Zpracování dat z routerů Turris v kostce

Jan Čermák • jan.cermak@nic.cz • 29. 11. 2014

CZ.NIC | SPRÁVCE DOMÉNY CZ

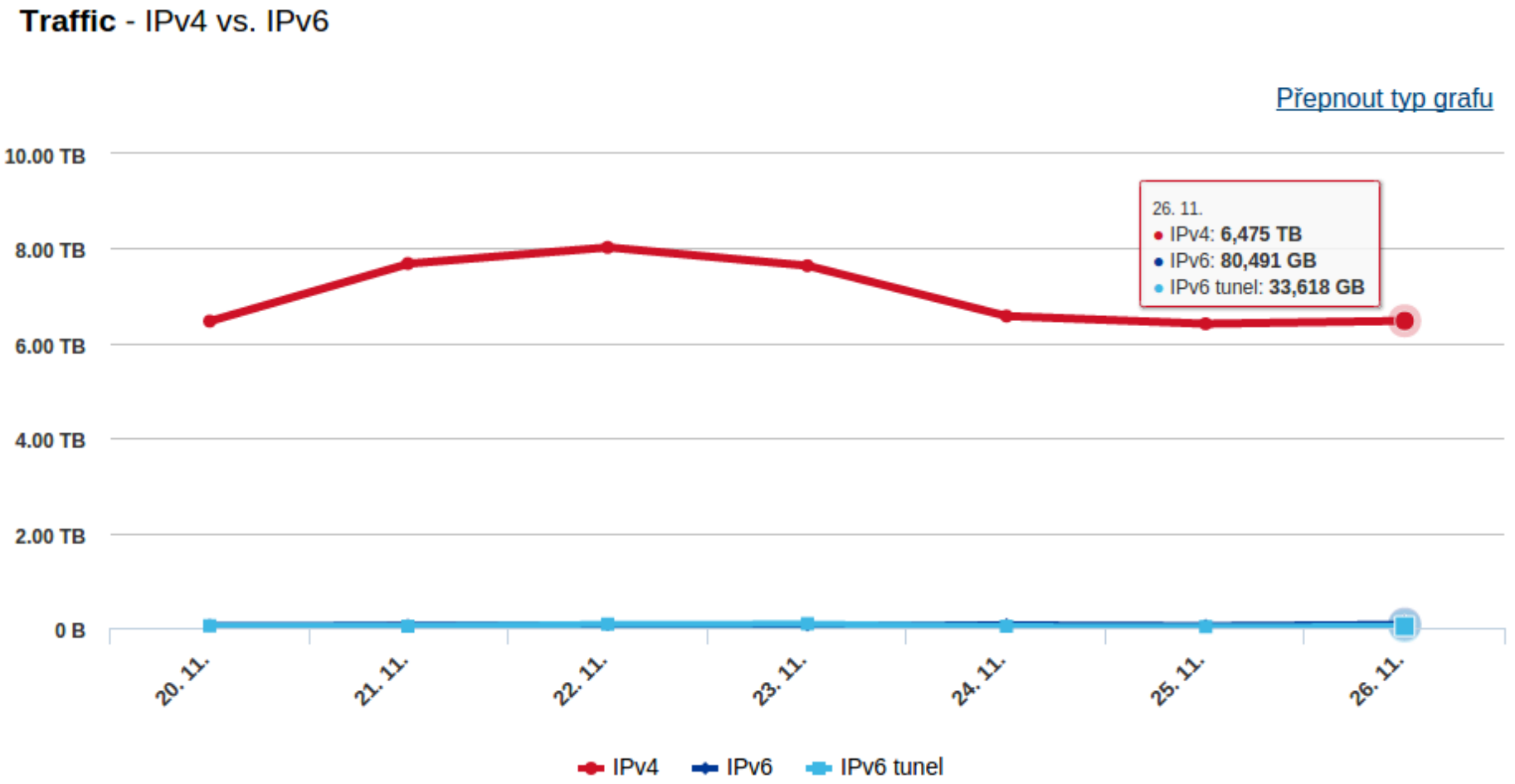
O čem si budeme povídat?

- Jaká data se zpracovávají.
- Jaká je jejich cesta z routeru na servery Turris.
- Co se s daty z routerů děje.
- Co se s daty z routerů bude dít.

Co? Typy zpracovávaných dat

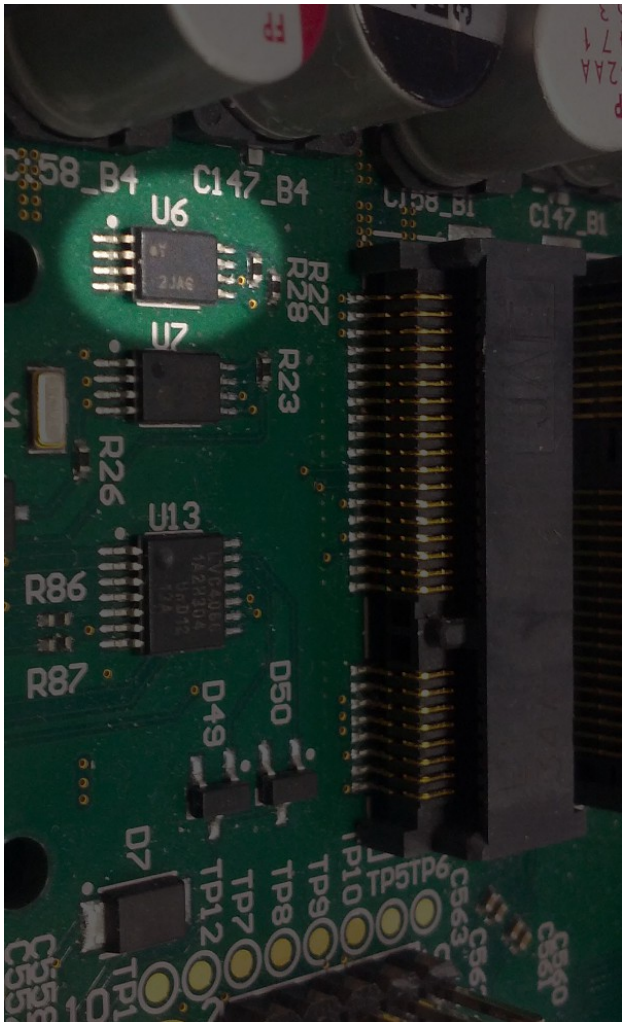
- **Logy** (*logsend*)
  - Relevantní služby
  - Provozní informace
- ***uCollect***
  - Buckets (anomálie), counts („statistiky“), flows
  - další viz GitLab: turris/ucollect – src/plugins
- **Data z firewallu** (*Nikola*)

https://www.turris.cz/cs/global-stats/



Vložka: co je ATSHA?

- ATSHA204 (Atmel®)
- Čip pro výpočet SHA-256
- 16 OTP klíčů
- Index klíče z DNS – DNS nezbytné pro funkci!



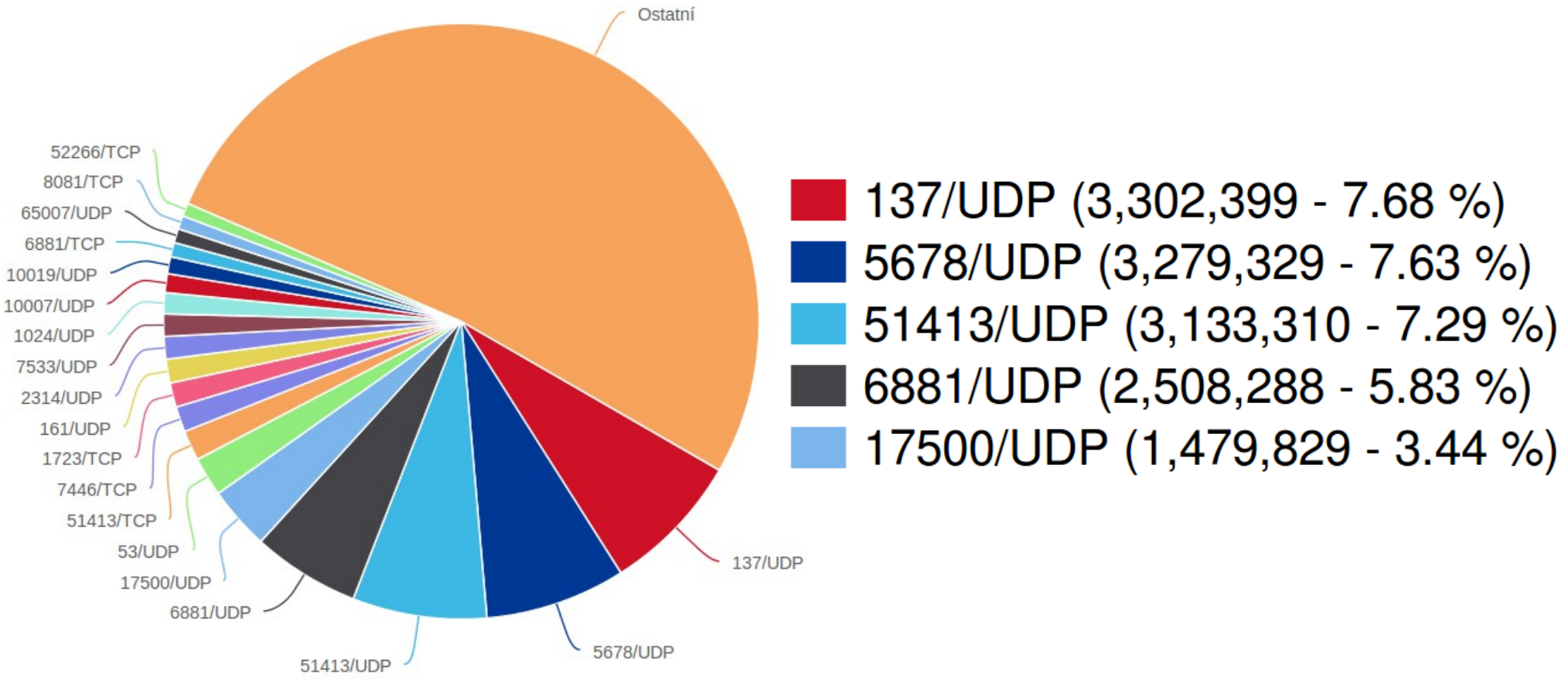
Kudy a kam? Cesta dat do úložiště

- **API** – veřejně přístupný
  - Servery (SW) pro příjem dat – autentizace ATSHA
- **DB** – neveřejný, dostupné jen některé služby
  - Authenticator – emuluje ATSHA
  - Perzistence dat jen 10 dní
- **Archive** – anonymizovaná data z DB
- **www.turris.cz**
  - Globální a uživatelské statistiky

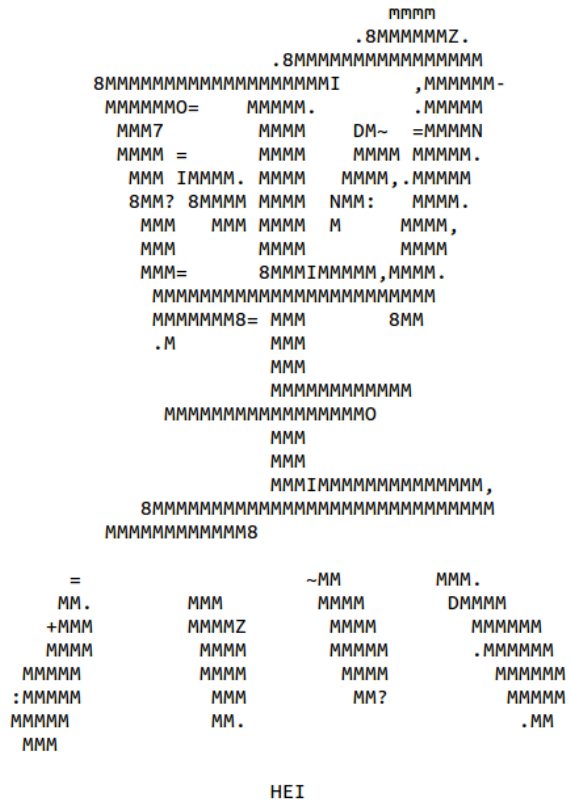
Co s tím?

- Prezentace dat z routeru uživateli
- Anomálie – statistická identifikace „škodné“
- Firewallové logy – hledání útočníků, odhalování vzorců chování
- Flows – analýza provozu (metadat) známých útočníků

Zablokované pakety – co je špatně?



Tvorba „greylistu“



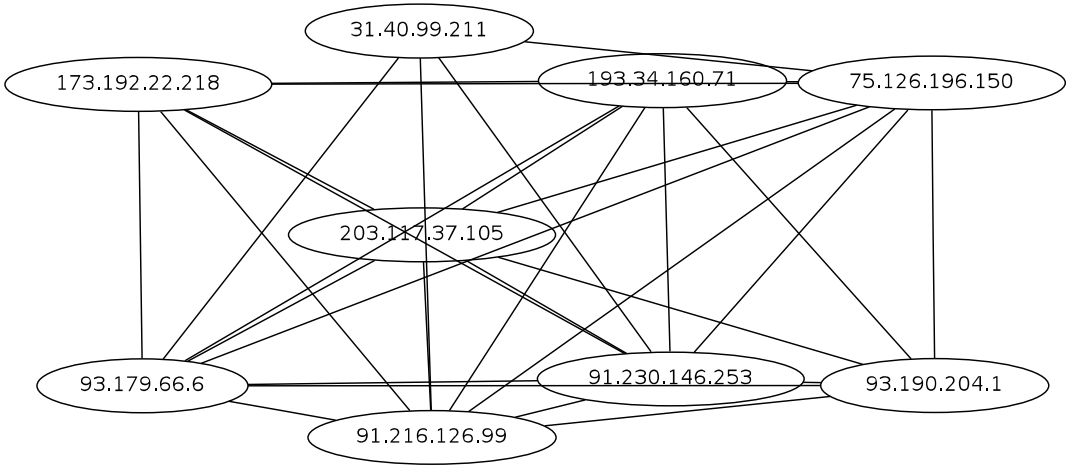
- Z firewallových logů
- Kdo, na jaký port, jak často
- Jednoduchá klasifikace – známé vzorce chování
- Ohodnocení podle „zákeřnosti“ chování
- U vysoce hodnocených adres – sledování flows
- Výsledky – např. odhalení výměny 100 MB dat s Albánským scannerem SMB

https://www.turris.cz/cs/greylist

Address	Country	Tags	ASN
1.1.1.2	AU	dns	15169
1.30.20.148	CN	low_ports,remote_access	4837
1.34.23.251	TW	http_scan,proxy_scan	3462
1.55.160.182	VN	http_scan,netbios	18403
1.93.17.96	CN	databases	4808
1.93.22.64	CN	low_ports	4808
1.93.23.125	CN	low_ports	4808
1.93.23.159	CN	low_ports	4808
1.93.23.173	CN	low_ports	4808

Co dál?

- Další metody analýzy FW logů (podobnost útočníků)
- Automatizace některých úkonů (upozorňování na podezřelé flows apod.)
- Nové sondy pro ucollect, sběr dalších dat atd...



Děkuji za pozornost

Jan Čermák • jan.cermak@nic.cz