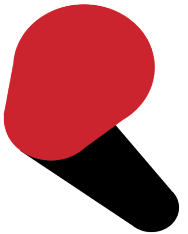
Project Turris

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



PROJECT:
TURRIS

Ondřej Filip • 6 Oct 2014 • NANOG • Baltimore

CZ.NIC, CZ.NIC Labs

- Domain name registry - .cz
  - 1.1M, 35% DNSSEC
- OS projects for local and global community

Knot DNS

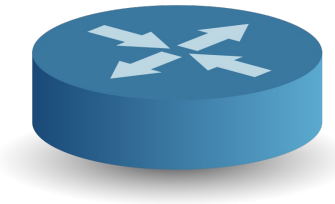
Project Turris - motivation

- Started in 2013 – project of shared cyberdefence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers

Project Turris - motivation

- Security research
  - Currently – Honeynet, DNS anomaly detection
  - Probes close to end users
  - Distributed in many networks
  - IP(v4/6) Anomaly detection
- End user security
  - Adaptive firewall based on collected data
  - Feed for CERT team (CSIRT.CZ)

Problems of current CPE devices

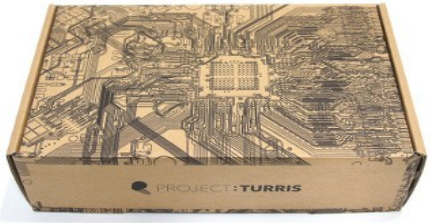


- SOHO routers
  - No or very bad support of IPv6
  - Problems with DNS, DNSSEC, no validation
  - No support for third party applications – app store
  - Limited security features
  - No automated software upgrades
  - Current security issues

Data collection - probes

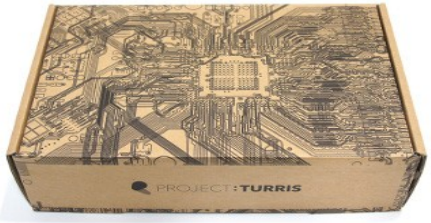
- Distribute 1000 probe - SOHO routers to end users for 3 year lease (for 1 CZK = 0,05 USD)
- Probe – powerful enough to forward 1Gbps of traffic with analysis – no HW found on the current market -> HW development
- Additional features to increase value for end users

Router Turris



- Developed from scratch
- 1000 pcs – produced in Czech Republic
  - Freescale 1.2 GHz dual core (PPC)
  - 2 GB DDR memory – slot
  - 256 MB NAND + 16 MB NOR flash
  - 5x LAN – 1 Gbps ports (Ethernet switch with 7 ports - 2 Gbps lines to CPU)
  - 1x WAN – 1 Gbps port (directly to CPU)

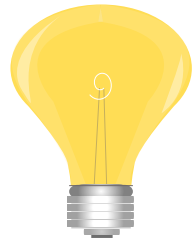
Router Turris



- 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
- Low power consumption – 9-14 W
- Open source license

Router Turris

Router Turris – killer feature

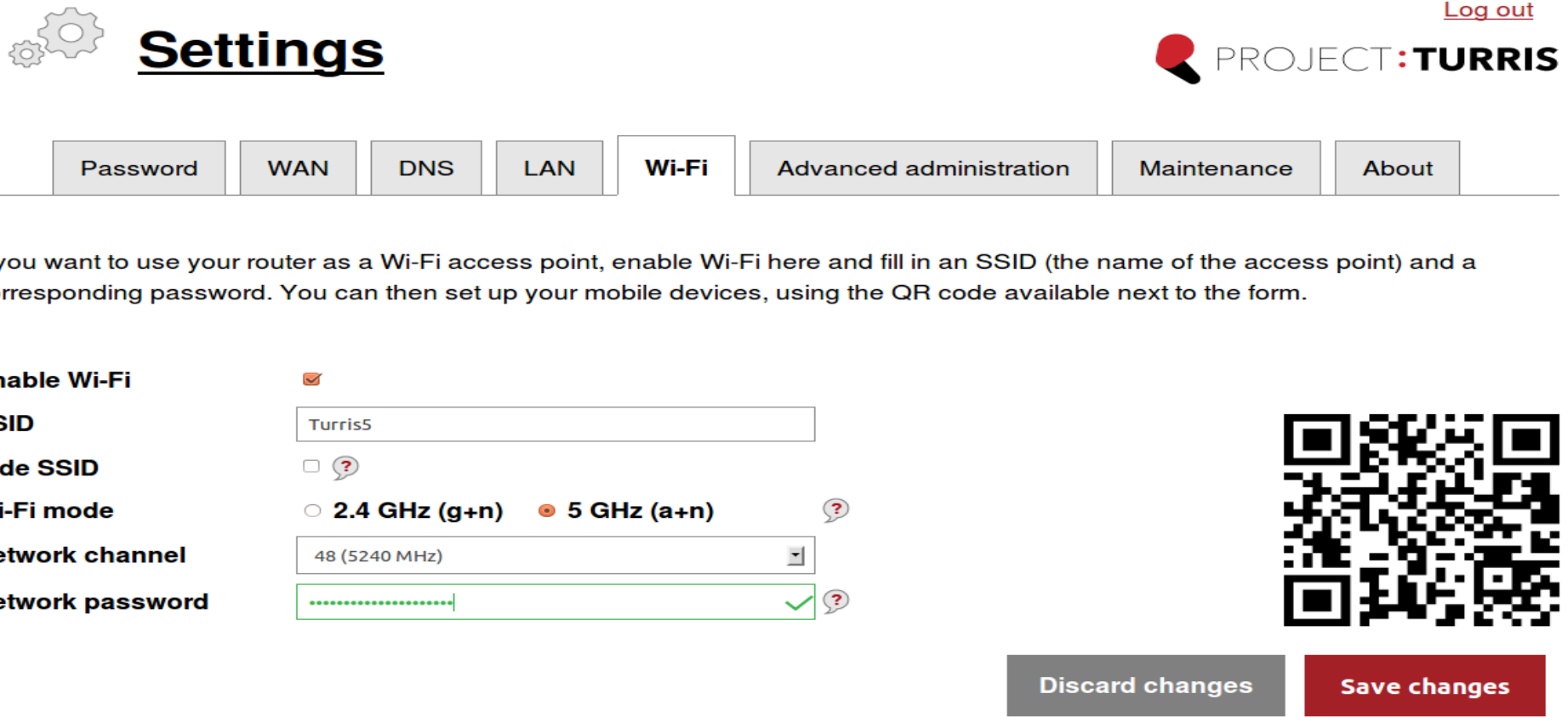


- LED brightness intensity tunable (!)
  - Software managed (RGB)
  - Button at the back
  - :-D

Router Turris – software

- Based on OpenWRT – open source
- Configuration wizard – based on NETCONF
- Automatic updates – user can set preferred time for reboots
- Encrypted communication with central server
- Data collector – only mandatory process
- IPv6, DNSSEC, passwords, ...
- Android application in beta stage

User interface



Data collection

- µCollect
  - Lightweight system for packet analysis with pluggable modules
  - The heart of active security monitoring
- Firewall logs
- Router logs - upgrade status, SW problems
- Other measures – temperature, load, memory and flash utilization etc.
- Secure connection to central server – crypto HW for authentication

Data collection - µCollect

- "count" – TCP/UDP/.. stats - displayed on portal
- “buckets“ - IP anomaly detection
  - Hashed by multiple functions
  - Central server tries to find anomaly
- “bandwidth” - passive network speed monitor
- “flow“ - netflow-like data for anomalies and connections with suspicious addresses (from CSIRT.CZ, firewall logs, etc.)

Network probing - µCollect

- “sniff“
  - Ping to high profile sites
  - DNS resolution and SSL certificate matching to detect possible MITM attacks
  - Netneutrality measuring
- “spoof”
  - IP spoofing tests - does ISP conform to BCP-38 and others?

Botnet monitoring

- Uses public and internal sources of botnet C&C centers' IP addresses
- Captures flow data for communication with such addresses
- Suspicious flows are reported to end users
- Users can easily trigger capturing of whole communication and voluntarily submit it to us
- Malware infection was successfully detected on about 20 end users' computers

Firewall log analysis

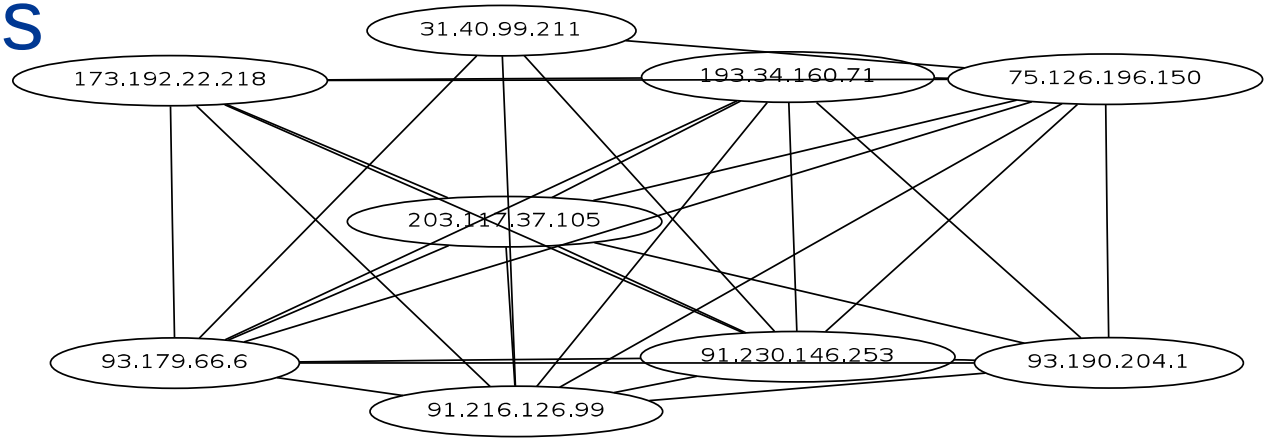
- About 6 million logs each day
- System of ranking is used to determine the most offending attackers
  - number of clients
  - attacked ports
  - other data sources - e.g. honeypot
- Resulting greylist is used as source for flow collection and analysis

Firewall log analysis

- Several misconfigured devices identified
  - DNS open to reflection attack
  - SAMBA open to the world and exchanging data with suspicious Chinese addresses, etc.
- Greylist will be published and updated weekly

Firewall log mining

- Uses similarity in attacker behavior adapted from text mining
- Groups similarly acting IP addresses together
- Work in progress



CSIRT.CZ cooperation

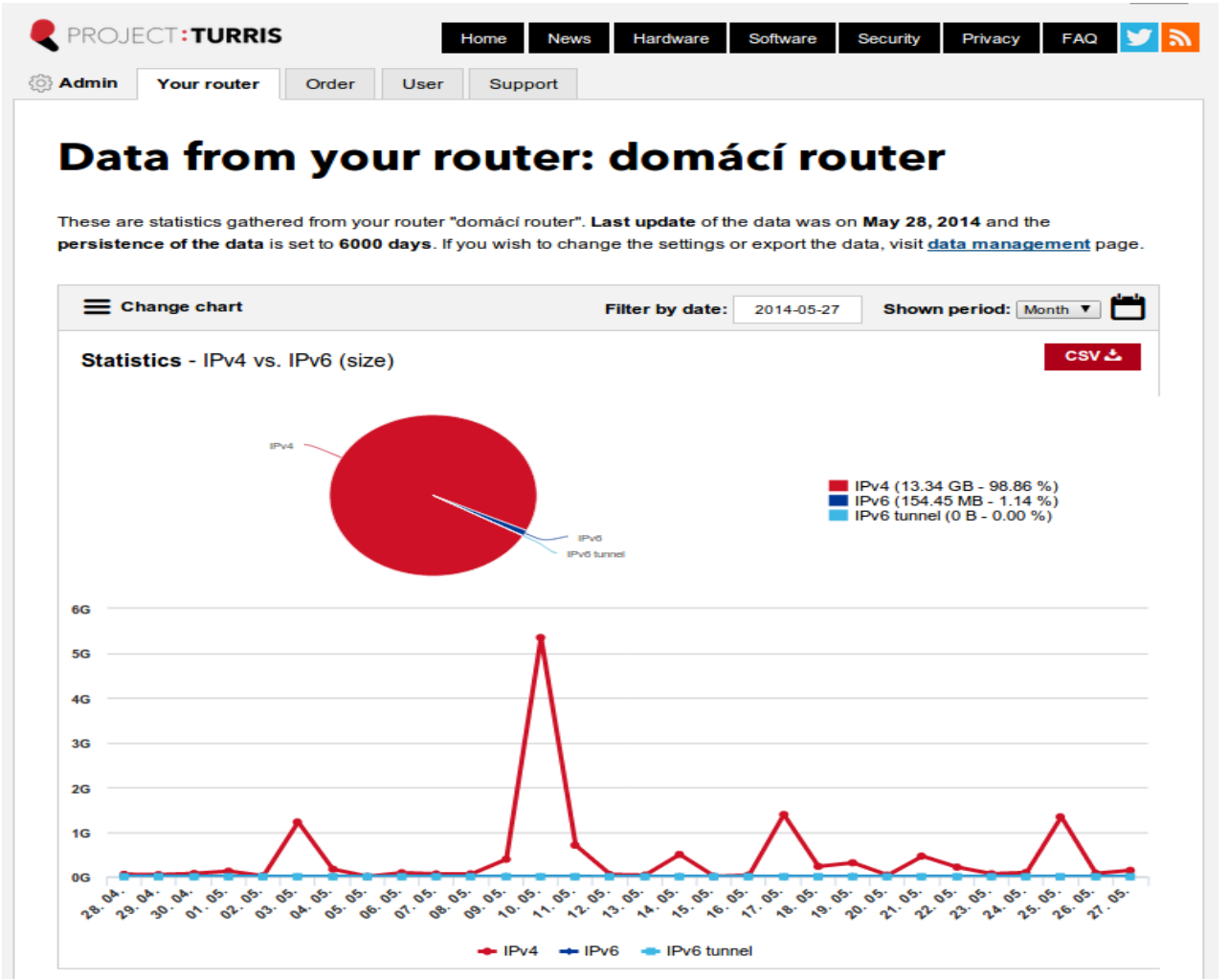
- Lists of malicious websites based on malware observed on .CZ domains
- Used in firewall on Turris to block or log
- Prevents malicious iframes from loading on compromised websites
- Several tens of accesses blocked already
- Topical cooperation – for example detection of Synology backdoor exploit attempts

In progress

- Majordomo - statistics of LAN devices' Internet activity (for accounting, rogue TV detection, etc.)
- Analysis of unsuccessful TCP connections from LAN to Internet
  - Detection of malware using high number of short lived potential IP addresses for C&C centers
- Cooperation with antivirus manufacturers in observation of new malware

End user portal

- Communication with users
- Graphs
- Tutorials - Turris as NAS, DLNA, VPN concentrator, multi WAN setup, 3G backup, VLAN setup, ...
- End user forum – very active – many other improvements


PROJECT:TURRIS
Home
News
Hardware
Software
Security
Privacy
FAQ
Admin
Your router
Order
User
Support
Data from your router: domácí router
These are statistics gathered from your router "domácí router". Last update of the data was on May 28, 2014 and the persistence of the data is set to 6000 days. If you wish to change the settings or export the data, visit data management page.
Change chart
Filter by date: 2014-05-27
Shown period: Month
Statistics - IPv4 vs. IPv6 (size)
CSV
IPv4
IPv6
IPv6 tunnel
IPv4 (13.34 GB - 98.86 %)
IPv6 (154.45 MB - 1.14 %)
IPv6 tunnel (0 B - 0.00 %)
6G
5G
4G
3G
2G
1G
0G
28. 04.
29. 04.
30. 04.
01. 05.
02. 05.
03. 05.
04. 05.
05. 05.
06. 05.
07. 05.
08. 05.
09. 05.
10. 05.
11. 05.
12. 05.
13. 05.
14. 05.
15. 05.
16. 05.
17. 05.
18. 05.
19. 05.
20. 05.
21. 05.
22. 05.
23. 05.
24. 05.
25. 05.
26. 05.
27. 05.
IPv4
IPv6
IPv6 tunnel

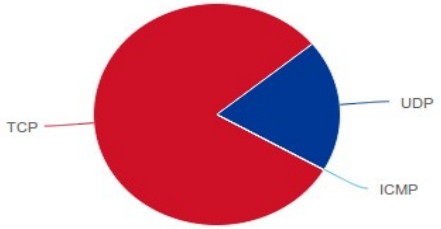
End user agreement

- Leasing, 3Ys + selling off
- Main router connecting to the Internet
- No switch off – non stop operation
- Open access – SSH + root
- Free modification except data collection and communication with central servers

Privacy issues

- Agreement
- Separate DB for accounts and data
- ISO 27001
- Consulted with personal data protection authority
- POSITIVE Big Brother Awards CZ 2013
- Open Source
- Packet headers, data retention

Interesting facts

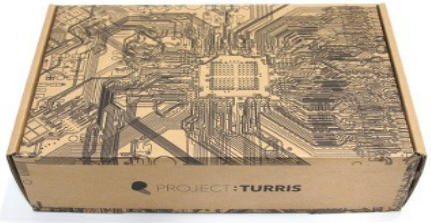


- 990 devices registered & on-line
- Roughly 6 TB of data transferred each day (IPv6 ~1 % + 0.6 % using tunnels)
- 8000 IP addresses trying to connect to more than 20 clients per week
- Automatic upgrades - 6 major and several minor releases
- Heartbleed fixed in a few days from disclosure (Shellshock as well)

Cooperation

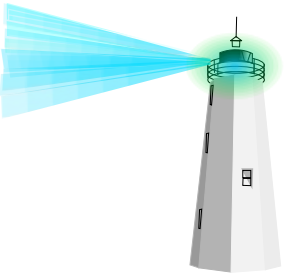
- Early stage cooperation with various parties
  - Comcast
  - RIPE Atlas
  - Antivirus companies
  - Traffic measurement

Router Turris v 1.1

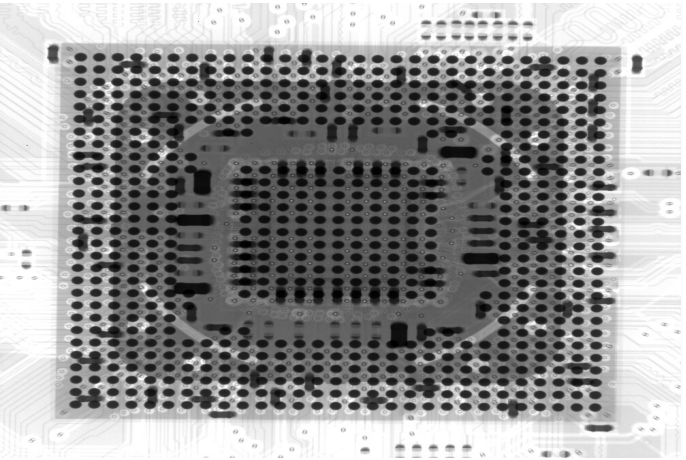


- New version – prototype ready
- Minor HW improvements – USB 3.0, SIM card slot
- Again 1000 pcs – to be distributed mainly in CZ
- Same model – continuation of the security research
- Small factor VDSL interface (USB powered)

Turris Lite



- „Raspberry PI for networking“
- Educational board – at least: dual core CPU 1GHz, 5x1Gbps, USB3.0, 512MB RAM, 128MB flash, microSD, 2xminiPCIe, SPI, GPIO, .. - open source HW
- Same OS as Turris with automatic updates available
- Optionally can use the Turris security features
- Ability to forward 1Gbps
- Not for profit - cover only variable costs
- Price target – board ~100 USD
- Interested? Sign-up at **http://lite.turris.cz**



Thank You!

PROJECT: TURRIS

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

CZ.NIC | CZ DOMAIN REGISTRY