Honeypot as a Service

Bedřich Košata • bedrich.kosata@nic.cz • 1. 6. 2016

It‘s easy to be open with good news, being open with bad news takes balls.

Co je honeypot?

- Napadnutelný počítač, který sleduje, co útočník dělá
- Většinou simulovaný nebo jinak oddělený, aby bránil skutečnému zneužití
- Pro různé protokoly (SSH, Telnet, SMTP, etc.)

Obecné problémy honeypotů

- Malý počet
- Pevné IP adresy z malého počtu rozsahů
  - časem se dostanou na “black-list” útočníků
- Nedokonalá simulace
  - útočník je schopen poznat, že je v honeypotu

- Bylo by zajímavé umístit honeypoty ke koncovým uživatelům

Project Turris

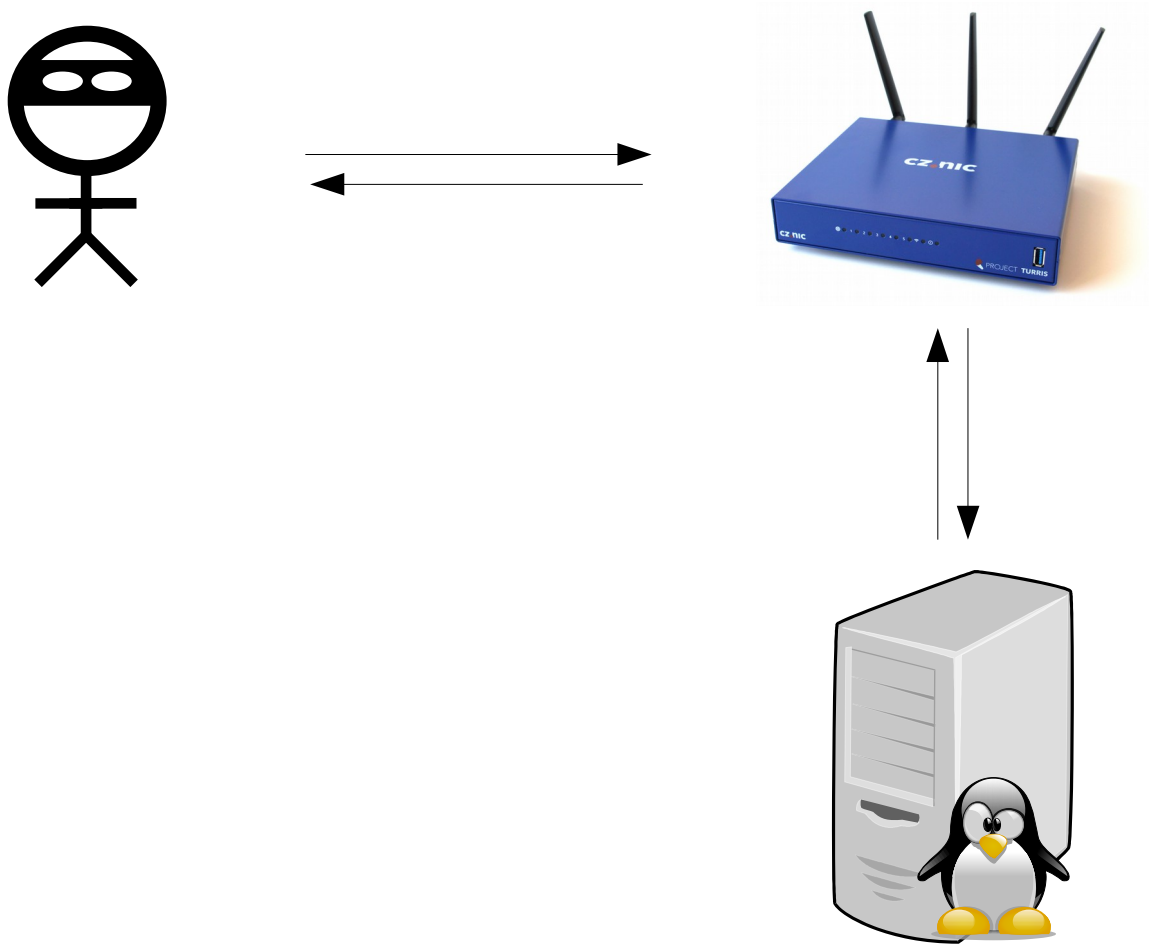
- 2000 routerů u uživatelů v ČR
- Používají se jako síťové bezpečnostní sondy
- Uživatelé by měli mít veřejnou IPv4 adresu

Turris jako honeypot

- Velké množství instancí
- Geograficky i topologicky rozdílné umístění
- Některé IP adresy se s časem mění

- Zajímavý “proof-of-concept”
- Nesmí ohrozit uživatele!

Honeypot as a Service



Honeypot as a Service

- Používaný pro SSH
- Běží na serverech CZ.NIC
- Na routeru stačí nainstalovat jednoduchý program
- Každý klient má vyhrazený jeden port/instanci
- Centrálně spravovaný
  - pomáhá bojovat s detekcí honeypotu útočníkem
- Nahraná sezení jsou prezentována uživatelům a centrálně analyzována

Technologie SSH honeypotu - server

- založené na Cowrie
  - napsáno v Pythonu
  - fork populárního honeypotu Kippo
- rozšířený o podporu více instancí na různých portech
- k dispozici na https://gitlab.labs.nic.cz/turris/cowrie-multiport

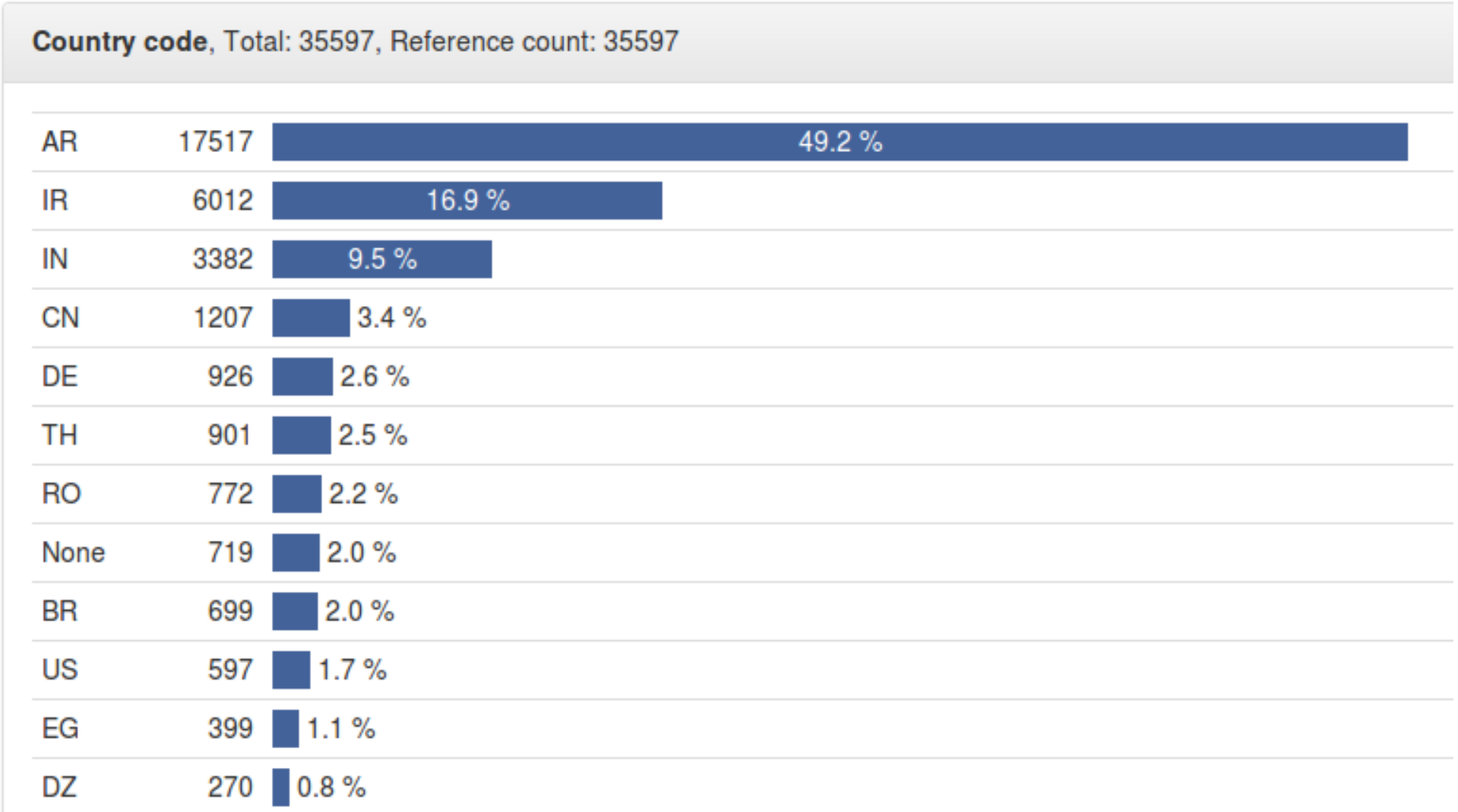
Technologie SSH honeypotu - klient

- založené na mitmproxy
  - dělá man-in-the-middle “útok” na spojení
- k dispozici na https://gitlab.labs.nic.cz/labs/mitmproxy

Výsledky SSH honeypotu - 2016

- Přibližně 350 uživatelů
- cca 2000 sezení/den, 4 přikazy/sezení
- 36 000 unikátních IP addres útočníků od 1. 1. 2016

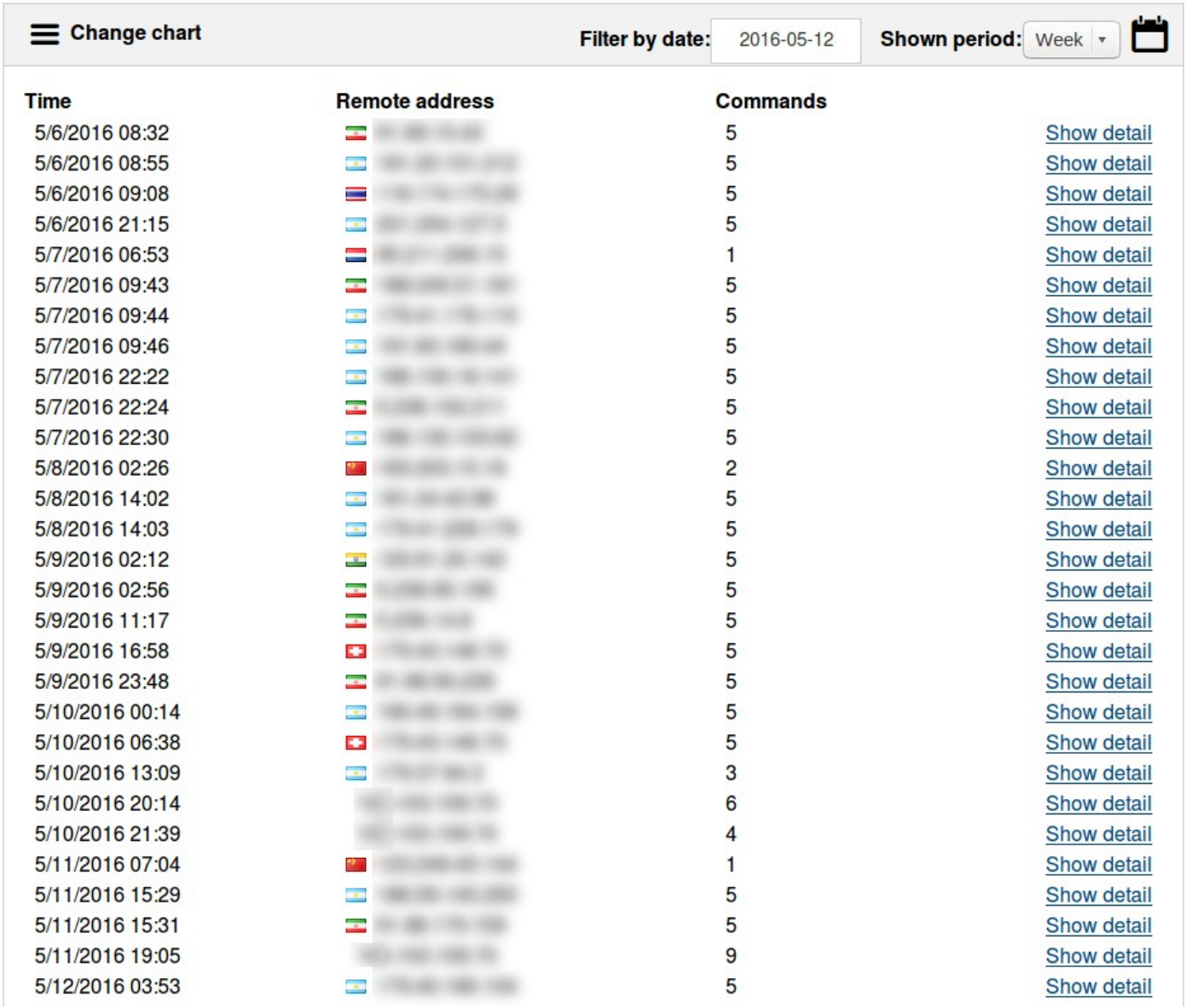
Výsledky SSH honeypotu – 2016



Analýza sezení za rok 2016

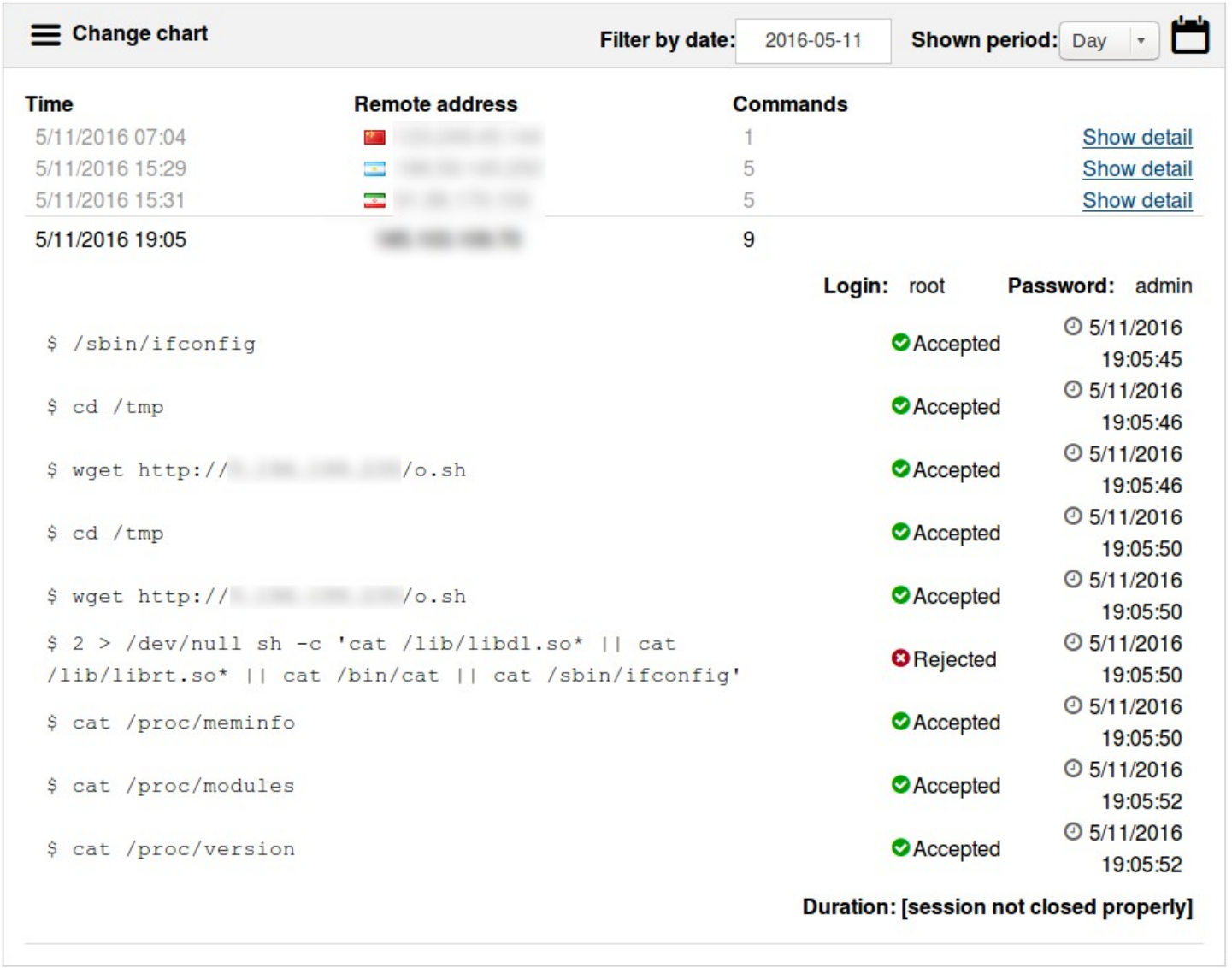
- různě velké skupiny útočníků s podobnou sadou příkazů
- 13 000 útočníků používá přesně stejnou sekvenci příkazů
- přes 70 % z nich jsou z Argentiny (převážně Telefonica de Argentina)
- přes 50 % má otevřený port 7547 (DSL provisioning)

Uživatelský portál



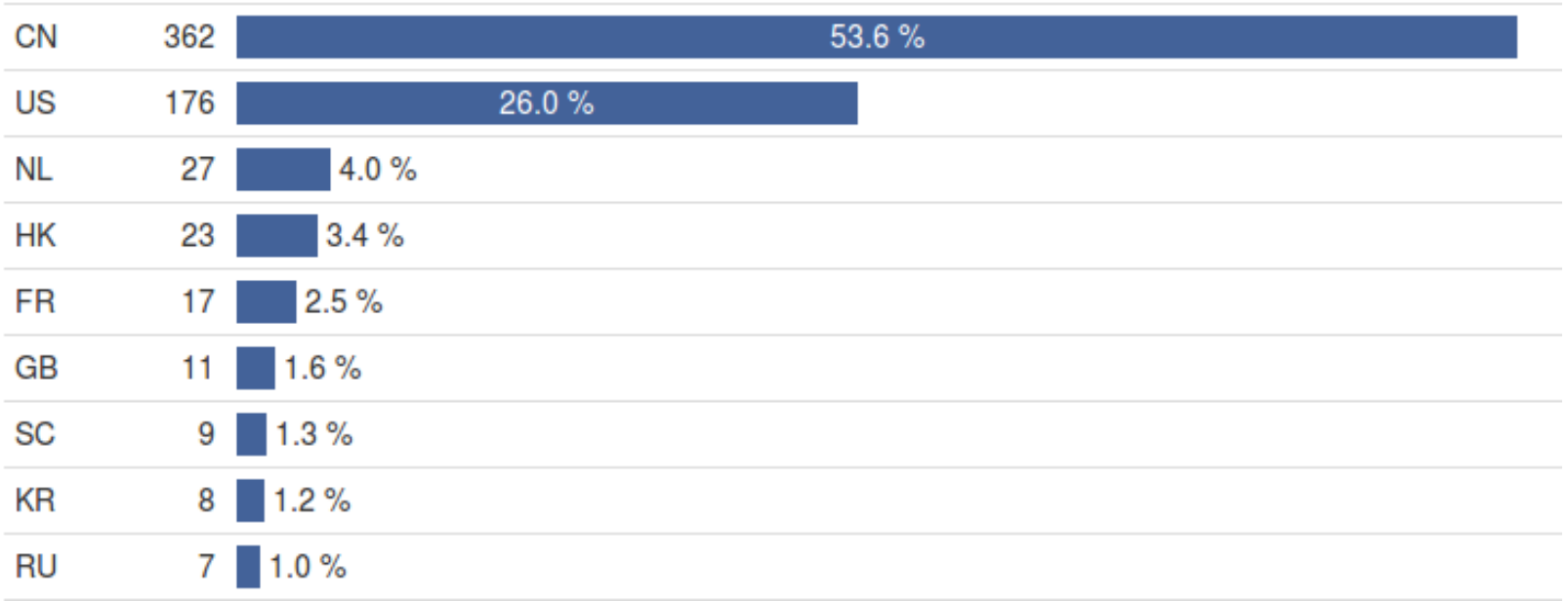
Time	Remote address	Commands	
5/6/2016 08:32		5	Show detail
5/6/2016 08:55		5	Show detail
5/6/2016 09:08		5	Show detail
5/6/2016 21:15		5	Show detail
5/7/2016 06:53		1	Show detail
5/7/2016 09:43		5	Show detail
5/7/2016 09:44		5	Show detail
5/7/2016 09:46		5	Show detail
5/7/2016 22:22		5	Show detail
5/7/2016 22:24		5	Show detail
5/7/2016 22:30		5	Show detail
5/8/2016 02:26		2	Show detail
5/8/2016 14:02		5	Show detail
5/8/2016 14:03		5	Show detail
5/9/2016 02:12		5	Show detail
5/9/2016 02:56		5	Show detail
5/9/2016 11:17		5	Show detail
5/9/2016 16:58		5	Show detail
5/9/2016 23:48		5	Show detail
5/10/2016 00:14		5	Show detail
5/10/2016 06:38		5	Show detail
5/10/2016 13:09		3	Show detail
5/10/2016 20:14		6	Show detail
5/10/2016 21:39		4	Show detail
5/11/2016 07:04		1	Show detail
5/11/2016 15:29		5	Show detail
5/11/2016 15:31		5	Show detail
5/11/2016 19:05		9	Show detail
5/12/2016 03:53		5	Show detail

Uživatelský portál



Výsledky SSH honeypotu - 2016

- 55,000 příkazů wget
- 2,000 unikátních URL pro stažení
- 676 unikátních IP adres pro stažení



Plány do budoucna

- Nabídneme uživatelům Turris Omnia
- Nabídneme honeypot jako službu veřejnosti
  - další routery, servery
- Vytvoření klientů pro další systémy
- Vydávání výsledků jako open data
- Vylepšování metod analýzy dat
- Zvyšování povědomí o bezpečnosti na Internetu

Možná spolupráce

- Instalace honeypot klienta na vašem zařízení
- Pomoc s vývojem serveru
- Instalace nezávislého honeypot serveru
- Vytvoření jednotného systému honeypotů v různých lokacích s jednotným sběrem dat

Děkuji za pozornost

Bedřich Košata • bedrich.kosata@nic.cz

T A
Č R

Realizace projektu **„Honeypot as a Service (HaaS)“** (TF02000057) byla podpořena Technologickou agenturou ČR v rámci 2. výzvy programu Delta.

Program Delta