Development of the “Domains classifier"

Tsvetkov Alexey (avt@tcinet.ru)

2013

Технический
Центр
Интернет

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.

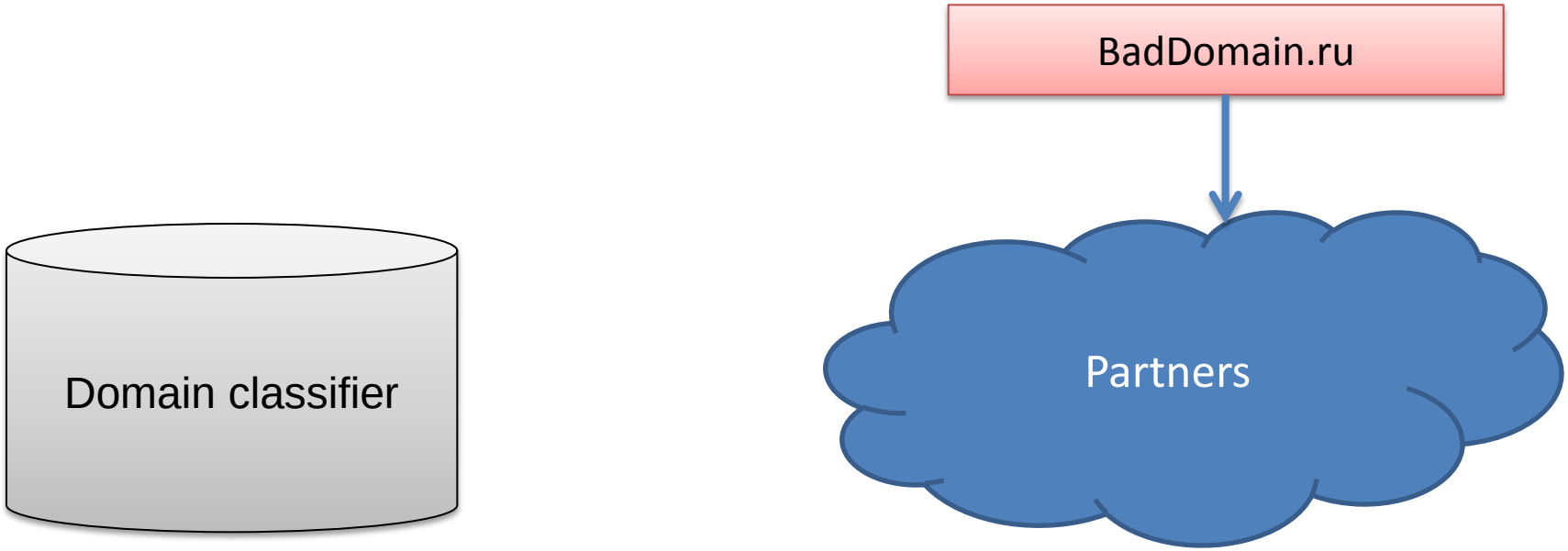
Технический
Центр
Интернет

Our partners:

Технический
Центр
Интернет

Scheme of work

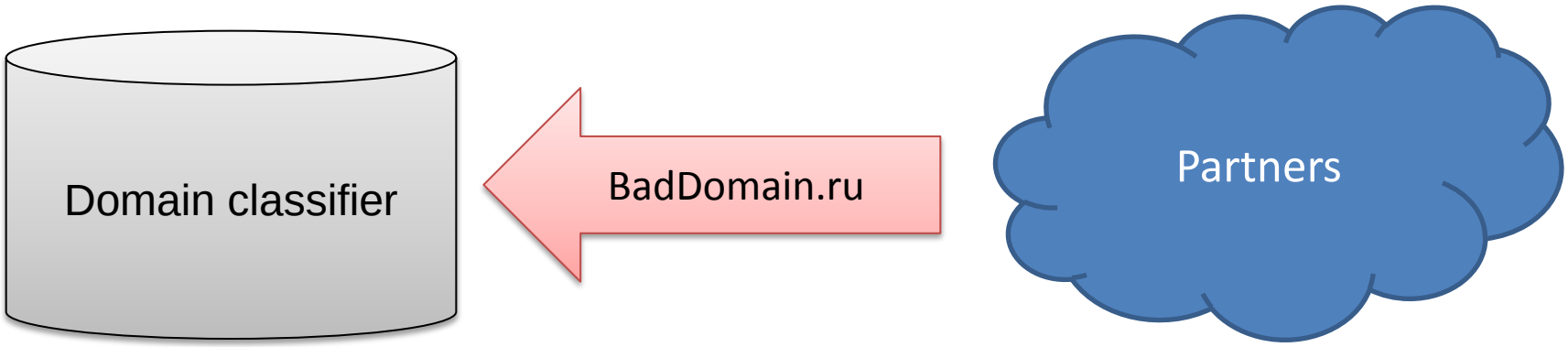
Step 1. Our partners get information about “bad domain”



Технический
Центр
Интернет

Scheme of work

Step 2. Our partners give this information to us



Технический
Центр
Интернет

Scheme of work

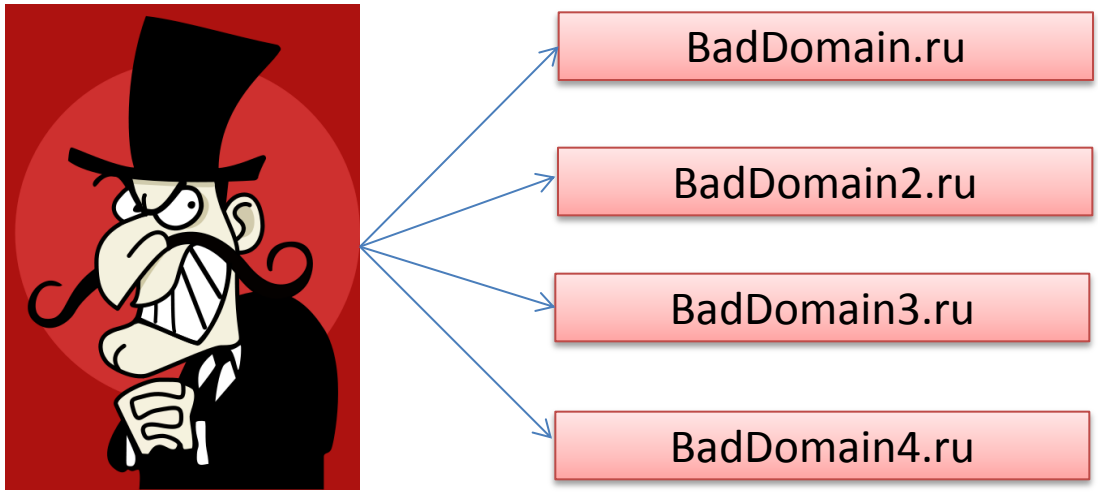
Step 3. We take information about all domains from registry

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

Технический
Центр
Интернет

Scheme of work

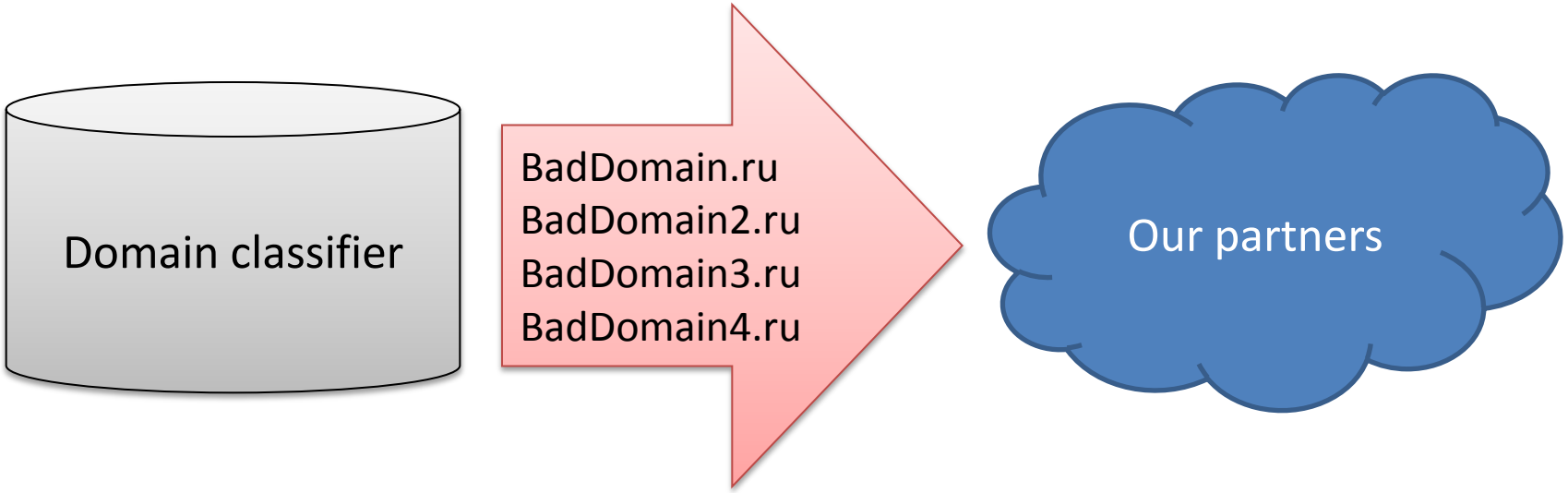
Step 4. «Bad guy» and all of his domains.



Технический
Центр
Интернет

Scheme of work

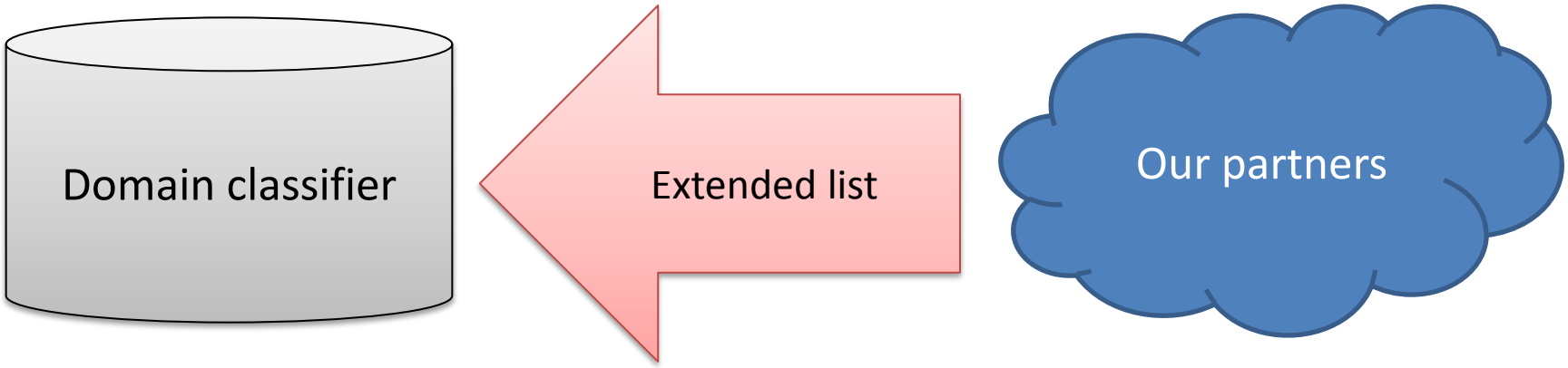
Step 5. We give list of all domains with the same hash



Технический
Центр
Интернет

Scheme of work

Step 6. Partners return classification of this list



Технический
Центр
Интернет

Some figures

Category	**Amount of domains**
All domains in project	1 102 802
Kaspersky Lab	808 400
RU-CERT	311 181
Malware	643 809
Phishing	12 854
Spam	14 938
More than one category	4 166

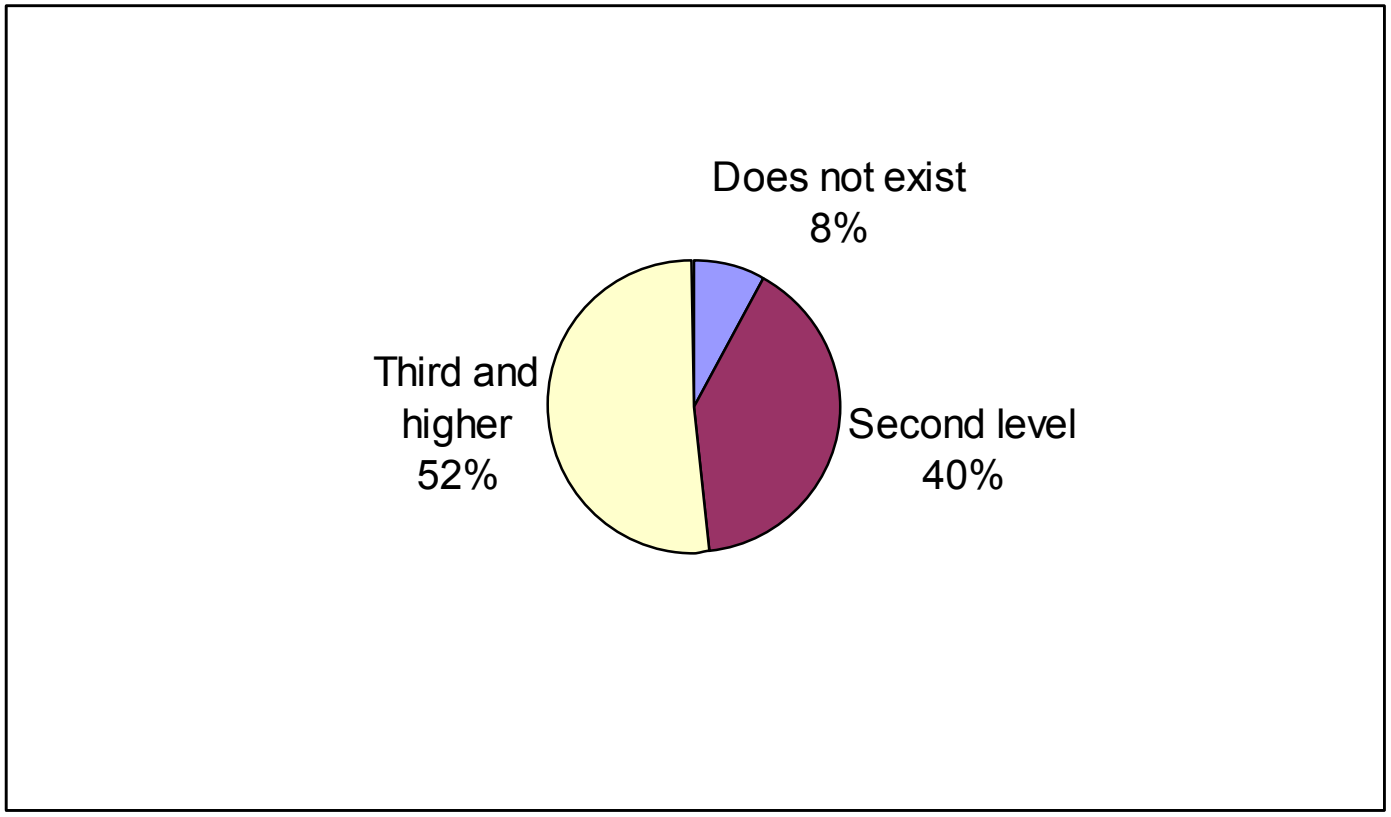
Технический
Центр
Интернет

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 ∩ RU-CERT	12 236	834

Технический
Центр
Интернет

Levels



Технический
Центр
Интернет

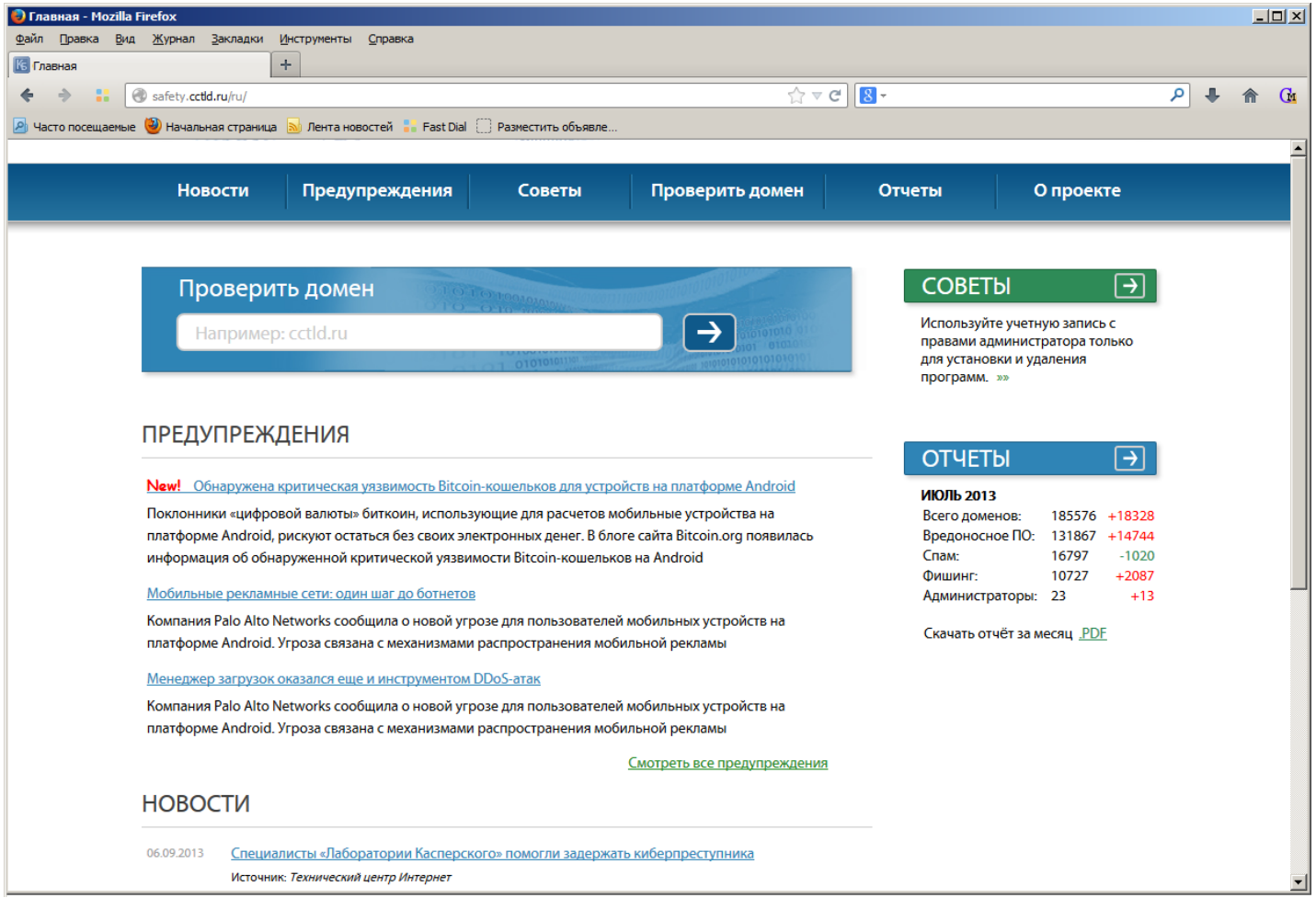
Top 10 of «bad guys»

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

Технический
Центр
Интернет

Our pilot site

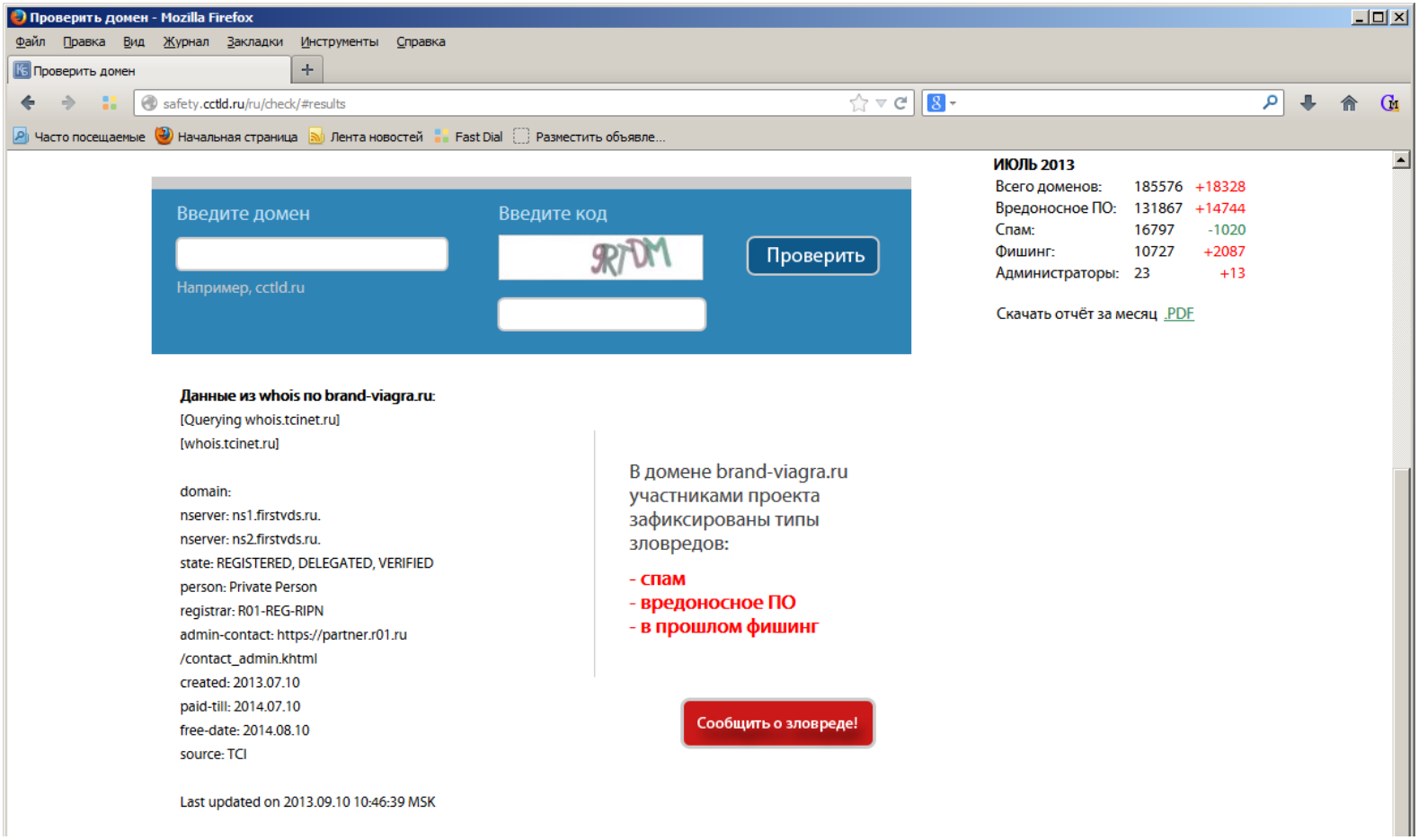
http://safety.cctld.ru/



Технический
Центр
Интернет

Domain checking

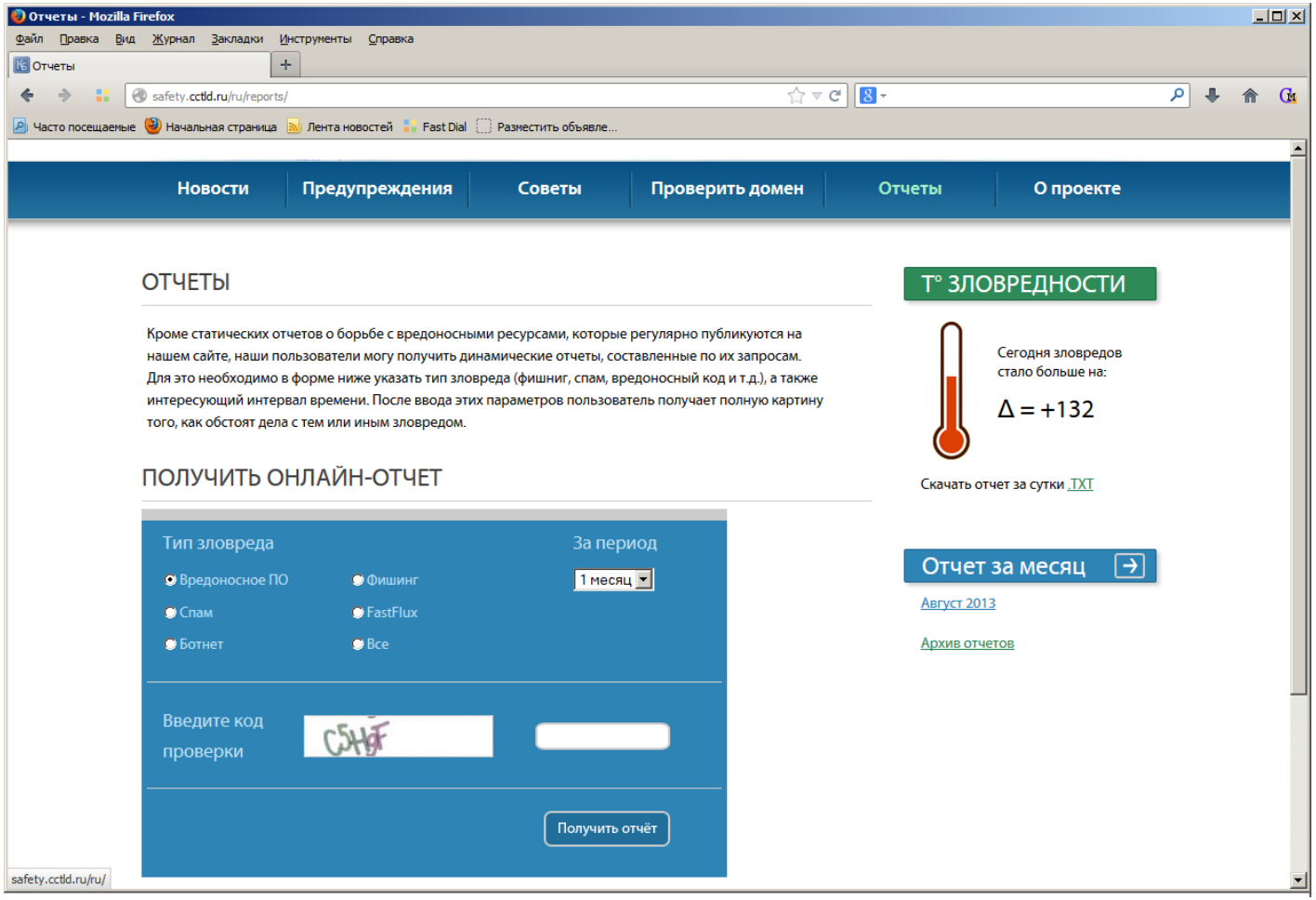
http://safety.cctld.ru/ru/check/



Технический
Центр
Интернет

Everyday reports

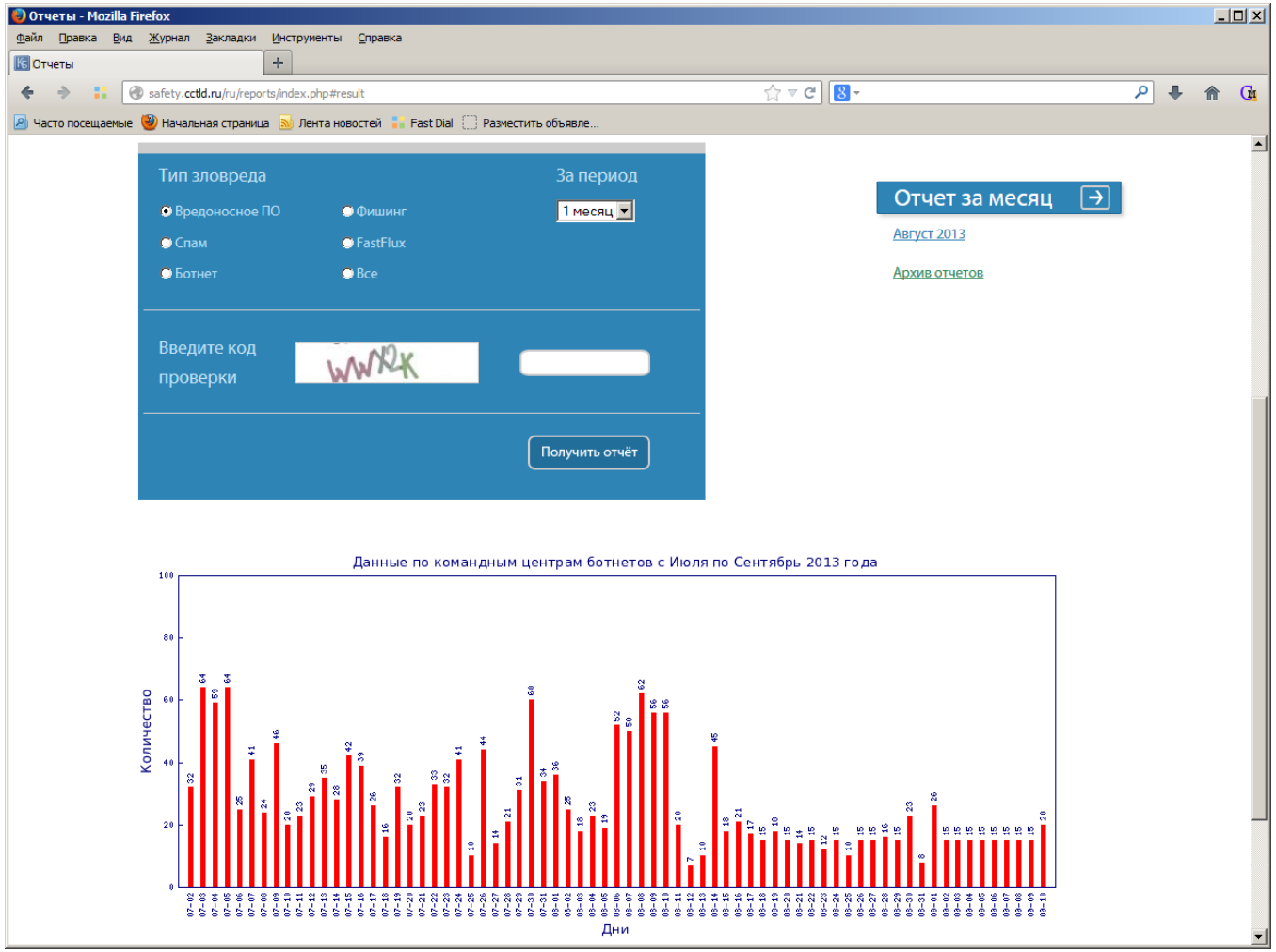
http://safety.cctld.ru/ru/reports/



Технический
Центр
Интернет

Statistic reports

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



Thank you!

Questions?

Tsvetkov Alexey (avt@tcinet.ru)