Яндекс

# Вирус подмены страниц: изменение поведения веб-сервисов без ведома их создателей

**Александр Матросов**
аналитик

РусКрипто'2009

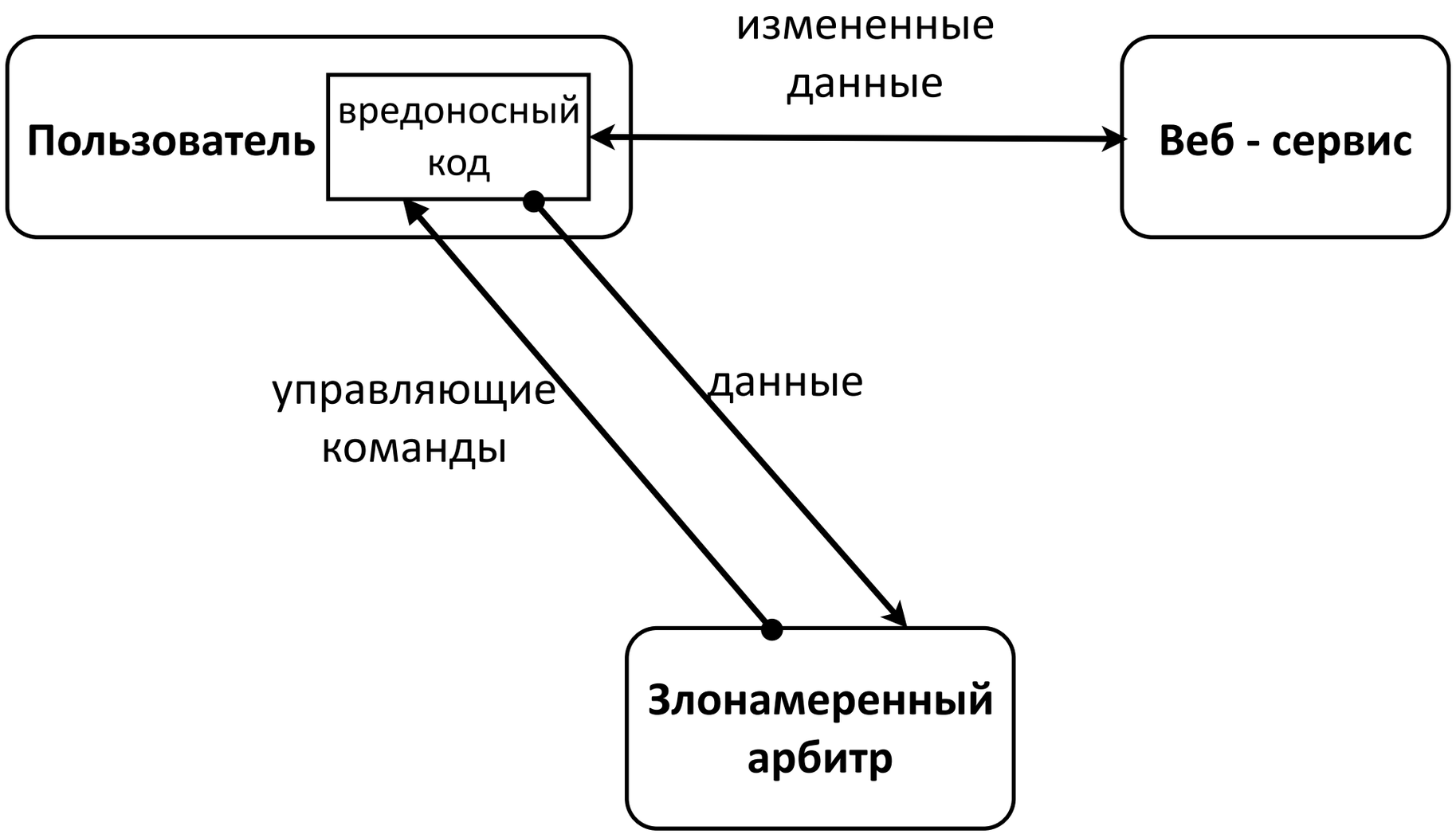
# План доклада:

- Вирус подмены страниц – проблема
- Масштабы угрозы
- Сколько на этом зарабатывают?
- Противодействие угрозе
- На сладкое ...

# Вирус подмены страниц – проблема

# Меняющаяся картина мира

# Меняющаяся картина мира

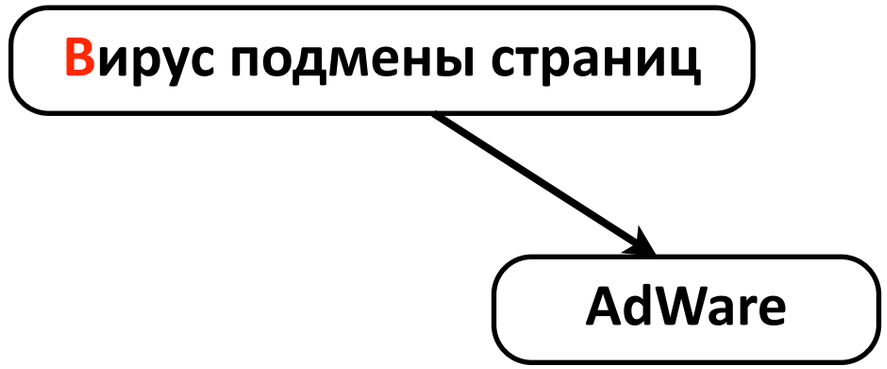


# Что за зверь – вирус подмены страниц ?

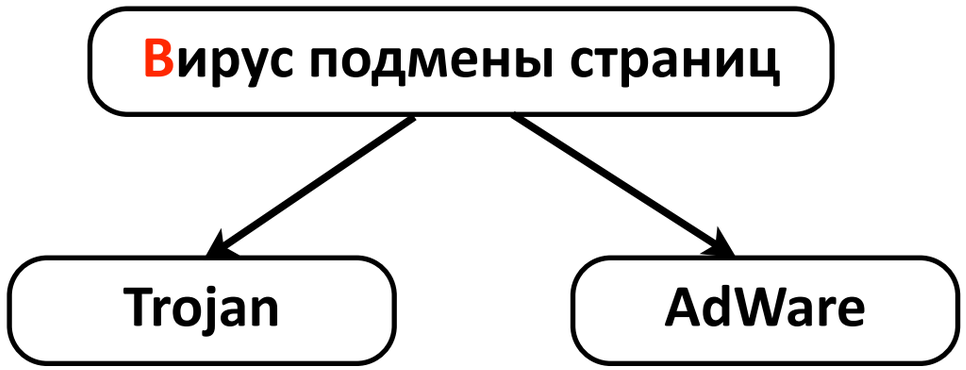
**Вирус подмены страниц** – это злонамеренный программный код влияющий на качество работы поисковых веб-сервисов на стороне пользователя, посредством модификации страницы с результатами поиска или изменения поведения браузера при кликах на ссылки.

# Что за зверь – вирус подмены страниц ?

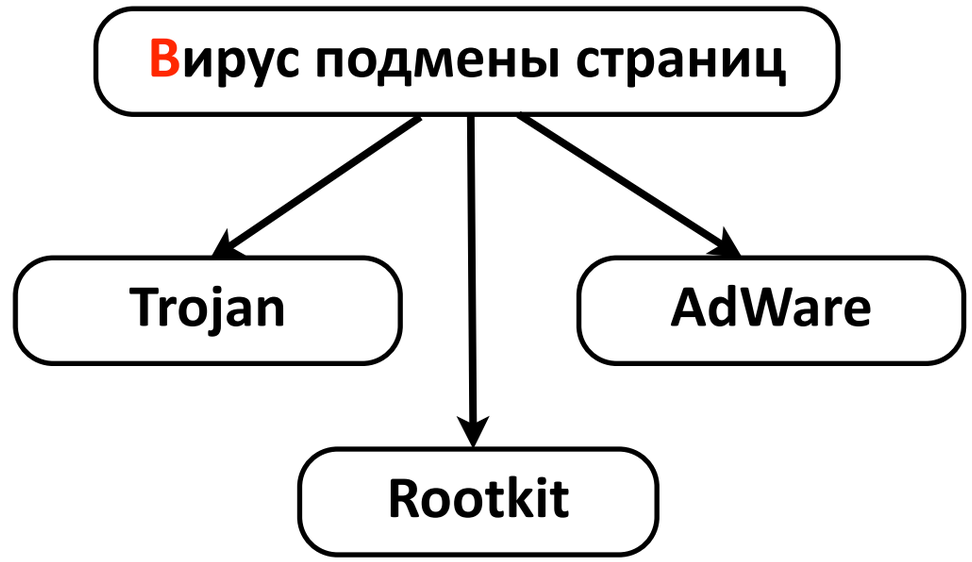
# Что за зверь – вирус подмены страниц ?



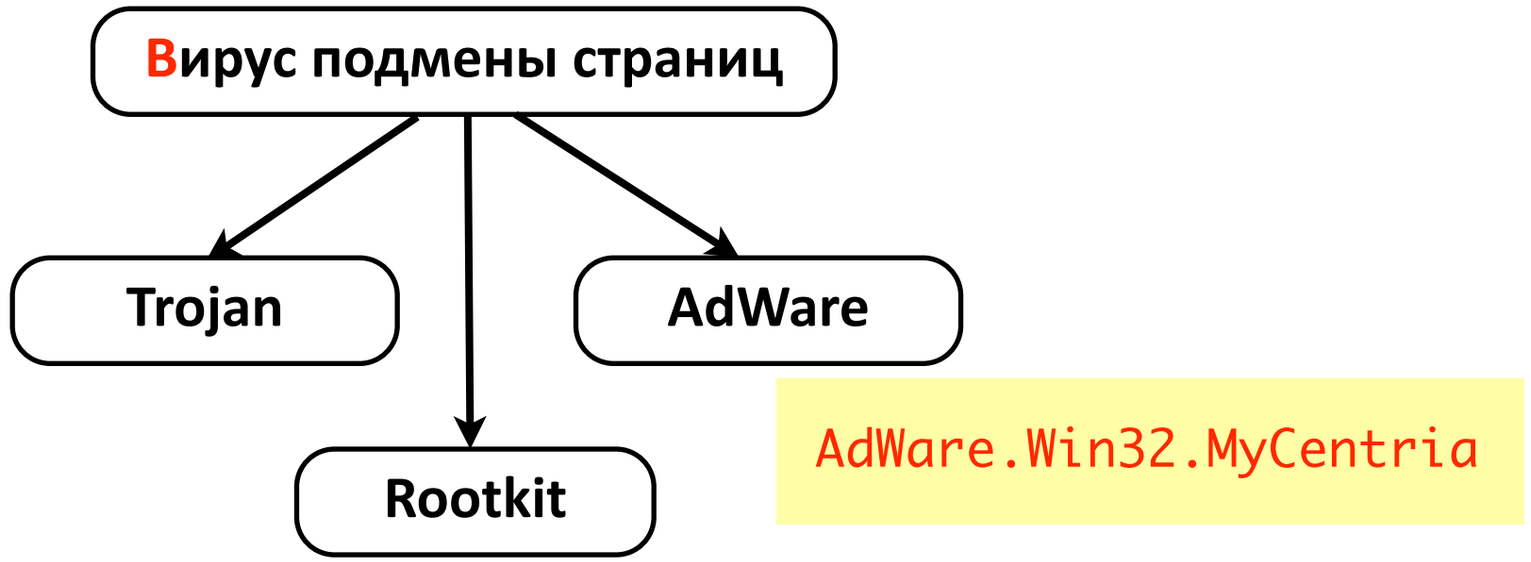
# Что за зверь – вирус подмены страниц ?



# Что за зверь – вирус подмены страниц ?

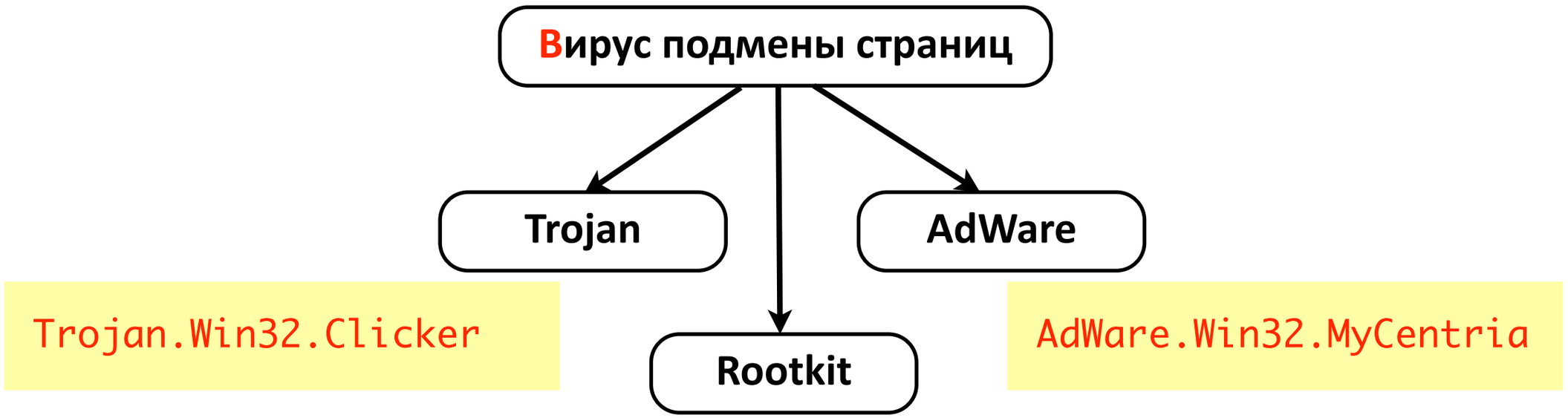


# Что за зверь – вирус подмены страниц ?

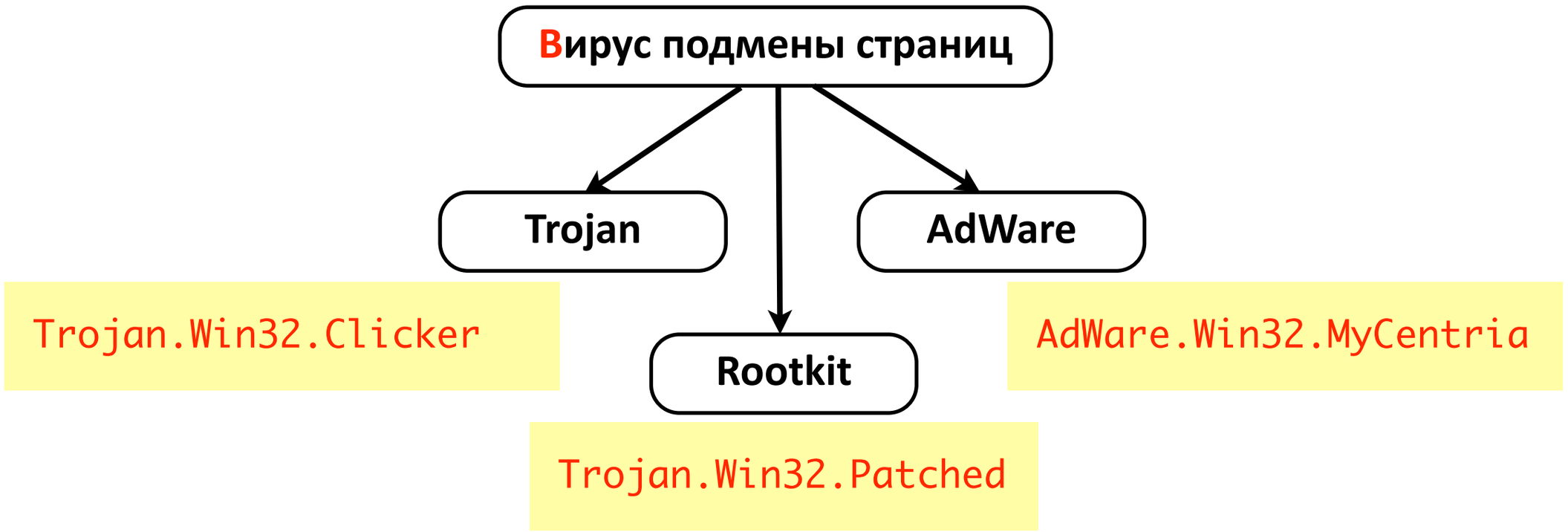



AdWare.Win32.MyCentria

# Что за зверь – вирус подмены страниц ?



# Что за зверь – вирус подмены страниц ?



# Выдержки из лицензионного соглашения для Adware

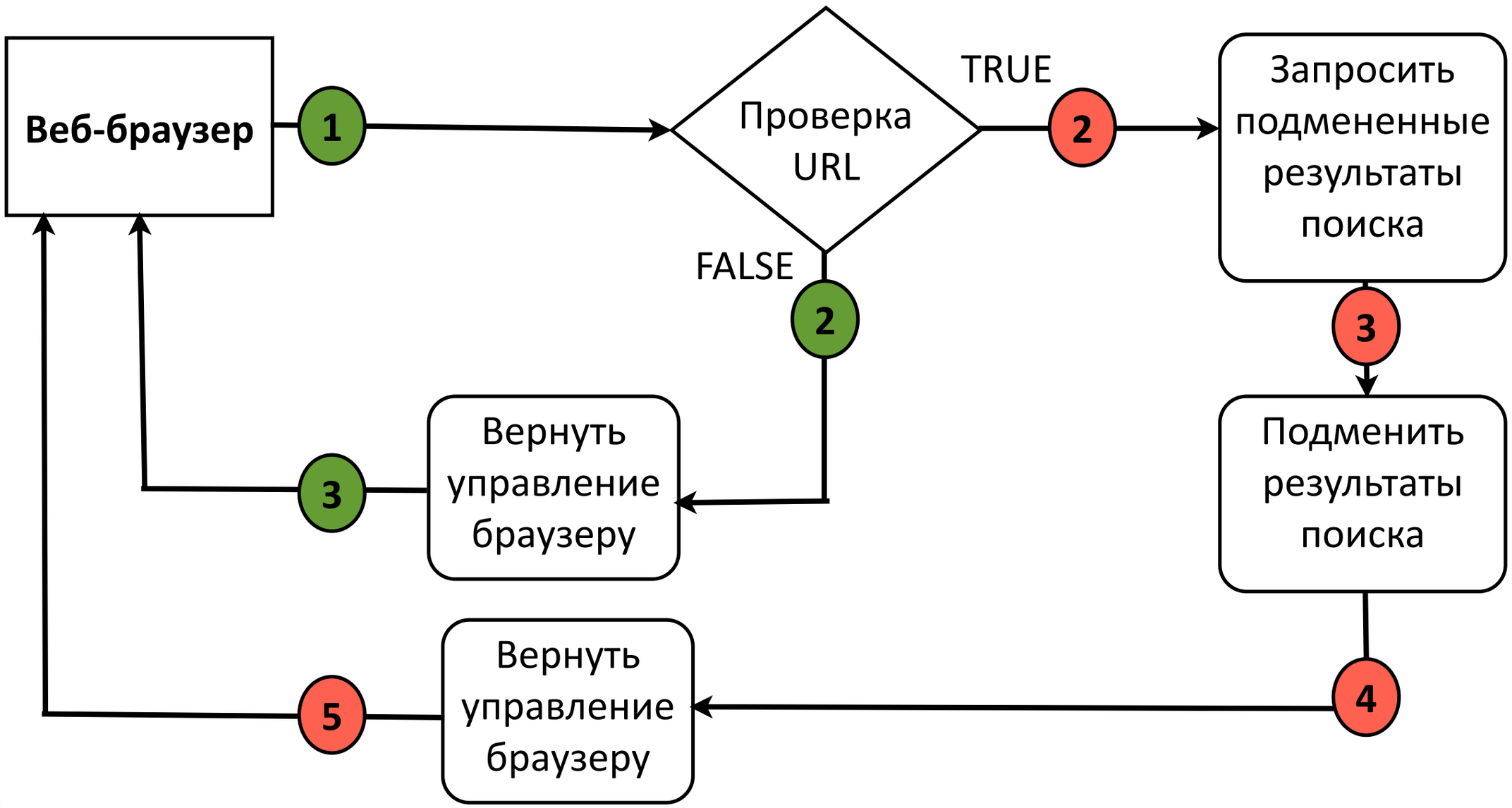
- «Информационная панель», размещенная внизу браузера, отображает ссылки на коммерческие и некоммерческие сайты исходя из содержания страницы.

- Компания по своему усмотрению может проводить обновления и / или улучшения программного обеспечения, как часть данного соглашения.

- Пользователь обязуется не совершать обратный анализ и декомпиляцию предоставляемого программного обеспечения.

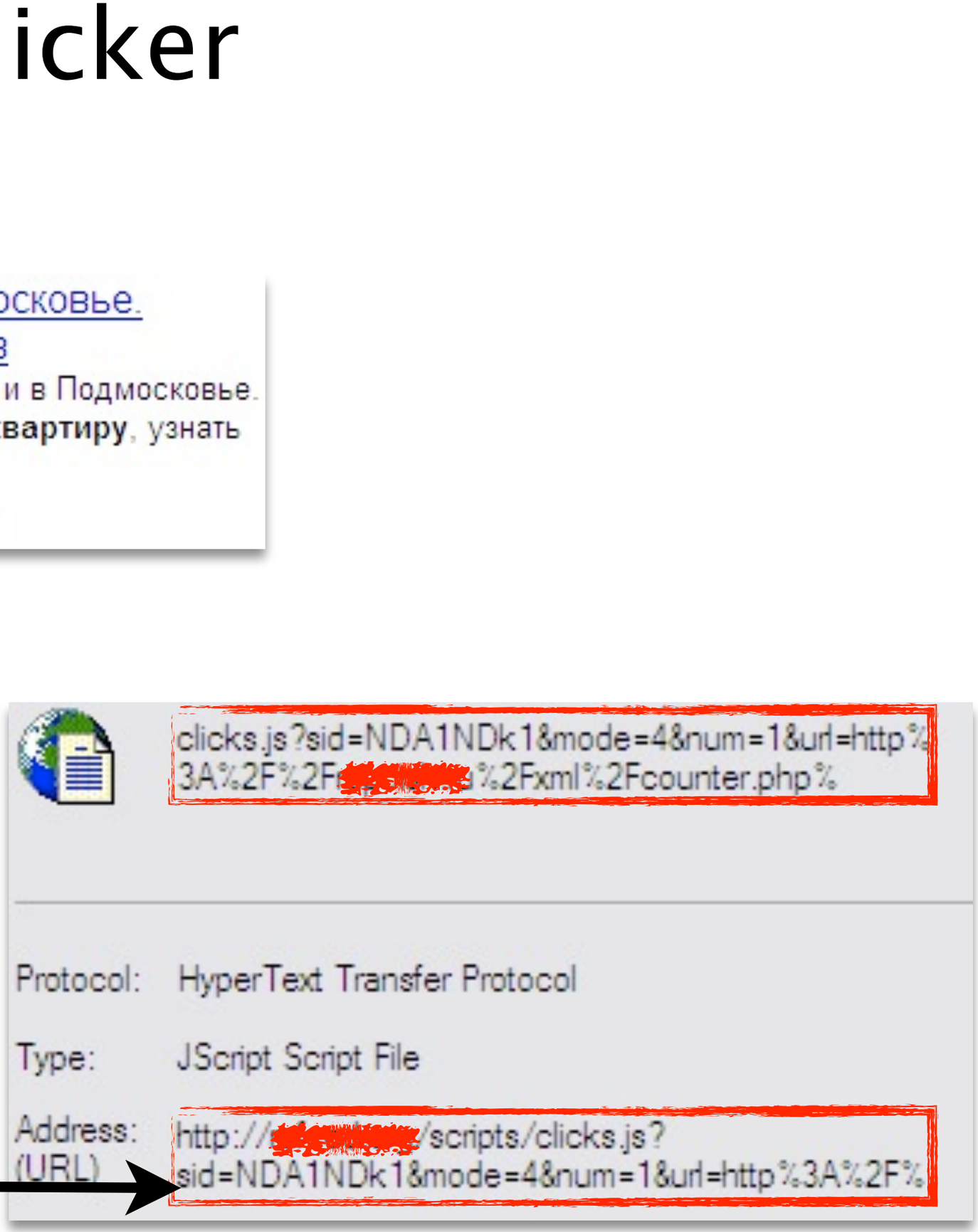
# Trojan.Win32.Clicker

## Алгоритм подмены результатов поиска:



# Trojan.Win32.Clicker

**Квартиры в Москве**. **Квартиры** в Подмосковье.
Стоимость **квартир**, цены на **квартиры** в
В каталоге сайта вы найдете **квартиры в Москве** и в Подмосковье. Эксперты помогут вам купить, продать, обменять **квартиру**, узнать цены на **квартиры в Москве**.
www.incom.ru/our-services/realty/?page=256 - 7 КБ



# Способы доставки и распространения

# Способы доставки и распространения

- **Trojan-Downloders** – доставка и установка злонамеренного кода.

# Способы доставки и распространения

- **Trojan-Downloders** – доставка и установка злонамеренного кода.

- **Софт-порталы** – распространение легальных и широко распространенных программ вместе с AdWare.

# Способы доставки и распространения

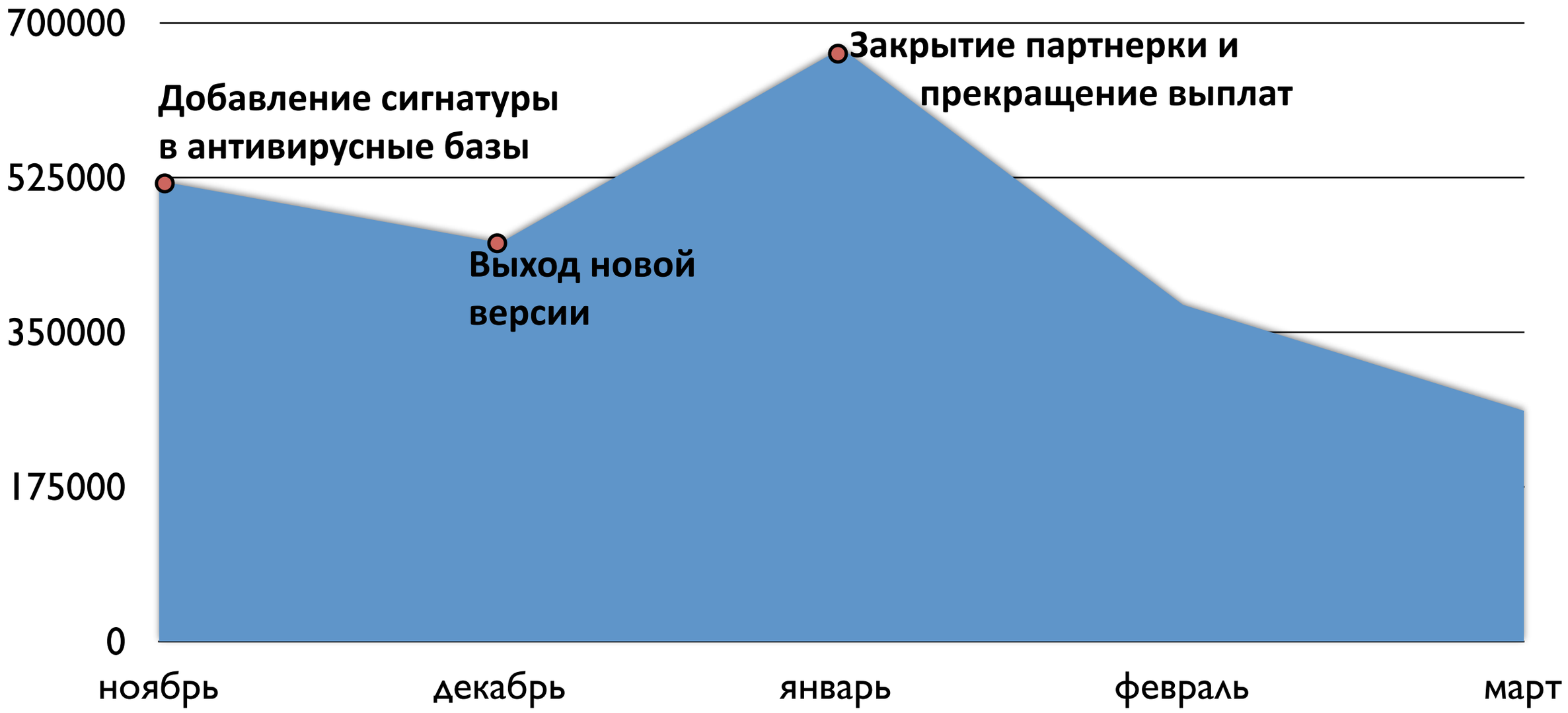
- **Trojan-Downloders** – доставка и установка злонамеренного кода.
- **Софт-порталы** – распространение легальных и широко распространенных программ вместе с AdWare.
- **Злонамеренные web-ресурсы** – сайты, предлагающие вам установить дополнительный плагин или кодек для более эффективной работы.

# Способы доставки и распространения

- **Trojan-Downloders** – доставка и установка злонамеренного кода.
- **Софт-порталы** – распространение легальных и широко распространенных программ вместе с AdWare.
- **Злонамеренные web-ресурсы** – сайты, предлагающие вам установить дополнительный плагин или кодек для более эффективной работы.
- **Другие способы ...**

# Масштабы угрозы

# Масштабы распространения Adware

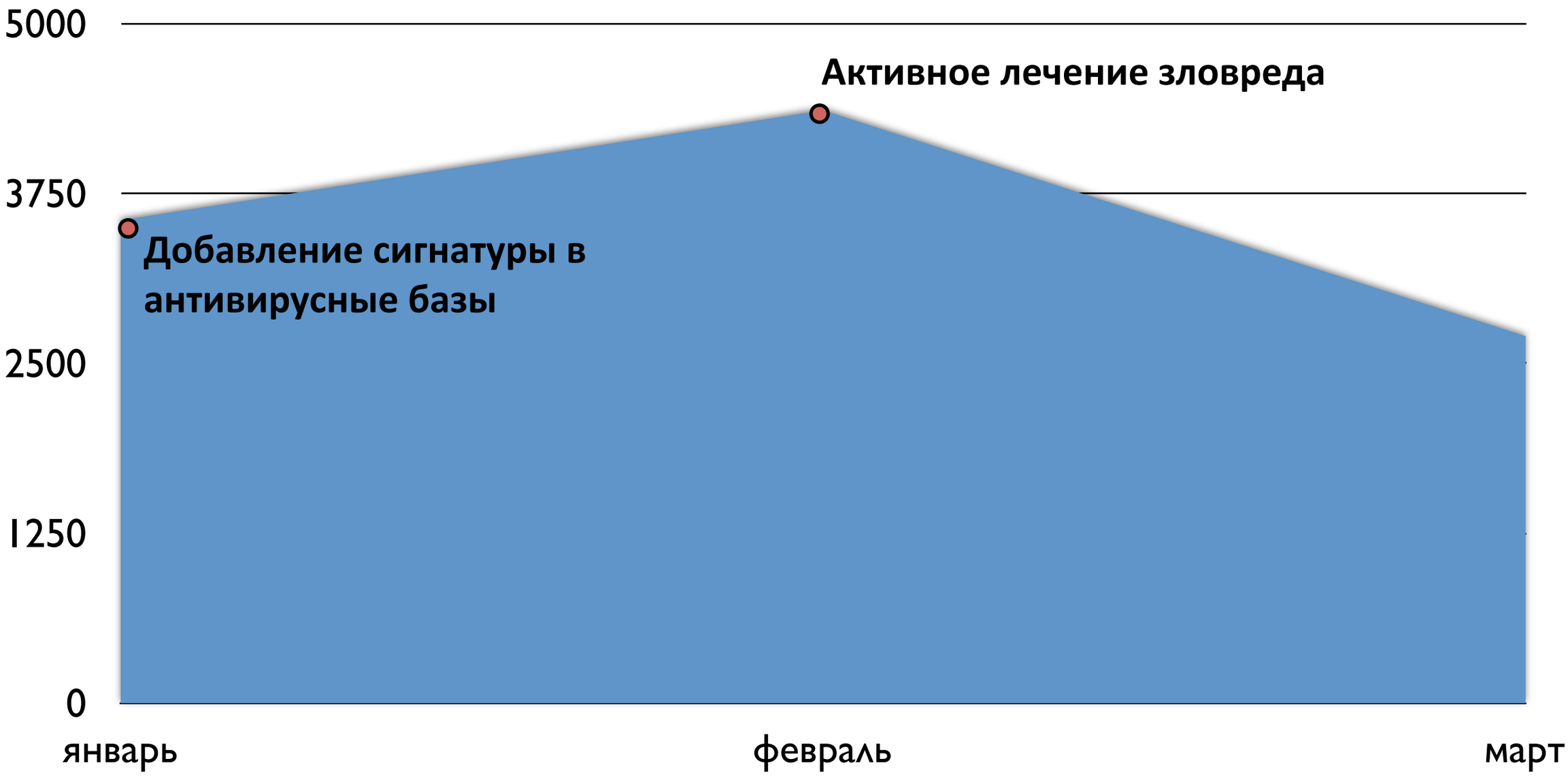



* по данным мониторинга компании Яндекс

# Проблемы

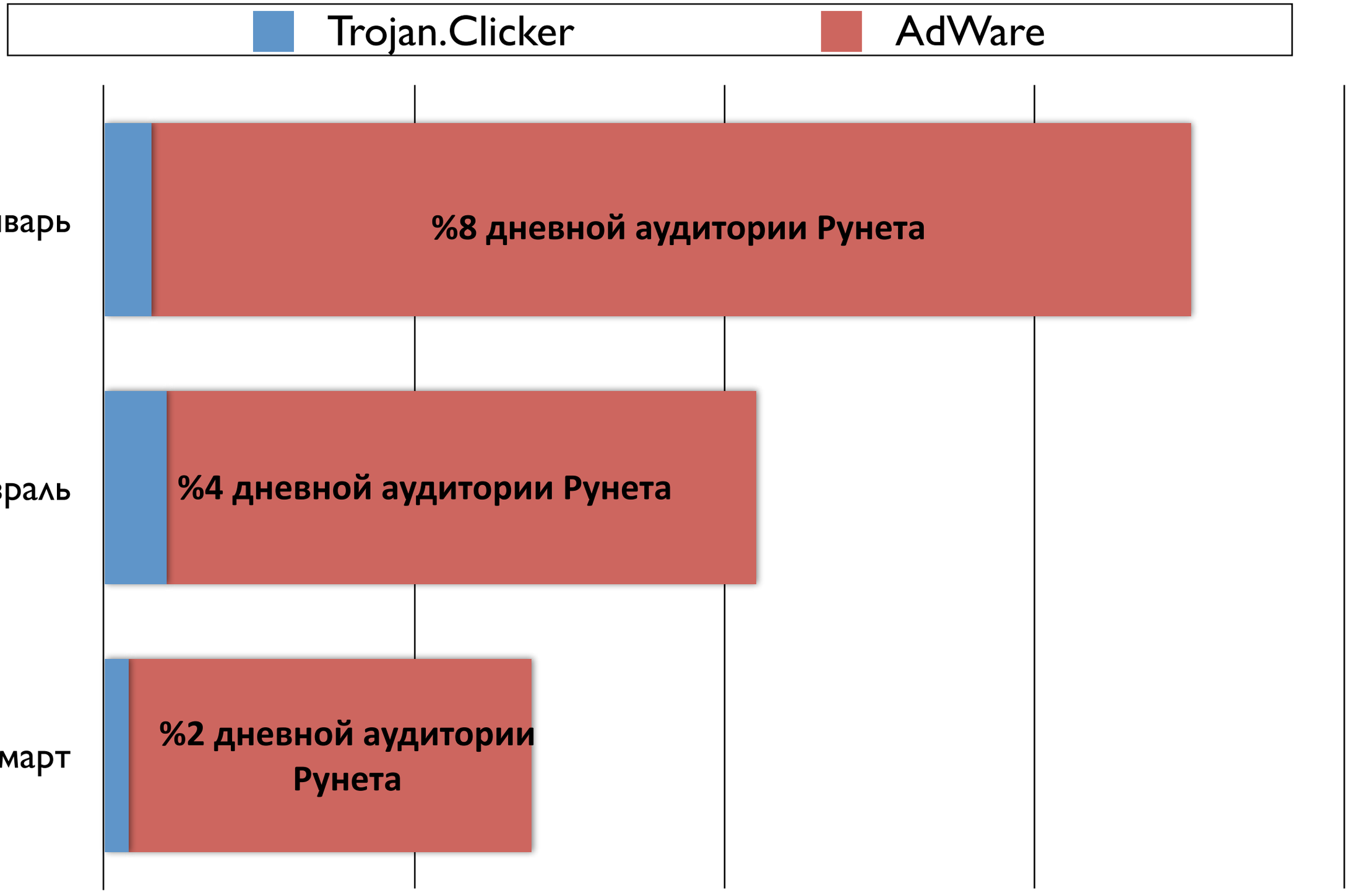
- Мягкие вердикты антивирусных компаний
- Большие масштабы распространения
- Приток новых зараженных пользователей превышает число  вылеченных
- Только неплатежи со стороны партнерки влияют на масштабы распространения

# Масштабы распространения Trojan.Clicker




* по данным http://stat.drweb.com

# AdWare vs Trojan



# Сколько на этом зарабатывают?

# Как на этом зарабатывают?

## Монетизация кликов:

- Редирект на рекламные площадки
- Контекстная реклама в дополнительном фрейме
- Редирект сразу на проплаченные сайты
- Другие ...

# Сколько на этом зарабатывают?

**Примерная оценка дневного заработка:**

средняя цена
за клик

**3 * 175 000 = 525 000 руб**

2% дневной
аудитории

*самые дорогие клики:
http://habrahabr.ru/blogs/begun/38901/

# Противодействие угрозе

# Как мы боремся с этой угрозой

- Взаимодействие с другими поисковыми системами
- Включение сигнатур в антивирусные базы
- Мониторинг угрозы, поиск новых экземпляров и противодействие им
- Работа с зараженными пользователями

# Как бороться с этой угрозой ?

# На сладкое …

# Trojan.Win32.Patched

Описание вредоносного функционала:

- ✳ Подмена результатов поиска
- ✳ Подмена контекстной рекламы
- ✳ Перенаправление всех поисковых запросов
- ✳ Работает независимо от браузера

*краткое описание зловреда от DrWeb:
http://news.drweb.com/show/?i=152&c=5&p=4

*статистика обнаружения по данным ресурса VirusTotal:
http://www.virustotal.com/ru/analisis/5ab81f809db8dd7b4276d090b932de71

# Trojan.Win32.Patched

## Деструктивная активность:

- ✳ Модифицируется системная библиотека ws2_32.dll
- ✳ Перехват экспроприируемых функций из ws2_32.dll
- ✳ Мониторинг информации в сетевых запросах
- ✳ Модификация сетевого трафика

*скачать зараженный сэмпл ws2_32.dll можно здесь:
http://www.offensivecomputing.net/?q=ocsearch&ocq=ba7b480af8293d78f0a7430100eb3de1


**Александр Матросов**

matrosov@yandex-team.ru

safesearch@yandex-team.ru