Domains in .RU & bad guys

Aleksey Tsvetkov, Pavel Khramtsov

“Bad Domain”. What does it mean?

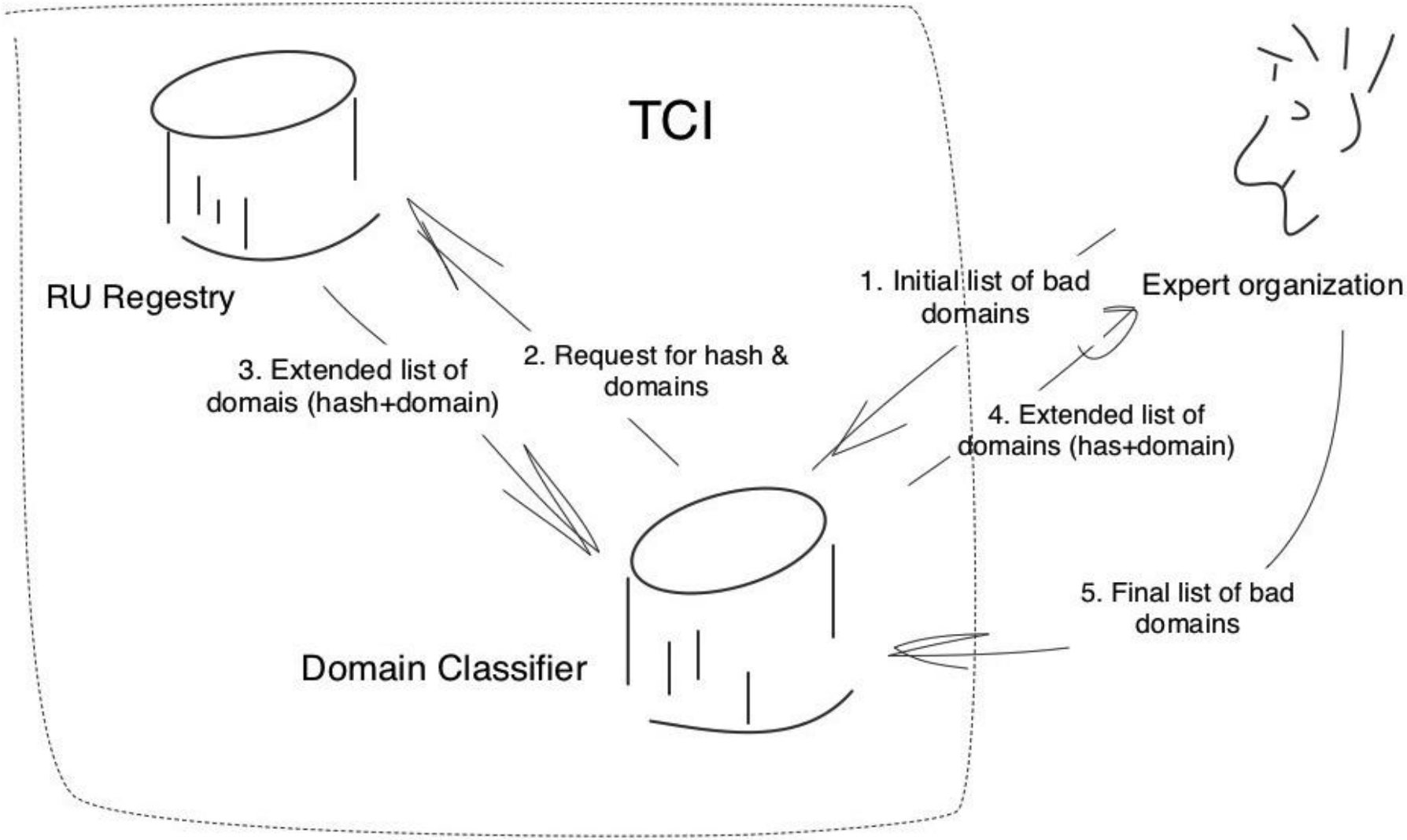
- malware delivery;
- Phishing;
- Spam delivery;
- Botnets control;
- Fast flux (bullet proof hosting);
- SEO Spam.

Some of the categories or all of them are fixed for domain name.

Data sources

- TCI (data base holder) – “hash” clean from personal sensitive data;
- Kaspersky Lab (malware, spam, phishing)
- RU-CERT (malware, phishing, botnets, fast flux)
- Yandex (malware, spam, phishing)
- Mail.ru (phishing)
- Group-IB (all categories, criminal investigations)

Data exchange procedure



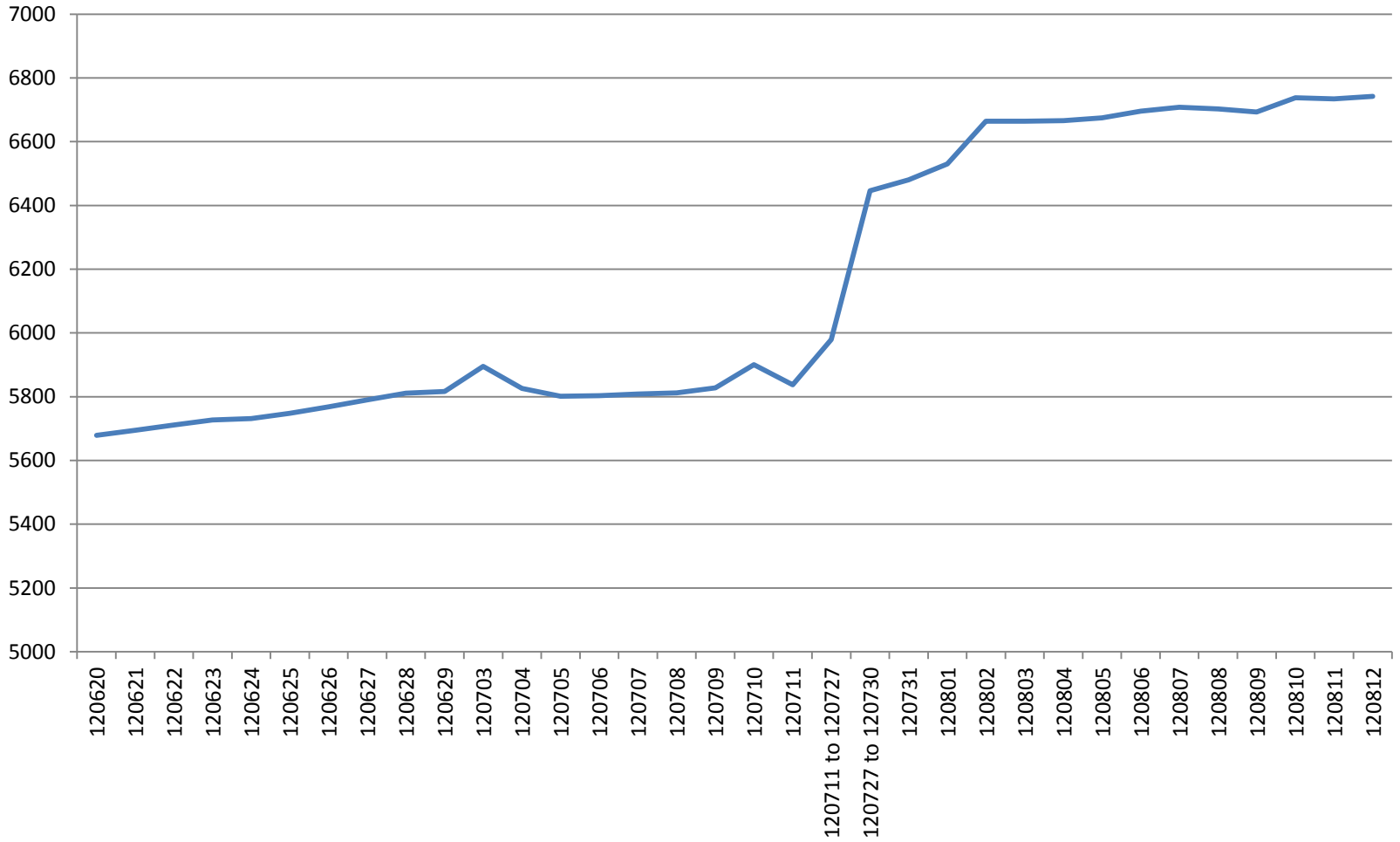
Express statistics

- “Bad” online activity is constantly fixing for 60 000 .RU domains;
- 1000 domains may be named “bad” with high reliability;
- 6800 registrants accounts from 1300000 (0.5%) are linked with “bad” domains.

Preliminary results

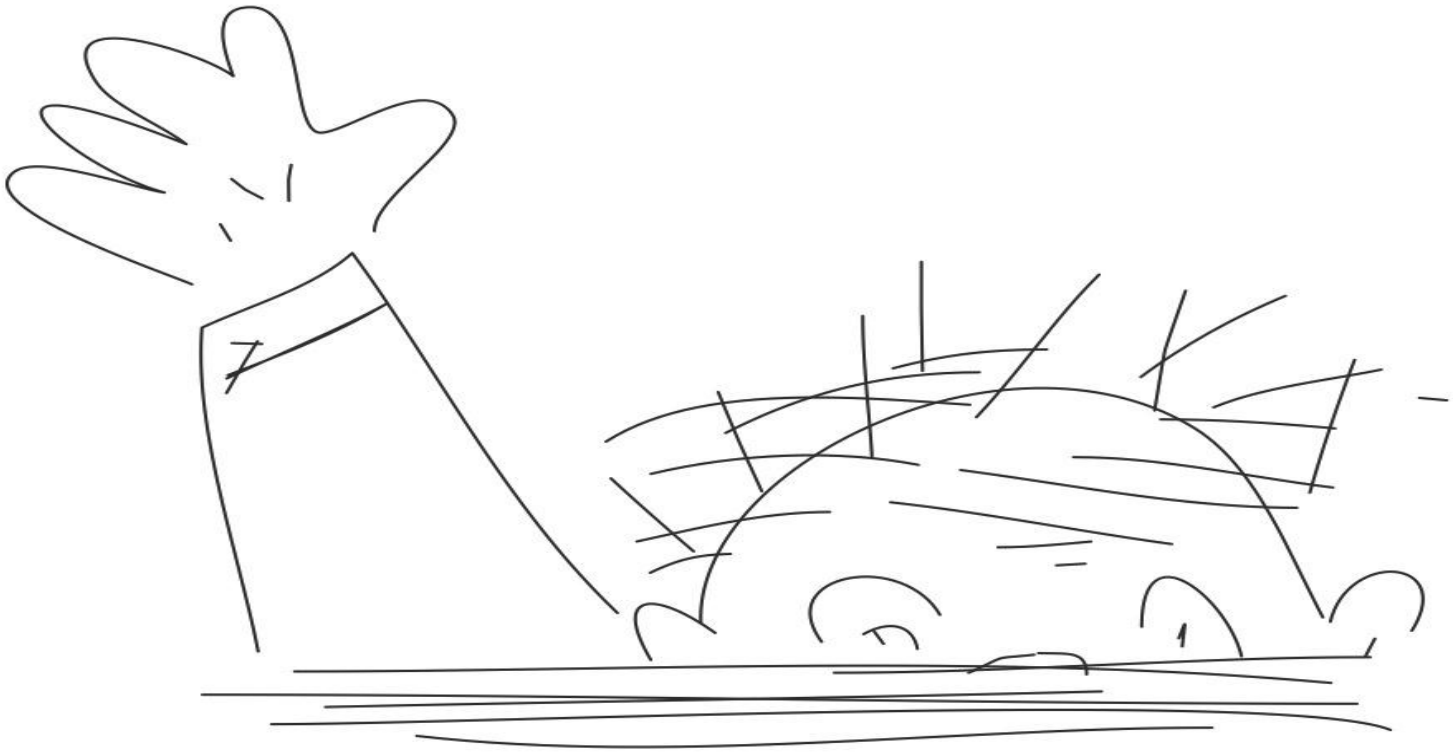
Number of tested domains	**294810**
Kaspersky Lab	**289732**
RU-CERT	**7808**
“Bad domains”	**243198**
Malware	**126853**
Phishing	**8982**
Spam	**37105**
Two categories simultaneously	**2359**
Deleted domains	**68931**

“bad” registrant dynamics



Conclusions

- Bad domains activity correlates with bulk registration;
- Bad domains activity correlates with SEO:
  - They run SEO and stuff “during the day”;
  - They run malware, botnet, etc “during the night”
- There are a bit of registrants involved in the illegal activity;
- The correlation of the illegal activity and provider networks will be studied



Questions?