Project Turris

http://www.turris.cz/en/

PROJECT:
TURRIS

Ondrej Filip • Tech Day • March 24, 2014 • Singapore

CZ DOMAIN REGISTRY

Project Turris

- Started in 2013 – project of shared cyberdefense
- CZ.NIC Labs
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers
  - Network measurements

Project Turris

- Security research
  - Currently – Honeynet, DNS anomaly detection
  - Probes close to end users
  - Distributed in many networks
  - Anomaly detection
- End user security
  - Adaptive firewall based on collected data
  - Feed for CERT team (CSIRT.CZ)

Project Turris

- SOHO routers
  - Bad support of IPv6, DNSSEC
  - Many problems with DNS
  - No support for third party applications – app store
  - Limited security features
  - No automated software upgrades
- Measurements – IPv6, DNSSEC, DNS anycast

Data collection - probes

- Distribute 1000 probes - SOHO routers to end users for three years for free (lease for 1 CZK = 0,03 EUR)
- Probe – powerfull enough to forward 1Gbps of traffic and analyzing it – no such HW found on the current market -> HW development
- Additional features to increase value for end users

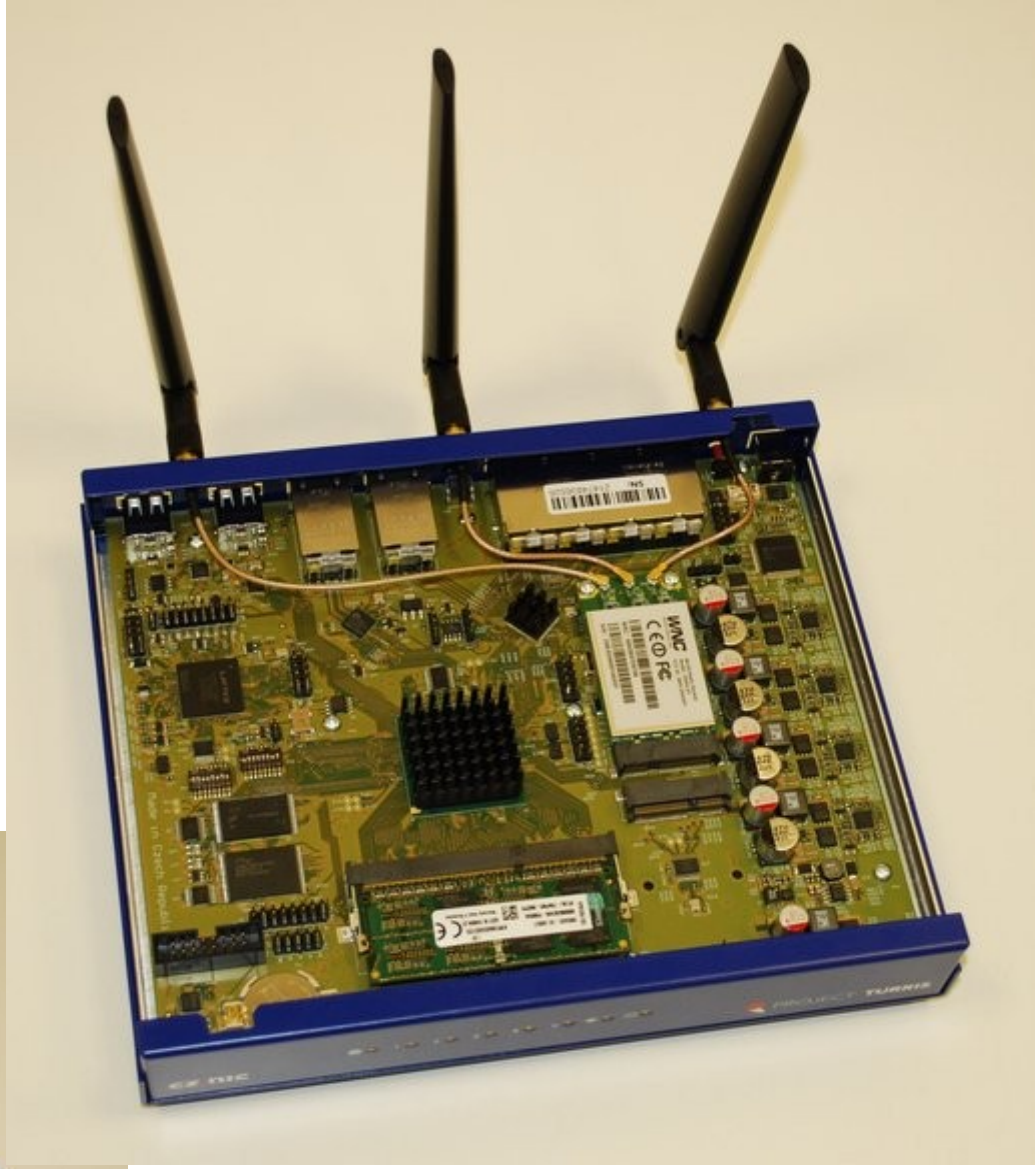
Router Turris

- Developed from scratch by CZ.NIC
- 1000 pcs – produced in Czech Republic
  - Freescale PPC 1.2GHz dual core
  - 2GB DDR memory – slot
  - 256MB NAND + 16MB NOR flash
  - 5x LAN Gbps ports (2Gbps to CPU)
  - 1x WAN Gbps port (directly to CPU)

Router Turris

- 2x miniPCIe (1 occupied by wifi)
- Wifi 802.11 a/b/g/n – 3x3 MIMO
- 2x USB 2.0
- UART, SPI, I2C, GPIO
- Free microSDHC slot
- ATSHA204 – crypto chip
- Low power consumption
- Open source - CERN Open HW License

Router Turris



cz.nic | CZ DOMAIN REGISTRY

Router Turris – killer feature

- LED brightness intensity tunable (!)
  - SW (colors)
  - Button at the back
  - :-D

Router Turris - software

- Based on OpenWRT – open source
- Own configuration wizard – based on NETCONF
- Automatic updates – user can avoid certain time periods
- Communication with central server crypted using TLS, crypto HW
- Data collector – only mandatory process
- IPv6, DNSSEC, passwords, ... (clock)

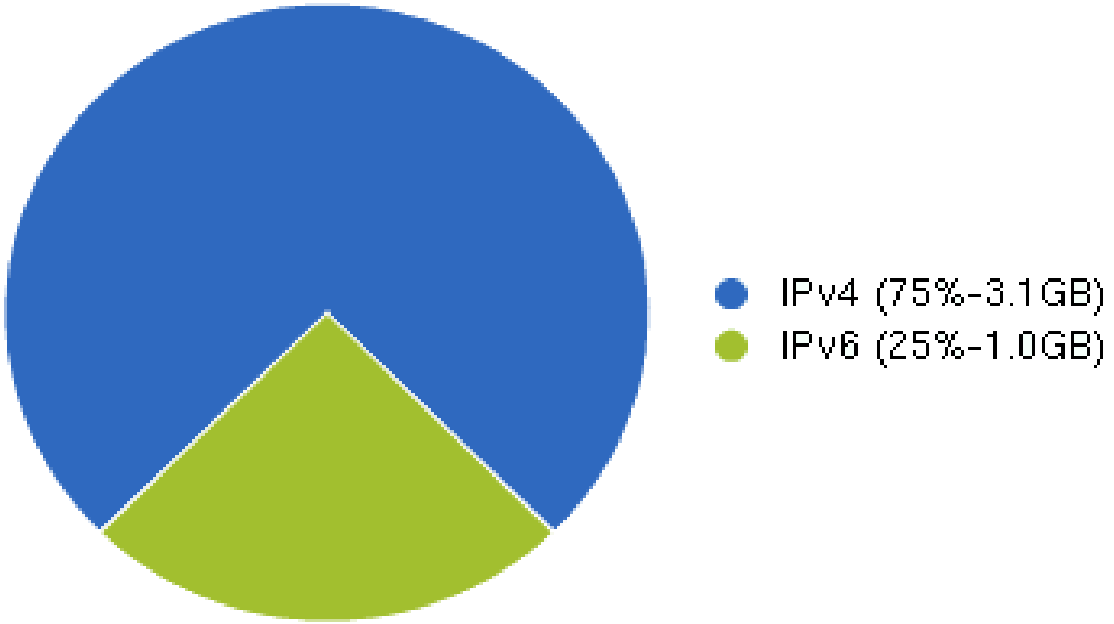
Data collection

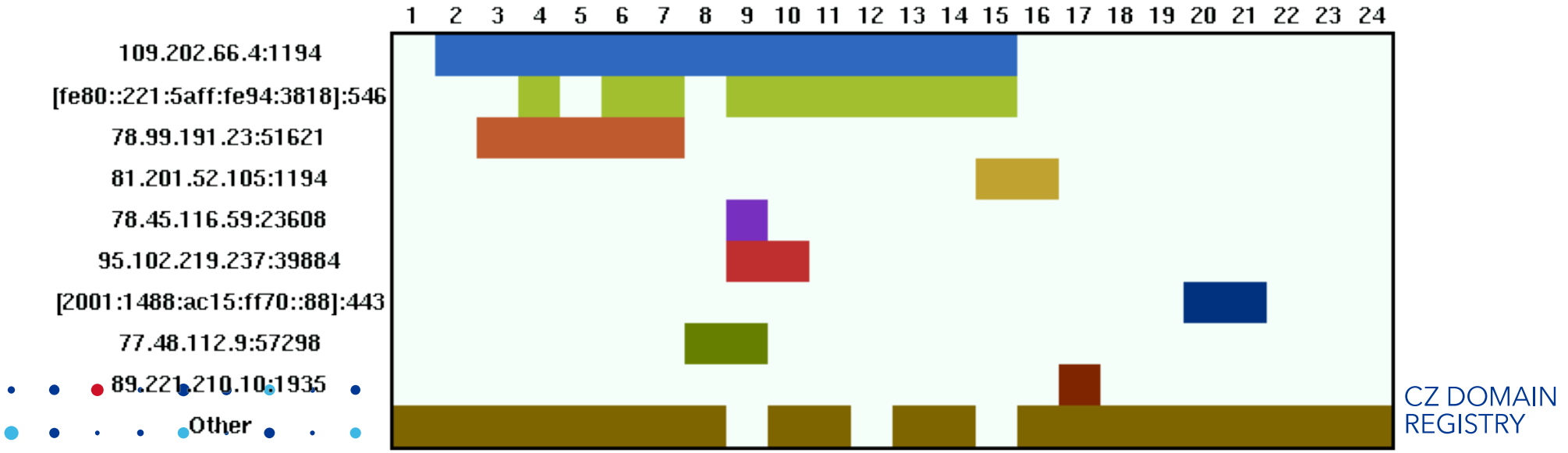
- Firewall logs
- Router logs - upgrade status, SW problems
- Physical quantities – temperature etc.
- uCollect
  - Basic stats, PCAP stats, anomaly detection
  - Modular system for data collection and reporting

Data collection – uCollect - modules

- Module "count" – TCP/UDP/.. stats - on portal
- Module “buckets“ - IP anomaly detection
  - Hashed by multiple functions
  - Send securely into central repository
  - Central server tries to find anomaly
  - (Similar to DNS anomaly detection presented at ICANN-45, Toronto)

Data collection - uCollect

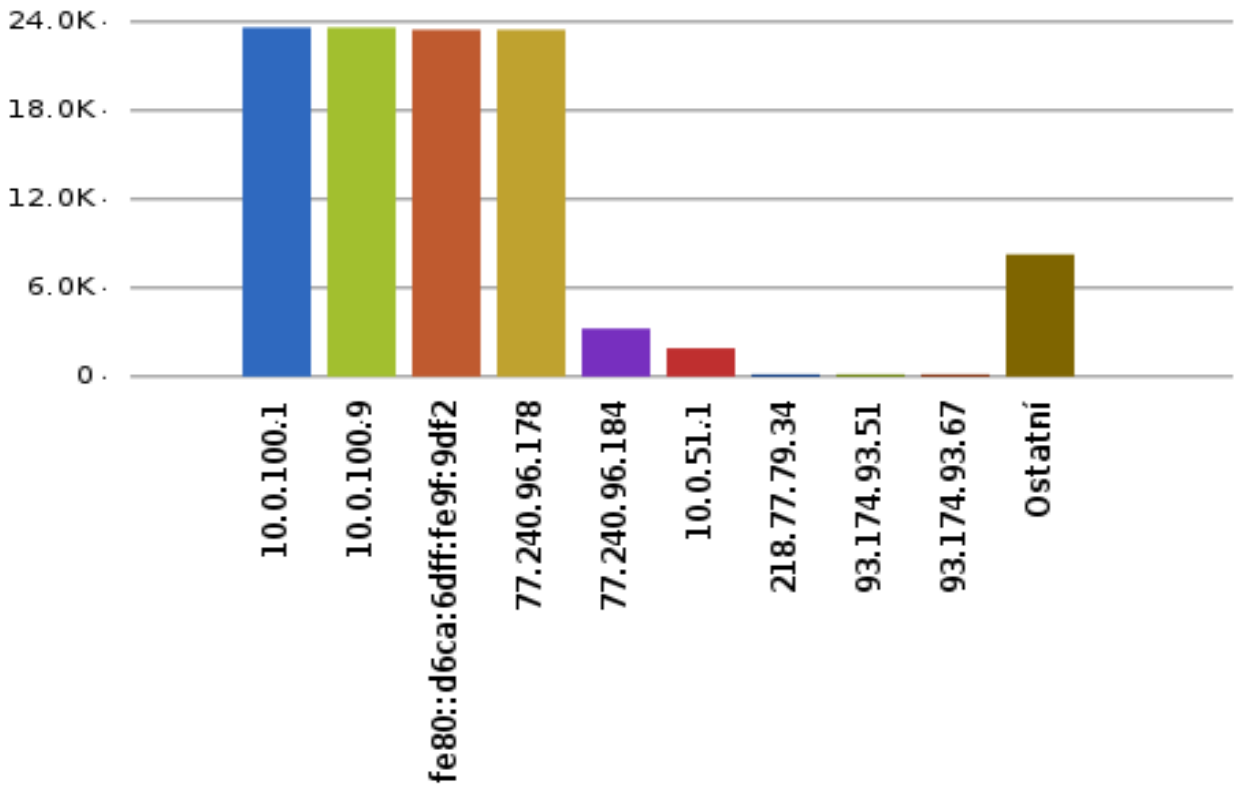




CZ DOMAIN REGISTRY

Central portal

- Communication with users – forum, support
- Graphs
- Tutorials



End user agreement

- Leasing - 3Ys + selling off
- Main gateway to the Internet – non stop
- CZ.NIC allowed to test reachability of 3rd party sites
- uCollect mandatory
- End user access allowed – even root
- Free modification except data colection and communication with central servers

Privacy issues

- Agreement
- Separate DB for account an data
- ISO27001
- Consulted with personal data protection authority
- POSITIVE Big Brother Awards CZ 2013
- Open Source
- Packet headers, data retention

Status

- 10% distributed to end users (and increasing)
- Improving detection methods
- OS improvements – based on feedback
- Tutorials – Turris and NAS, DLNA, VPN concentrator, ...

Future

- First results!
- Another batch of 800 routers planned this year
- VDSL interface
- SW improvements – OS + ucollect
- Universal OS for SOHO routers
  - Market
- Sweet to the end users – HW upgrades, tutorials – e.g. camera, smart home

Thank You!

PROJECT:
TURRIS

Ondrej Filip • ondrej.filip@nic.cz • http://www.turris.cz

CZ DOMAIN REGISTRY