Analýza bezpečnosti SOHO routerů

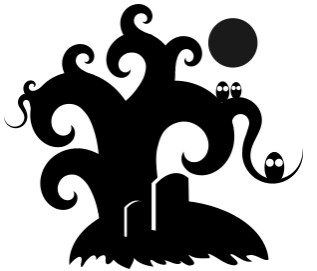
Bedřich Košata • bedrich.kosata@nic.cz • 13. 11. 2015
Tomáš Hlaváček • tomas.hlavacek@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

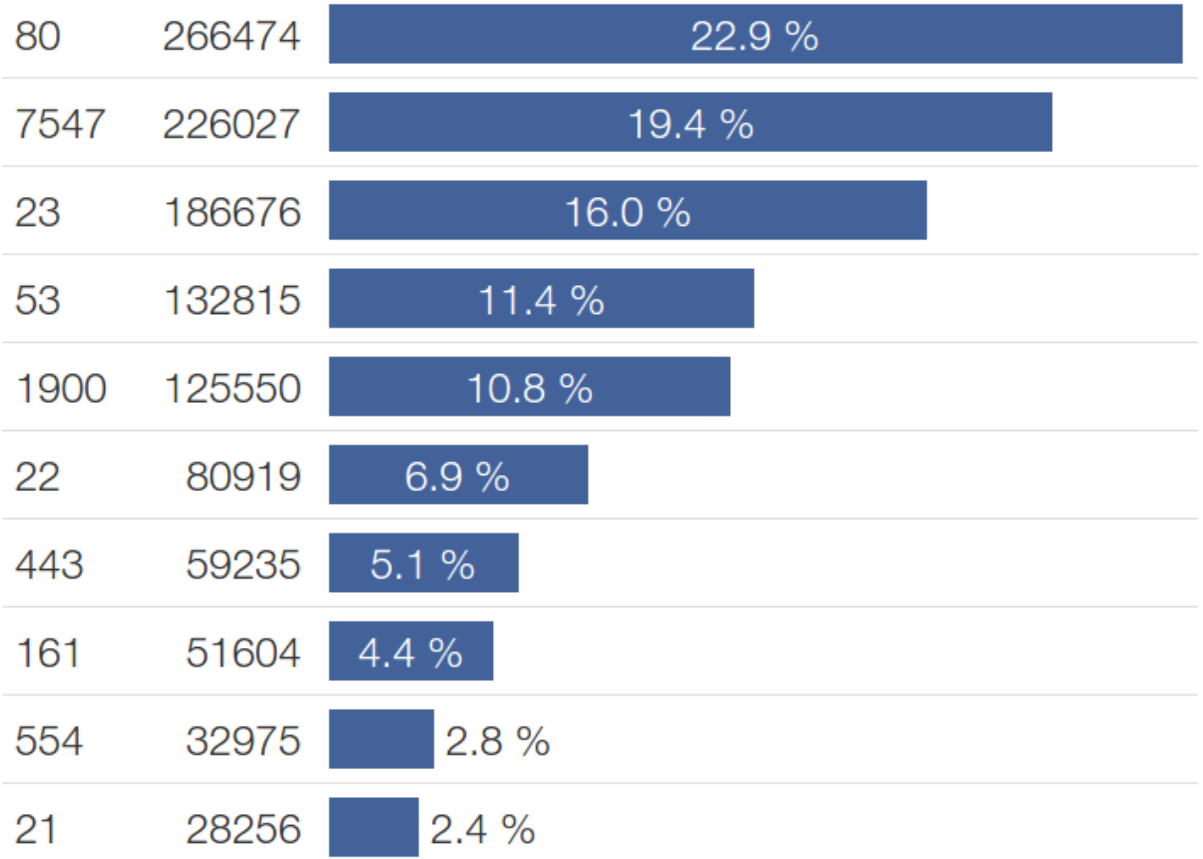
Router	Vulnerabilities					
	Buffer Overflow	SMB Symlink	Race Condition	Web Attacks	Backdoor	Improper File Permissions
Linksys EA6500		X		X		X
Netgear WNDR4700		X			X	X
ASUS RT-AC66U	X	X				X
ASUS RT-N56U		X				X
TP LINK TL-WDR4300		X		X		X
TP LINK TL-1043ND		X	X	X		
TRENDnet TEW-812DRU	X			X	X	
Netgear WNR3500		X			X	X
D-LINK DIR-865L		X	X	X	X	X
Belkin N900		X				X

Zdroj: https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf

Z vlastní zkušenosti

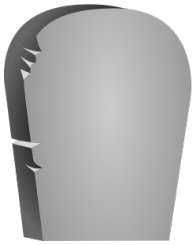


- Analýza botnetů útočících na Telnet
  - nejméně 47 000 routerů a firewallů Zy..L
  - nejméně 20 000 routerů A..S
  - další routery, online kamerové systémy, SIP „krabičky“, atp.
- ROM-0 zranitelnost DSL routerů



Otevřené porty na útočících zařízeních

Z vlastní zkušenosti



- router A..S
- čerstvě zakoupený router
  - firmware starý minimálně 1,5 roku
- obsahuje online kontrolu nového firmware
  - bohužel chybně tvrdí, že novější neexistuje
- do týdne napaden známou zranitelností
  - heslo uvedené v HTML kódu chybové stránky

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

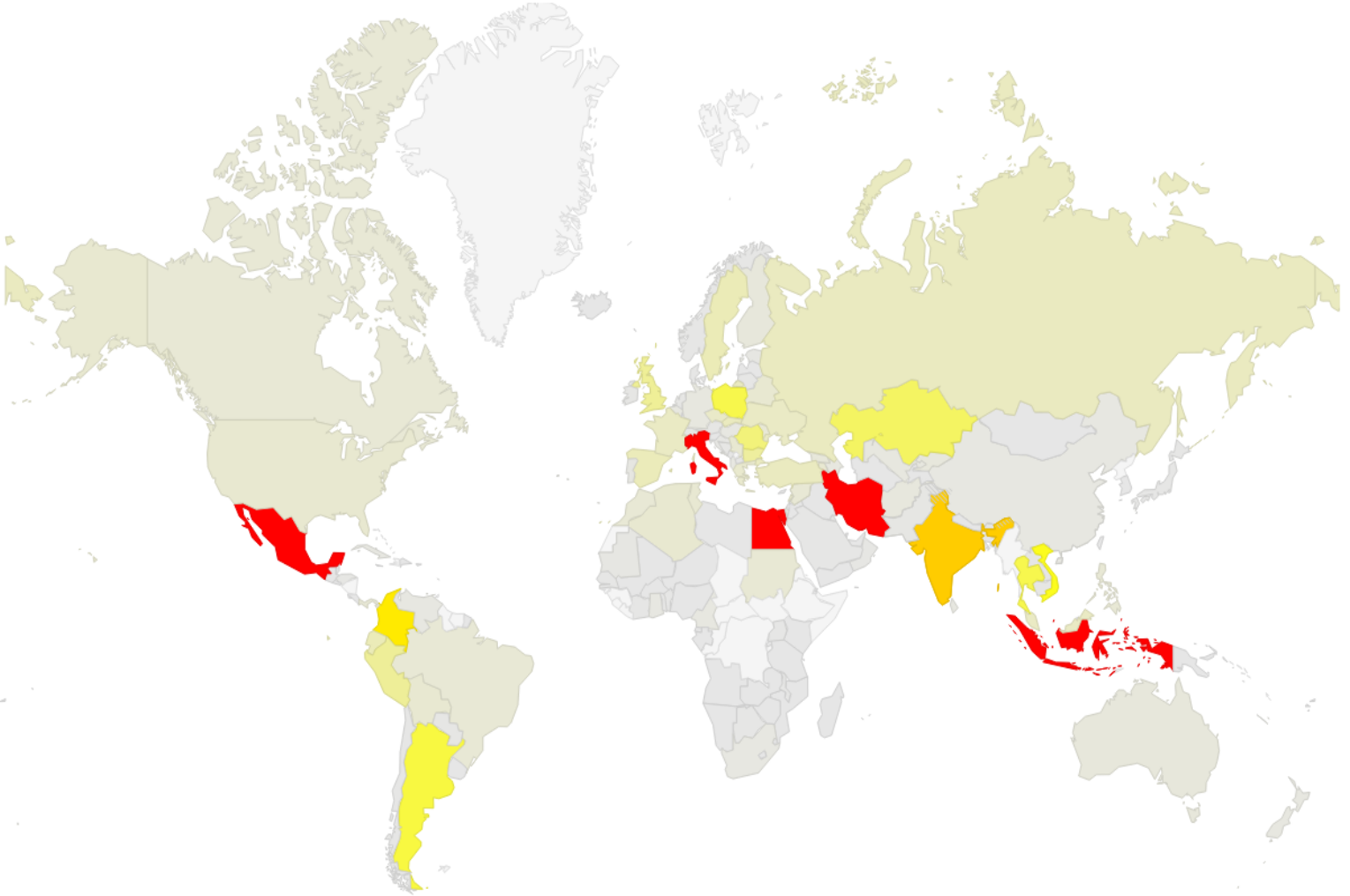
- Scan Internetu: HTTP HEAD /rom-0
- Rozpoznání:
  - Status code: 200
  - Content-length: 16384

Výsledky (Květen 2014)

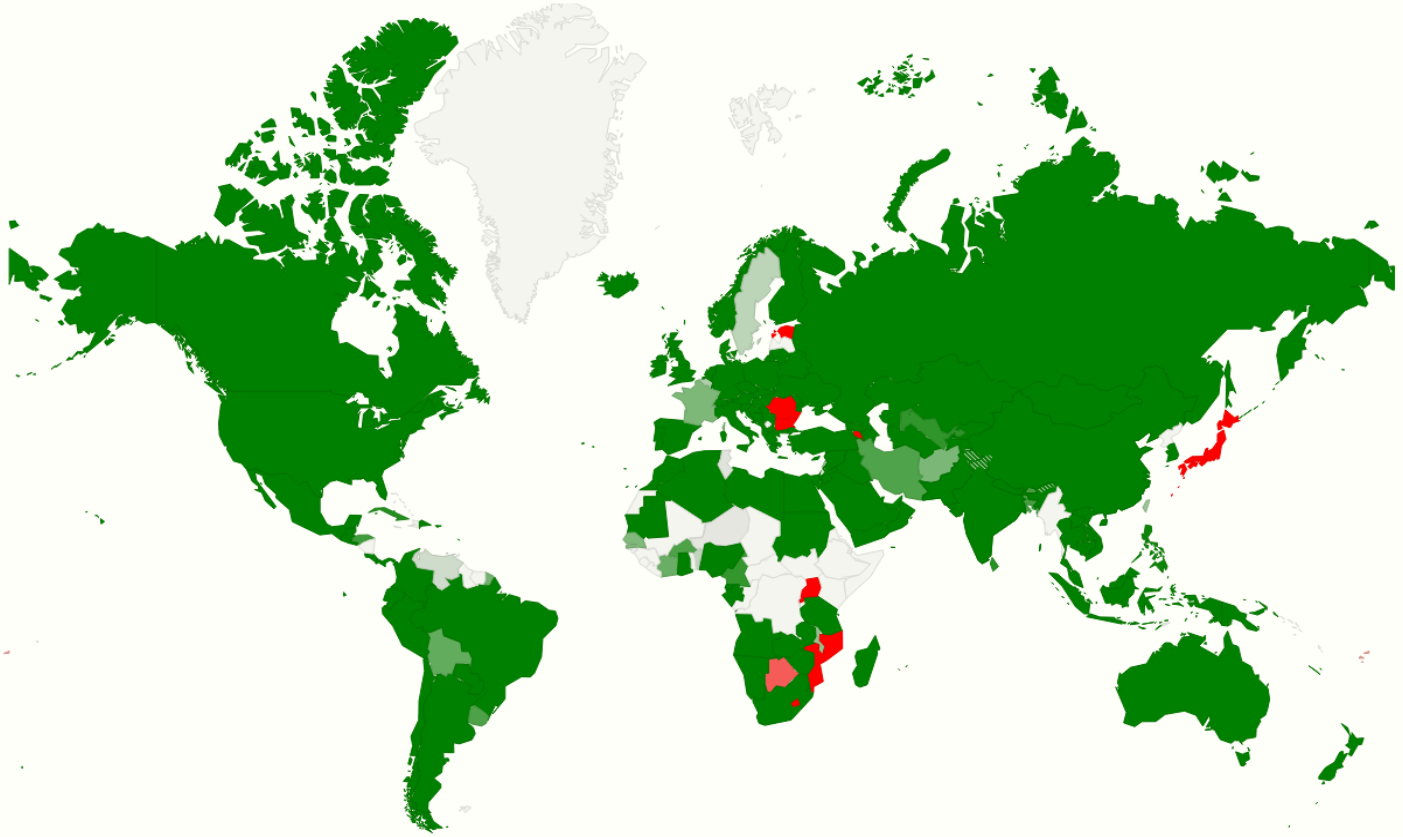
- První scan: 17-18 května 2014
- Otestováno ~71M HTTP
- Zranitelných 1 219 985
- Česká Republika: 5 368
- Nejvíce v EU: Itálie (116 731), Polsko (22 702)
- Nejvíce ve světě: Thajsko (167 505), Kolumbie (139 976)

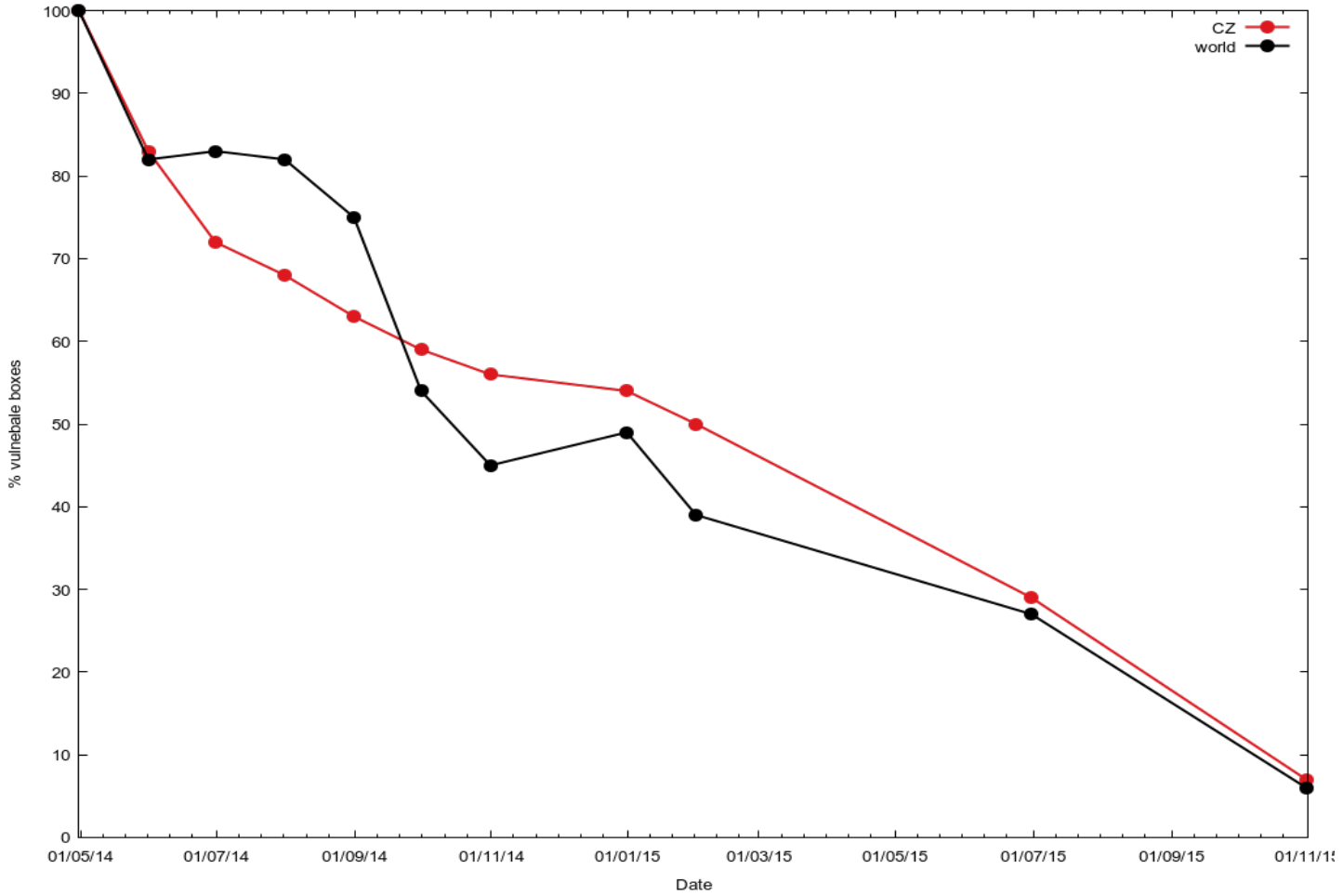
Výsledky (Listopad 2015)

- Poslední scan: 10-11 listopadu 2015
- Otestováno ~70M HTTP
- Zranitelných 74 419
- Česká Republika: 813



Změny (05/2014 - 11/2015)



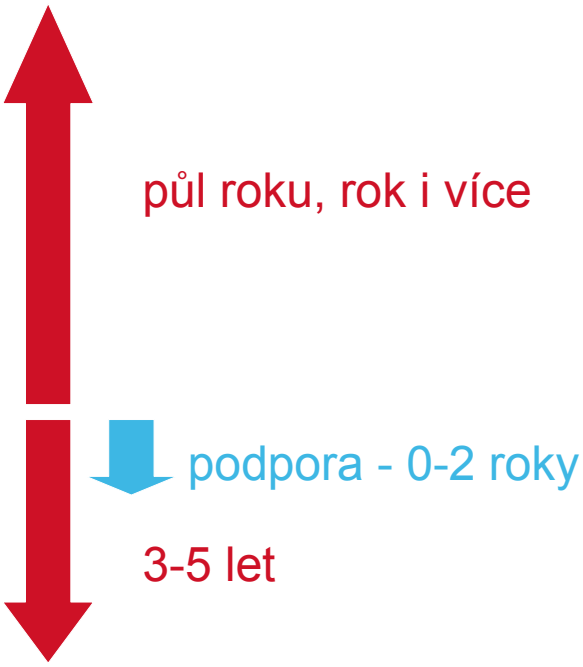

CZ
world
% vulnebale boxes
100
90
80
70
60
50
40
30
20
10
0
01/05/14
01/07/14
01/09/14
01/11/14
01/01/15
01/03/15
01/05/15
01/07/15
01/09/15
Date

V čem je problém?

- Každý software obsahuje chyby
- Router je levné zařízení - málo zdrojů na firmware
- Bezpečnost vs. uživatelská přívětivost
- Zaplatím, zapojím, zapomenu
- Aktualizace jsou třeba jako sůl

Životní cyklus SOHO routeru

- Výroba firmware
- Výroba routeru
- Cesta lodí do cílové destinace
- Uskladnění u distributora a v e-shopu
- Zakoupení a instalace
- Zapomenutí
- Rozbití a nahrazení



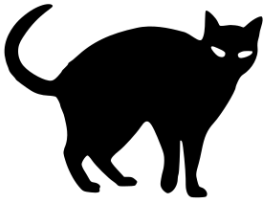
Aktualizace firmware

- Upozornění na aktualizaci v rozhraní routeru
  - předpokládá, že se tam někdo kouká
  - když nefunguje, je to horší než nic
- Firmware ke stažení na stránkách výrobce
  - zdlouhavé, problém s hw revizemi
- Nic
  - po jisté době nevyhnutelné – jednoúčelový software

Nejčastější a nejnebezpečnější chyby

- admin/admin
- backdoors – chtěné i nechtěné
  - naivní použití ukázkového kódu v produkci
- hloupé chyby
  - heslo admina umístěné v kódu stránky
- špatná implementace autorizace přístupu
  - např. specifické URL pro upgrade firmware bez hesla

Závěr



- Připojili byste roky neaktualizovaný počítač „na přímo“ k síti?
- Na trvalo?
- Firewall a NAT vás „kryje“...
- ...když není sám napadený
- router není mimo zorné pole útočníků
- zvlášť když je tak snadné ho napadnout!

Děkujeme za pozornost

Bedřich Košata • bedrich.kosata@nic.cz
Tomáš Hlaváček • tomas.hlavacek@nic.cz

Zdroj obrázků: https://openclipart.org/