Results of malware mining in national domains with netoscope.ru machine

49th ICANN Meeting
Singapore, March 2014
Data exchange process

1. Initial list of bad domains
2. Request for Hash & domains
3. Extend list of domains (hash + domain)
4. Extend list of domains (hash + domain)
5. Final list of bad domains

RU, РФ, SU Registry

Domain Classifier

Technical Center of Internet

Partner
Growth of the Netoscope database

- **Domain names with verified malicious activity, mln**
- **Domain names suspected in malicious activity, mln**
- **Total number of domain names in the Netoscope database, mln**

**21 000 new domains since start of year**
**inc. 8 700 malicious domains**
Malicious domains by category

- Malware: 61,377 (7%), 136,587 (14%), 5,970 (other)
- Phishing: 2,124 (other)
- Spam: 754,425 (79%), 79%
Growth since start of year
By category and by domains level

Jan.14

Feb.14

Mar.15

second-level, malware
second-level, phishing
second-level, spam
third-level, malware
third-level, phishing
third-level, spam
The existence of second-level domain

21,5% 30,8% 31,4%

Sep 13 Dec 13 Mar 14

Still in the ccTLD registry database

Deleted from the ccTLD registry database

29 962 domains deleted from registry data base since start of year
In cooperation with…
Questions?