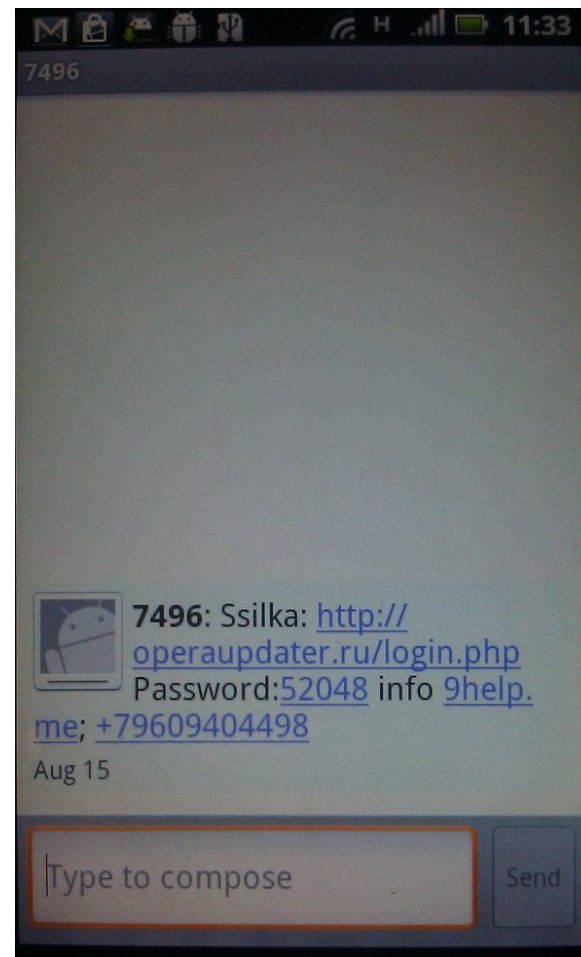
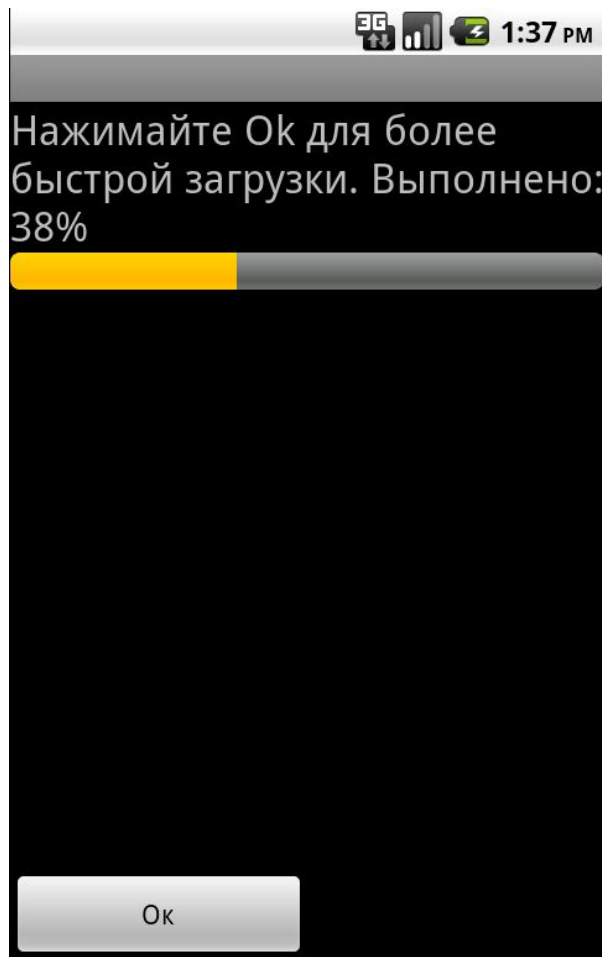
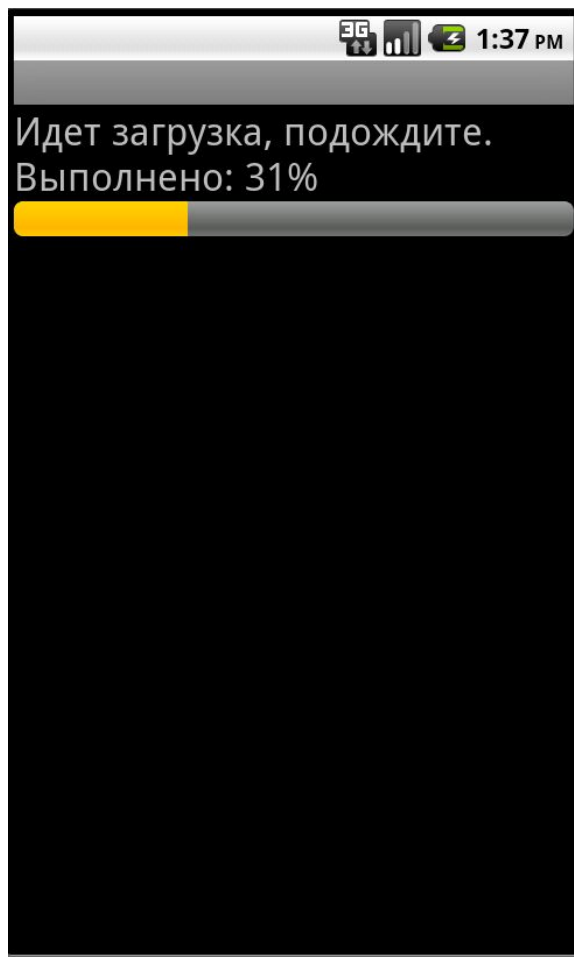
[Обновить Орега Мiни 6.1](#)



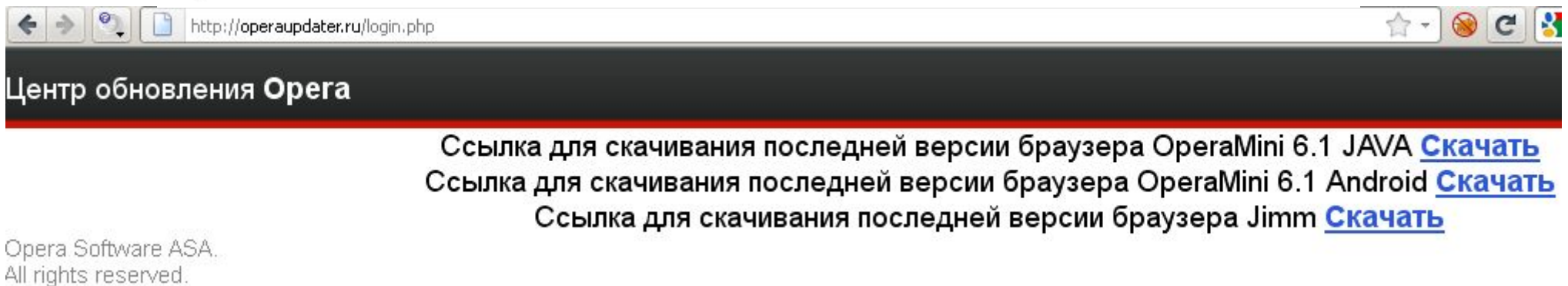
# Пример схемы мошенничества



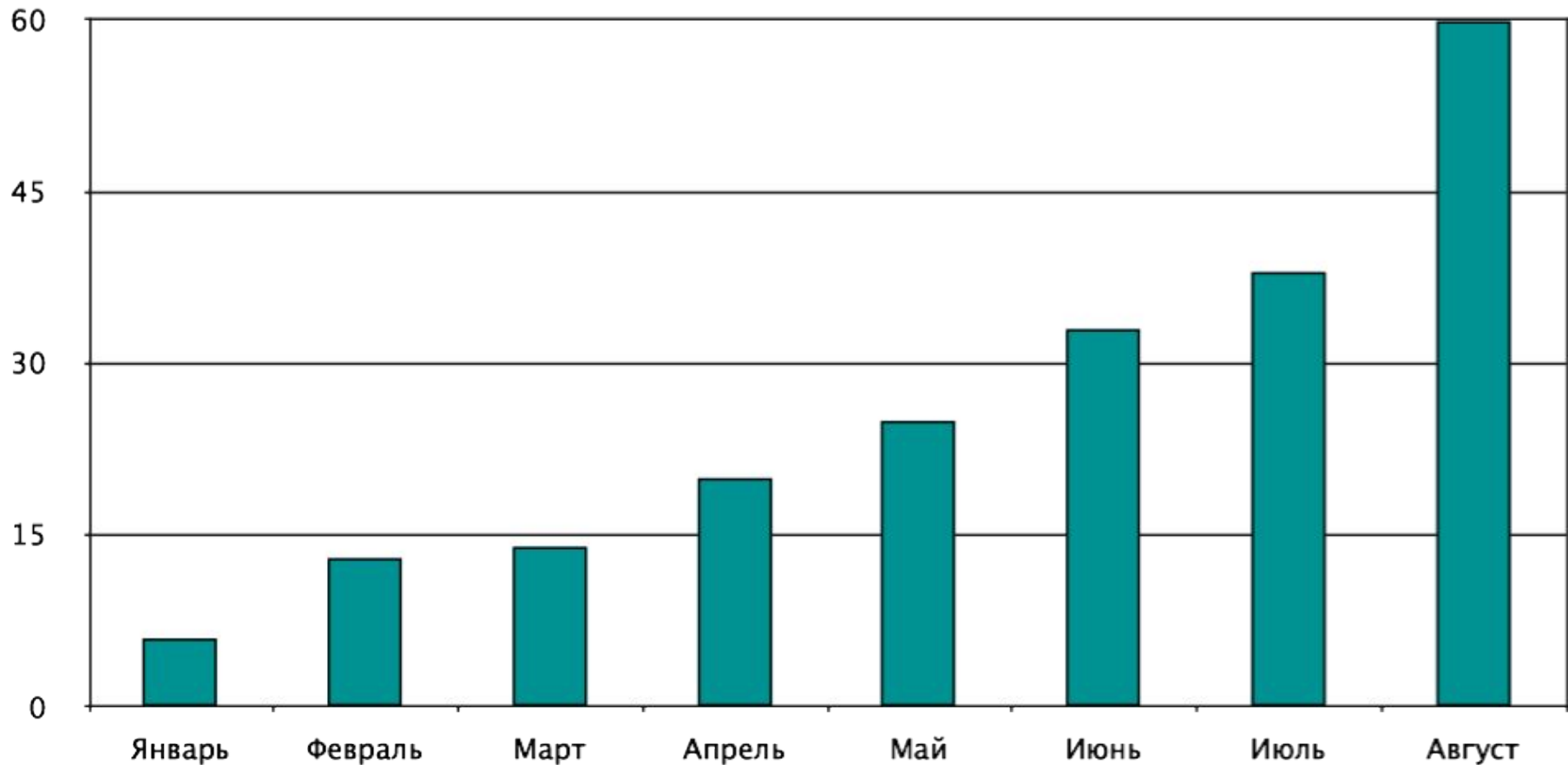
# Пример схемы мошенничества



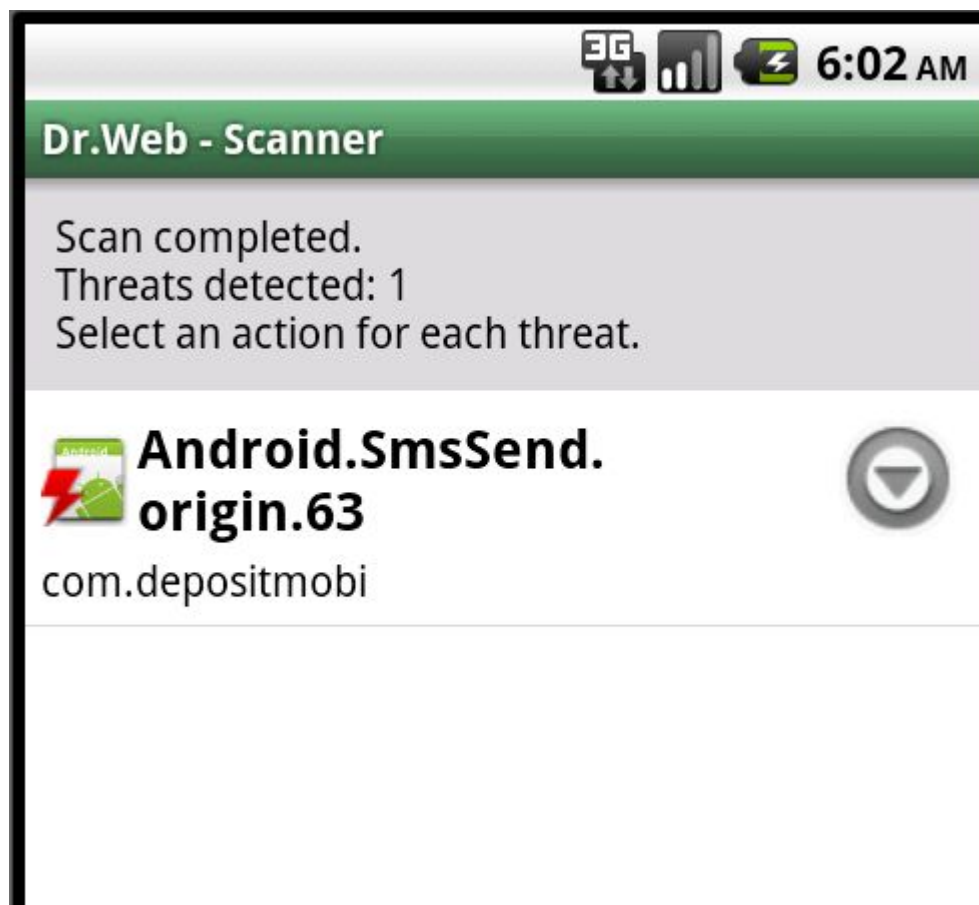
# Пример схемы мошенничества



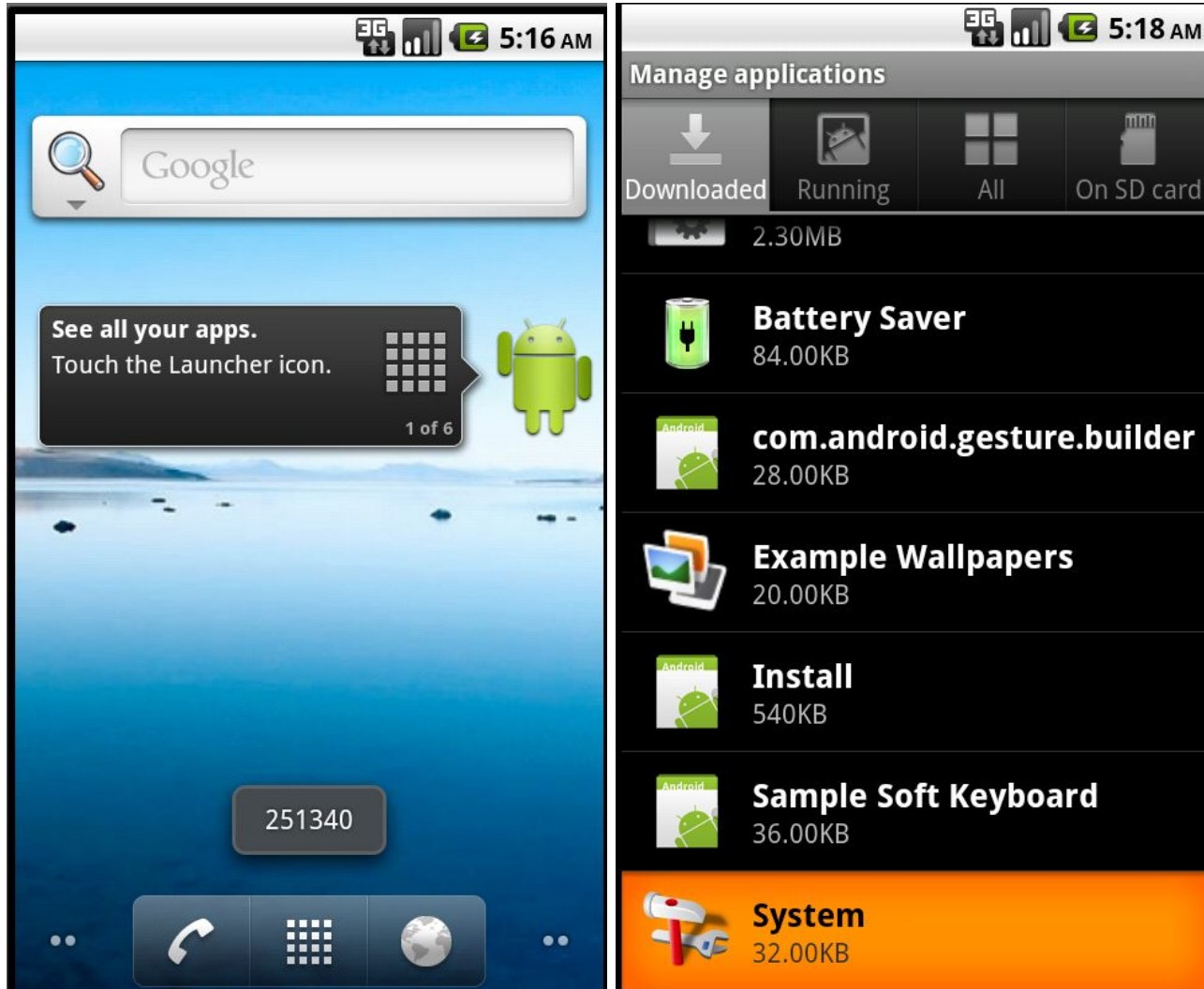
# Количество модификаций Android.SmsSend



# Детектирование новых угроз с помощью технологии Origin Tracing



# Android.SpyEye.1



# 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>
```



Protect Your Children | Catch Cheating Spouses

Live Support  
BACK SOON

[Home](#) | [Features](#) | [Phones](#) | [Demo](#) | [Support](#) | [Community](#) | [Reseller](#) | [Affiliates](#) | [About Us](#) | [Cart](#)

**Is Someone Keeping Secrets from You?  
Reveal All with the Worlds Most Powerful Spyphone**

- ≡ Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase.
- ≡ Catch cheating wives or cheating husbands, stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.
- ≡ Learn all about FlexiSPY. Still have questions, try Live Chat who are waiting to help.

**FlexiSPY America**




**Blackberry** [Start here](#)

**Nokia** [Start here](#)

**Win Mobile** [Start here](#)

**iPhone** [Start here](#)

**Android** [Start here](#)

**Maemo** [Start here](#)

**FLEXISPY - PRO - X**

**PRO-X** | [FULL DETAILS](#) | [Supported Phones](#)

**iPhone** | [FULL DETAILS](#)

**TOP OF THE RANGE SPYPHONE**

- ▣ Listen to actual phone calls
- ▣ Use as a secret mobile gps tracker
- ▣ Includes all PRO features
- ▣ Change phones as often as you like
- ▣ Symbian, Windows Mobile & BlackBerry

**ORDER NOW: \$349** (per year)

LEARN ABOUT SPYPHONE FEATURES HERE

Buy Now

**NEW FLEXISPY iPhone**

**iPhone** | [FULL DETAILS](#)

**Worlds Most powerful iPhone spy phone**

- ▣ Secretly read SMS, Email, Call Logs
- ▣ Track location on map
- ▣ Make secret spy calls
- ▣ BASIC version from \$ 39.99

**ORDER NOW: \$349** (per year)

Buy Now

Now Available – Flexispy Pro-X for Android and Flexispy Light for iPhone 4.0



Protect Your Children | Catch Cheating Spouses

START

**FLEXISPY - PRO**

**PRO** | [FULL DETAILS](#) | [Supported Phones](#)

**MID RANGE SPYPHONE**

- ▣ Spyphone to bug a room or person
- ▣ Read their SMS, EMAIL and Call Logs
- ▣ BUY NOW for Instant Download

**NEW FLEXIRECORD**

**RECORD** | [FULL DETAILS](#)

**RECORD SPYCALLS ON A PC**

- ▣ Automatically records SPY calls to PC
- ▣ Ideal companion to any PRO or PROX
- ▣ Control multiple target directly from PC

HOW CAN FLEXISPY HELP YOU

- ≡ UNCOVER Employee espionage
- ≡ CATCH cheating husbands and cheating wives
- ≡ TRACK THEIR location using GPS
- ≡ PROTECT your children from SMS abuse.
- ≡ ARCHIVE all your own SMS for the future.
- ≡ SAVE your call history.
- ≡ BUG Meeting rooms and CHECK babysitters
- ≡ Ten Day MONEY BACK GUARANTEE

Winners Choose FlexiSPY

SEE WHY FLEXISPY IS THE



**MOBILE SPY®**  
SPY SOFTWARE FOR SMARTPHONES

*Monitor Android, iPhone, BlackBerry and more!  
Silently Record Text Messages,  
GPS Locations and Call Details!*



## *Spy Software for Mobile Phones*

Monitor Text Messages, Calls and GPS Online!

USA Based Support  
1(888)475-5345



*Hot New Add-on!  
LIVE Control Panel*



View Phone's Screen LIVE  
Get LIVE GPS Positions  
Perform LIVE Commands  
Log Delivery via Email

[HOME >](#)

[FEATURES >](#)

[PURCHASE >](#)

[LOGIN >](#)

[AFFILIATES >](#)

[SUPPORT >](#)



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

Listen Phone Calls

Listen Phone Surroundings

Track Current Location

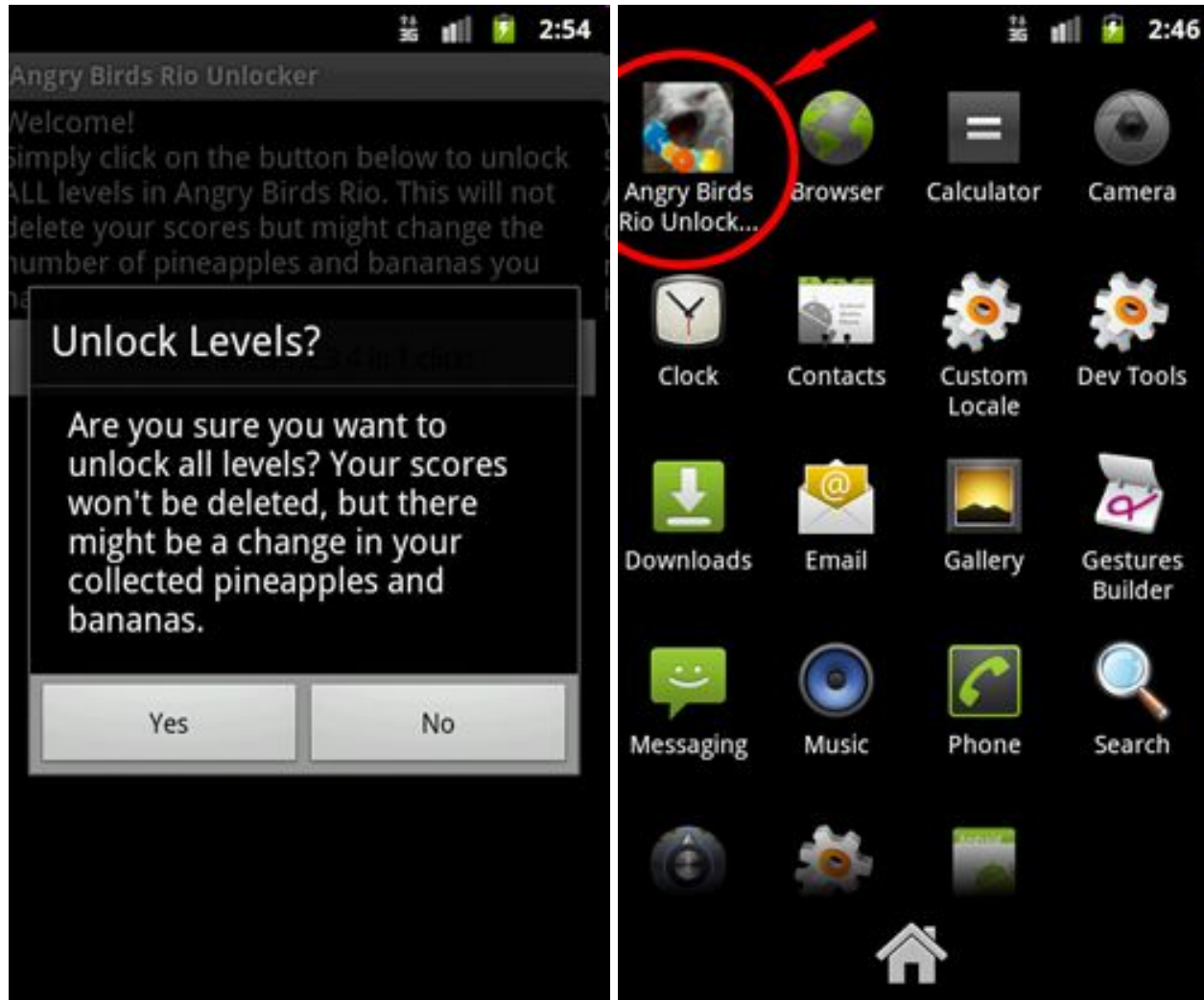
Monitor Text Messages

View Web History

**MONITORING**  
for Software  
**Mobile Phones**



# Android.Plankton.1

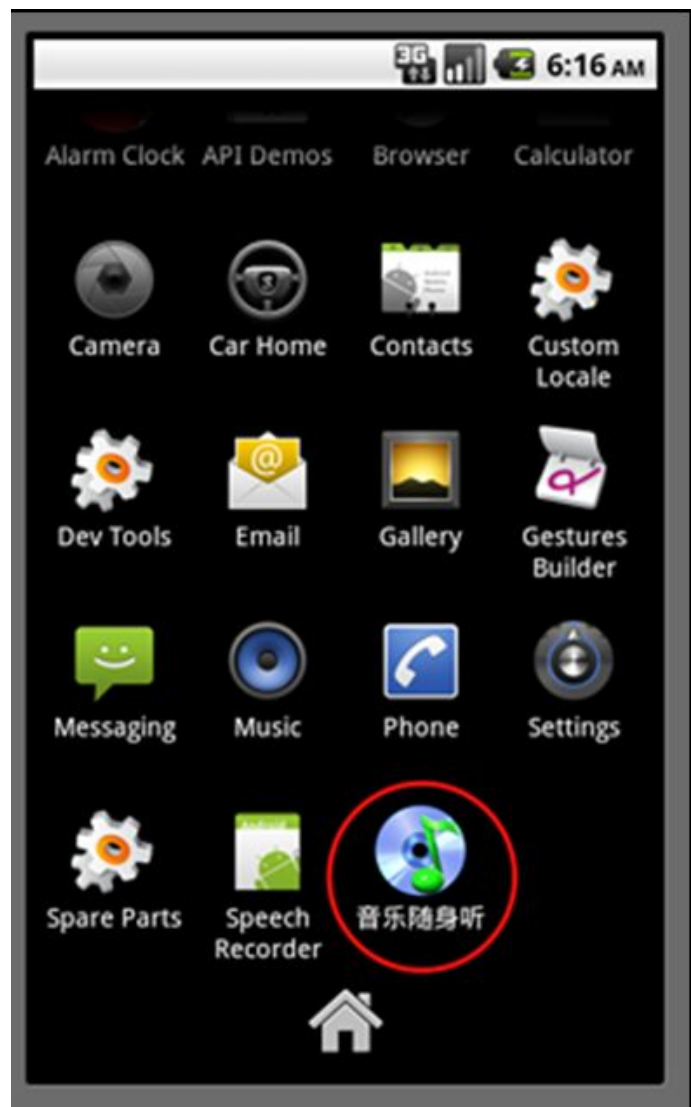


# Android.Plankton.1

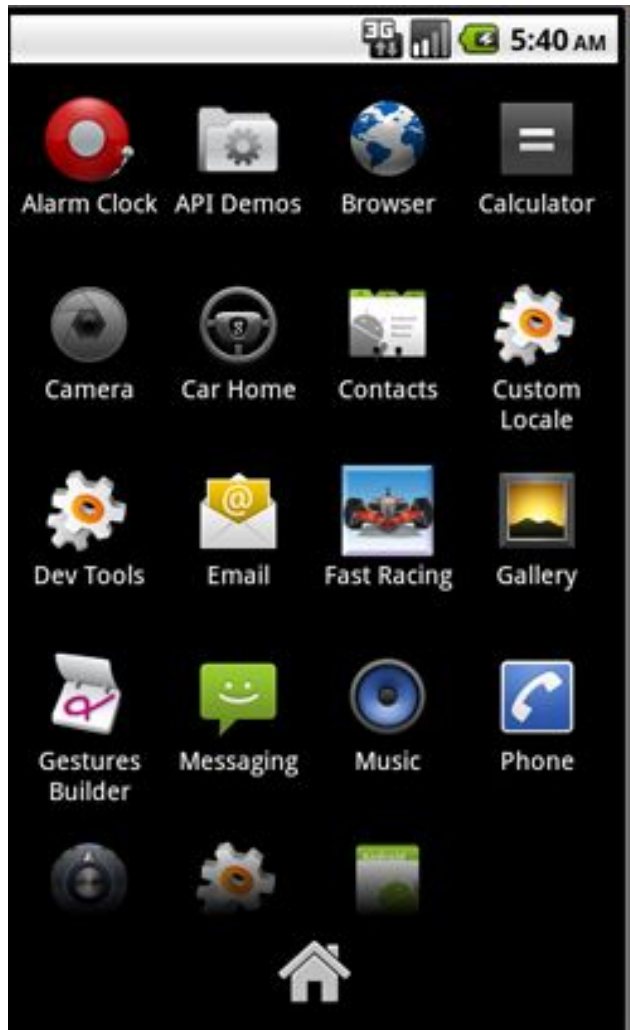
- 150000 загрузок с официального Android Market
- Сбор и передача информации о зараженном устройстве
- Выполнение различные команды, получаемые от удаленного центра

# Android.Gongfu.1

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



# Android.GoldDream.1



# 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 команде от сервера

# Android.AntaresSpy.1





# Android.AntaresSpy.1

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

Вопросы ??? ☺