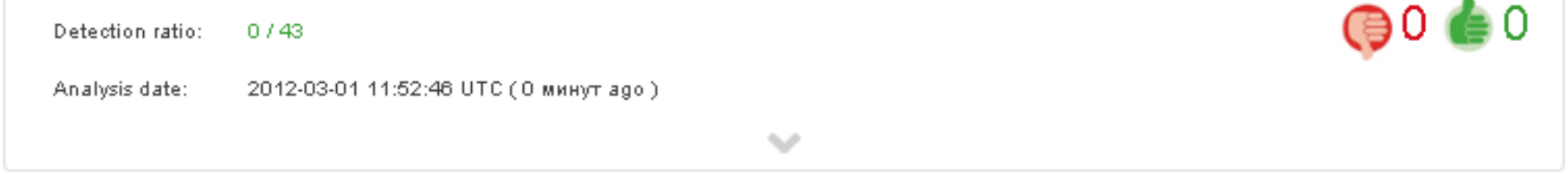



| Antivirus | Result | Update |
|---|---|---|
| DrWeb | - | 20120301 |
| Emsisoft | - | 20120301 |
| eSafe | - | 20120229 |
| Fortinet | - | 20120229 |
| GData | - | 20120301 |

# Тренды сетевых атак вызванных активными действиями пользователей:честная и нечестная монетизация бесплатных ресуров.

Данные на период:12/2011-03/2012



Vladimir B. Kropotov, Fyodor Yarochkin

# Об авторах и источниках информации

Мы – независимые иследователи криминальной активности в Интернет.

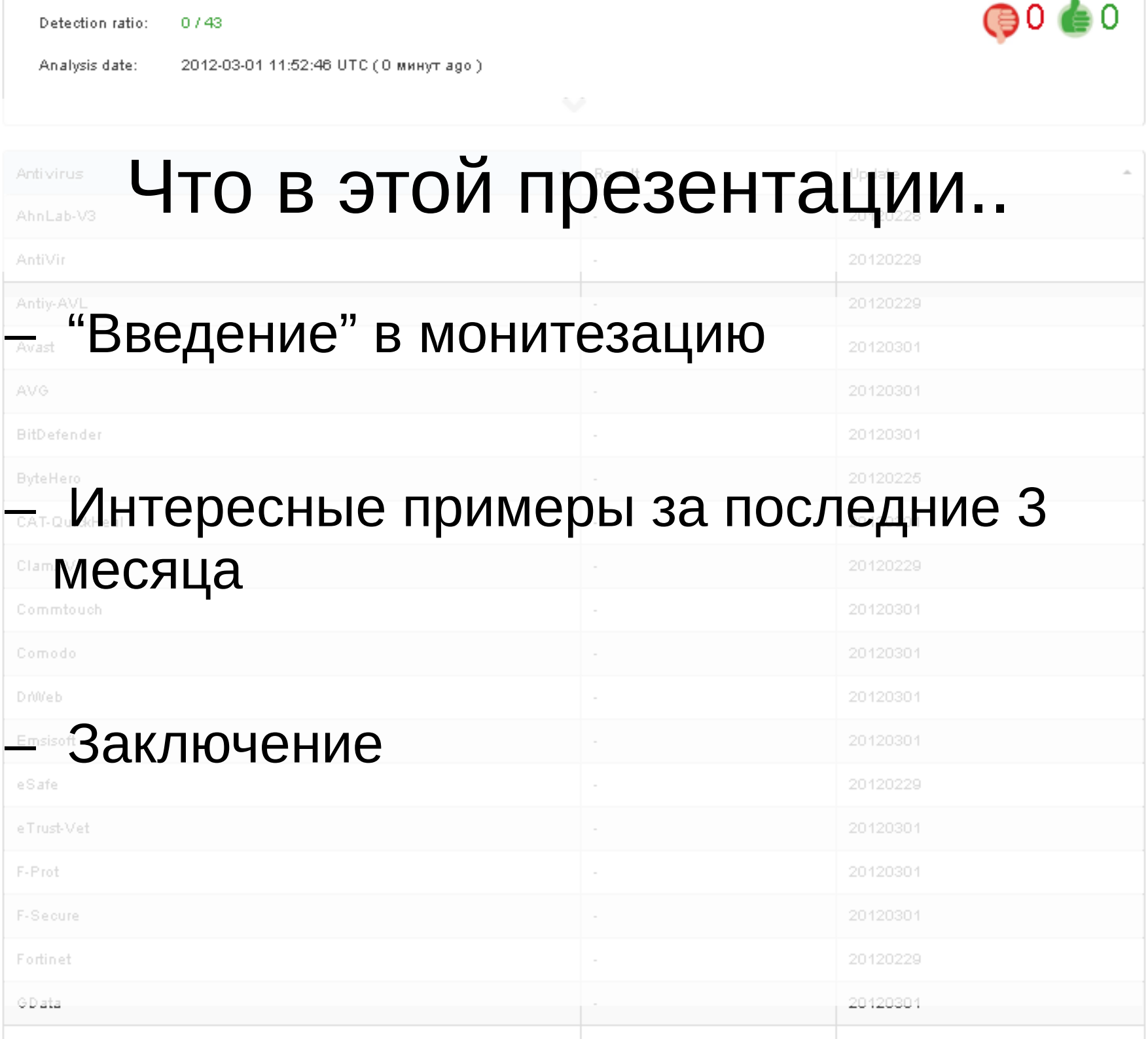
Источники данных

– отслеживание системных логов

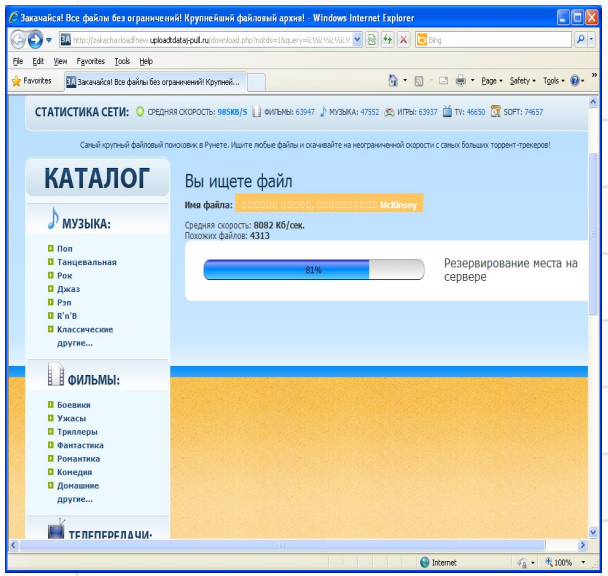
– системы  обнаружения атак

– проактивное исследование сети

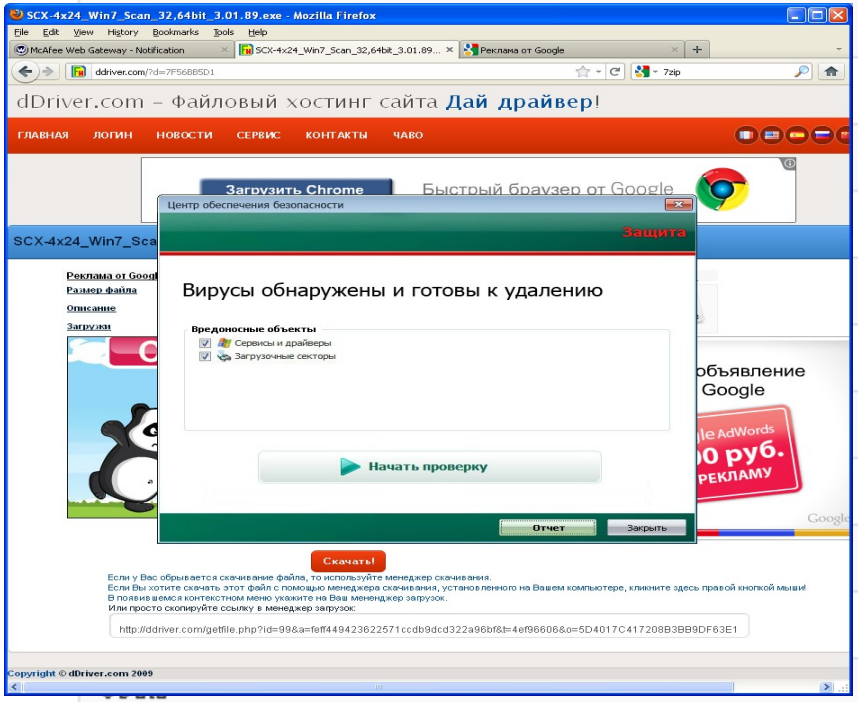
– пассивные и активные “приманки” и др.


Detection ratio: 0 / 43
0 0
Analysis date: 2012-03-01 11:52:46 UTC ( 0 минут ago )
Что в этой презентации..
– “Введение” в монитезацию
– Интересные примеры за последние 3 месяца
– Заключение

# Что общего между этими ресурсами?









Бесплатный сыр только в мышеловке!

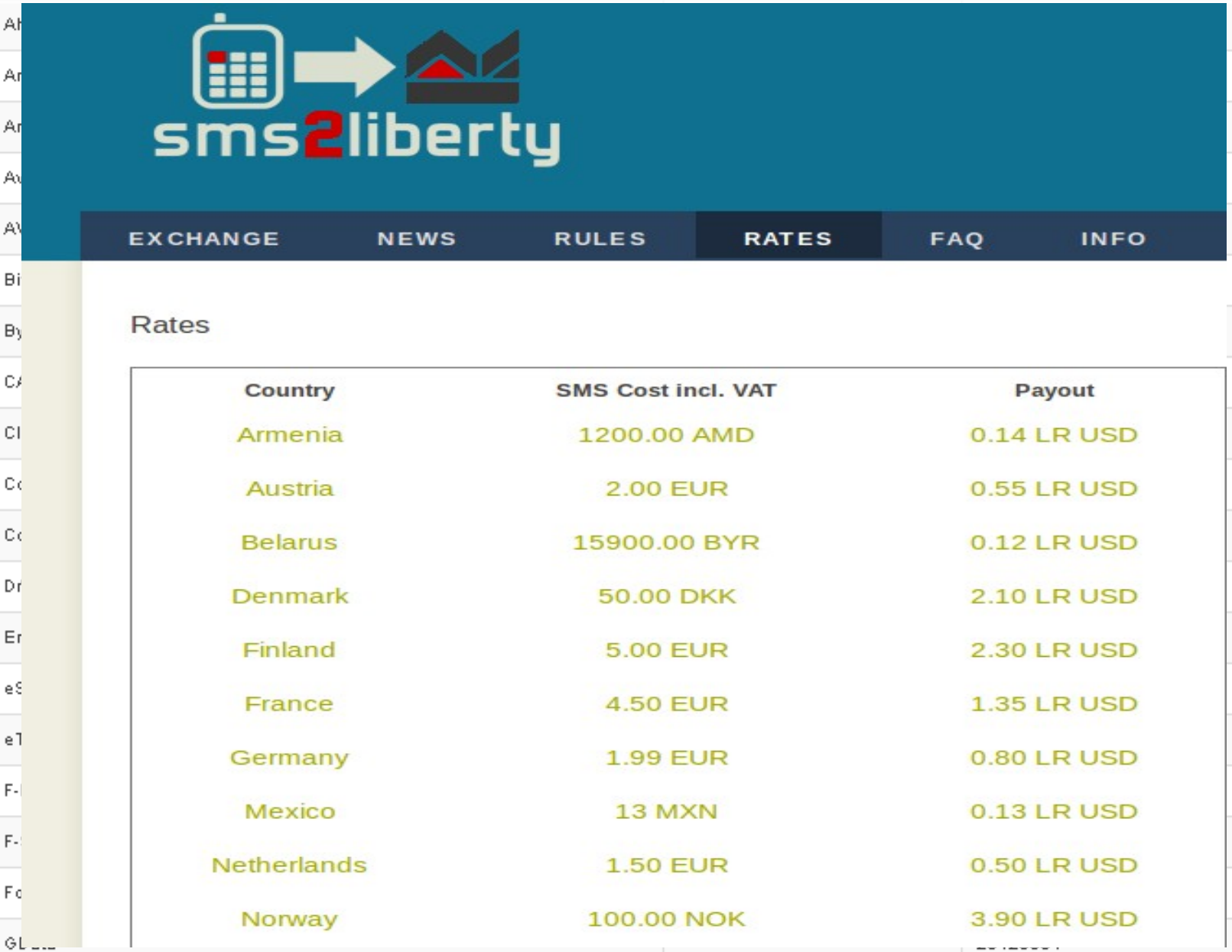
Но ведь мышеловку можно и сломать

# Телефон – современный “кошелек”

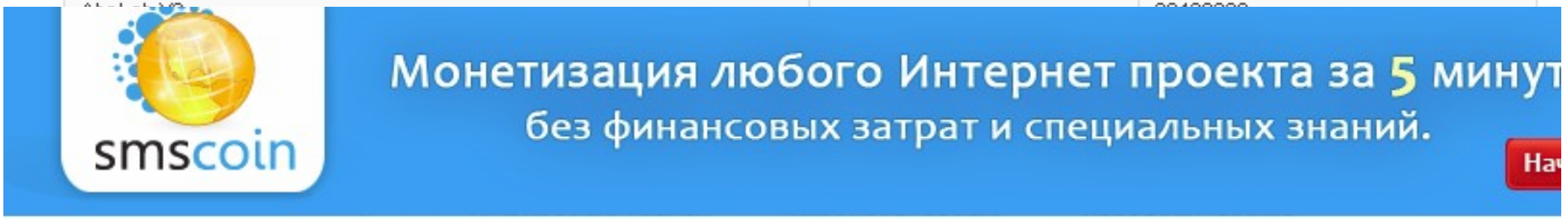
Баланс может быть переведен в наличные

- через короткие сообщения на платные номера
- через “подписывание” абонента на платную услугу (“контент провайдер”)
- через прямой перевод баланса (оффициально доступно в Индии, странах Африки)

# Перевод СМС в Деньги: вполне легальный бизнес



# Перевод СМС в Деньги: вполне легальный бизнес




## СНГ (10)

- Армения
- Азербайджан
- Беларусь
- Грузия
- Казахстан
- Киргизия
- Молдавия
- Россия
- Таджикистан
- Украина

## Европа (35)

- Австрия
- Албания
- Бельгия
- Болгария
- Босния и Герцеговина
- Великобритания
- Венгрия
- Германия
- Греция
- Дания
- Ирландия
- Испания
- Италия
- Кипр
- Косово
- Латвия
- Литва
- Люксембург
- Македония

## Азия и Океания(11)

- Австралия
- Вьетнам
- Гонконг
- Индия
- Индонезия
- Камбоджа
- Китай
- Малайзия
- Новая Зеландия
- Таиланд
- Тайвань

## Америка (20)

- Аргентина
- Боливия

## Африка и Ближний Восток (16)

- Алжир
- Гана

Detection ratio: 0 / 43

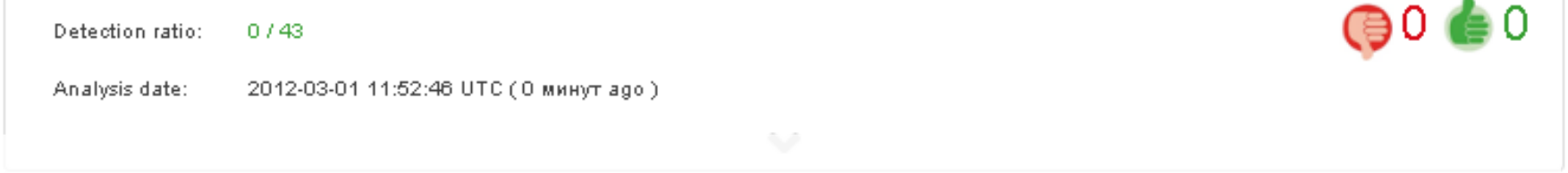
Analysis date: 2012-03-01 11:52:46 UTC ( 0 минут ago )

# Обнал. Баланса: М-ПЕСА в Кении (Индии, ..) похожий сервис доступен и по россии


**FREXsk** -> *Обналичу баланс Билайн (на WebMoney)* (28.11.2010 3:01:59)

Обналичу баланс с сим карт билайн, на вебманей - следующим способом.
Вы мне с симки переводите средства на мой номер, я перевожу 60% от суммы на Ваш кошелек. Принимаю любые деньги, кроме корпоративных сим. Суммы от 200 руб до - 5000 за ра
Гарантии - БЛ 300 Перс Атт.
ICQ - 3-856-шесть-шесть-шесть

| | | |
|---|---|---|
| Fortinet | - | 20120229 |
| GData | - | 20120301 |




# Как монетизировать?

- Деньги с телефона при отправке СМС сообщений на короткие номера самим пользователем
- Деньги с телефона, через подписку на платные СМС сервисы
- Получение денег напрямую с сотового телефона
- Монетизация через заражение ПК и использование украденных с ПК данных

# Деньги с телефона при отправке СМС сообщений на короткие номера

Механизм:

По соглашению с Телекомом Контент-провайдер получает процент от денег, зарабатываемых за счет отправки сообщений пользователями на короткие номера

Как правило, информация о том, что услуга платная указана на сайте

Управление предприятием
Управление бизнес проектами и консалтинг
Интернет коммерция
Экономическая статистика
Экономика
Другая бизнес литература

Бауэр сформировал новый подход к управлению в бизнесе, основанный на лучших человеческих качествах: уважении к людям, чувстве собственного достоинства и смелости.
Его концепция лидерства заключается в том, что каждый сотрудник вносит неоценимый вклад в общее руководство организации, максимально проявляя свои профессиональные и лидерские способности в соответствии с ценностными ориентирами компании.
Элизабет Эдершайм прослеживает жизненный путь этого необыкновенного человека, а также размышляет над тем, что сделало его компанию неоспоримым лидером в своей области, среди клиентов которой — не только крупнейшие мировые корпорации, но и американское правительство.
Книга адресована руководителям, предпринимателям, а также специалистам в области консалтинга.

## Где скачать бесплатно книгу Эдершайм Э. Марвин Бауэр, основатель McKinsey & Company: стратегия, лидерство, создание управленческого консалтинга?



В нашем большом каталоге книг по бизнесу представлено более десяти тысяч наименований. Тут книгу можно **скачать бесплатно Эдершайм Э. Марвин Бауэр, основатель McKinsey & Company: стратегия, лидерство, создание управленческого консалтинга** в формате pdf, djvu, doc, txt, rtf, rar. Для этого используйте ссылки, представленные выше. {ссылки временно недоступны}

**Скачать Марвин Бауэр, основатель McKinsey & Company: стратегия, лидерство, создание управленческого консалтинга**

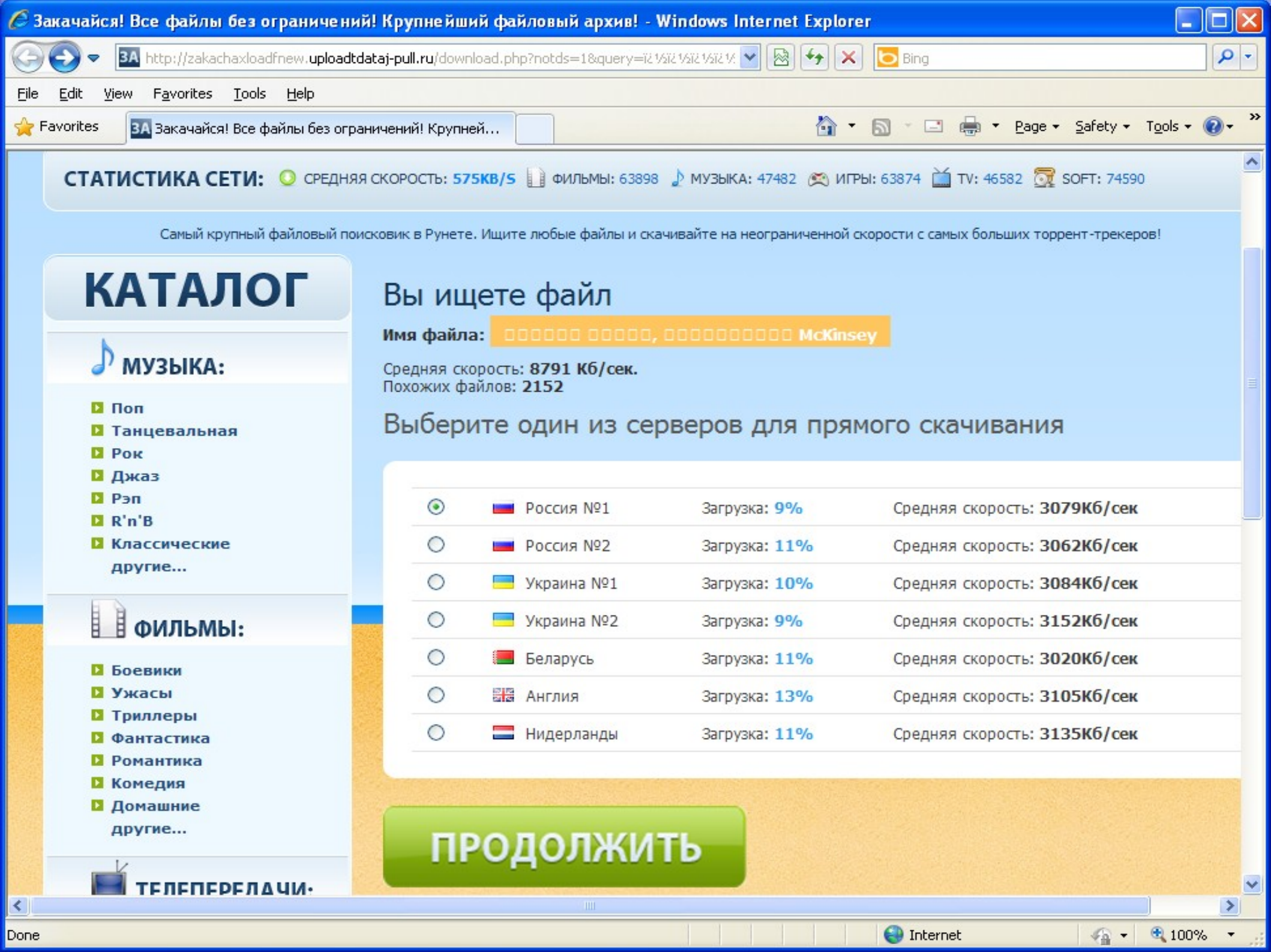
Голосовать
Результаты опрос

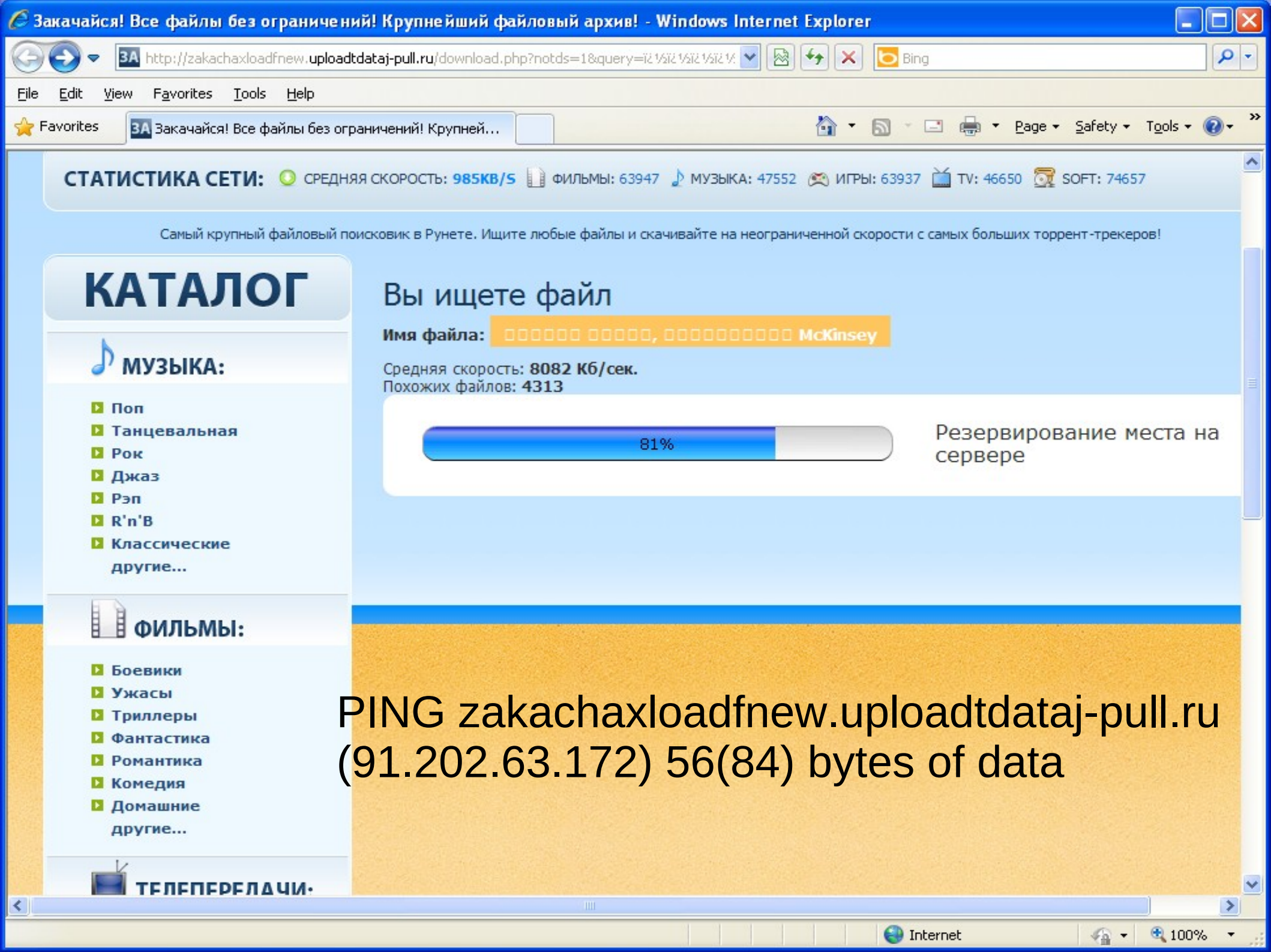
Популярные книги:

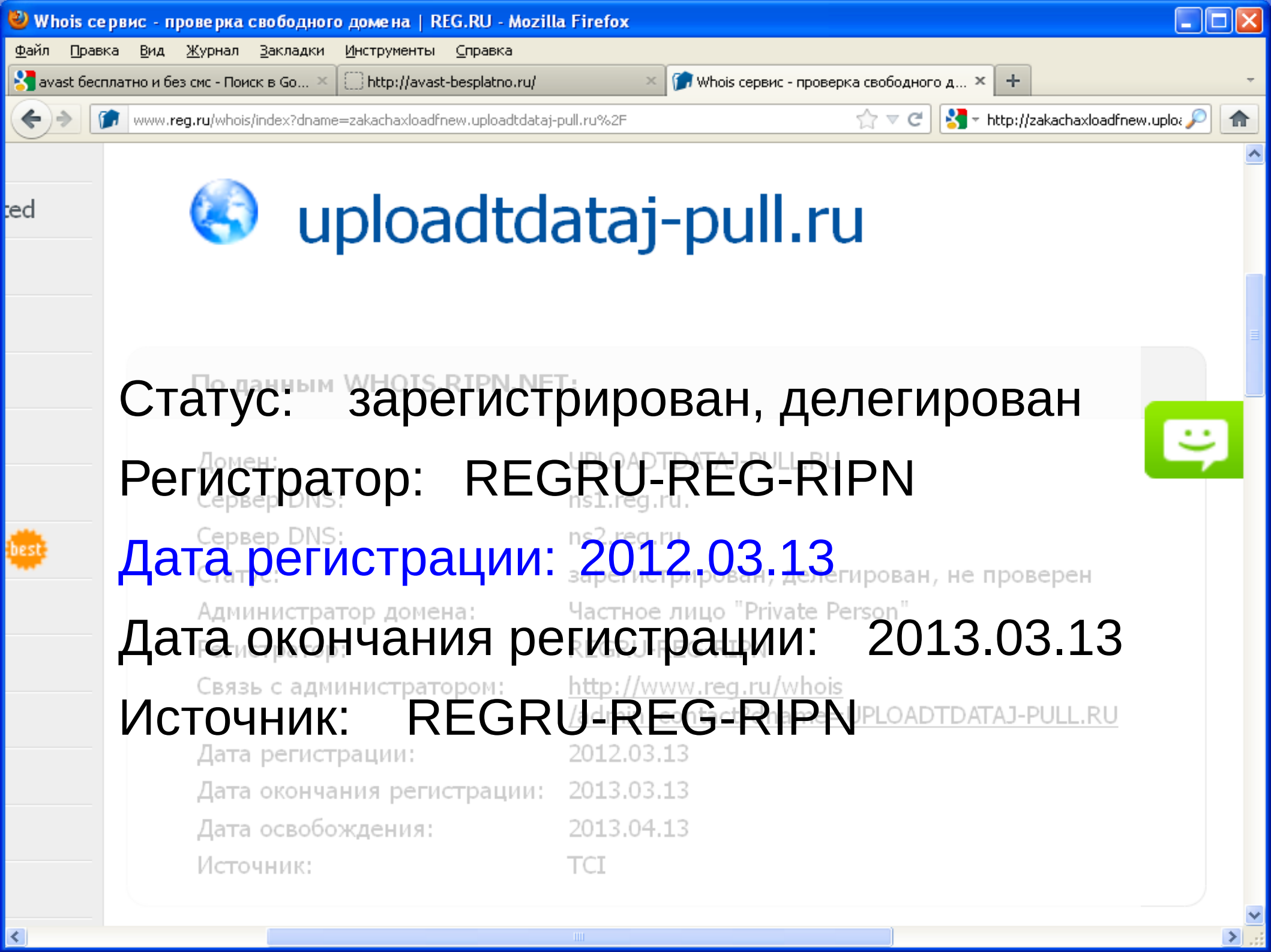
Самые богатые евреи мира бизнес-династий скачать бесплатно

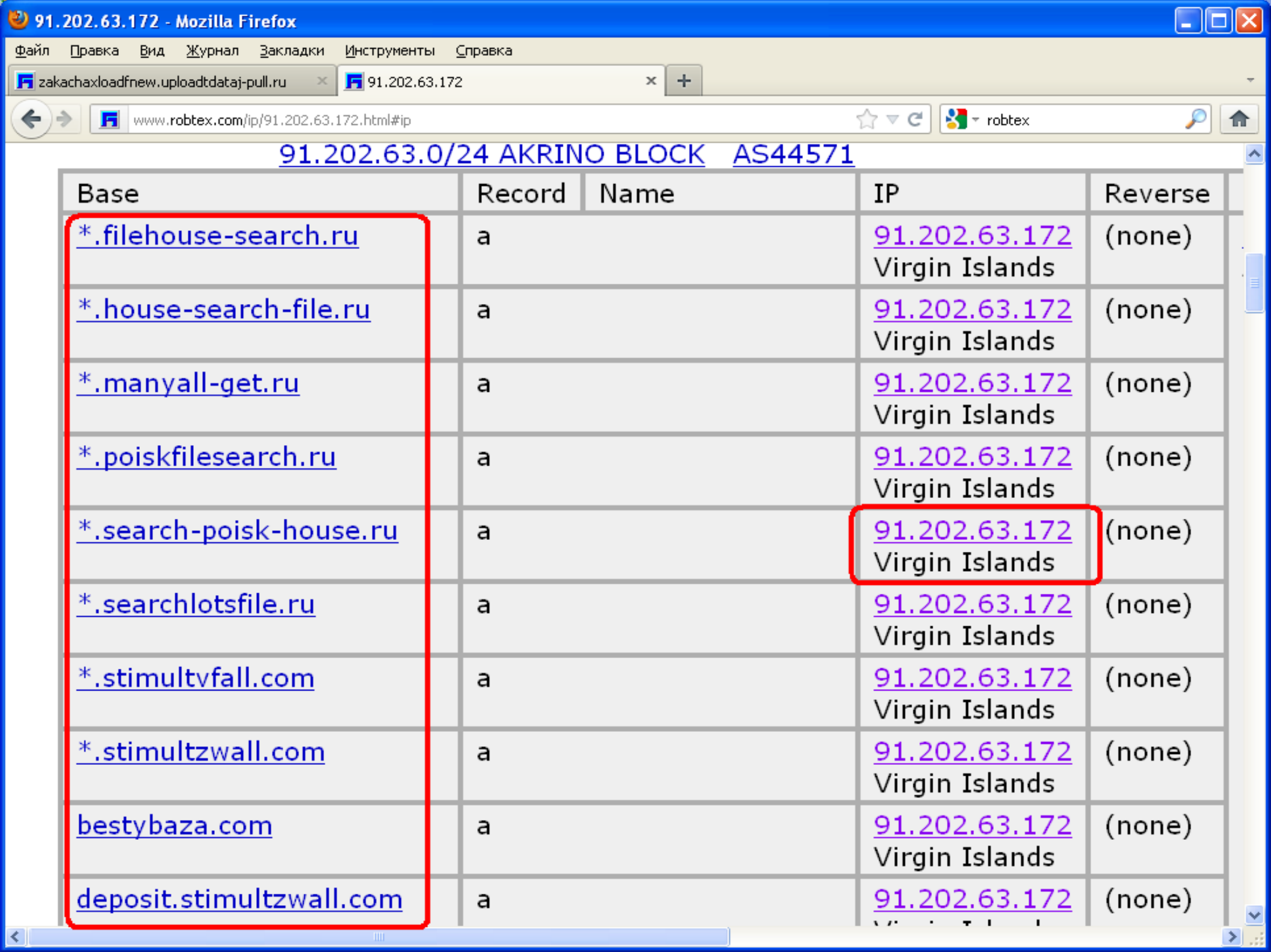

Повышение эффективности бюджетных расходов скача бесплатно

Популярное
» Как привлечь зарубежные инвестиции
» Скажем переработкам НЕТ!
» Статистика. Учебное пособие
» Богатый папа, бедный папа для подростков
» План счетов бухгалтерского учета. Комментарии к примене ...
» ВТО: введение в правовую


Закачайся! Все файлы без ограничений! Крупнейший файловый архив! - Windows Internet Explorer
http://zakachaxloadfnew.uploadtdataj-pull.ru/download.php?notds=1&query=
Bing
File Edit View Favorites Tools Help
Favorites
Закачайся! Все файлы без ограничений! Крупней...
Page Safety Tools
СТАТИСТИКА СЕТИ: СРЕДНЯЯ СКОРОСТЬ: 575KB/S ФИЛЬМЫ: 63898 МУЗЫКА: 47482 ИГРЫ: 63874 TV: 46582 SOFT: 74590
Самый крупный файловый поисковик в Рунете. Ищите любые файлы и скачивайте на неограниченной скорости с самых больших торрент-трекеров!
КАТАЛОГ
МУЗЫКА:
Поп
Танцевальная
Рок
Джаз
Рэп
R'n'B
Классические
другие...
ФИЛЬМЫ:
Боевики
Ужасы
Триллеры
Фантастика
Романтика
Комедия
Домашние
другие...
Вы ищете файл
Имя файла: McKinsey
Средняя скорость: 8791 Кб/сек.
Похожих файлов: 2152
Выберите один из серверов для прямого скачивания
Россия №1 Загрузка: 9% Средняя скорость: 3079Кб/сек
Россия №2 Загрузка: 11% Средняя скорость: 3062Кб/сек
Украина №1 Загрузка: 10% Средняя скорость: 3084Кб/сек
Украина №2 Загрузка: 9% Средняя скорость: 3152Кб/сек
Беларусь Загрузка: 11% Средняя скорость: 3020Кб/сек
Англия Загрузка: 13% Средняя скорость: 3105Кб/сек
Нидерланды Загрузка: 11% Средняя скорость: 3135Кб/сек
ПРОДОЛЖИТЬ
Done
Internet
100%

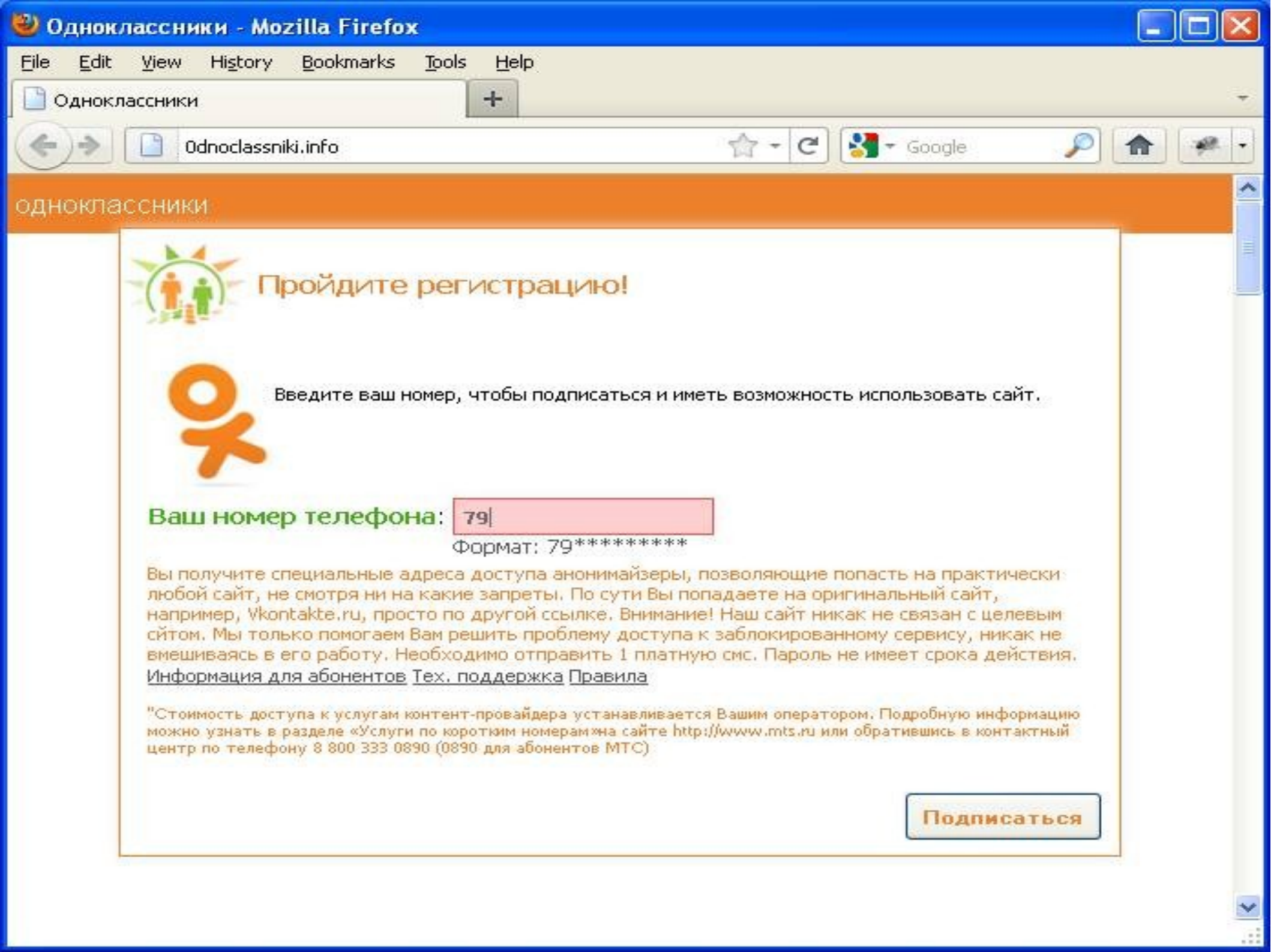

Закачайся! Все файлы без ограничений! Крупнейший файловый архив! - Windows Internet Explorer
http://zakachaxloadfnew.uploadtdataj-pull.ru/download.php?notds=1&query=
Bing
File Edit View Favorites Tools Help
Favorites
Закачайся! Все файлы без ограничений! Крупней...
Page Safety Tools
СТАТИСТИКА СЕТИ: СРЕДНЯЯ СКОРОСТЬ: 985KB/S ФИЛЬМЫ: 63947 МУЗЫКА: 47552 ИГРЫ: 63937 TV: 46650 SOFT: 74657
Самый крупный файловый поисковик в Рунете. Ищите любые файлы и скачивайте на неограниченной скорости с самых больших торрент-трекеров!
КАТАЛОГ
МУЗЫКА:
Поп
Танцевальная
Рок
Джаз
Рэп
R'n'B
Классические
другие...
ФИЛЬМЫ:
Боевики
Ужасы
Триллеры
Фантастика
Романтика
Комедия
Домашние
другие...
Вы ищете файл
Имя файла: McKinsey
Средняя скорость: 8082 Кб/сек.
Похожих файлов: 4313
81%
Резервирование места на сервере
PING zakachaxloadfnew.uploadtdataj-pull.ru
(91.202.63.172) 56(84) bytes of data
Internet
100%


Whois сервис - проверка свободного домена | REG.RU - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
avast бесплатно и без смс - Поиск в Go...
http://avast-besplatno.ru/
Whois сервис - проверка свободного д...
www.reg.ru/whois/index?dname=zakachaxloadfnew.uploadtdataj-pull.ru%2F
http://zakachaxloadfnew.uplo
uploadtdataj-pull.ru
По данным WHOIS.RIPN.NET:
Домен: UPLOADTDATAJ-PULL.RU
Сервер DNS: ns1.reg.ru.
Сервер DNS: ns2.reg.ru.
Статус: зарегистрирован, делегирован, не проверен
Администратор домена: Частное лицо "Private Person"
Регистратор: REGRU-REG-RIPN
Связь с администратором: http://www.reg.ru/whois
Дата регистрации: 2012.03.13
Дата окончания регистрации: 2013.03.13
Дата освобождения: 2013.04.13
Источник: TCI
Статус: зарегистрирован, делегирован
Регистратор: REGRU-REG-RIPN
Дата регистрации: 2012.03.13
Дата окончания регистрации: 2013.03.13
Источник: REGRU-REG-RIPN




91.202.63.0/24 AKRINO BLOCK AS44571

| Base | Record | Name | IP | Reverse |
|---|---|---|---|---|
| *.filehouse-search.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.house-search-file.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.manyall-get.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.poiskfilesearch.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.search-poisk-house.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.searchlotsfile.ru | a | | 91.202.63.172 Virgin Islands | (none) |
| *.stimultvfall.com | a | | 91.202.63.172 Virgin Islands | (none) |
| *.stimultzwall.com | a | | 91.202.63.172 Virgin Islands | (none) |
| bestybaza.com | a | | 91.202.63.172 Virgin Islands | (none) |
| deposit.stimultzwall.com | a | | 91.202.63.172 | (none) |


Одноклассники - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Одноклассники
Odnoclassniki.info
Google
одноклассники
Пройдите регистрацию!
Введите ваш номер, чтобы подписаться и иметь возможность использовать сайт.
Ваш номер телефона: 79
Формат: 79*********
Вы получите специальные адреса доступа анонимайзеры, позволяющие попасть на практически любой сайт, не смотря ни на какие запреты. По сути Вы попадаете на оригинальный сайт, например, Vkontakte.ru, просто по другой ссылке. Внимание! Наш сайт никак не связан с целевым сйтом. Мы только помогаем Вам решить проблему доступа к заблокированному сервису, никак не вмешиваясь в его работу. Необходимо отправить 1 платную смс. Пароль не имеет срока действия.
Информация для абонентов Тех. поддержка Правила
"Стоимость доступа к услугам контент-провайдера устанавливается Вашим оператором. Подробную информацию можно узнать в разделе «Услуги по коротким номерам»на сайте http://www.mts.ru или обратившись в контактный центр по телефону 8 800 333 0890 (0890 для абонентов МТС)
Подписаться

Detection ratio: 0 / 43

Analysis date: 2012-03-01 11:52:46 UTC ( 0 минут ago )

0 0

# Информация о домене

Domain Name: 0DNOCLASSNIKI.INFO

Created On:24-Mar-2012 13:03:39 UTC

IP-адрес:173.245.61.111

Reverse DNS: Имя хоста

cf-173-245-61-111.cloudflare.com

Location: United States

| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | - | 20120228 |
| AntiVir | - | 20120229 |
| Antiy-AVL | - | 20120229 |
| Avast | - | 20120301 |
| AVG | - | 20120301 |
| BitDefender | - | 20120301 |
| ByteHero | - | 20120225 |
| CAT-QuickHeal | - | 20120301 |
| ClamAV | - | 20120229 |
| Commtouch | - | 20120301 |
| Comodo | - | 20120301 |
| DrWeb | - | 20120301 |
| Emsisoft | - | 20120301 |
| eSafe | - | 20120229 |
| ESET-NOD32 | - | 20120301 |
| F-Prot | - | 20120301 |
| F-Secure | - | 20120301 |
| Fortinet | - | 20120229 |
| GData | - | 20120301 |

# Деньги с телефона, через подписку на платные СМС сервисы

Механизм:

По соглашению с Телекомом Контент-провайдер может подписать абонента на Контент при предоставлении кода подтверждения

Получение кода подтверждения возможно через веб, но не только ...

Detection ratio: 0 / 43

Analysis date: 2012-03-01 11:52:46 UTC ( 0 минут ago )

0 0

# Формальности с телекомом. На примере: http://x-bill.ru/usl.php

***Наши Услуги:***

**1. Премиум – SMS** – это усл
сообщения на короткий номе
смс, цену короткого номера м

- ***Номера от 3 до 300 рубл***
- ***Индивидуальные префи***
- ***Подробная статистика***
- ***14 стран – список посто***

Подробнее

**2. MT подписка(Россия, Укр**
период времени, в течение
информацию/доступ/действи

- ***Тихие ребиллы***
- ***Четыре оператора для***
- ***Быстрое подключение***
- ***Помощь в настройки***
- ***МТС, Билайн ребиллы на***
- ***МТС, Билайн подключени***

Подробнее

1) Клиент сообщает свой MSISDN Web/WAP ресурсу. (MSISDN – номер телефона прим.)
2) Сайт отправляет запрос в систему на создание подписки (**CreateSubscription**), указывая MSISDN (номер клиента), StartTimeUtc (время отправки SMS PIN, обычно следует ставить текущее время), BillingStartTimeUtc (время первого платежа). Если биллинг для указанного MSISDN поддерживается и пройдены другие проверки, создается запись подписки. После чего следует перевести клиента на страницу ввода PIN-кода. MSISDN клиента рекомендуется сохранить (в cookies или другое хранилище) для дальнейшего использования в методе **ApproveSubscription**.
3) В момент времени, заданный в StartTimeUtc, клиенту отправляется SMS, содержащая PIN-код.
4) Клиент вводит PIN в форму на сайте.
5) Сайт отправляет запрос в систему на активацию подписки (**ApproveSubscription**), передавая MSISDN и PIN. Если PIN верный, подписка активируется. Дается 3 попытки подбора PIN. Если подписка не была активирована в течении 3 часов, запись аннулируется.
6) В случае успешной активации, сайт получает уведомление от системы об изменении статуса подписки.

**3. Псевдо подписки** – аналог автоматических MT подписок, с одноразовой тарификацией абонента. После того как абонент ввел свой номер на сайте, ему приходит бесплатное смс, которое содержит информацию, что нужно сделать для получения услуги на Вашем проекте, ответив на это сообщение произвольным текстом в абонента снимается «энная сумма». После

Поиск файлов

Фильмы:
11285 файла

Музыка:
91591 файла

Игры:
18281 файла

Софт:
56840 файла

## Что вы хотите найти?

Введите запрос для поиска...

Найти

Например, Пираты карибского моря

# Регистрация

**Для получения полного доступа**, а также возможности скачивать **без ограничения скорости**,

Введите Ваш номер телефона, на него придет SMS с **кодом активации**, чтобы подписаться на услугу

например: +79008007060

Зарегистрироваться

Если Вам уже известен код, введите его здесь

# Телеком в доле:







ДАТА: 20 МАР 2012 КОММ: 0 КОММЕНТ

## Подробная информация по номеру 770109. Как отписаться / отказаться от услуги.

Наименование контент-провайдера i-Free Тариф Стоимость СМС 3,39 руб.с НДС Горячая линия +7 (812) 43 81 679 Сайт

ДАТА: 20 МАР 2012 КОММ: 0 КОММЕНТ

## Подробная информация по номеру 7222. Как отписаться / отказаться от услуги.

Наименование контент-провайдера Связной Загрузка Тариф Стоимость СМС 16,94 руб.с НДС Горячая линия +7 (495) 28 70 333 Сайт

сразу проверяю, и сняли 98руб !!!! после чего залез на этот самый сайт и увидел что можно отписаться введя свой имей...

Стандартные действия, актуальны [...]

подсказкам меню и отключаем [...]

ДАТА: 19 МАР 2012 КОММ: 0 КОММЕНТ

## Подробная информация по номеру 770654. Как отписаться / отказаться от услуги.

Наименование контент-провайдера Информ-мобил (ИММО) Тариф Стоимость СМС 1,5 руб.с НДС Горячая линия +7 (495) 99 58 995 Сайт контент-провайдера www.inform-mobil.ru Как отписаться от рассылки Для остановки услуги «Подписка на новости»

ДАТА: 18 МАР 2012 КОММ: 0 КОММЕНТ

## Популярные схемы SMS-мошенничества.

Защита от компьютерного вируса Ваш компьютер заражается вредоносной программой, которая блокирует или нарушает его работу, Вам предлагают отправить SMS-сообщение на короткий номер, чтобы разблокировать компьютера. После тог как SMS отправлено разблокировки не происходит, а

# Деньги с телефона после скачивания файла

Механизм: Вам дают возможность бесплатно скачать файл. Как правило это файл с двойным расширением, например zip.exe.

Далее, после запуска файла Вас просят ввести номер телефона для продолжения распаковки скачанного содержимого.


# Пример события IDS в Январе

**Date/Time 2012-01-30 14:44:28 MSK**

**Tag Name HTTP_Executable_Transfer**

**:arg id=101956&size=45223**

**:server qfile.files-boomloaders.ru**

**:URL /download/file**

**Packet DestinationAddress 10.X.X.X**

**Packet DestinationPort 60876**

**Packet SourceAddress 91.223.77.122**

**Packet SourcePort 80**

Antivirus scan for 3cb5b90d856b5377bb0183266298cdb0 at 2012-01-30 12:18:16 UTC - VirusTotal - Mozilla Firefox

Antivirus scan for 3cb5b90... | 91.223.77.124 | Whois сервис - проверка с...

virustotal.com https://www.virustotal.com/file/9b960ec7d89e806226a822a8435341ba

Google

Home Community Statistics Documentation FAQ About Join our community


File name: Dr_Web_for_Windows__antivirus_antispam____rabochie_klyuchi___instruktsiya_p[1].zip.exe

Detection ratio: 17 / 43

Analysis date: 2012-01-30 12:18:16 UTC ( 1 month, 2 weeks ago )

| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | Trojan/Win32.ADH | 20120129 |
| AntiVir | TR/Fraud.Gen2 | 20120130 |
| Antiy-AVL | - | 20120129 |
| Avast | - | 20120130 |
| AVG | - | 20120130 |
| BitDefender | Gen:Variant.Buzy.2504 | 20120130 |
| ByteHero | - | 20120126 |
| CAT-QuickHeal | - | 20120130 |


# Пример события IDS в Марте

**Date/Time 2012-03-20 12:52:37 MSK**

**Tag Name HTTP_Executable_Transfer**

***:server* woyrneygfilez.zone.be**

***:URL* /download/8473**

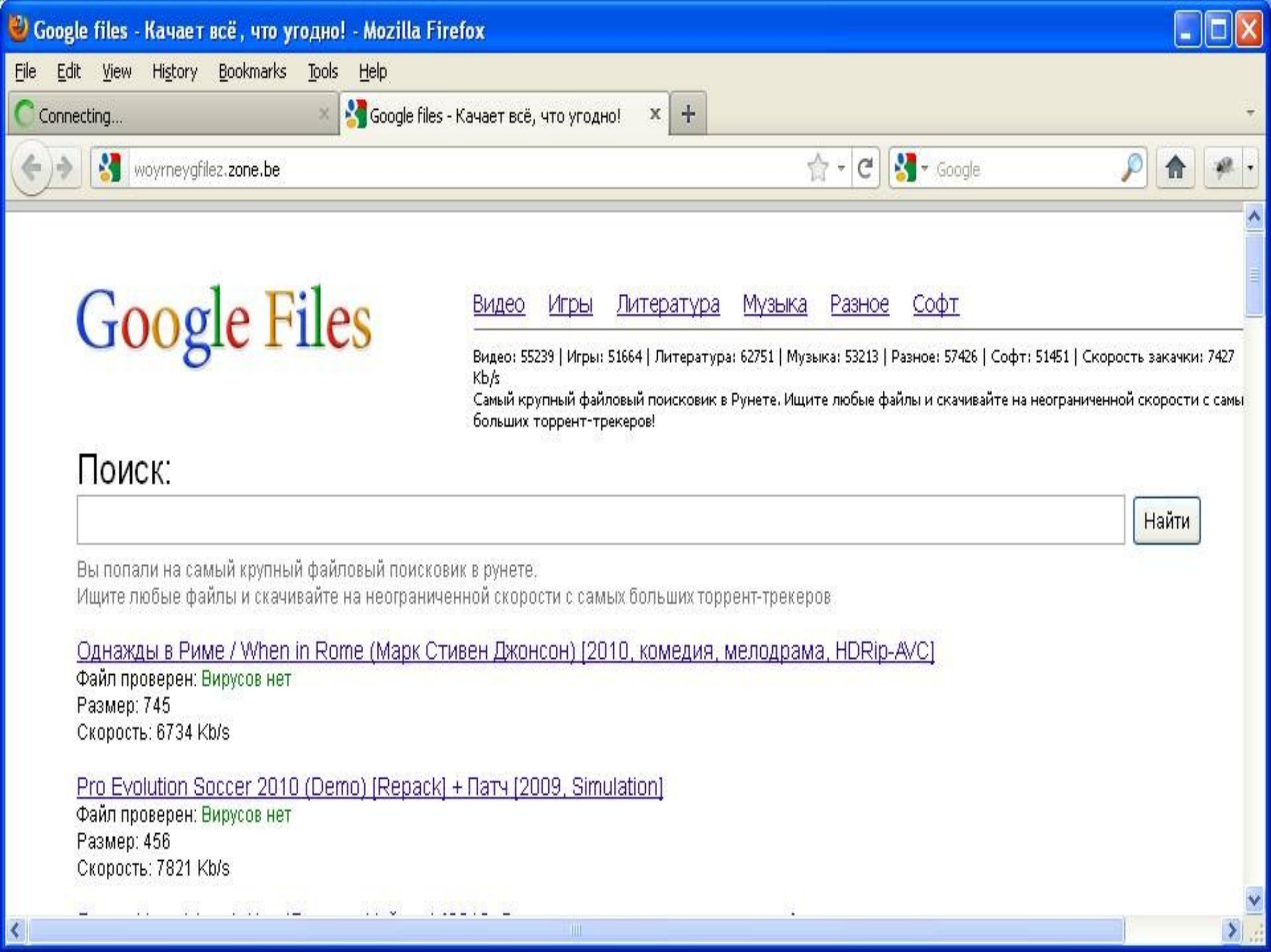
**Packet DestinationAddress 10.X.X.X**

**Packet DestinationPort 60703**

**Packet SourceAddress 91.223.77.124**

**Packet SourcePort 80**

| | | |
|---|---|---|
| F-Prot | - | 20120301 |
| F-Secure | - | 20120301 |
| Fortinet | - | 20120229 |
| GData | - | 20120301 |


Google files - Качает всё, что угодно! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
Google files - Качает всё, что угодно!
woyrneygfilez.zone.be
Google
Google Files
Видео Игры Литература Музыка Разное Софт
Видео: 55239 | Игры: 51664 | Литература: 62751 | Музыка: 53213 | Разное: 57426 | Софт: 51451 | Скорость закачки: 7427 Kb/s
Самый крупный файловый поисковик в Рунете. Ищите любые файлы и скачивайте на неограниченной скорости с самы больших торрент-трекеров!
Поиск:
Найти
Вы попали на самый крупный файловый поисковик в рунете.
Ищите любые файлы и скачивайте на неограниченной скорости с самых больших торрент-трекеров
Однажды в Риме / When in Rome (Марк Стивен Джонсон) [2010, комедия, мелодрама, HDRip-AVC]
Файл проверен: Вирусов нет
Размер: 745
Скорость: 6734 Kb/s
Pro Evolution Soccer 2010 (Demo) [Repack] + Патч [2009, Simulation]
Файл проверен: Вирусов нет
Размер: 456
Скорость: 7821 Kb/s

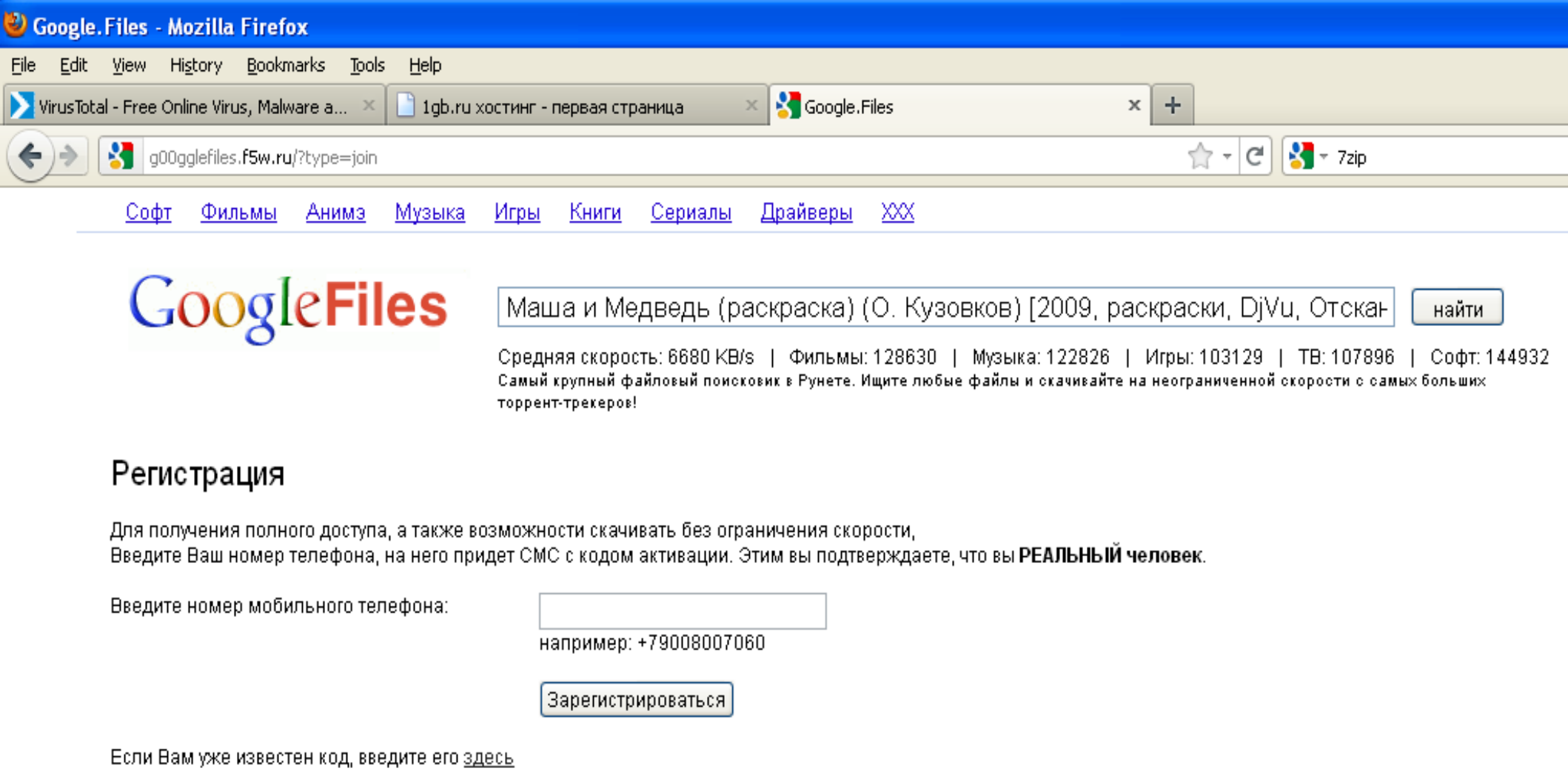

SHA256: b66e93522b25ff555aebc61b28163e0505c55b0556336edb50d623cc3280ac79

File name: Odnagdi_v_Rime___When_in_Rome__Mark_Stiven_Dgonson___2010__komediya__melodr.zip.exe

Detection ratio: 7 / 41

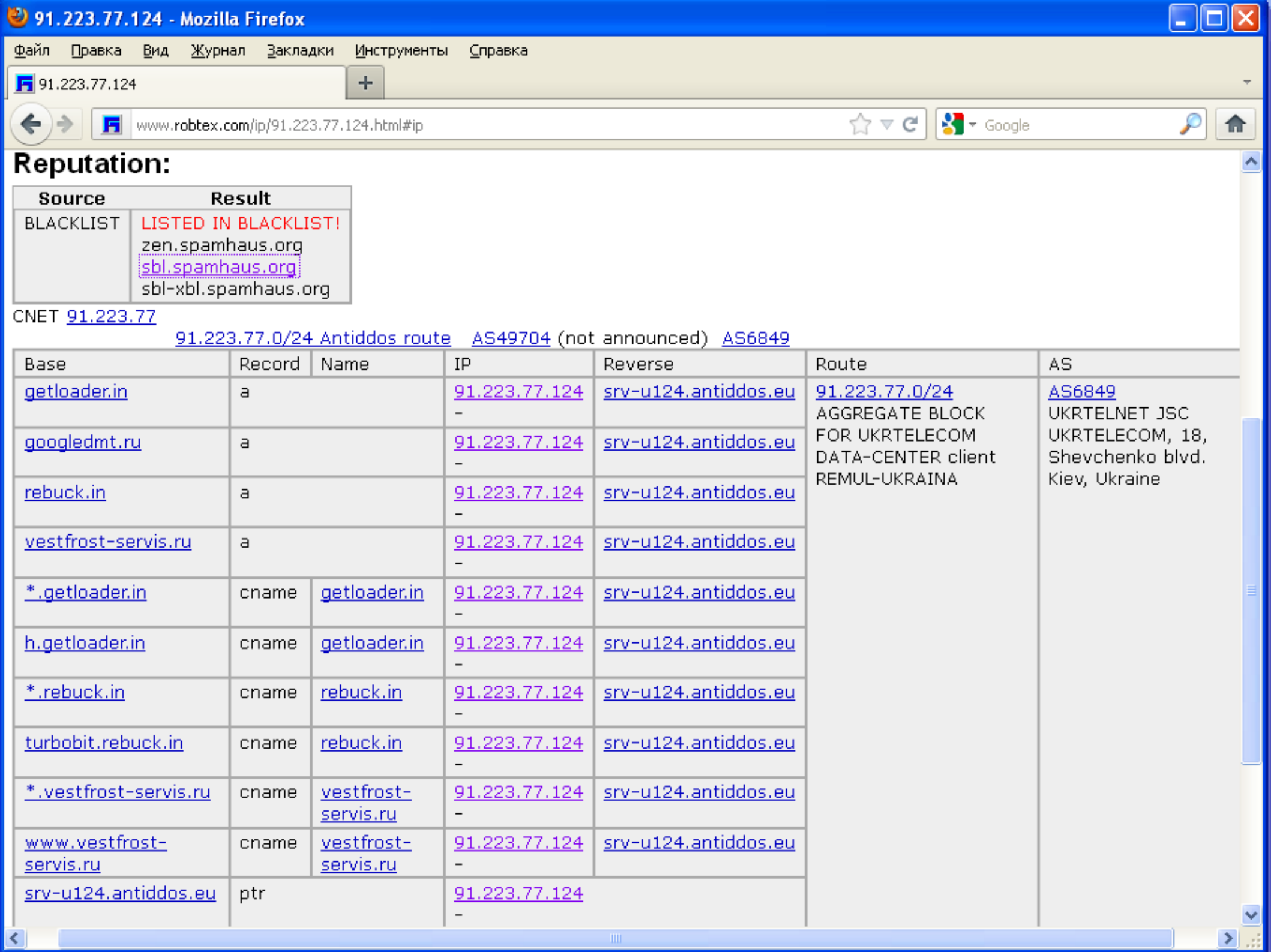
Analysis date: 2012-03-20 10:13:56 UTC ( 6 hours, 23 minutes ago )

| Antivirus | Result | Update |
|---|---|---|
| AntiVir | TR/Fraud.Gen2 | 20120320 |
| Antiy-AVL | - | 20120320 |
| Avast | Win32:SMSSend-FW [Trj] | 20120317 |
| AVG | - | 20120319 |
| BitDefender | Gen:Variant.Adware.SMSHoax.16 | 20120320 |
| ByteHero | - | 20120319 |
| CAT-QuickHeal | - | 20120320 |




[15/Dec/2011:15:54:23 +0300] GET

http://g00gglefiles.f5w.ru/?r=4088%26q=%CA%E0%F0%F2%E0+%ED%E8%E6%ED%E5%E2%E0%F0%F2%EE%E2%F1%EA%E0+%F1%EE+%F1%EF%F3%F2%ED%E8%EA%E0 HTTP/1.0 91.202.63.126



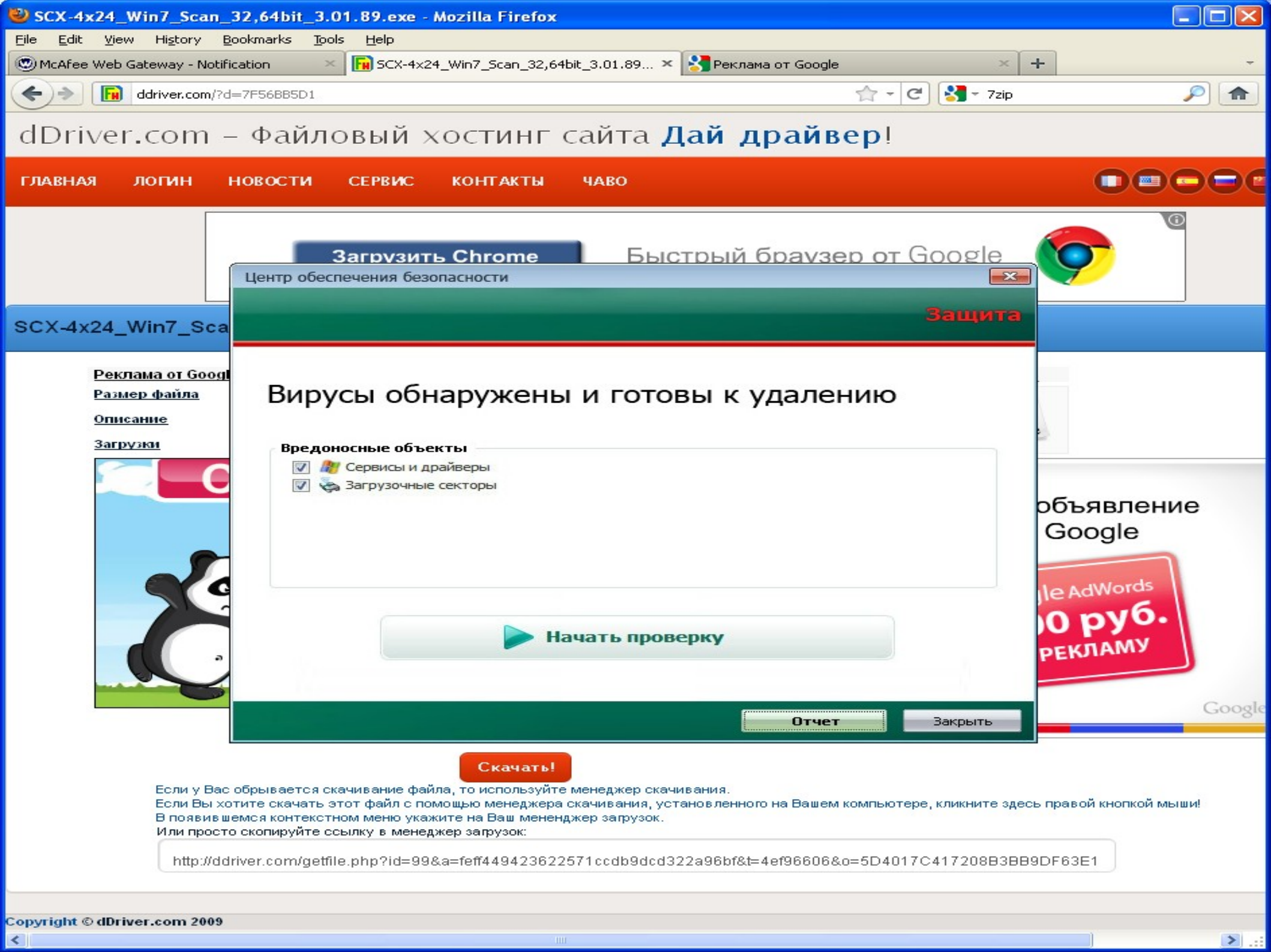

# Reputation:

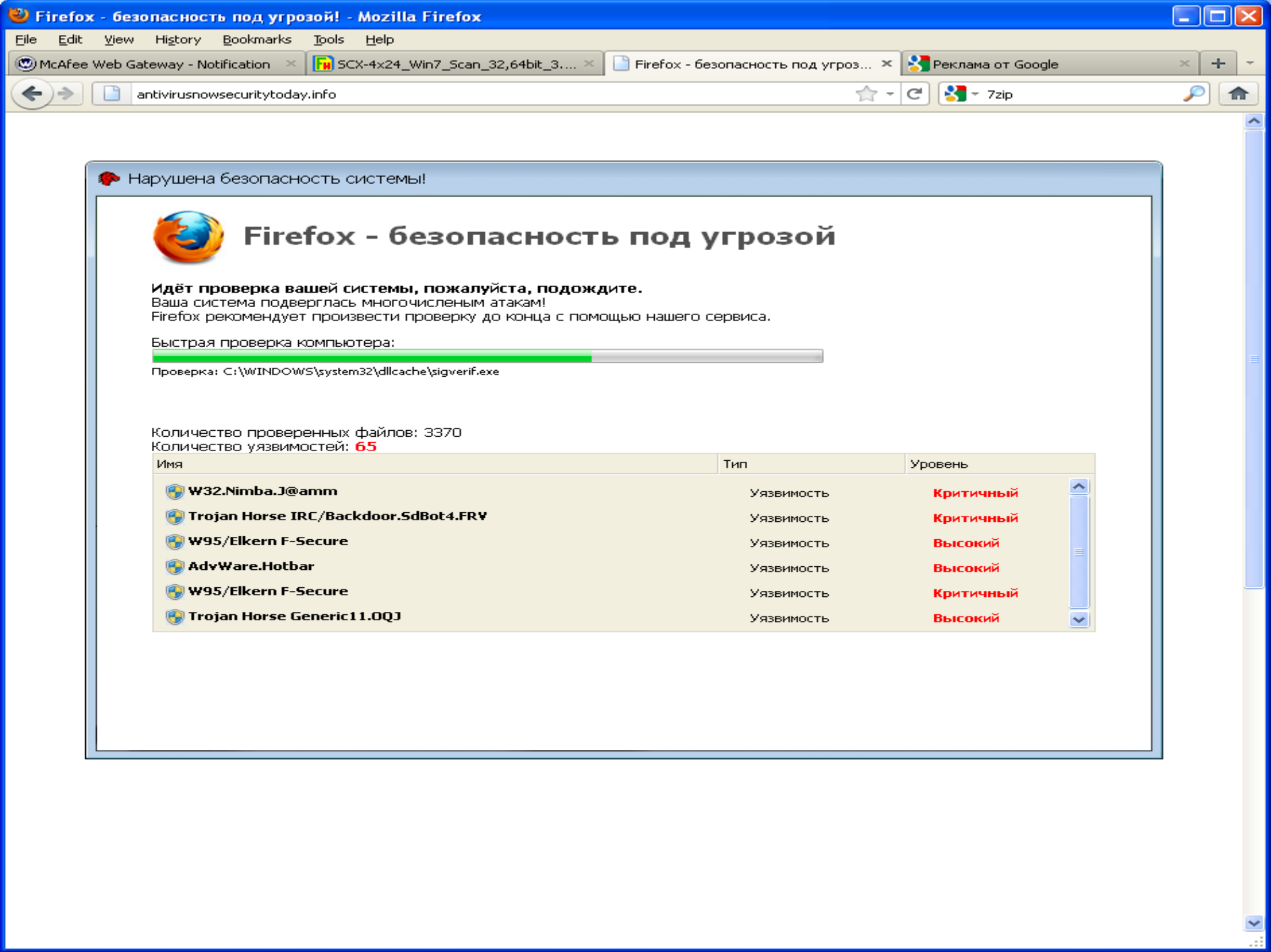
| Source | Result |
|---|---|
| BLACKLIST | LISTED IN BLACKLIST!<br>zen.spamhaus.org<br>sbl.spamhaus.org<br>sbl-xbl.spamhaus.org |

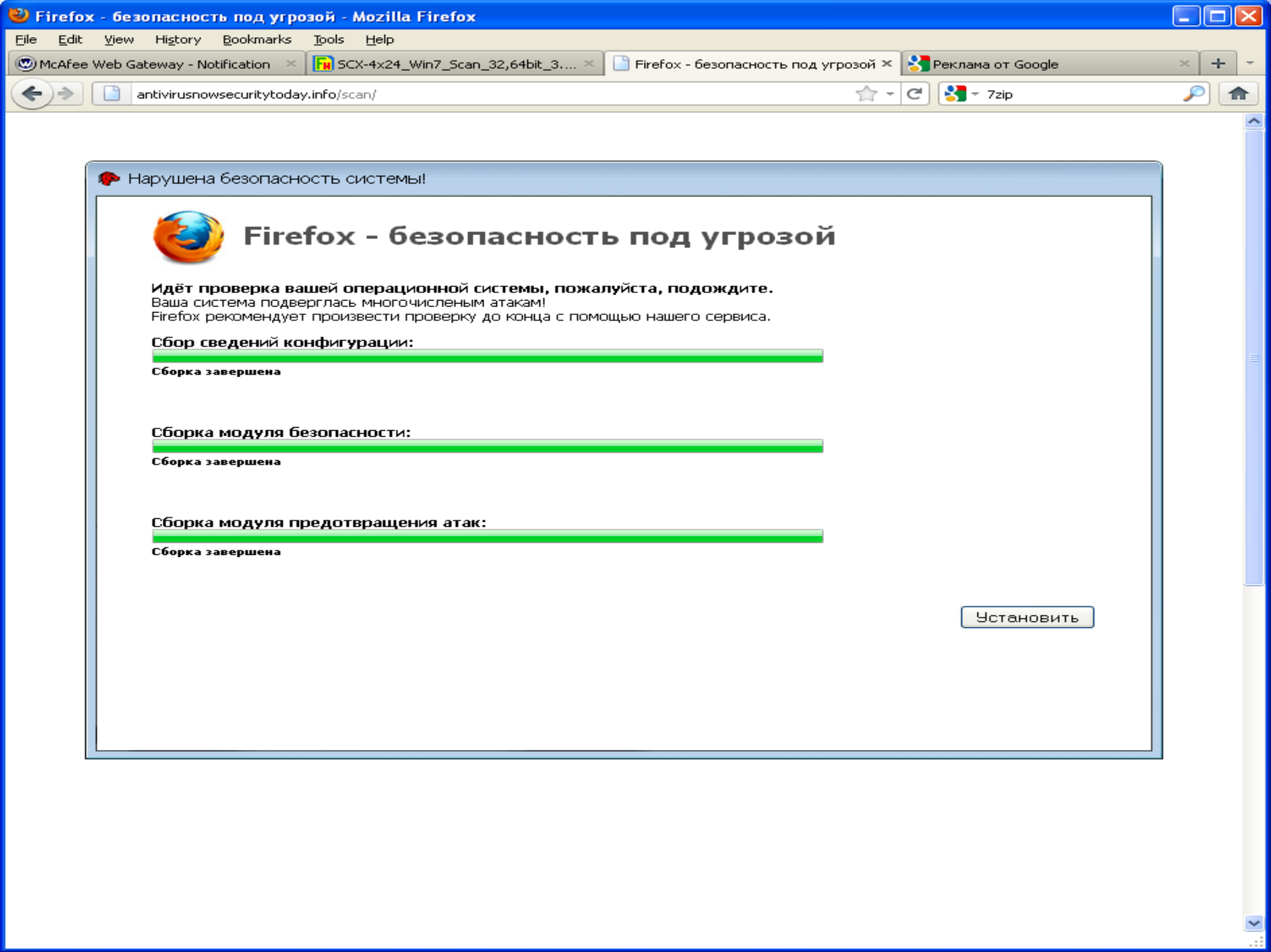
CNET 91.223.77

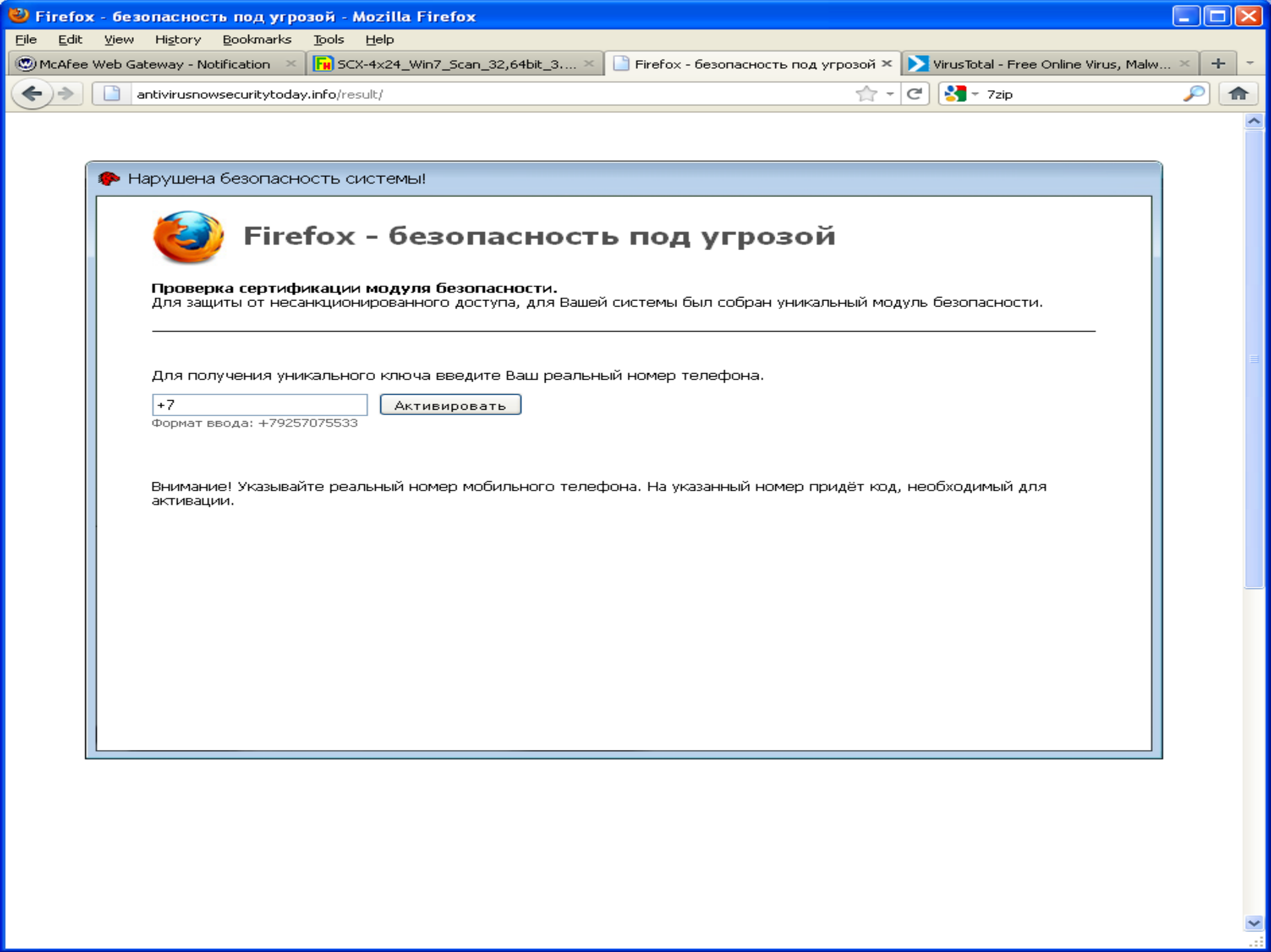
91.223.77.0/24 Antiddos route AS49704 (not announced) AS6849

| Base | Record | Name | IP | Reverse | Route | AS |
|---|---|---|---|---|---|---|
| getloader.in | a | | 91.223.77.124 - | srv-u124.antiddos.eu | 91.223.77.0/24 AGGREGATE BLOCK FOR UKRTELECOM DATA-CENTER client REMUL-UKRAINA | AS6849 UKRTELNET JSC UKRTELECOM, 18, Shevchenko blvd. Kiev, Ukraine |
| googledmt.ru | a | | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| rebuck.in | a | | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| vestfrost-servis.ru | a | | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| *.getloader.in | cname | getloader.in | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| h.getloader.in | cname | getloader.in | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| *.rebuck.in | cname | rebuck.in | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| turbobit.rebuck.in | cname | rebuck.in | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| *.vestfrost-servis.ru | cname | vestfrost-servis.ru | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| www.vestfrost-servis.ru | cname | vestfrost-servis.ru | 91.223.77.124 - | srv-u124.antiddos.eu | | |
| srv-u124.antiddos.eu | ptr | | 91.223.77.124 - | | | |


SCX-4x24_Win7_Scan_32,64bit_3.01.89.exe - Mozilla Firefox
File Edit View History Bookmarks Tools Help
McAfee Web Gateway - Notification
SCX-4x24_Win7_Scan_32,64bit_3.01.89...
Реклама от Google
ddriver.com/?d=7F56BB5D1
7zip
dDriver.com – Файловый хостинг сайта Дай драйвер!
ГЛАВНАЯ ЛОГИН НОВОСТИ СЕРВИС КОНТАКТЫ ЧАВО
Загрузить Chrome
Быстрый браузер от Google
Центр обеспечения безопасности
Защита
Вирусы обнаружены и готовы к удалению
Вредоносные объекты
Сервисы и драйверы
Загрузочные секторы
Начать проверку
Отчет
Закрыть
SCX-4x24_Win7_Sca
Реклама от Googl
Размер файла
Описание
Загрузки
объявление
Google
AdWords
руб.
РЕКЛАМУ
Скачать!
Если у Вас обрывается скачивание файла, то используйте менеджер скачивания.
Если Вы хотите скачать этот файл с помощью менеджера скачивания, установленного на Вашем компьютере, кликните здесь правой кнопкой мыши!
В появившемся контекстном меню укажите на Ваш менеджер загрузок.
Или просто скопируйте ссылку в менеджер загрузок:
http://ddriver.com/getfile.php?id=99&a=feff449423622571ccdb9dcd322a96bf&t=4ef96606&o=5D4017C417208B3BB9DF63E1
Copyright © dDriver.com 2009


Firefox - безопасность под угрозой! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
McAfee Web Gateway - Notification
SCX-4x24_Win7_Scan_32,64bit_3....
Firefox - безопасность под угроз...
Реклама от Google
antivirusnowsecuritytoday.info
7zip
Нарушена безопасность системы!
Firefox - безопасность под угрозой
Идёт проверка вашей системы, пожалуйста, подождите.
Ваша система подверглась многочисленым атакам!
Firefox рекомендует произвести проверку до конца с помощью нашего сервиса.
Быстрая проверка компьютера:
Проверка: C:\WINDOWS\system32\dllcache\sigverif.exe
Количество проверенных файлов: 3370
Количество уязвимостей: 65
Имя
Тип
Уровень
W32.Nimba.J@amm
Уязвимость
Критичный
Trojan Horse IRC/Backdoor.SdBot4.FRV
Уязвимость
Критичный
W95/Elkern F-Secure
Уязвимость
Высокий
AdvWare.Hotbar
Уязвимость
Высокий
W95/Elkern F-Secure
Уязвимость
Критичный
Trojan Horse Generic11.OQJ
Уязвимость
Высокий


Firefox - безопасность под угрозой - Mozilla Firefox
File Edit View History Bookmarks Tools Help
McAfee Web Gateway - Notification
SCX-4x24_Win7_Scan_32,64bit_3....
Firefox - безопасность под угрозой
Реклама от Google
antivirusnowsecuritytoday.info/scan/
7zip
Нарушена безопасность системы!
Firefox - безопасность под угрозой
Идёт проверка вашей операционной системы, пожалуйста, подождите.
Ваша система подверглась многочисленым атакам!
Firefox рекомендует произвести проверку до конца с помощью нашего сервиса.
Сбор сведений конфигурации:
Сборка завершена
Сборка модуля безопасности:
Сборка завершена
Сборка модуля предотвращения атак:
Сборка завершена
Установить

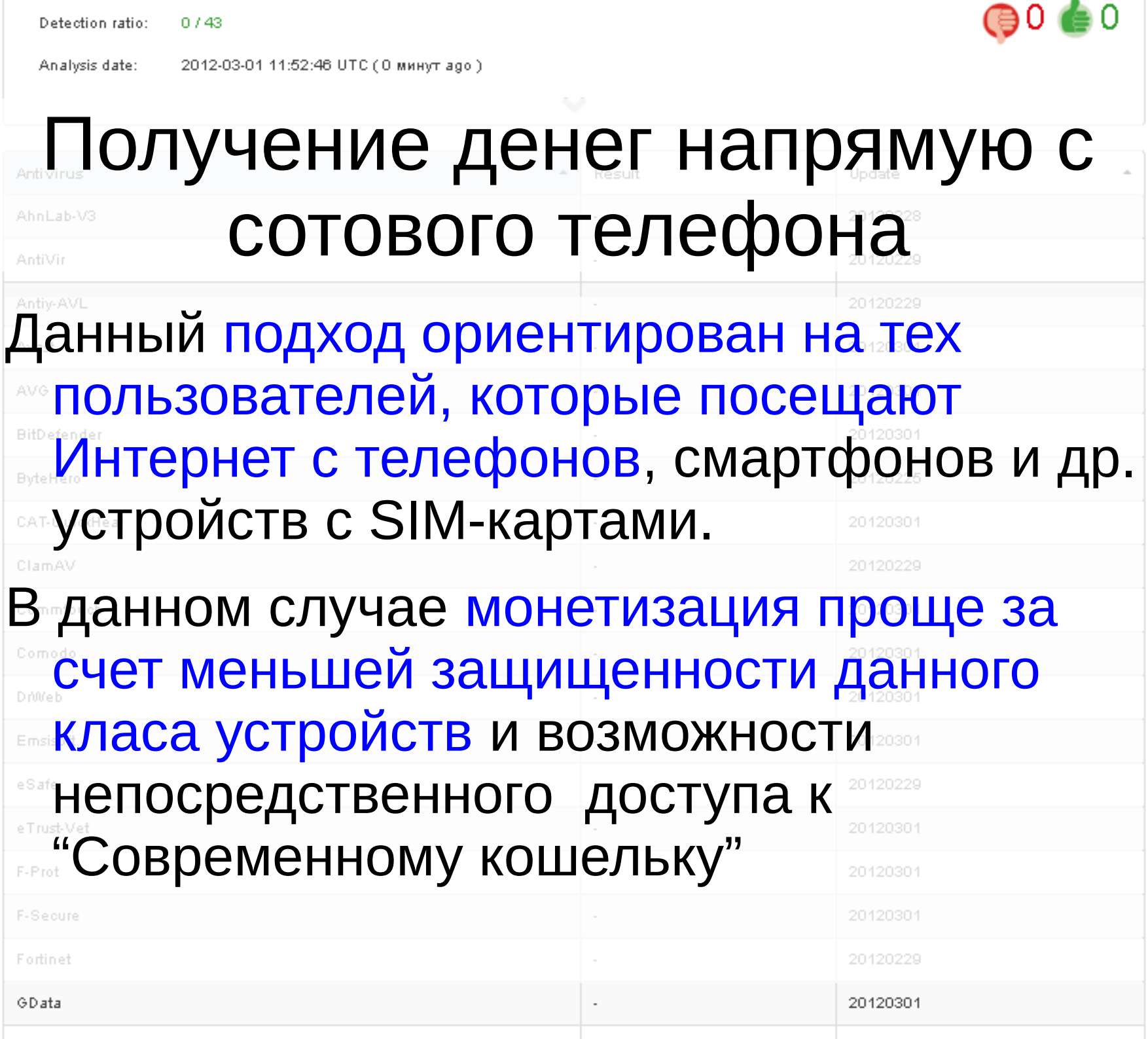

Firefox - безопасность под угрозой - Mozilla Firefox
File Edit View History Bookmarks Tools Help
McAfee Web Gateway - Notification
SCX-4x24_Win7_Scan_32,64bit_3....
Firefox - безопасность под угрозой
VirusTotal - Free Online Virus, Malw...
antivirusnowsecuritytoday.info/result/
7zip
Нарушена безопасность системы!
Firefox - безопасность под угрозой
Проверка сертификации модуля безопасности.
Для защиты от несанкционированного доступа, для Вашей системы был собран уникальный модуль безопасности.
Для получения уникального ключа введите Ваш реальный номер телефона.
+7
Активировать
Формат ввода: +79257075533
Внимание! Указывайте реальный номер мобильного телефона. На указанный номер придёт код, необходимый для активации.

# Номера? Вот они!

| | | | | |
|---|---|---|---|---|
| 2o11-2o12.net | 91.223.77.108 | 80 | pay_code | 4175 |
| 2o11-2o12.net | 91.223.77.108 | 80 | iagree | on |
| 2o11-2o12.net | 91.223.77.108 | 80 | submit.x | 195 |
| 2o11-2o12.net | 91.223.77.108 | 80 | submit.y | 30 |
| 2o11-2o12.net | 91.223.77.108 | 80 | | |
| 2o11-2o12.net | 91.223.77.108 | 80 | pay_phone | 89161[redacted] |
| 2o11-2o12.net | 91.223.77.108 | 80 | captcha_key | 24517 |
| 2o11-2o12.net | 91.223.77.108 | 80 | x | 133 |
| 2o11-2o12.net | 91.223.77.108 | 80 | y | 32 |
| dieta-dom.ru | 91.223.77.108 | 80 | | |
| newbrowserbest2013.info | 94.228.217.240 | 80 | | |
| newbrowserbest2013.info | 94.228.217.240 | 80 | as81ar | 14752 |
| newbrowserbest2013.info | 94.228.217.240 | 80 | m173sc | 1123 |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | phone | +79091[redacted] |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | activation | Âêòèâèðîâàòü |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | action | phone |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | cOpqzws | ie |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | cOpqzws | ie |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | phone | +79091[redacted] |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | activation | Âêòèâèðîâàòü |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | action | phone |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | cOpqzws | ie |
| ANTIVIRUSFORU.INFO | 94.228.217.240 | 80 | | |

| | | | | |
|---|---|---|---|---|
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | email | ns[redacted].com |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | description | Спам+в+виде+СМС |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | | |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | captcha | 457 |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | links | Прекратите+слать+СМС+об+услугах+на+мой+телефон. |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | phone | +7-985[redacted] |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | email | ns[redacted]va@[redacted].com |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | sirname | <empty> |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | lastname | Наталья |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | name | [redacted]+ |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | language | ru |
| 2012-03-12 09:13:07 ... | 91.202.63.111 | www.google-file.com | action | abuse |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | captcha | 457 |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | links | Прекратите+слать+СМС+об+услугах+на+мой+телефон. |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | description | Спам+в+виде+СМС |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | phone | +7-985-[redacted] |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | email | ns[redacted]va@[redacted]com |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | sirname | <empty> |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | lastname | Наталья |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | name | [redacted]+ |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | language | ru |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | action | abuse |
| 2012-03-12 08:15:35 ... | 91.202.63.111 | www.google-file.com | | |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | captcha | 457 |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | links | Прекратите+слать+СМС+об+услугах+на+мой+телефон. |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | description | Спам+в+виде+СМС |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | phone | +7-985[redacted] |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | sirname | |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | lastname | Наталья |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | name | [redacted] |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | language | ru |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | action | abuse |
| 2012-03-12 08:11:22 ... | 91.202.63.111 | www.google-file.com | | |

# Проблемы? Вот они!

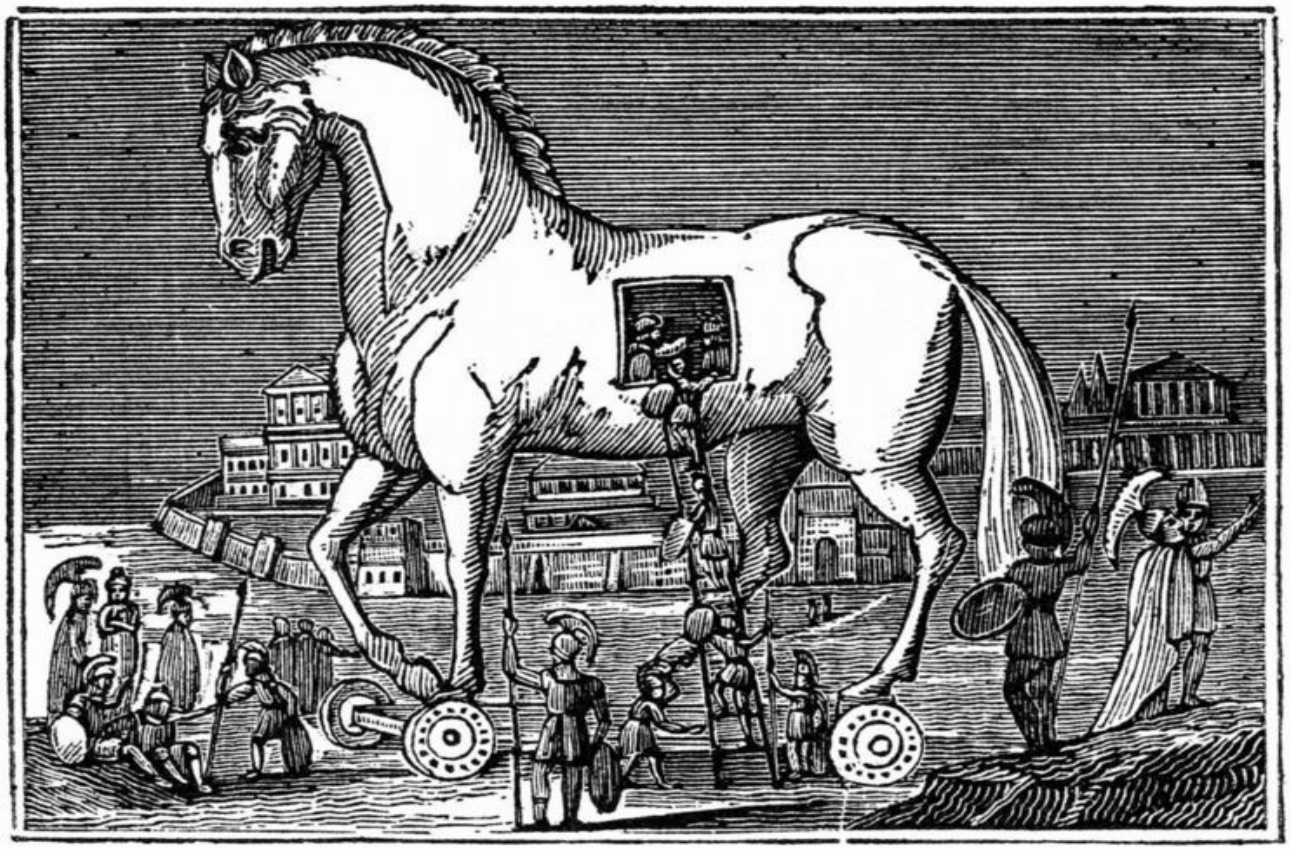



# Получение денег напрямую с сотового телефона

Данный подход ориентирован на тех пользователей, которые посещают Интернет с телефонов, смартфонов и др. устройств с SIM-картами.

В данном случае монетизация проще за счет меньшей защищенности данного класа устройств и возможности непосредственного доступа к “Современному кошельку”

# Установка ПО для мобильных устройств из недоверенных источников или зачем платить, если можно скачать бесплатно?)



*Trojans Deceived.*

Скачать Opera Mini для телефонов с поддержкой JAVA - Mozilla Firefox

File Edit View History Bookmarks Tools Help

VirusTotal - F... | 1gb.ru хости... | Google.Files | Google.Files | Google Safe ... | 146.185.242... | Скачать ... | MalwareURL | elatedshop.c... | elatedshop.c...

rossyyy.ru

tedshop.com

Главная Дополнения Разработка Компания

OPERA software

## Opera Mini Mobile

Загрузить Инструкция по установке Написать нам Пользовательское соглашение


ЛУЧШИЙ ВЫБОР СОВРЕМЕННОСТИ

скачали 22791 раз

СКАЧАТЬ

Загрузить мгновенно

JAR: **Скачать Opera Mini** (21 Кб)
Для всех телефонов.

### Простота просмотра

Просматривать веб-сайты с помощью мобильного телефона теперь так же просто, как с настольного компьютера. Вне зависимости от модели телефона, вы оцените непревзойденное удобство работы в Интернете.

### Высочайшая скорость работы в Интернете

Самый быстрый доступ в Интернет из всех, что возможны для вашего телефона. Скорость визуализации и эффективность средств управления позволили браузеру Opera обогнать другие мобильные браузеры на много световых лет.

### Экономия денег

Экономьте деньги на оплате услуг передачи данных, воспользовавшись технологией сжатия Opera, которая сокращает расходы на передачу данных до 10% от обычного уровня.

### Смотреть видео

**Opera** – один из известнейших браузеров. Достаточно удобный, имеющий много функций и не ограничивающий скорость. Opera была создана норвежскими разработчиками и имеет множество версий. Ранние версии отличаются от более современных своими функциями и дизайном. Начиная с 5 версии, в программе присутствует ICQ, но её использование не самое удобное.

В опере присутствуют все необходимые инструменты для удобной работы, также в программе присутствует модуль защиты от мошенников, блокировка всплывающих окон, диспетчер загрузок, менеджер паролей, голосовое управление, виджеты , разные скины

Find: ela Next Previous Highlight all Match case

File name: **Opera_Mini_6_5.jar**
Submission date: **2011-12-26 11:42:49 (UTC)**
Current status: **finished**
Result: **8/ 43 (18.6%)**

not reviewed
Safety score: -

Compact | Print results

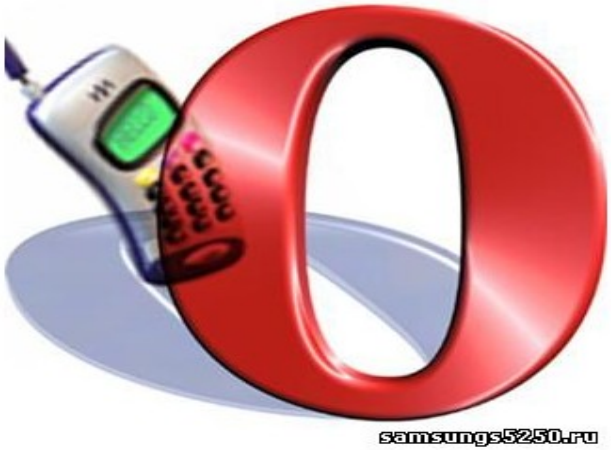
| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2011.12.25.01 | 2011.12.26 | - |
| AntiVir | 7.11.20.18 | 2011.12.25 | - |
| Antiy-AVL | 2.0.3.7 | 2011.12.26 | Trojan/J2ME.OpFake |
| Avast | 6.0.1289.0 | 2011.12.25 | - |
| AVG | 10.0.0.1190 | 2011.12.26 | Java/Agent.GP |
| BitDefender | 7.2 | 2011.12.26 | - |
| ByteHero | 1.0.0.1 | 2011.12.07 | - |
| CAT-QuickHeal | 12.00 | 2011.12.26 | - |
| ClamAV | 0.97.3.0 | 2011.12.26 | - |
| Commtouch | 5.3.2.6 | 2011.12.25 | - |
| Comodo | 11093 | 2011.12.26 | UnclassifiedMalware |
| DrWeb | 5.0.2.03300 | 2011.12.26 | Java.SMSSend.717 |
| Emsisoft | 5.1.0.11 | 2011.12.26 | Trojan.Java.Agent!IK |
| eSafe | 7.0.17.0 | 2011.12.25 | - |
| eTrust-Vet | 37.0.9642 | 2011.12.23 | - |
| F-Prot | 4.6.5.141 | 2011.12.25 | - |
| F-Secure | 9.0.16440.0 | 2011.12.26 | - |
| Fortinet | 4.3.388.0 | 2011.12.26 | - |
| GData | 22.320/22.605 | 2011.12.26 | - |
| Ikarus | T3.1.1.109.0 | 2011.12.26 | Trojan.Java.Agent |
| Jiangmin | 13.0.900 | 2011.12.25 | - |
| K7AntiVirus | 9.120.5757 | 2011.12.23 | - |
| Kaspersky | 9.0.0.837 | 2011.12.26 | Trojan-SMS.J2ME.OpFake.hp |
| McAfee | 5.400.0.1158 | 2011.12.26 | - |
| McAfee-GW-Edition | 2010.1E | 2011.12.26 | - |
| Microsoft | 1.7903 | 2011.12.26 | - |
| NOD32 | 6742 | 2011.12.26 | J2ME/TrojanSMS.Agent.BC |
| Norman | 6.07.13 | 2011.12.25 | - |
| nProtect | 2011-12-26.01 | 2011.12.26 | - |
| Panda | 10.0.3.5 | 2011.12.25 | - |
| PCTools | 8.0.0.5 | 2011.12.26 | - |
| Prevx | 3.0 | 2011.12.26 | - |

Мобильная версия сайта PDA
Полная версия сайта
Игры для Samsung S5250/S5233T/S5230/ S5260/S7230
Игры для Samsung S8500/S8530
Программы для Samsung S5250/S5233T/S5230/ S5260/S7230
Программы для Samsung S8500/S8530
Темы для Samsung S5250/S5233T/S5230/ S5260/S7230
Темы для Samsung S3850
Темы для Samsung S5250
Темы для samsung S5260 Star
Темы для Samsung S5330
Темы для Samsung S5750
Темы для Samsung S6712
Темы для Samsung S7230
Темы для Samsung S8500/S8530
Всё для Android
Программы для Android
Игры для Android
Живые обои для Android



# "Opera mini 6-0" 240x400 для Samsung S5250/S5233T/S5230/S5260/S7230/S5330/ скачать

16.06.2011, 01:17




***"Opera mini 6-0" для Samsung S5250/S5233T/S5230/S5260/S7230/S5330/.***

Представляем Вашему вниманию очень удобный браузер "opera mini 6-0" для samsung s5250/ s5233t/ s5230/ s5260/ s7230/ s5330/. При помощи этого браузера Вы с легкостью сможете посещать страницы интернета, а также любимые сайты такие как: **samsungs5250. ru**, **одноклассники. ru**, **в контакте. ru** и многие другие. Браузер "opera mini 6-0" предназначен как для телефонов так и для смартфонов, в этой версии браузера появилась поддержка сенсорного управления, а следовательно и виртуальная клавиатура, также теперь любимые сайты будут отображаться в виде скриншотов страницы, а не простым текстом. Предлагаем Всем воспользоваться браузером "opera mini 6-0" для samsung s5250/ s5233t/ s5230/ s5260/ s7230/ s5330/ и вы существенно сэкономите свои деньги так как этот браузер не глючит и не тормозит, а также сервер "opera mini 6-0" предварительно обрабатывает веб страницы и отсеивает лишнее.

Жанр: Программы

Скачать

VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox

File Edit View History Bookmarks Tools Help

VirusTotal - Free... | 1gb.ru хостинг - пе... | Google.Files | Google.Files | Google Safe Browsi... | 146.185.242.40 mal... | Скачать Opera Mini... | "Opera mini 6-0" 24...

www.virustotal.com/file-scan/report.html?id=4eb75f66081a58a8e508558bdcc13b7e0c004914434a585355d8afed1c3e04a4-1324900186

tedshop.com

TOTAL

of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **Opera_Mini_6_5(1).jar**
Submission date: **2011-12-26 11:49:46 (UTC)**
Current status: **finished**
Result: **8/ 43 (18.6%)**

**VT Community**

not reviewed
Safety score: -

Compact

Print results

| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2011.12.25.01 | 2011.12.26 | - |
| AntiVir | 7.11.20.18 | 2011.12.25 | - |
| Antiy-AVL | 2.0.3.7 | 2011.12.26 | Trojan/J2ME.OpFake |
| Avast | 6.0.1289.0 | 2011.12.25 | - |
| AVG | 10.0.0.1190 | 2011.12.26 | Java/Agent.GP |
| BitDefender | 7.2 | 2011.12.26 | - |
| ByteHero | 1.0.0.1 | 2011.12.07 | - |
| CAT-QuickHeal | 12.00 | 2011.12.26 | - |
| ClamAV | 0.97.3.0 | 2011.12.26 | - |
| Commtouch | 5.3.2.6 | 2011.12.25 | - |
| Comodo | 11093 | 2011.12.26 | UnclassifiedMalware |
| DrWeb | 5.0.2.03300 | 2011.12.26 | Java.SMSSend.717 |
| Emsisoft | 5.1.0.11 | 2011.12.26 | Trojan.Java.Agent!IK |
| eSafe | 7.0.17.0 | 2011.12.25 | - |
| eTrust-Vet | 37.0.9642 | 2011.12.23 | - |
| F-Prot | 4.6.5.141 | 2011.12.25 | - |
| F-Secure | 9.0.16440.0 | 2011.12.26 | - |
| Fortinet | 4.3.388.0 | 2011.12.26 | - |
| GData | 22 | 2011.12.26 | - |
| Ikarus | T3.1.1.109.0 | 2011.12.26 | Trojan.Java.Agent |
| Jiangmin | 13.0.900 | 2011.12.25 | - |
| K7AntiVirus | 9.120.5757 | 2011.12.23 | - |
| Kaspersky | 9.0.0.837 | 2011.12.26 | Trojan-SMS.J2ME.OpFake.hp |
| McAfee | 5.400.0.1158 | 2011.12.26 | - |
| McAfee-GW-Edition | 2010.1E | 2011.12.26 | - |
| Microsoft | 1.7903 | 2011.12.26 | - |
| NOD32 | 6742 | 2011.12.26 | J2ME/TrojanSMS.Agent.BC |

Find: ela Next Previous Highlight all Match case

TOTAL

of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **scientific-calculator-v.1.00_.jar**
Submission date: **2011-12-26 10:18:26 (UTC)**
Current status: **finished**
Result: **4/ 43 (9.3%)**

**VT Community**

not reviewed
Safety score: -

Compact

Print results

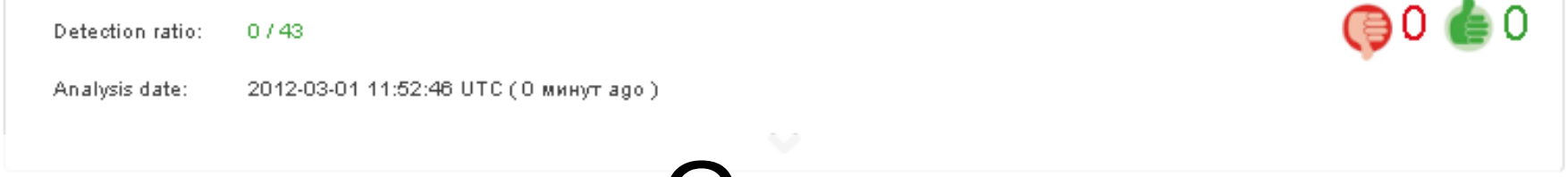
| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2011.12.25.01 | 2011.12.26 | - |
| AntiVir | 7.11.20.18 | 2011.12.25 | JAVA/SMSSend.AF |
| Antiy-AVL | 2.0.3.7 | 2011.12.26 | - |
| Avast | 6.0.1289.0 | 2011.12.25 | - |
| AVG | 10.0.0.1190 | 2011.12.25 | - |
| BitDefender | 7.2 | 2011.12.26 | - |
| ByteHero | 1.0.0.1 | 2011.12.07 | - |
| CAT-QuickHeal | 12.00 | 2011.12.26 | - |
| ClamAV | 0.97.3.0 | 2011.12.26 | - |
| Commtouch | 5.3.2.6 | 2011.12.25 | - |
| Comodo | 11093 | 2011.12.26 | UnclassifiedMalware |
| DrWeb | 5.0.2.03300 | 2011.12.26 | - |
| Emsisoft | 5.1.0.11 | 2011.12.26 | Trojan.Sms.J2me!IK |
| eSafe | 7.0.17.0 | 2011.12.25 | - |
| eTrust-Vet | 37.0.9642 | 2011.12.23 | - |
| F-Prot | 4.6.5.141 | 2011.12.25 | - |
| F-Secure | 9.0.16440.0 | 2011.12.26 | - |
| Fortinet | 4.3.388.0 | 2011.12.26 | - |
| GData | 22.320/22.604 | 2011.12.26 | - |
| Ikarus | T3.1.1.109.0 | 2011.12.26 | Trojan.Sms.J2me |
| Jiangmin | 13.0.900 | 2011.12.25 | - |
| K7AntiVirus | 9.120.5757 | 2011.12.23 | - |
| Kaspersky | 9.0.0.837 | 2011.12.26 | - |
| McAfee | 5.400.0.1158 | 2011.12.26 | - |
| McAfee-GW-Edition | 2010.1E | 2011.12.26 | - |
| Microsoft | 1.7903 | 2011.12.26 | - |
| NOD32 | 6742 | 2011.12.26 | - |
| Norman | 6.07.13 | 2011.12.25 | - |

# Порно Игры: Silly games

```
f.java:        this.jdField_a_of_type_I = new i(this, "0%. Необходимо нажать на
кнопку 'Стоп' как можно быстрее!", 128, 128);
```

```
24    private static boolean a(String paramString1, String paramString2)
25    {
26      try
27      {
28        MessageConnection localMessageConnection;
29        TextMessage localTextMessage;
30        (localTextMessage = (TextMessage)(localMessageConnection =
31                                          (MessageConnection)Connector.open
    ("sms://" +
32                                                    paramString1)).newMessage("te
    xt")).setAddress("sms://" +
33                                                  paramString1);
34        localTextMessage.setPayloadText(paramString2);
35        localMessageConnection.send(localTextMessage);
36        localMessageConnection.close();
37        return true;
```

| | | |
|---|---|---|
| F-Secure | - | 20120301 |
| Fortinet | - | 20120229 |
| GData | - | 20120301 |




# Суть

Телефон при отсылке сообщения выдает запрос на подтверждение отсылки.

Чтобы обойти данное ограничение, надо заставить пользователя упорно “жать” на “ОК” :)

Сообщение идет на которкий номер

# Альтернативные схемы

Рассылка СМС спама с кодом в URL

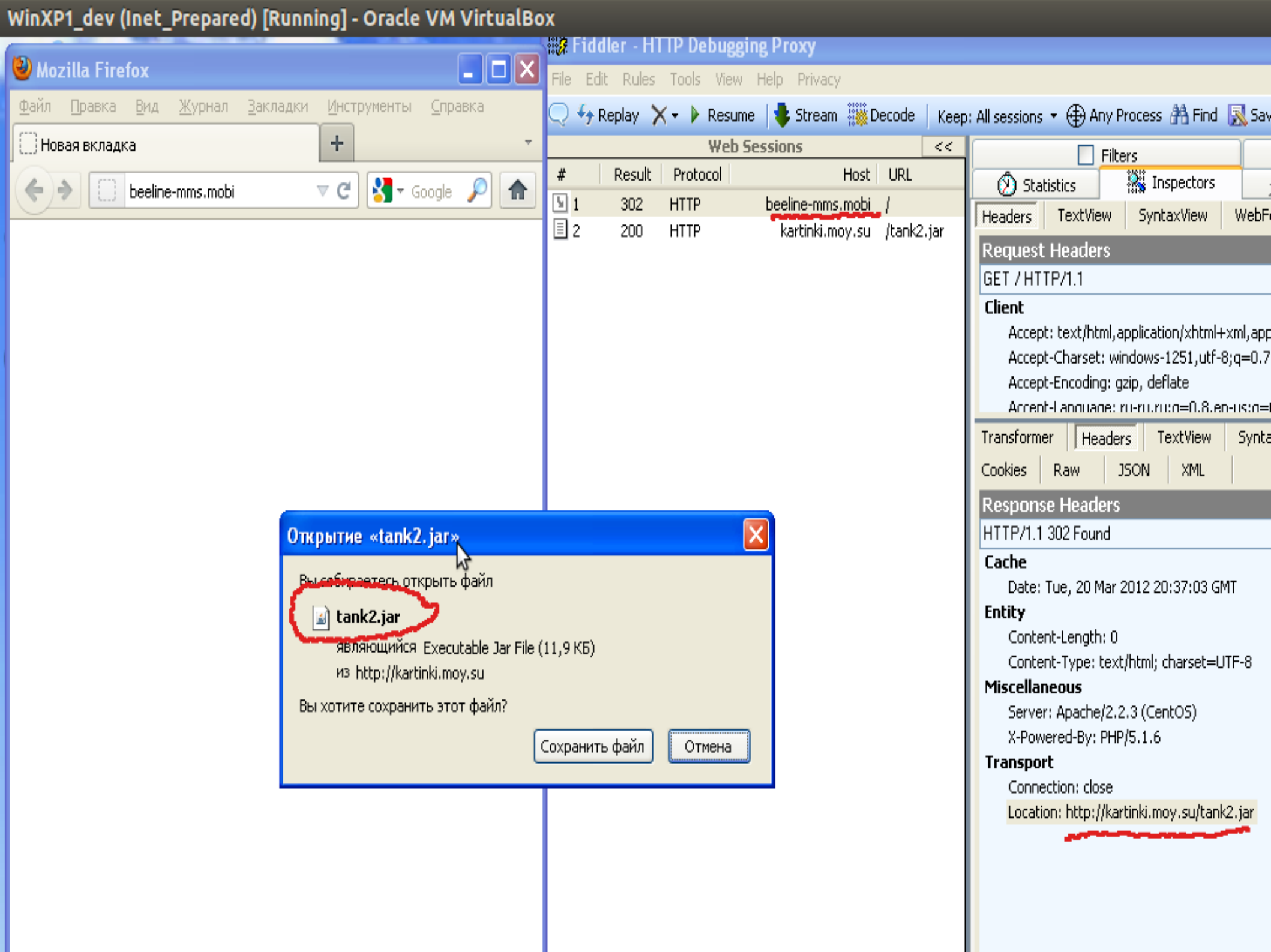
( hint: контент провайдер может указать

Шаблон сообщения)

Пользователю приходит сообщения с URL, он переходит по ссылке и получает...

http://www.cforum.ru/t4/forum/rkikyd?start=100: ...

*Ещё в конце декабря получил СМС следующего содержания: ваш друг прислал открытку и ссылка на http://mobipage.ru/a/ Решил посмотреть, что за открытка. Но переходить с телефона по ссылке не стал, а ввёл её на компьютере в браузере "Opera". Зашёл, там какая-то ерунда. Вышел и забыл. СМС удалил. 3-го января снова пришла какая-то СМС от них, даже читать не стал, удалил. 5-го числа проверил баланс и ох...*


WinXP1_dev (Inet_Prepared) [Running] - Oracle VM VirtualBox
Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
Новая вкладка
beeline-mms.mobi
Google
Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help Privacy
Replay Resume Stream Decode Keep: All sessions Any Process Find
Web Sessions
# Result Protocol Host URL
1 302 HTTP beeline-mms.mobi /
2 200 HTTP kartinki.moy.su /tank2.jar
Filters
Statistics Inspectors
Headers TextView SyntaxView
Request Headers
GET / HTTP/1.1
Client
Accept: text/html,application/xhtml+xml,app
Accept-Charset: windows-1251,utf-8;q=0.7
Accept-Encoding: gzip, deflate
Transformer Headers TextView
Cookies Raw JSON XML
Response Headers
HTTP/1.1 302 Found
Cache
Date: Tue, 20 Mar 2012 20:37:03 GMT
Entity
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Miscellaneous
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Transport
Connection: close
Location: http://kartinki.moy.su/tank2.jar
Открытие «tank2.jar»
Вы собираетесь открыть файл
tank2.jar
являющийся Executable Jar File (11,9 КБ)
из http://kartinki.moy.su
Вы хотите сохранить этот файл?
Сохранить файл
Отмена

SHA256: ac51816e627b6f137fd3848eb29a9c03ef6f9c9aeb256d2e152a3

File name: tank2.jar

Detection ratio: 26 / 42

Analysis date: 2012-03-20 20:41:10 UTC ( 1 минута ago )

This file has a reputation of 0 in an scale from -100 to 100


| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | JAVA/Smser | 20120320 |
| AntiVir | Tr/SMSer.S.14 | 20120320 |
| Antiy-AVL | Trojan/win32.agent | 20120320 |
| Avast | Java:SMSSend-CO [Trj] | 20120320 |
| AVG | Java/SMS.AM | 20120320 |
| BitDefender | Trojan.Java.SMSsend.G | 20120320 |
| ByteHero | - | 20120319 |
| CAT-QuickHeal | - | 20120320 |
| ClamAV | Trojan.SMS-58 | 20120320 |

Whois сервис - проверка свободного домена | REG.RU - Mozilla Firefox

Antivirus scan for 66c7d0... | 91.212.226.198 | Whois сервис - проверка... | Whois сервис - проверка...

www.reg.ru/whois/index?dname=beeline-mms.mobi

Google

# beeline-mms.mobi

**IP-адрес:** 91.212.226.198

**По данным whois.dotmobiregistry.net:**

Domain ID:D6693028-MOBI
Domain Name:BEELINE-MMS.MOBI
Created On:13-Mar-2012 12:27:30 UTC
Last Updated On:13-Mar-2012 12:27:31 UTC
Expiration Date:13-Mar-2013 12:27:30 UTC
Sponsoring Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a
PublicDomainRegistry.com (R63)
Created by Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a
PublicDomainRegistry.com (R63)
Last Updated by Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a
PublicDomainRegistry.com (R63)
Status:CLIENT TRANSFER PROHIBITED
Status:TRANSFER PROHIBITED
Registrant ID:DI-2169252

Created On:13-Mar-2012 12:27:30 UTC

Expiration Date:13-Mar-2013 12:27:30 UTC

Last Updated by Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a

Registrant Name:Aleksandr Kroshkin

Registrant City:Novosibirsk

virustotal

SHA256: e0b41f3ed86395a0166b6db29e4a07c2e5b7647aee516a63b85e33ce1ee3eaf4

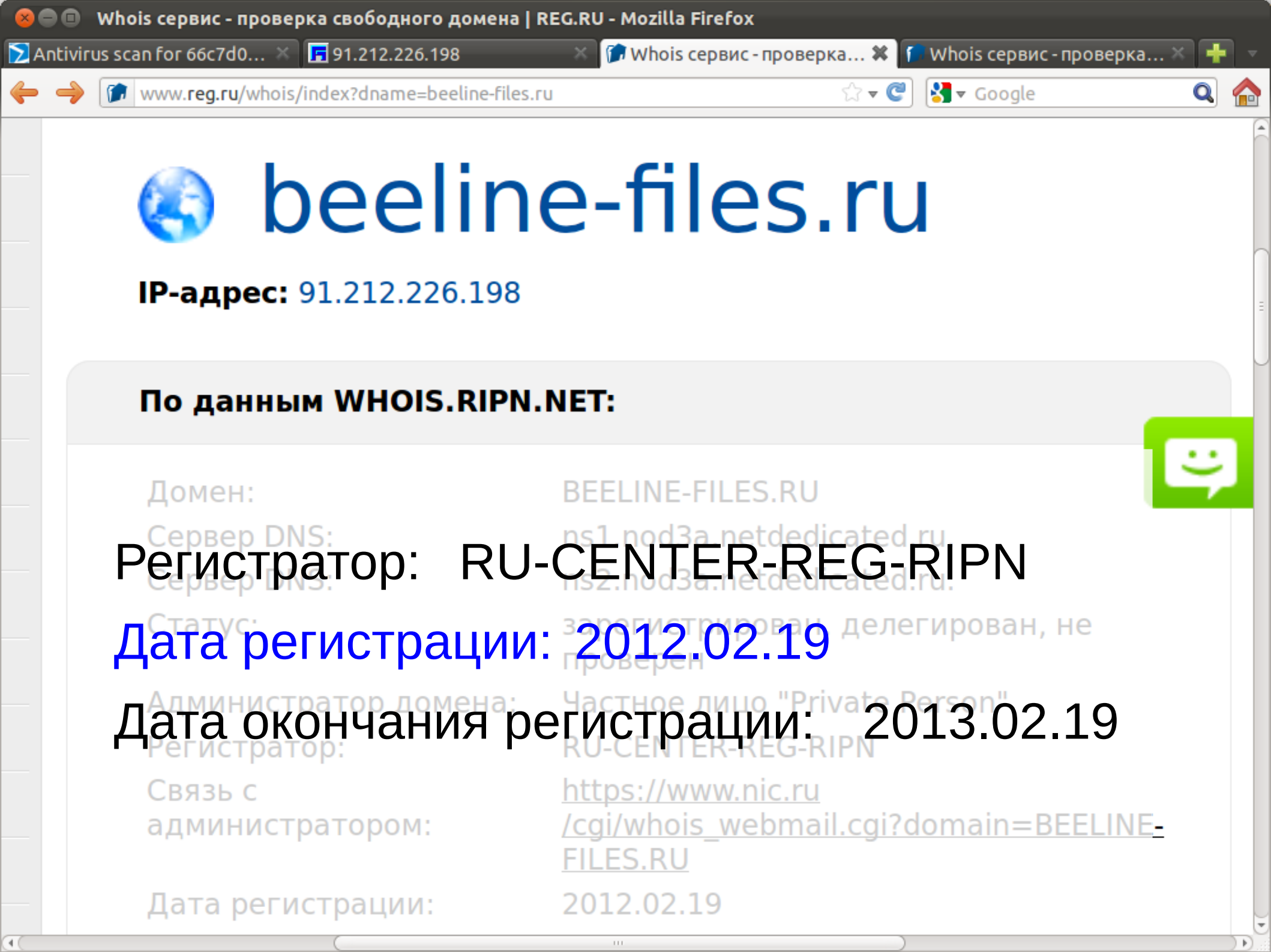
File name: bbbb.jar

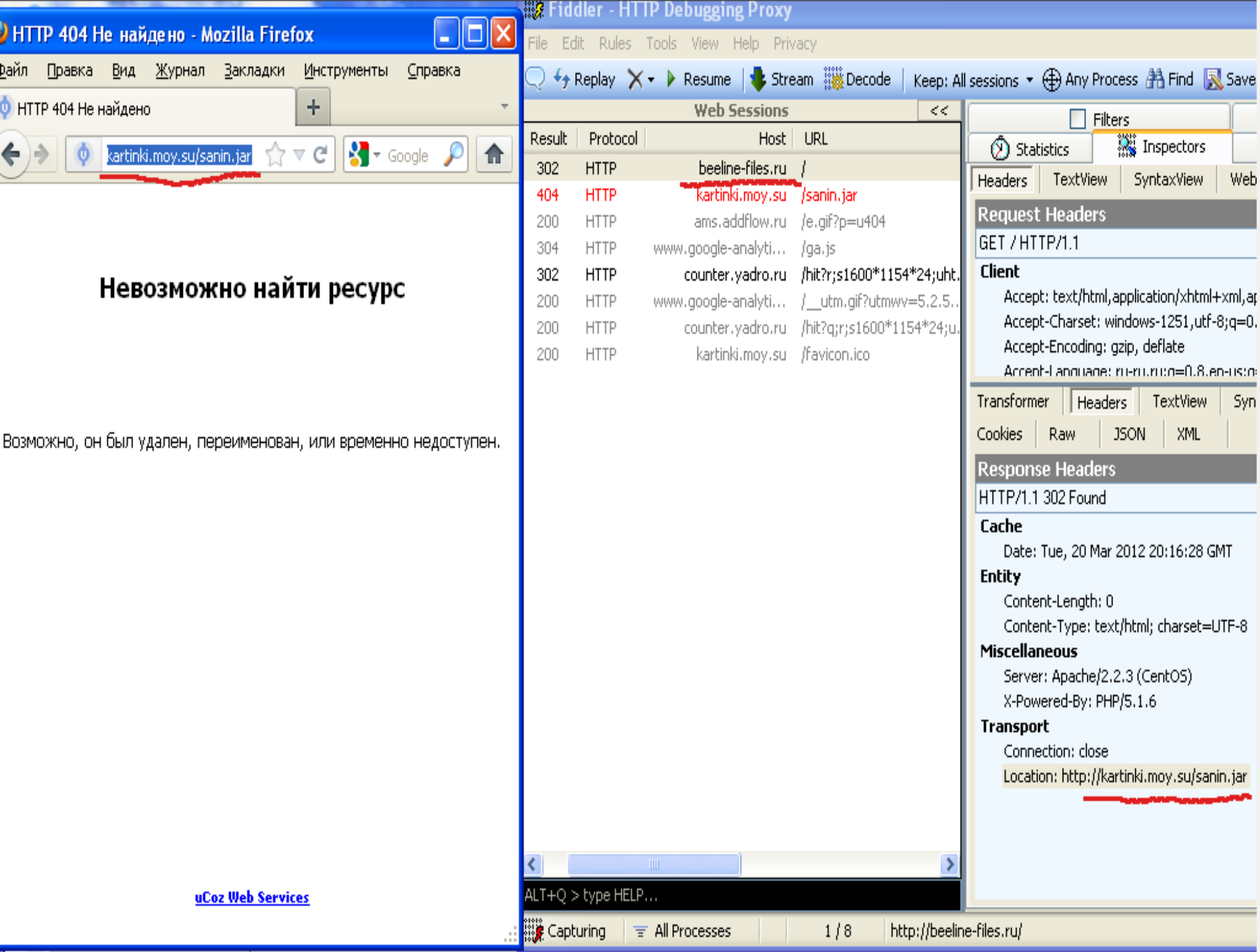
Detection ratio: 24 / 42

Analysis date: 2012-03-13 08:15:32 UTC ( 1 minute ago )

Beeline-files.ru
sample

| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | - | 20120312 |
| AntiVir | Tr/SMSer.S.14 | 20120313 |
| Antiy-AVL | Trojan/win32.agent | 20120313 |
| Avast | Java:SMSSend-CO [Trj] | 20120312 |
| AVG | Java/SMS.AM | 20120313 |
| BitDefender | Trojan.Java.SMSsend.G | 20120313 |
| ByteHero | - | 20120309 |


Whois сервис - проверка свободного домена | REG.RU - Mozilla Firefox
Antivirus scan for 66c7d0...
91.212.226.198
Whois сервис - проверка...
Whois сервис - проверка...
www.reg.ru/whois/index?dname=beeline-files.ru
Google
beeline-files.ru
IP-адрес: 91.212.226.198
По данным WHOIS.RIPN.NET:
Домен: BEELINE-FILES.RU
Сервер DNS: ns1.nod3a.netdedicated.ru
Сервер DNS: ns2.nod3a.netdedicated.ru
Статус: зарегистрирован, делегирован, не проверен
Администратор домена: Частное лицо "Private Person"
Регистратор: RU-CENTER-REG-RIPN
Связь с администратором: https://www.nic.ru/cgi/whois_webmail.cgi?domain=BEELINE-FILES.RU
Дата регистрации: 2012.02.19
Регистратор: RU-CENTER-REG-RIPN
Дата регистрации: 2012.02.19
Дата окончания регистрации: 2013.02.19

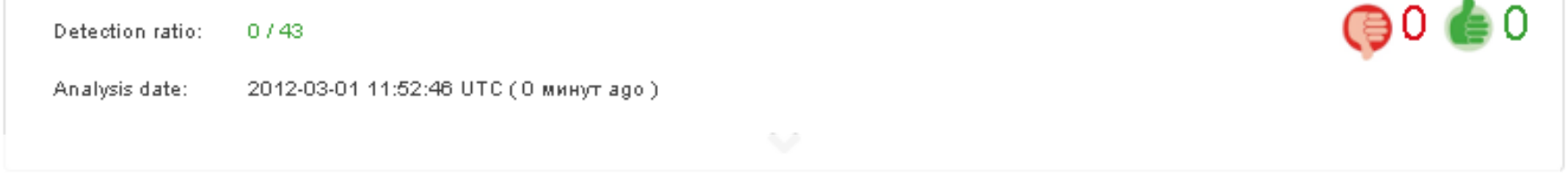

HTTP 404 Не найдено - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
HTTP 404 Не найдено
kartinki.moy.su/sanin.jar
Google
Невозможно найти ресурс
Возможно, он был удален, переименован, или временно недоступен.
uCoz Web Services
Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help Privacy
Replay Resume Stream Decode Keep: All sessions Any Process Find Save
Web Sessions
Result Protocol Host URL
302 HTTP beeline-files.ru /
404 HTTP kartinki.moy.su /sanin.jar
200 HTTP ams.addflow.ru /e.gif?p=u404
304 HTTP www.google-analyti... /ga.js
302 HTTP counter.yadro.ru /hit?r;s1600*1154*24;uht.
200 HTTP www.google-analyti... /__utm.gif?utmwv=5.2.5..
200 HTTP counter.yadro.ru /hit?q;r;s1600*1154*24;u.
200 HTTP kartinki.moy.su /favicon.ico
ALT+Q > type HELP...
Filters
Statistics
Inspectors
Headers TextView SyntaxView Web
Request Headers
GET / HTTP/1.1
Client
Accept: text/html,application/xhtml+xml,ap
Accept-Charset: windows-1251,utf-8;q=0.
Accept-Encoding: gzip, deflate
Transformer Headers TextView Syn
Cookies Raw JSON XML
Response Headers
HTTP/1.1 302 Found
Cache
Date: Tue, 20 Mar 2012 20:16:28 GMT
Entity
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Miscellaneous
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Transport
Connection: close
Location: http://kartinki.moy.su/sanin.jar
Capturing All Processes 1 / 8 http://beeline-files.ru/

# Reputation:

| Source | Result |
|---|---|
| BLACKLIST | LISTED IN BLACKLIST!<br>zen.spamhaus.org<br>sbl.spamhaus.org<br>sbl-xbl.spamhaus.org |

CNET 91.212.226
91.212.226.0/24 Netdedicated Solutions AS5577

| Base | Record | Name | IP | Reverse | Route |
|---|---|---|---|---|---|
| beeline-mms.mobi | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | 91.212.226.0/2<br>Netdedicated So |
| freerumms.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| lovemmsru.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.freerumms.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.lovemmsru.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.mms-rus.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.repa4ok.biz | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.ru-mms.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mail.rummsfree.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |
| mms-rus.com | a | | 91.212.226.198<br>Russian Federation | ip-91-212-226-198.as5577.net | |




# Монетизация через заражение ПК и использование украденных с ПК данных

Вы думаете компьютер еще Ваш?

Да что с моего компьютера можно взять?

Вы неправы, у Вас могут увести все пароли, включая почту, соц. Сети, на доступ к ПК, сделать дамп аппаратных ключей защиты, начать рассылать СПАМ, сообщения Вашим друзьям от Вашего имени с различными просьбами и заработать на этом.


# Пример события IDS в Феврале

Date/Time 2012-02-23 11:04:13 YEKT

Tag Name HTTP_Executable_Transfer

Target IP Address 31.170.163.188

Target Port 80

:arg fname=drayvera-posledovatelniy-port-pci

:server sdhhhgffff.bugs3.com

:URL /1/download.php

virustotal

SHA256: 760563aaab12983b816600f04473fa5acce6c3c3a25588152bc1c0b9ee27c3ef

File name: draywera-posledovatelniy-port-pc.exe

Detection ratio: 10 / 43

Analysis date: 2012-03-13 10:58:38 UTC ( 1 week ago ) View latest


| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | - | 20120312 |
| AntiVir | - | 20120313 |
| Antiy-AVL | - | 20120312 |
| Avast | - | 20120313 |
| AVG | - | 20120313 |
| BitDefender | - | 20120313 |

virustotal

SHA256: 760563aaab12983b816600f04473fa5acce6c3c3a25588152bc1c0b9ee27c3ef

File name: 66c7d096e050804e74dcbfb0cef04815

Detection ratio: 24 / 43

Analysis date: 2012-03-16 18:55:15 UTC ( 3 days, 23 hours ago )


| Antivirus | Result | Update |
|---|---|---|
| AhnLab-V3 | - | 20120316 |
| AntiVir | TR/Vundo.OD.897 | 20120316 |
| Antiy-AVL | Trojan/Win32.Cidox.gen | 20120316 |
| Avast | Win32:Crypt-LWJ [Trj] | 20120316 |
| AVG | Generic27.ASBM | 20120316 |
| BitDefender | Trojan.Generic.7315328 | 20120316 |

| Source | Result |
|---|---|
| BLACKLIST | not listed in any blacklists |

CNET 31.170.163
31.170.160.0/21 CB/Immedion/II Hosting AS36167 (not announced) AS47583 (not announced)
31.170.160.0/22 MAIN HOSTING US AS47583
31.170.162.0/23 AS47583 (not registered)
31.170.163.0/24 AS47583 (not registered)

| Base | Record | Name | IP | Reverse |
|---|---|---|---|---|
| *.casting18.com | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| admahmud.co.cc | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| burnfat-loseweight.info | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| carloanswithbadcredittoday.com | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| casting18.com | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| celestineleonida82.realservers.info | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| ckap.info | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| dentysci.tk | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| dingoditches.info | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| docug.icopo.nuzoka.com | a | | 31.170.163.188 United States | 31-170-163-188.main-hosting.com |
| docug.uxade.nuzoka.com | a | | 31.170.163.188 | 31-170-163-188.main- |

Ymishow.info, kug6.com, casting18.com, and at least 43 other hosts point to 31.170.163.188.


Кому: 'abuse@burst.net'

Тема: Please suspend: Exploit and malware hosting 46.37.181.23

Dear colleagues.

We detected malware download from your IP range.

Please suspend the hosting account responsible for the following URL:

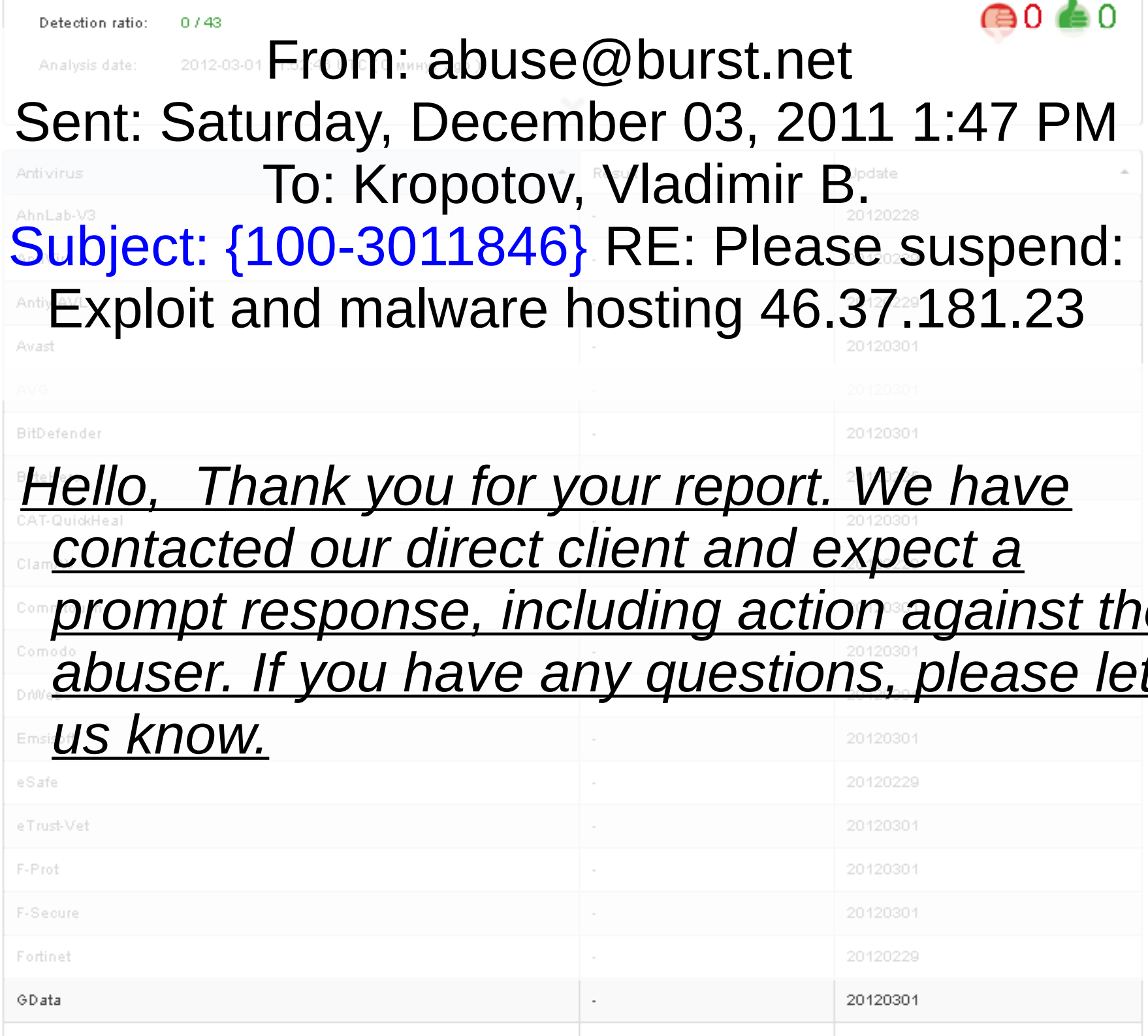
46.37.181.23

Date/Time 2011-11-29 10:01:29 MSK

Tag Name HTTP_Executable_Transfer

:server allmondrage.ru

:URL /photo-00254/002400254/IMG_1693.scr



From: abuse@burst.net
Sent: Saturday, December 03, 2011 1:47 PM
To: Kropotov, Vladimir B.
Subject: {100-3011846} RE: Please suspend: Exploit and malware hosting 46.37.181.23

*Hello, Thank you for your report. We have contacted our direct client and expect a prompt response, including action against the abuser. If you have any questions, please let us know.*

File name: **IMG_1693.scr**
Submission date: **2011-11-29 13:19:45 (UTC)**
Current status: **finished**
Result: **25/ 43 (58.1%)**

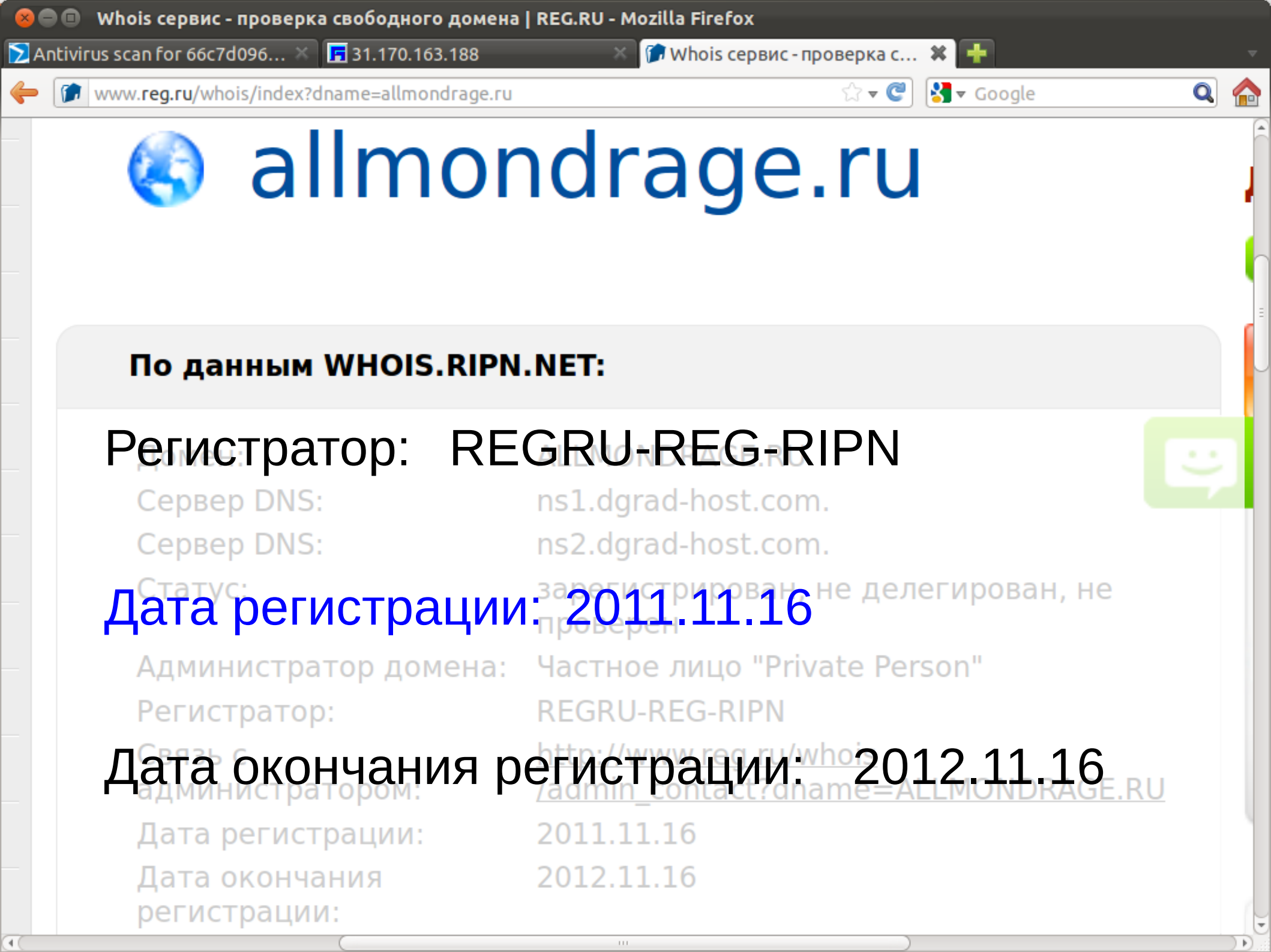
not reviewed

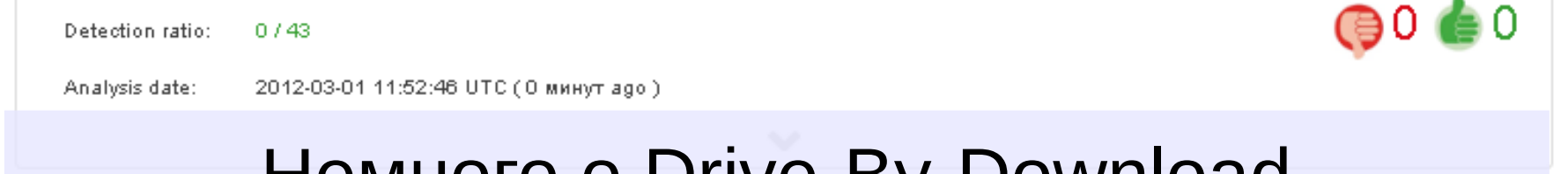
Safety score: -

Compact

Print results

| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2011.11.29.00 | 2011.11.29 | Trojan/Win32.Qhost |
| AntiVir | 7.11.18.119 | 2011.11.29 | - |
| Antiy-AVL | 2.0.3.7 | 2011.11.29 | Trojan/Win32.Qhost.gen |
| Avast | 6.0.1289.0 | 2011.11.29 | Win32:Rootkit-gen [Rtk] |
| AVG | 10.0.0.1190 | 2011.11.29 | unknown virus Win32/DH.00000000{00000080-00000000-00000000} |
| BitDefender | 7.2 | 2011.11.29 | - |
| ByteHero | 1.0.0.1 | 2011.11.29 | Trojan.Win32.Heur.089 |
| CAT-QuickHeal | 12.00 | 2011.11.29 | - |
| ClamAV | 0.97.3.0 | 2011.11.29 | BC.Heuristic.Trojan.SusPacked.TMS |
| Commtouch | 5.3.2.6 | 2011.11.29 | - |
| Comodo | 10793 | 2011.11.29 | UnclassifiedMalware |
| DrWeb | 5.0.2.03300 | 2011.11.29 | Trojan.KillFiles.7479 |
| Emsisoft | 5.1.0.11 | 2011.11.29 | Trojan.Win32.Qhost!IK |


Whois сервис - проверка свободного домена | REG.RU - Mozilla Firefox
Antivirus scan for 66c7d096...
31.170.163.188
Whois сервис - проверка с...
www.reg.ru/whois/index?dname=allmondrage.ru
Google
allmondrage.ru
По данным WHOIS.RIPN.NET:
Сервер DNS: ns1.dgrad-host.com.
Сервер DNS: ns2.dgrad-host.com.
Статус: зарегистрирован, не делегирован, не проверен
Администратор домена: Частное лицо "Private Person"
Регистратор: REGRU-REG-RIPN
Дата регистрации: 2011.11.16
Дата окончания регистрации: 2012.11.16
Регистратор: REGRU-REG-RIPN
Дата регистрации: 2011.11.16
Дата окончания регистрации: 2012.11.16




# Немного о Drive-By-Download
# Интересный случай с интернет-магазином*

Домены, которые участвовали в атаке:

google.ru – поисковый сервер

kitaycev.net – интернет магазин

presto.bee.pl – промежуточный сервер

industry.bee.pl – сервер с вредоносным ПО

**при анализе нам помогал*
*Владимир Воронцов из ONsec*


# URL, участвующие в атаке

http://www.google.ru/url?sa=t&rct=j&q=epos%20epos%20originale%203387.152.24.20.15&source=web&cd=54&ved=0CD4QFjADODI&url=http%3A%2F%2Fkitaycev.net%2Findex.php%3Fpage%3Dshop.browse%26category_id%3D41%26option%3Dcom_virtuemart%26Itemid%3D7&ei=gBc6T6zrJfTb4QS60pmMCw&usg=AFQjCNHjF2Po-ekXnnG20wUBzTLjDHaDbw&cad=rjt

http://kitaycev.net/index.php?page=shop.browse&category_id=41&option=com_virtuemart&Itemid=7

http://industry.bee.pl/

http://presto.bee.pl/main.php?page=e4a99b291b9c52c5

http://presto.bee.pl/w.php?f=17&e=2

http://presto.bee.pl/content/rin.jar

# Роль google.ru

Для того, чтобы средства защиты видели легитимный домен

Страница, которая открывается по URL из Log  содержит такой код:

```
<META http-equiv="refresh" content="0;URL='http://kitaycev.net/index.php?
    page=shop.browse&amp;category_id=41&amp;option=com_virtuemart&
    amp;Itemid=7'">
```

Она перенаправляет пользователя на на следующий хост.

Адрес этого хоста (URL-декодированном виде) передается в параметре GET url google:

```
http://kitaycev.net/index.php?
    page=shop.browse&category_id=41&option=com_virtuemart&Itemid=7
```

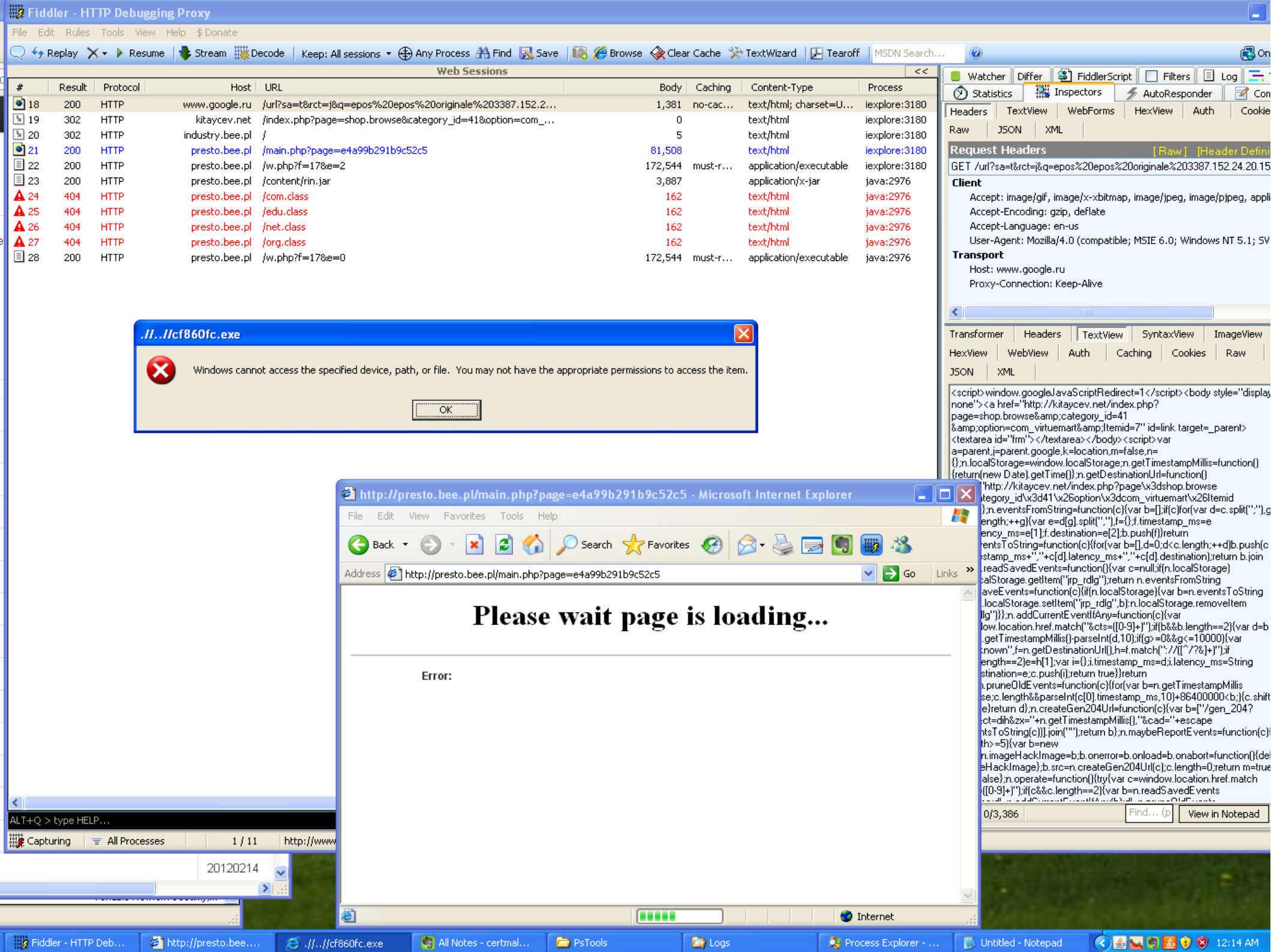
# Роль kitaycev.net

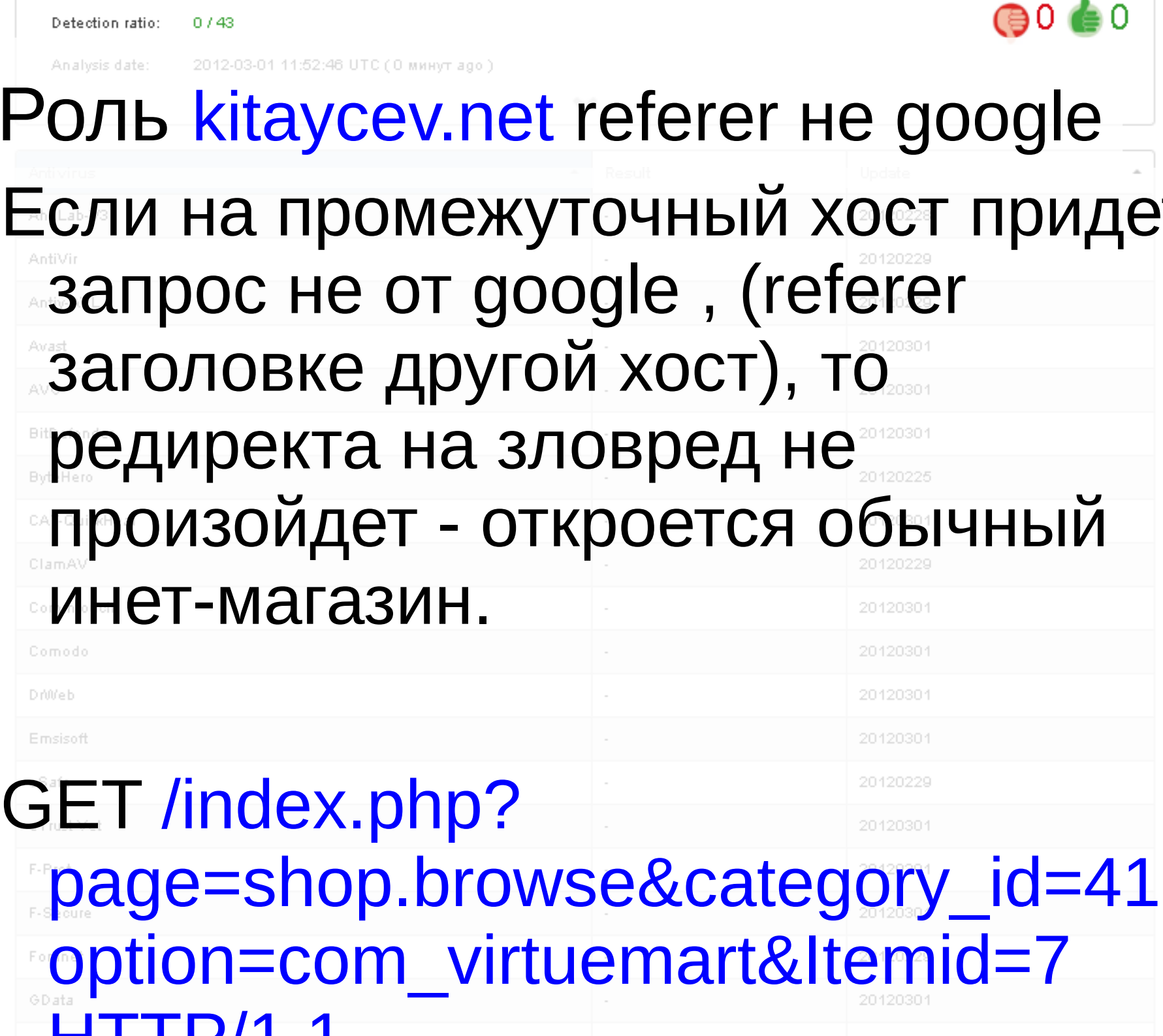
Если на промежуточный хост придет запрос от google, этот хост в свою очередь отрабатывает следующим редиректом уже на целевой хост с зловредом:

Вот запрос пользователя, когда в рефере стоит гугл:

GET /index.php?page=shop.browse&category_id=41&option=com_virtuemart&Itemid=7 HTTP/1.1

Host: kitaycev.net


Fiddler - HTTP Debugging Proxy
File Edit Rules Tools View Help $ Donate
Replay Resume Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...
Web Sessions
# Result Protocol Host URL Body Caching Content-Type Process
18 200 HTTP www.google.ru /url?sa=t&rct=j&q=epos%20epos%20originale%203387.152.2... 1,381 no-cac... text/html; charset=U... iexplore:3180
19 302 HTTP kitaycev.net /index.php?page=shop.browse&category_id=41&option=com_... 0 text/html iexplore:3180
20 302 HTTP industry.bee.pl / 5 text/html iexplore:3180
21 200 HTTP presto.bee.pl /main.php?page=e4a99b291b9c52c5 81,508 text/html iexplore:3180
22 200 HTTP presto.bee.pl /w.php?f=17&e=2 172,544 must-r... application/executable iexplore:3180
23 200 HTTP presto.bee.pl /content/rin.jar 3,887 application/x-jar java:2976
24 404 HTTP presto.bee.pl /com.class 162 text/html java:2976
25 404 HTTP presto.bee.pl /edu.class 162 text/html java:2976
26 404 HTTP presto.bee.pl /net.class 162 text/html java:2976
27 404 HTTP presto.bee.pl /org.class 162 text/html java:2976
28 200 HTTP presto.bee.pl /w.php?f=17&e=0 172,544 must-r... application/executable java:2976
Watcher Differ FiddlerScript Filters Log
Statistics Inspectors AutoResponder
Headers TextView WebForms HexView Auth Cookie
Raw JSON XML
Request Headers [Raw] [Header Defini
GET /url?sa=t&rct=j&q=epos%20epos%20originale%203387.152.24.20.15
Client
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, appli
Accept-Encoding: gzip, deflate
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV
Transport
Host: www.google.ru
Proxy-Connection: Keep-Alive
Transformer Headers TextView SyntaxView ImageView
HexView WebView Auth Caching Cookies Raw
JSON XML
<script>window.googleJavaScriptRedirect=1</script><body style="display
none"><a href="http://kitaycev.net/index.php?
page=shop.browse&category_id=41
&option=com_virtuemart&Itemid=7" id=link target=_parent>
<textarea id="frm"></textarea></body><script>var
a=parent,j=parent.google,k=location,m=false,n=
{};n.localStorage=window.localStorage;n.getTimestampMillis=function()
{return(new Date).getTime()};n.getDestinationUrl=function()
0/3,386
Find... (p
View in Notepad
.//..//cf860fc.exe
Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.
OK
http://presto.bee.pl/main.php?page=e4a99b291b9c52c5 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://presto.bee.pl/main.php?page=e4a99b291b9c52c5
Go Links
Please wait page is loading...
Error:
Internet
ALT+Q > type HELP...
Capturing All Processes 1 / 11 http://www
20120214
Fiddler - HTTP Deb...
http://presto.bee....
.//..//cf860fc.exe
All Notes - certmal...
PsTools
Logs
Process Explorer - ...
Untitled - Notepad
12:14 AM




Роль kitaycev.net referer не google

Если на промежуточный хост придет запрос не от google , (referer заголовке другой хост), то редиректа на зловред не произойдет - откроется обычный инет-магазин.

GET /index.php?page=shop.browse&category_id=41&option=com_virtuemart&Itemid=7 HTTP/1.1

Epos - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://kitaycev.net/index.php?page=shop.browse&category_id=41&option=com_virtuemart&Itemid=7&vmcchk=1&Itemid=7

Go Links

Главная | Оплата и доставка | Гарантии | Отзывы | Контакты

8 499 343 32 74

Звоните с 9 до 21 - 00
(без выходных)

***Интернет магазин наручных часов***

КОРЗИНА:
*0 товара(ов)*
оформить заказ...

Не можете выбрать?
Закажите звонок

Контактная почта
zakaz@kitaycev.net

**Гарантия возврата денег**

Вы можете вернуть товар в течении 7 дней без объяснения причин


**Бесплатная доставка по России**

Мы осуществляем бесплатную доставку по всей России!

**Внимание! Акция!**

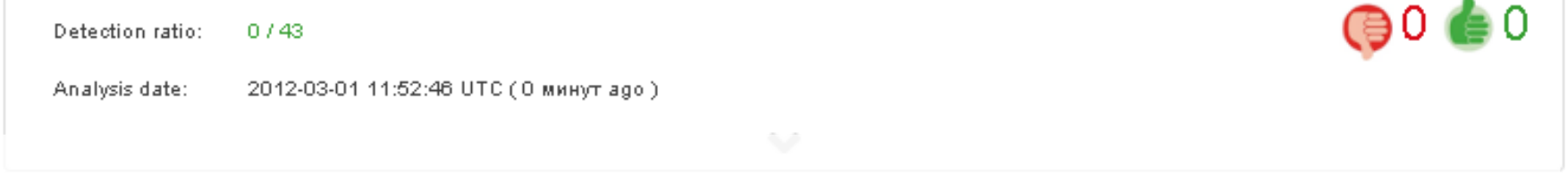
При заказе на сумму 5000р. вы получаете скидку 10%

КАТАЛОГ ТОВАРОВ

- LED часы
  - Phosfor
    - Мужские
      - F link

Done Internet

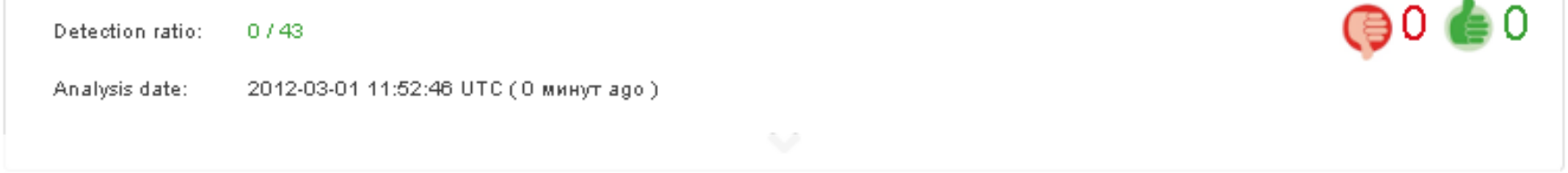
# Географическое положение хостингов




# Темы, которые не затронули

- Монетизация через альтернативные системы оплаты (например Ваучеры)
- Вымогательство (например WinLock)

| | | |
|---|---|---|
| AhnLab-V3 | - | 20120229 |
| AntiVir | - | 20120229 |
| Antiy-AVL | - | 20120229 |
| Avast | - | 20120301 |
| AVG | - | 20120301 |
| CAT-QuickHeal | - | 20120301 |
| ClamAV | - | 20120229 |
| Commtouch | - | 20120301 |
| DrWeb | - | 20120301 |
| Emsisoft | - | 20120301 |
| eSafe | - | 20120229 |
| eTrust-Vet | - | 20120301 |
| F-Prot | - | 20120301 |
| F-Secure | - | 20120301 |
| Fortinet | - | 20120229 |
| GData | - | 20120301 |




# Выводы

- Участвовать в распространении вредоносного ПО может любой из хостов интернет от поисковой системы до интернет магазина
- Надо с бОльшей осторожностью относиться к ресурсам которые требуют ввода сотового телефона, особенно должны настораживать СМС, которые требуют ответа
- Загрузка исполняемых файлов на любые платформы должна производиться

virustotal.com https://www.virustotal.com/file/8d9e5c1122b0de9e640d312a953cfc1a3a8d54e490a067ed8de852e Google

Начало Community Statistics Документация FAQ About Join our community Sign in

SHA256: 8d9e5c1122b0de9e640d312a953cfc1a3a8d54e490a067ed8de852ef6b9cf3cd

File name: Applet.class

Detection ratio: 0 / 43

Analysis date: 2012-02-16 06:15:15 UTC ( 0 минут ago )


SHA256: 8d9e5c1122b0de9e640d312a953cfc1a3a8d54e490a067ed8de852ef6b9cf3cd

File name: Applet.class

Detection ratio: 2 / 43

Analysis date: 2012-02-21 05:12:25 UTC ( 3 дней, 2 часов ago )

Спасибо!


SHA256: 8d9e5c1122b0de9e640d312a953cfc1a3a8d54e490a067ed8de852ef6b9cf3cd

File name: Applet.class

Detection ratio: 3 / 43

Analysis date: 2012-02-24 07:31:14 UTC ( 0 минут ago )

# Монетизация через ваучеры

Работает, чаще встречается за границей: