



Blacklists aggregator: New service by TCI

Dmitry Belyavsky, TCI

ENOG 9

Kazan, Russia, 9-10 June 2015

Internet is dangerous

SPAM

Malware



Phishing

FastFlux

What else???

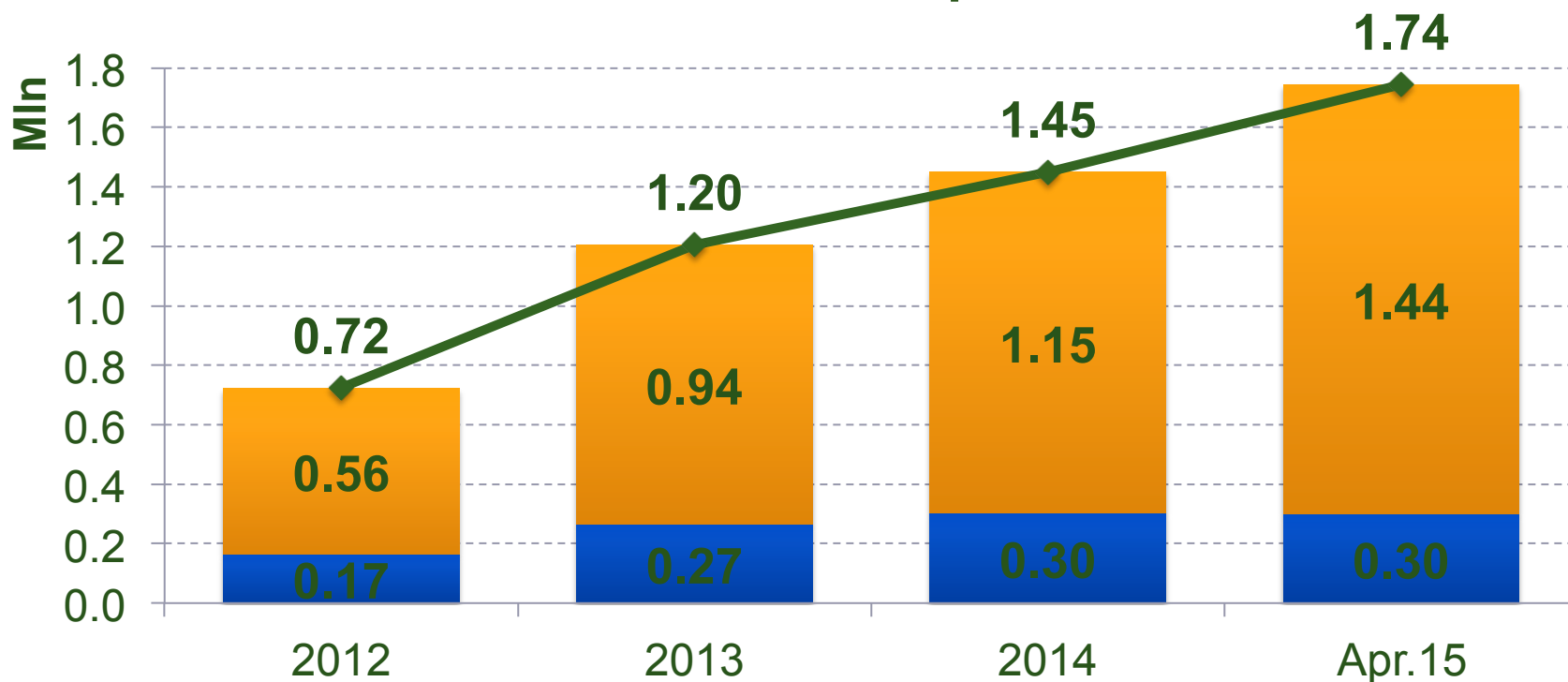
Netoscope

<http://netoscope.ru>
<http://нетоскоп.рф>

The 1st in Russia unique analytical resource,
the Netoscope project aims at making the Russian
domain space safer for users



Growth of the Netoscope database



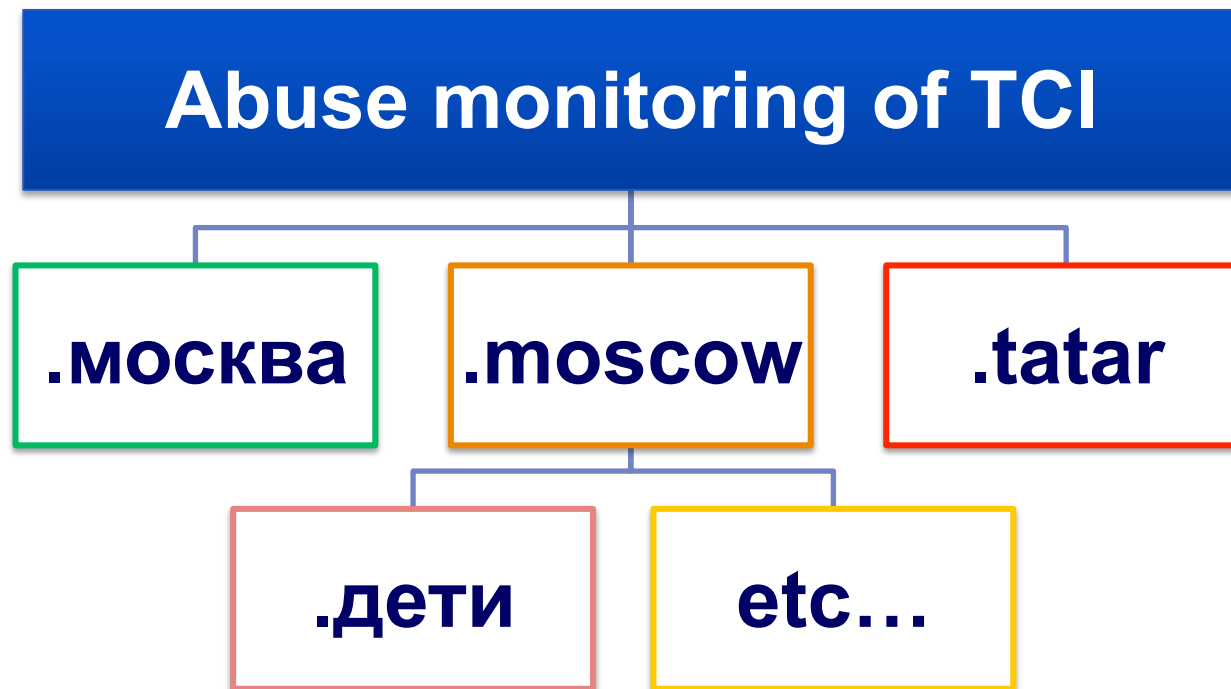
Domain names with verified malicious activity, mln

Domain names suspected in malicious activity, mln

Total number of domain names in the Netoscope database, mln

ICANN: abuse monitoring

Welcome to us!



Blacklists aggregator

Sources:

SURBL, Netoscope, etc...

**Filter for interesting
domains**

**Aggregate Unify
classification - TBD**

Reports (daily, monthly...)

Implemented with

Perl

**Pluggable architecture
to add new lists**

PostgreSQL

**Domain – source –
categories – details**

**ftp, WebDaV,
email**

Daily Report

Nothing extraordinary!

Implemented for...

Now

Registries

**Required by
ICANN for new
gTLDs**

Tomorrow

Registrar

After day?

Hosters

**Who can watch
yoursite.com?**



Drop them at:

beldmit@tcinet.ru