

Development of the “Domains classifier”

Tsvetkov Alexey (avt@tcinet.ru)

2013

Main purposes

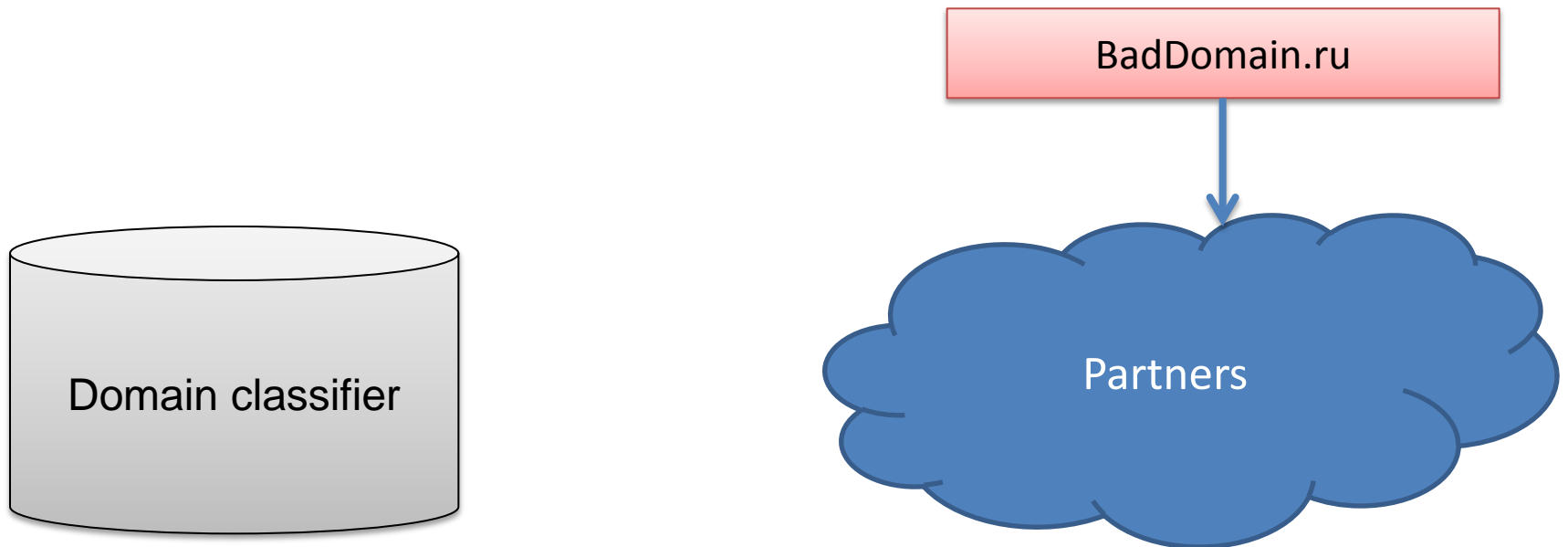
1. Information exchange between our partners, about domains, containing:
 - Malware
 - Phishing
 - Spam
 - Botnet C&C
 - Etc.
2. Data analyzing
3. Collecting statistics how owner uses domain.

Our partners:



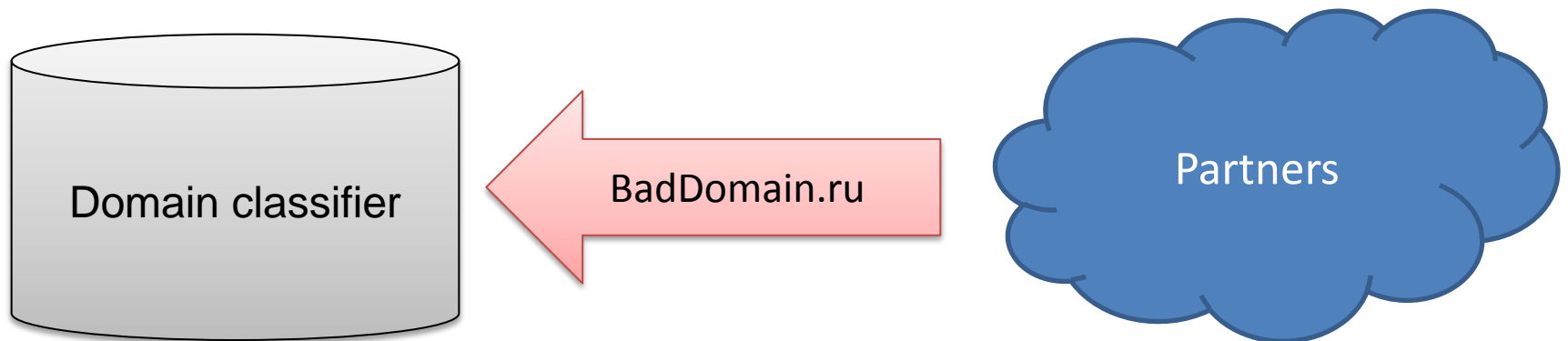
Scheme of work

Step 1. Our partners get information about “bad domain”



Scheme of work

Step 2. Our partners give this information to us



Scheme of work

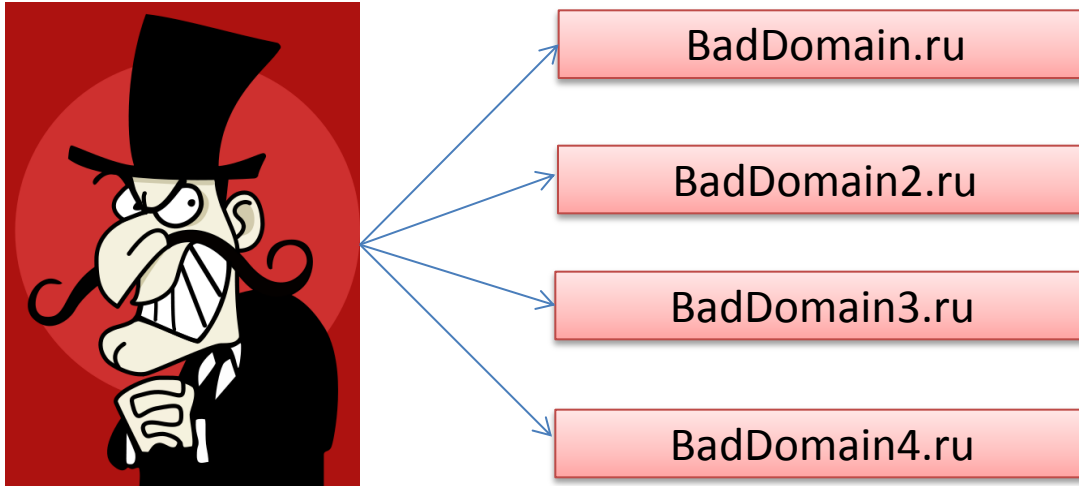
Step 3. We take information about all domains from registry



Domain name	Hash of owner
Domain1.ru	7b026a8558acf7bf45a903423afcf55d
Domain2.ru	7b026a8558acf7bf45a903423afcf55d
BadDomain.ru	C27702d55c023722bd8c3f497ce6a42d
AnotherDomain.ru	Aec169dff489b8b189145682a2a16791
SomeDomain.ru	aec169dff489b8b189145682a2a16791

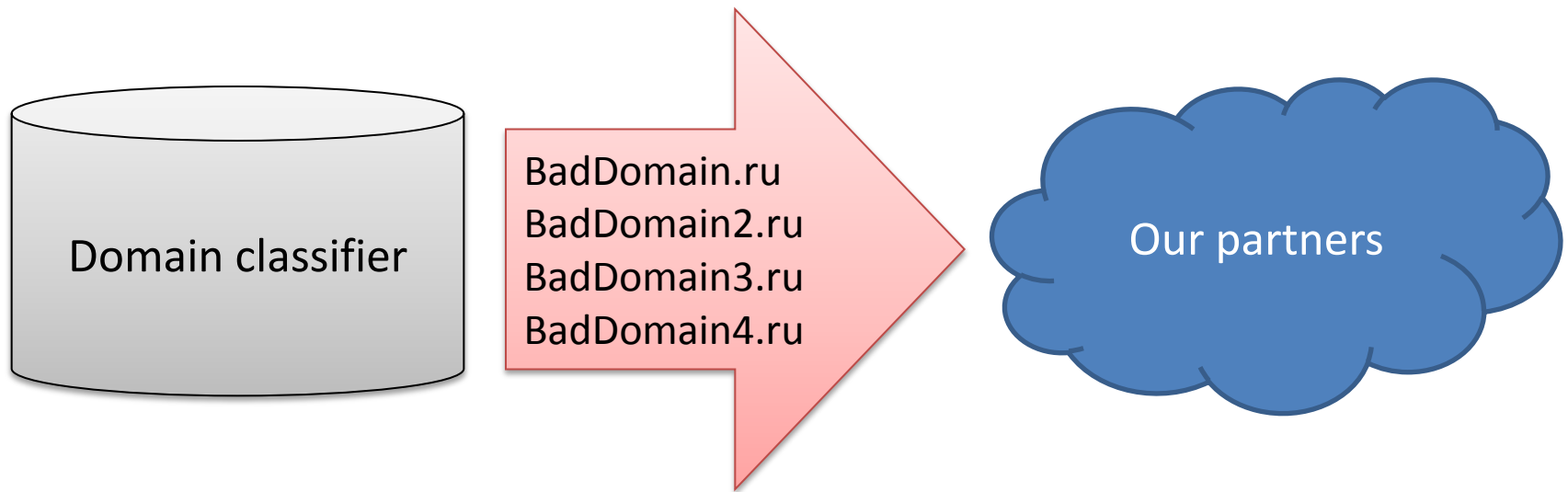
Scheme of work

Step 4. «Bad guy» and all of his domains.



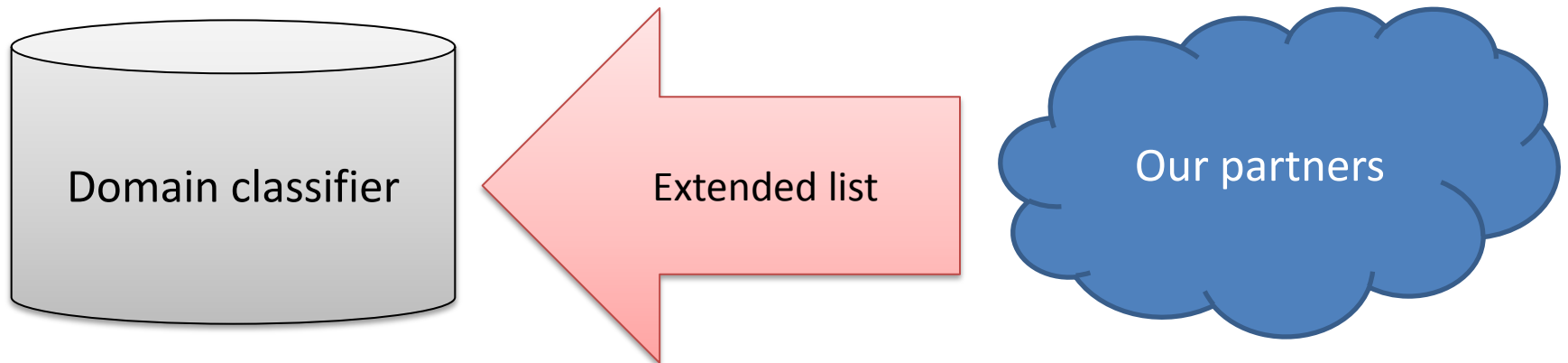
Scheme of work

Step 5. We give list of all domains with the same hash



Scheme of work

Step 6. Partners return classification of this list



Some figures

Category

All domains in project
Kaspersky Lab
RU-CERT

Amount of domains

1 102 802
808 400
311 181

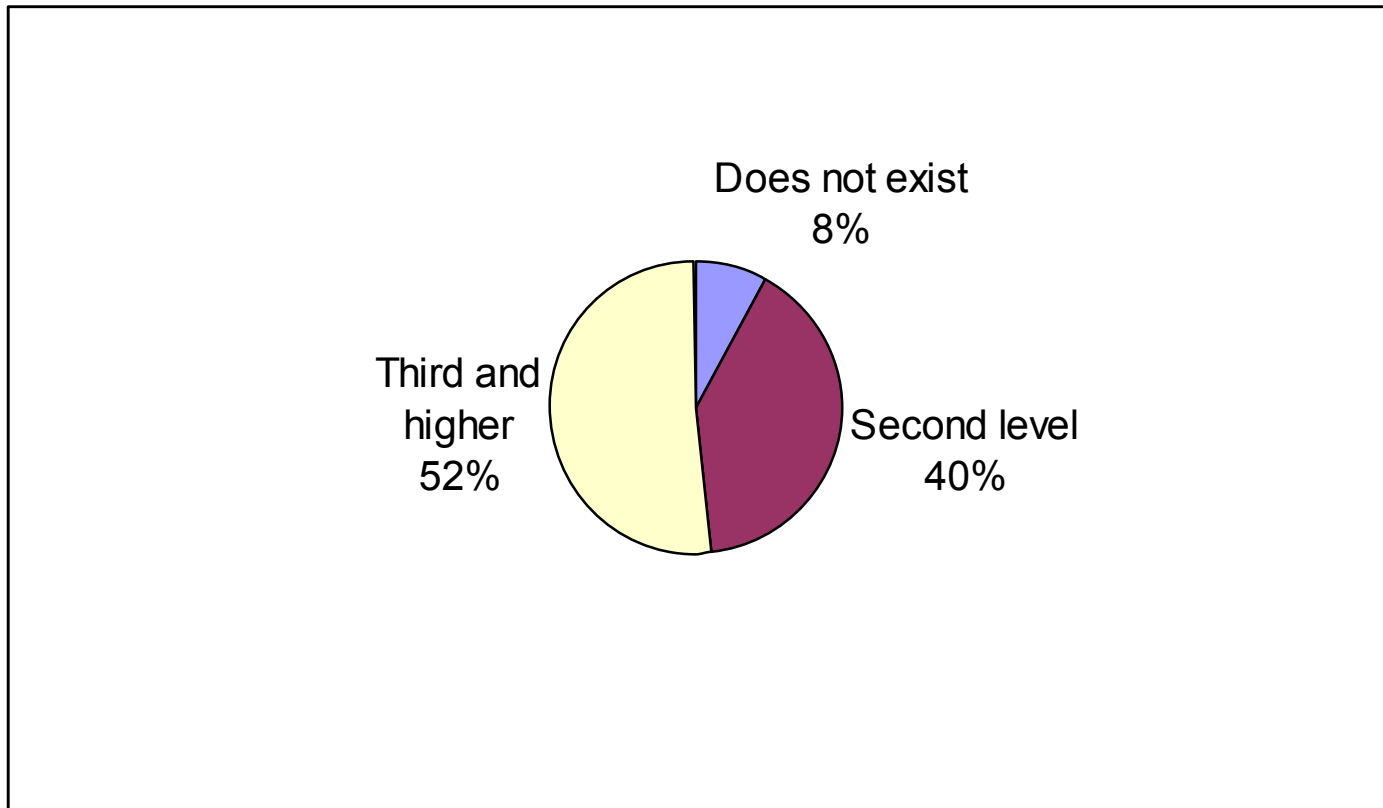
Malware
Phishing
Spam
More than one category

643 809
12 854
14 938
4 166

Yandex Safe Browsing

Category	Amount	
	All	Marked in SB
All domains in project	1 102 802	17 288
All domains from Kaspersky Lab	808 400	14 520
All domains from RU-CERT	311 181	3 604
Kaspersky Lab \cap RU-CERT	12 236	834

Levels

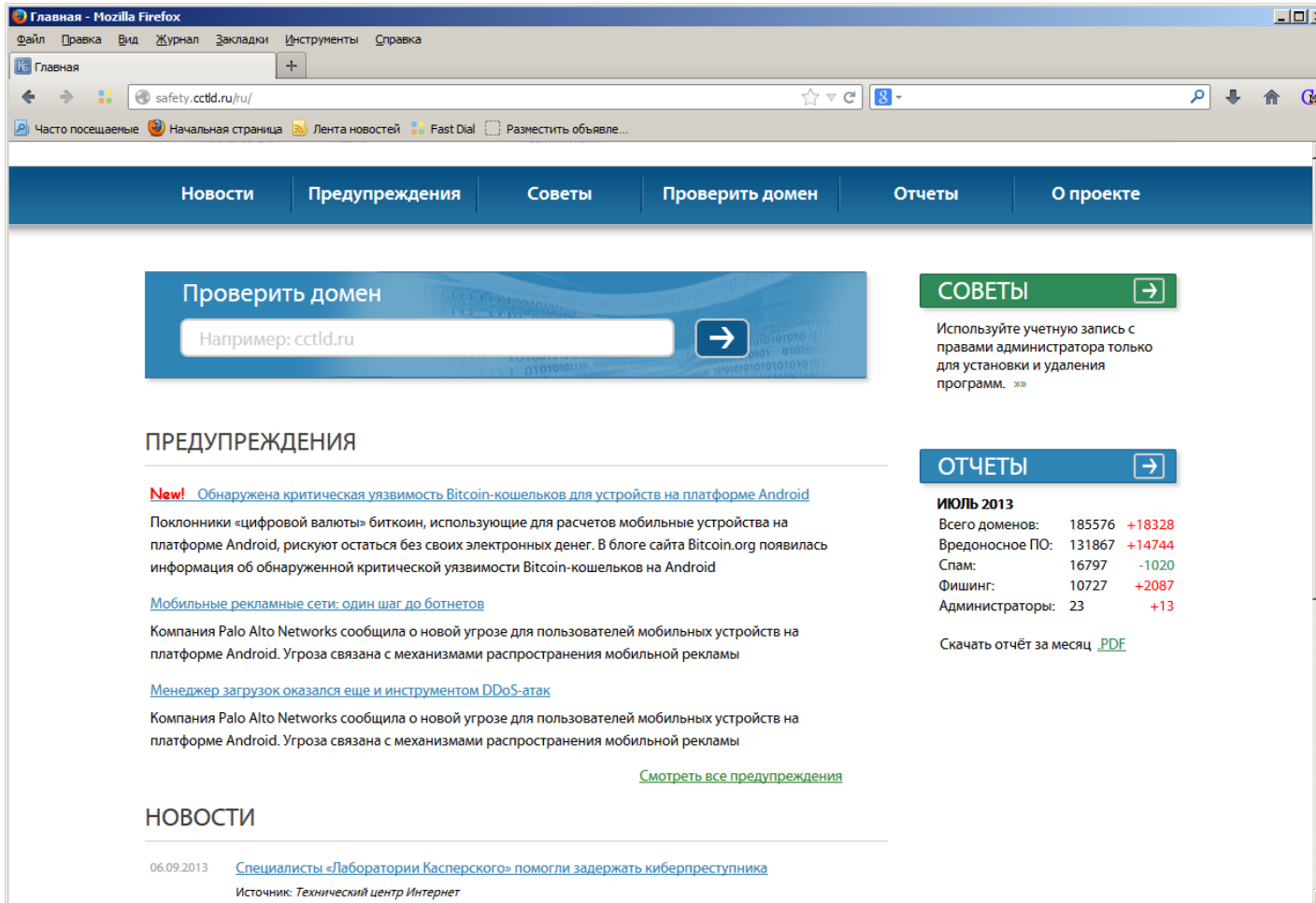


Top 10 of «bad guys»

Hash	Amount of domains with this hash	Amount of domains marked like «bad»	%
7b026a8558acf7bf45a903423afcf55d	8006	7782	97,20
c27702d55c023722bd8c3f497ce6a42d	4420	4420	100,00
b19d7c54bbbe567634dbdcac55bc61e6	4441	4144	93,31
83595a2345dd16e40f5e3f0f2c68b6ab	3033	3031	99,93
8f96be8a02c24cf3b26476675bbac5ab	3192	2549	79,86
23ce93a0b6ddf59e57834445c93d734a	2334	2289	98,07
2fab601c3f9977b0fd1b303165267259	2200	2200	100,00
8e99aca779ff58fc9c5a86e5af686991	1985	1985	100,00
92a1a520131122c93daa75649ba7f68d	1700	1677	98,65
d0ac56d8aa8d446b38d669c4a1845629	1540	1540	100,00

Our pilot site

<http://safety.cctld.ru/>



Главная - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Главная

safety.cctld.ru/

Часто посещаемые Начальная страница Лента новостей Fast Dial Разместить объявление...

Новости Предупреждения Советы Проверить домен Отчеты О проекте

Проверить домен

Например: cctld.ru

СОВЕТЫ

Используйте учетную запись с правами администратора только для установки и удаления программ. »»

ПРЕДУПРЕЖДЕНИЯ

New! [Обнаружена критическая уязвимость Bitcoin-кошельков для устройств на платформе Android](#)

Поклонники «цифровой валюты» биткоин, использующие для расчетов мобильные устройства на платформе Android, рискуют остаться без своих электронных денег. В блоге сайта Bitcoin.org появилась информация об обнаруженной критической уязвимости Bitcoin-кошельков на Android

[Мобильные рекламные сети: один шаг до ботнетов](#)

Компания Palo Alto Networks сообщила о новой угрозе для пользователей мобильных устройств на платформе Android. Угроза связана с механизмами распространения мобильной рекламы

[Менеджер загрузок оказался еще и инструментом DDoS-атак](#)

Компания Palo Alto Networks сообщила о новой угрозе для пользователей мобильных устройств на платформе Android. Угроза связана с механизмами распространения мобильной рекламы

[Смотреть все предупреждения](#)

ОТЧЕТЫ

ИЮЛЬ 2013

Всего доменов:	185576	+18328
Вредоносное ПО:	131867	+14744
Спам:	16797	-1020
Фишинг:	10727	+2087
Администраторы:	23	+13

Скачать отчет за месяц [.PDF](#)

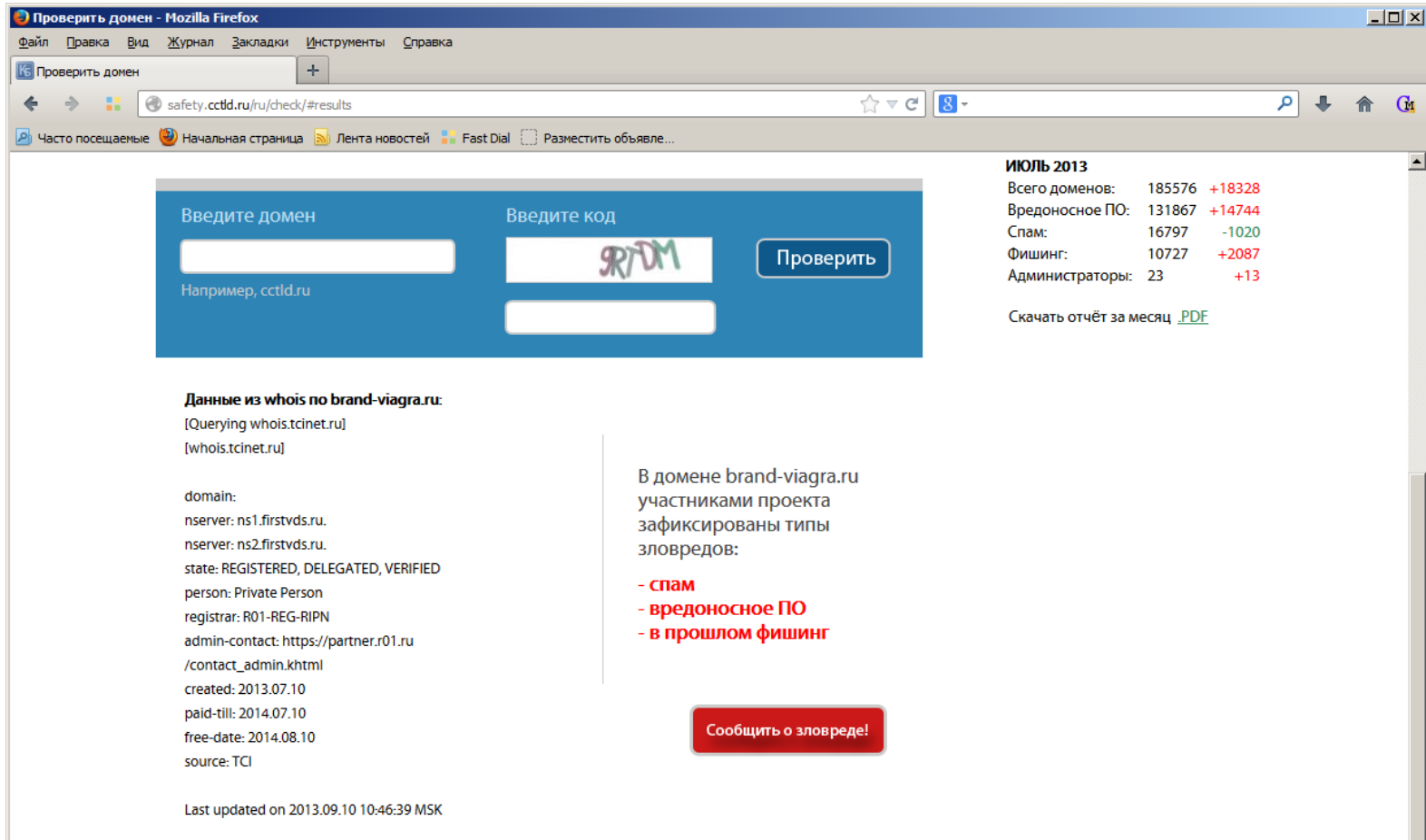
НОВОСТИ

06.09.2013 [Специалисты «Лаборатории Касперского» помогли задержать киберпреступника](#)

Источник: [Технический центр Интернет](#)

Domain checking

<http://safety.cctld.ru/ru/check/>



Проверить домен - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Проверить домен

safety.cctld.ru/ru/check/#results

Часто посещаемые Начальная страница Лента новостей Fast Dial Разместить объявление...

Введите домен Например, cctld.ru

Введите код

ИЮЛЬ 2013

Всего доменов:	185576	+18328
Вредоносное ПО:	131867	+14744
Спам:	16797	-1020
Фишинг:	10727	+2087
Администраторы:	23	+13

Скачать отчёт за месяц [.PDF](#)

Данные из whois по brand-viagra.ru:
[Querying whois.tcinet.ru]
[whois.tcinet.ru]

domain:
nserver: ns1.firstvds.ru.
nserver: ns2.firstvds.ru.
state: REGISTERED, DELEGATED, VERIFIED
person: Private Person
registrar: R01-REG-RIPN
admin-contact: https://partner.r01.ru/contact_admin.khtml
created: 2013.07.10
paid-till: 2014.07.10
free-date: 2014.08.10
source: TCI

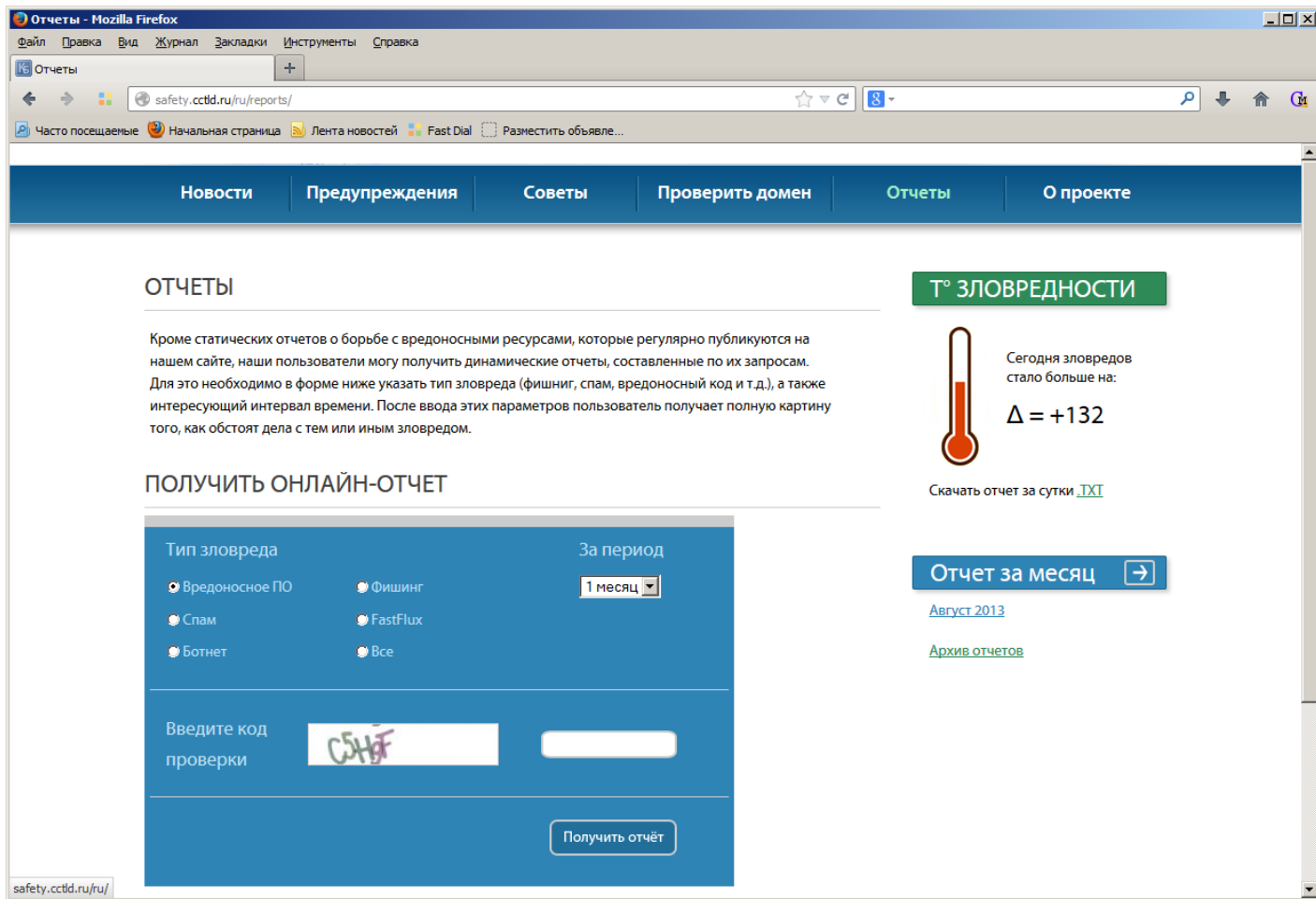
В домене brand-viagra.ru участниками проекта зафиксированы типы зловредов:

- спам
- вредоносное ПО
- в прошлом фишинг

Last updated on 2013.09.10 10:46:39 MSK

Everyday reports

<http://safety.cctld.ru/ru/reports/>



Отчеты - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Отчеты

safety.cctld.ru/ru/reports/

Часто посещаемые Начальная страница Лента новостей Fast Dial Разместить объявление...

Новости Предупреждения Советы Проверить домен **Отчеты** О проекте

ОТЧЕТЫ

Кроме статических отчетов о борьбе с вредоносными ресурсами, которые регулярно публикуются на нашем сайте, наши пользователи могут получить динамические отчеты, составленные по их запросу. Для это необходимо в форме ниже указать тип зловреда (фишинг, спам, вредоносный код и т.д.), а также интересующий интервал времени. После ввода этих параметров пользователь получает полную картину того, как обстоят дела с тем или иным зловредом.

ПОЛУЧИТЬ ОНЛАЙН-ОТЧЕТ

Тип зловреда

Вредоносное ПО Фишинг

Спам FastFlux

Ботнет Все

За период

1 месяц

Введите код проверки

Получить отчёт

Т° ЗЛОВРЕДНОСТИ

Сегодня зловредов стало больше на:

$\Delta = +132$

Скачать отчет за сутки [.TXT](#)

Отчет за месяц [→](#)

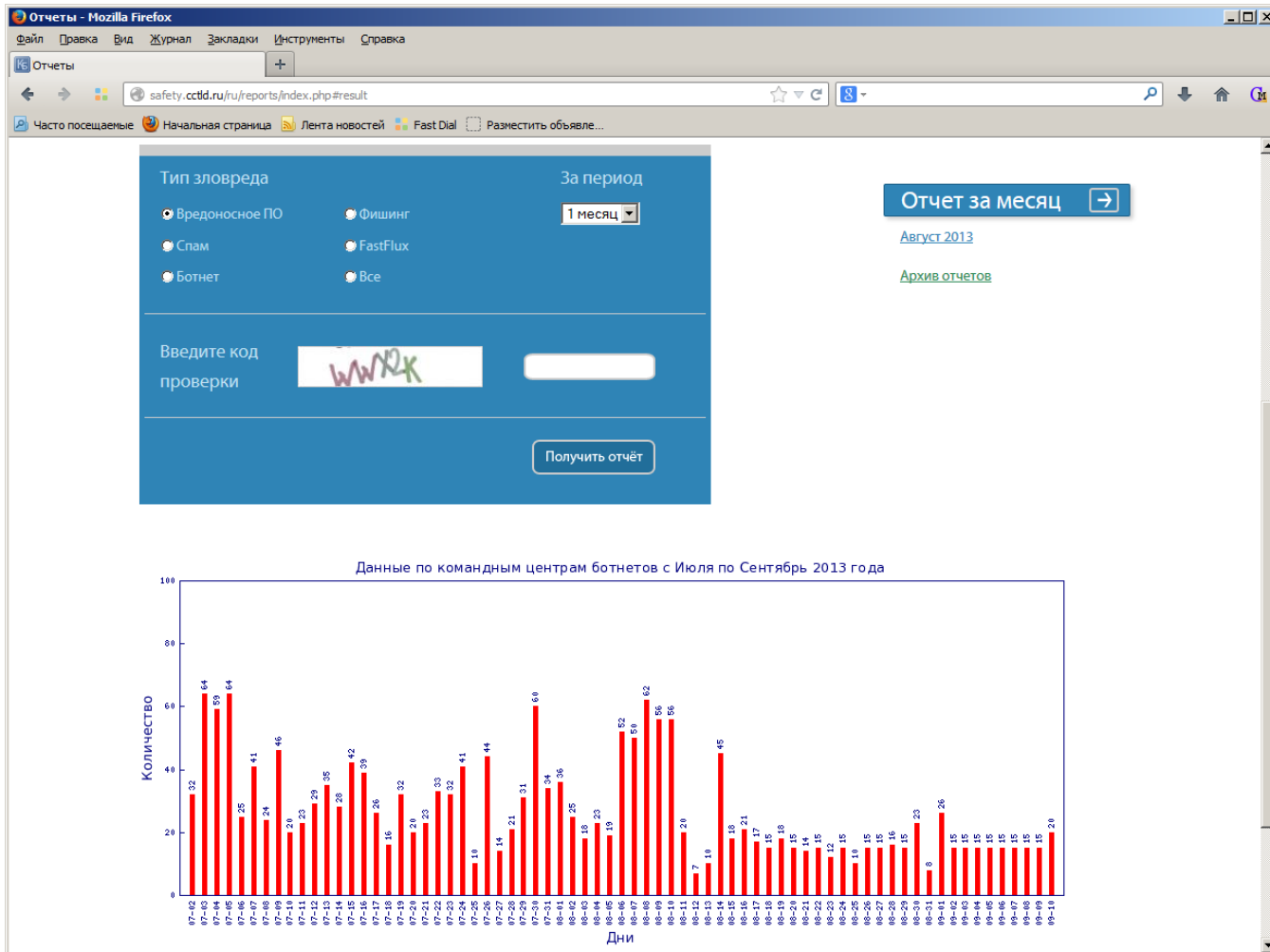
[Август 2013](#)

[Архив отчетов](#)

safety.cctld.ru/ru/

Statistic reports

<http://safety.cctld.ru/ru/reports/>



Thank you!

Questions?

Tsvetkov Alexey (avt@tcinet.ru)