Project Turris - news
And its child Turris Omnia

Ondřej Filip • 19 Oct 2015 • ICANN Tech Day • Dublin
Project Turris - motivation

- Presented at ICANN 49 / Tech day
- Started in 2013 – project of shared cyberdefence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers
Data collection - probes

- Distribute 1000 + 1000 probes - SOHO routers to end users for 3 year lease (for 1 CZK = 0.04 USD)
- Additional features to increase value for end users
- Probe – powerful enough to forward 1Gbps of traffic with analysis – no capable HW found on the current market -> HW development
Project Turris - news

- 10 major releases of Turris OS - Heartbleed and Shellshock fixed in days from disclosure
- Majordomo – watch your home network
- Turris Gadgets – IoT and your home router
- Telnet and ssh honeypots
- Other project outputs – grey list & open data
- Turris Omnia
Majordomo

- Project Turris is not focused on devices inside LAN
- Strange communication originated from “smart” devices (LG Smart TV case)
- Majordomo – check who are your devices talking to
- Interface integrated with OpenWRT (LUCI)
Majordomo

Majordomo - monthly statistics (2014-11)

Go back to overview

Available daily statistics for this client are: 2014-11-14

e8:92:a4:98:95:74

<table>
<thead>
<tr>
<th>Destination address</th>
<th>Port/Protocol</th>
<th>Count (download)</th>
<th>Packet size (download)</th>
<th>Payload size (download)</th>
<th>Count (upload)</th>
<th>Packet size (upload)</th>
<th>Payload size (upload)</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail.nic.cz</td>
<td>143/TCP</td>
<td>744</td>
<td>543.72 KB</td>
<td>505.79 KB</td>
<td>908</td>
<td>83.82 KB</td>
<td>37.43 KB</td>
</tr>
<tr>
<td>trubka.network.cz</td>
<td>993/TCP</td>
<td>211</td>
<td>77.81 KB</td>
<td>67.02 KB</td>
<td>337</td>
<td>30.43 KB</td>
<td>13.25 KB</td>
</tr>
<tr>
<td>ea-in-f95.1e100.net</td>
<td>443/TCP</td>
<td>25</td>
<td>20.65 KB</td>
<td>19.36 KB</td>
<td>28</td>
<td>4.66 KB</td>
<td>3.22 KB</td>
</tr>
<tr>
<td>fra07s27-in-f17.1e100.net</td>
<td>443/TCP</td>
<td>21</td>
<td>6.78 KB</td>
<td>5.70 KB</td>
<td>29</td>
<td>4.27 KB</td>
<td>2.77 KB</td>
</tr>
<tr>
<td>ec2-54-183-216-231.us-west-1.compute.amazonaws.com</td>
<td>443/TCP</td>
<td>18</td>
<td>7.33 KB</td>
<td>6.41 KB</td>
<td>31</td>
<td>3.66 KB</td>
<td>2.09 KB</td>
</tr>
<tr>
<td>ea-in-f188.1e100.net</td>
<td>5228/TCP</td>
<td>15</td>
<td>1.61 KB</td>
<td>848.00 KB</td>
<td>28</td>
<td>2.91 KB</td>
<td>1.43 KB</td>
</tr>
<tr>
<td>d172ud.forpsi.com</td>
<td>80/TCP</td>
<td>14</td>
<td>1.77 KB</td>
<td>1.22 KB</td>
<td>33</td>
<td>2.12 KB</td>
<td>726.00 B</td>
</tr>
<tr>
<td>ber01s08-in-f7.1e100.net</td>
<td>443/TCP</td>
<td>11</td>
<td>5.77 KB</td>
<td>5.20 KB</td>
<td>18</td>
<td>3.70 KB</td>
<td>2.77 KB</td>
</tr>
<tr>
<td>ec2-54-241-32-13.us-west-1.compute.amazonaws.com</td>
<td>443/TCP</td>
<td>10</td>
<td>5.29 KB</td>
<td>4.78 KB</td>
<td>13</td>
<td>2.21 KB</td>
<td>1.54 KB</td>
</tr>
</tbody>
</table>
Turris Gadgets

- IoT - cooperation with Jablotron
- Selected 100 most active users – what you can do with those?
- Magnetic door detector, PIR motion detector, smoke detector, power relay – socket, ...
### Honeypot

<table>
<thead>
<tr>
<th>Time</th>
<th>Remote address</th>
<th>Commands</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/24/2015 03:28</td>
<td>175.139.185.238</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 03:43</td>
<td>175.139.185.238</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 04:06</td>
<td>94.224.60.106</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 04:08</td>
<td>209.153.38.166</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 04:08</td>
<td>175.139.185.238</td>
<td>4</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 04:12</td>
<td>175.139.185.238</td>
<td>4</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 04:53</td>
<td>94.224.60.106</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 05:15</td>
<td>209.153.38.166</td>
<td>2</td>
<td>Accepted</td>
</tr>
<tr>
<td>8/24/2015 08:11</td>
<td>94.224.60.106</td>
<td>4</td>
<td>Rejected</td>
</tr>
</tbody>
</table>

```bash
$ mkdir /tmp/.xs/
$ cat >/tmp/.xs/daemon.armv4l.mod
$ chmod 777 /tmp/.xs/daemon.armv4l.mod
$ /tmp/.xs/daemon.armv4l.mod
```

Login: root  
Password: root

Duration: 43 s
Honeypot

- Large botnet of ASUS routers
- Using telnet – yes, really
- Trying even non trivial passwords
- Using C&C
- About 8000 devices
Knot DNS Resolver testing

- Knot DNS resolver in alpha stage
- Works for us – more testing needed
- Deployment on Turris
  - Voluntarily in the first phase
  - By default later
Other outputs

- Greylist of suspicious IP addresses
- PorTrend – ports blocked on firewalls
- Response time of selected internet servers + connection speed – published as open data

- Everything published on https://www.turris.cz/
Statistics - Bandwidth utilization - download

By size of transmitted data

- 30–40 Mbps: 7.74 MB
- 20–30 Mbps: 18.51 MB
- 18–19 Mbps: 4.50 MB
- 17–18 Mbps: 4.36 MB
- 15–16 Mbps: 3.94 MB
- 14–15 Mbps: 3.51 MB
- 13–14 Mbps: 13.52 MB
- 12–13 Mbps: 3.05 MB
- 10–11 Mbps: 5.34 MB
- 9–10 Mbps: 2.28 MB
- 8–9 Mbps: 8.52 MB
- 7–8 Mbps: 1.77 MB
- 6–7 Mbps: 6.45 MB
- 5–6 Mbps: 6.79 MB
- 4–5 Mbps: 9.04 MB
- 3–4 Mbps: 11.27 MB
- 2–3 Mbps: 13.20 MB
- 1–2 Mbps: 12.07 MB
- 750–1,000 kbps: 5.06 MB
- 500–750 kbps: 8.73 MB
- 250–500 kbps: 8.24 MB
- 0–250 kbps: 53.07 MB
Turris "Lite" - concept

- A lot of demand – SamKnows, Comcast support
- Reuse our experience - HW, Turris OS
- No agreement, no participation on security research required
- Not much open hardware related to networking on the market
- Suitable for education in networking
- Price optimized
Turris Omnia – more than a router

- New generation
- One of the most powerful SOHO routers
  - Forwarding 1Gbps (small packets)
- Open source SW & HW
- Security research optional
- Mother board for less than $100 (production price only! no development costs)
Omnia – hardware details

- SoC Marvell Armada 385 @ 2 x 1.6 GHz
- 1 GB RAM
- 4 GB eMMC + 8 MB NOR
- 5 + 1 Gbit port + SFP
  - dedicated line for WAN port + SFP
  - 2 lines between CPU and switch chip
Turris Omnia – HW

SoC

Switch-chip

Port5 Port6

Port0 Port1 Port2 Port3 Port4

LAN1 LAN2 LAN3 LAN4 LAN5

OR

WAN SFP
Omnia – more hardware details

- 2 x USB 3.0
- 3 x miniPCIe (one switchable to mSATA)
  - optional WiFi in 2 slots (2.4 + 5 GHz), SIM slot
- RTC chip with battery backup
- Cryptochip for better entropy in RNG
- Dimmable programmable RGB LEDs
- 10x GPIO, 2x UART, SPI, I2C on pinheader
Omnia - benchmarks

extra acceleration off in Omnia

MD5 benchmark

Able to forward 1Gbps (with full BGP routing table)
Omnia - status

- First prototype running with bugs to fix
- Second prototype batch in November
- ~3000 routers preordered (non-bindingly) on our website
- Indiegogo campaign in preparation
- Manufacturing in Q1 2016
Would you like one?

Pre-order at https://omnia.turris.cz/

Ondřej Filip • ondrej.filip@nic.cz