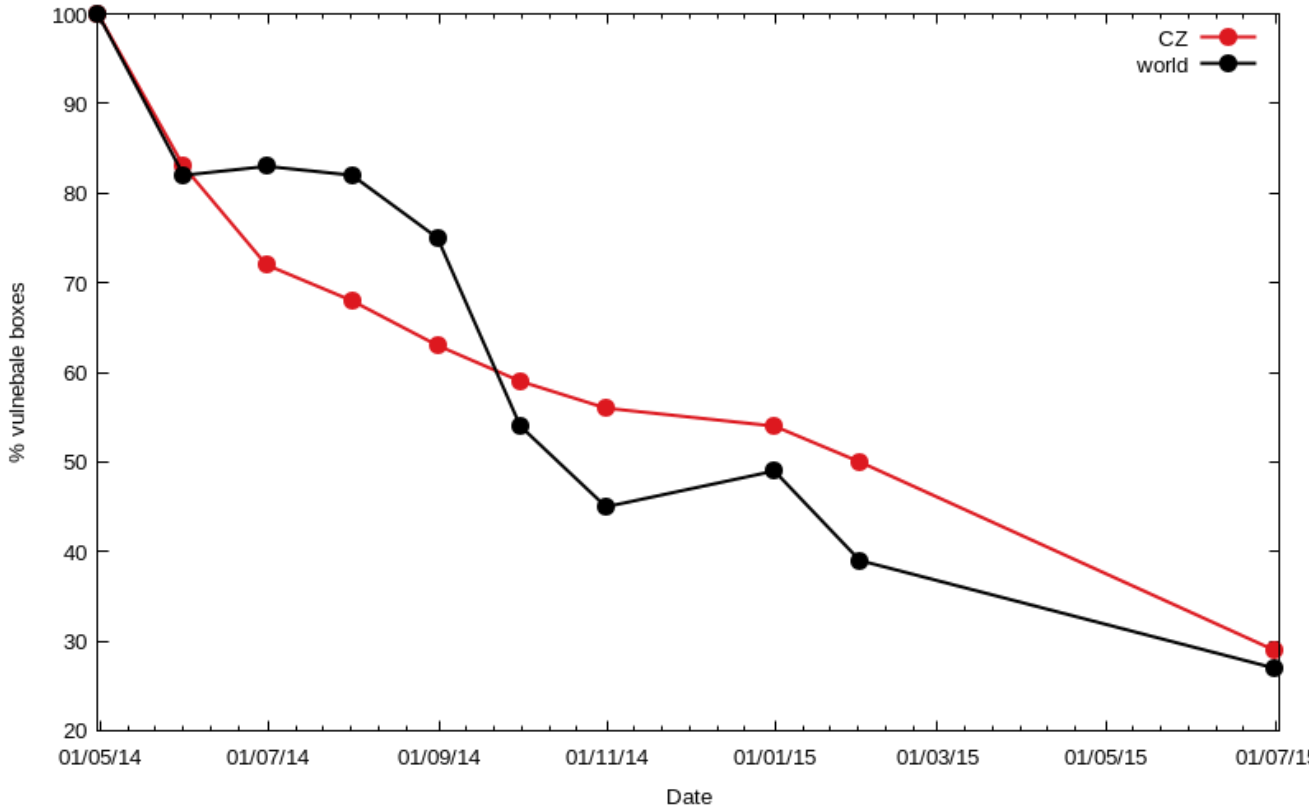
6.8.

The “rom-0” vulnerability one year later (http://en.blog.nic.cz/2015/08/06/the-rom-0-vulnerability-one-year-later/)

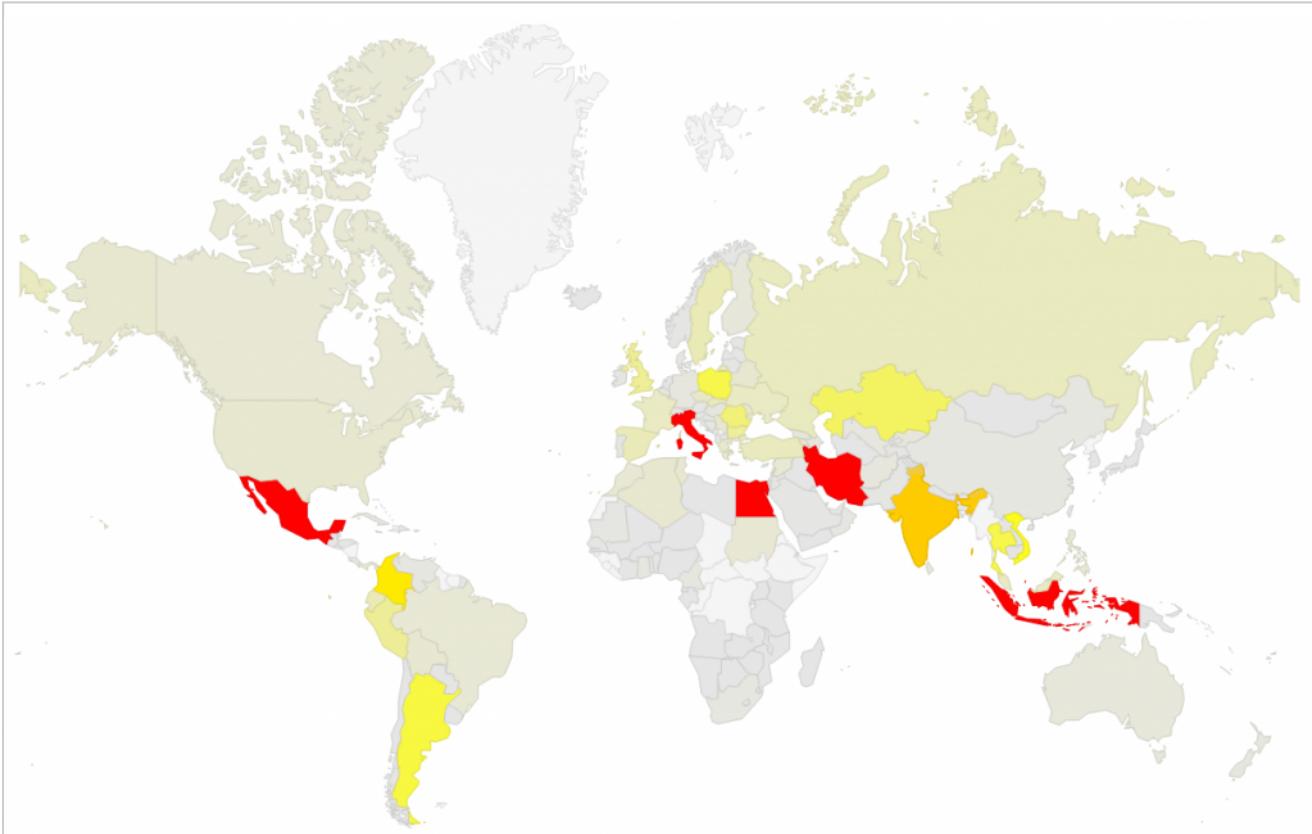
In previous blogposts on the “rom-0” bug in 2014 and earlier this year, I first explained its nature and gave instructions on its patching (http://en.blog.nic.cz/2014/12/11/vulnerability-of-rom-0-after-half-year/).

Then I began publishing the results of counting the routers vulnerable to the “rom-0” bug and encouraging the community of network administrators and security professionals in eliminating the cause or at least neutralizing the impact of this bug. The testing website http://rom-0.cz (http://rom-0.cz/index/?language=en) was created, several presentations at professional conferences took place and the issue managed to attract the attention of the media that spread awareness of the “rom-0” bug among the general public. Media coverage of the security risk has proved to be a very effective and meaningful assistance, which put the Czech Republic ahead of the rest of the world in disposing of this threat, as is also shown by the graphs of the number of vulnerable devices.



(http://blog.nic.cz/wp-content/uploads/2015/07/CZ2.png)

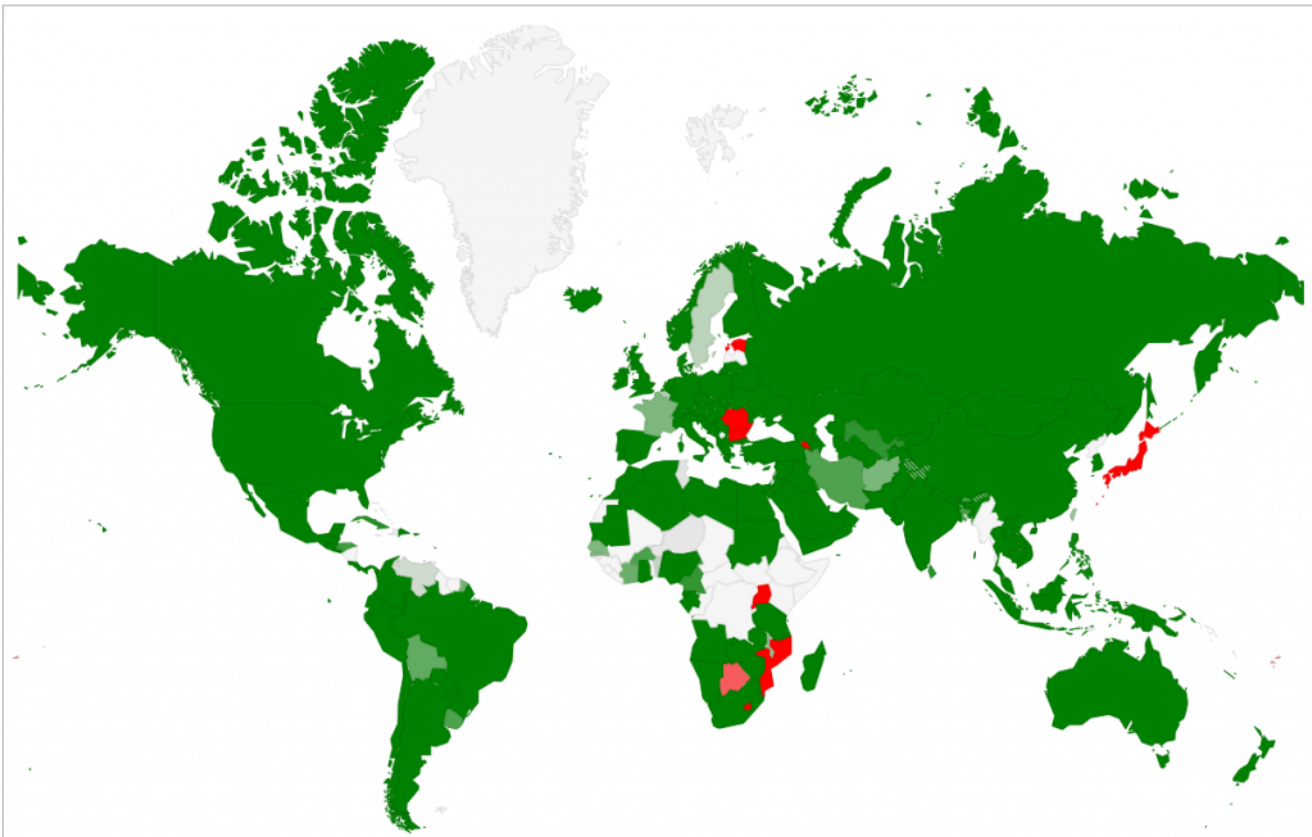
The heterogeneous environment of the Czech Republic, where there is a large number of competing ISPs, is relying on “computer literacy” and individual responsibility of users and home network administrators. Unlike other countries with monopoly providers, our environment does not allow deploying a centralized solution, such as total prohibition of access to ports running the routers’ administration interfaces. In terms of the reduction percentage, the Czech Republic has, despite its initial leadership, lost to the rest of the world over the last year. In any case, it is good news that a large part of networks, administrators and operators has found its way to eliminate a total of hundreds of thousands of vulnerable boxes. The following graph shows the number of vulnerable devices in individual countries, according to the last counting in July 2015.



(http://blog.nic.cz/wp-content/uploads/2015/07/lastmap-201507.png)

Worldwide distribution of vulnerable routers as of July 2015

Since the initial contact with the “rom-0” bug and our first counting in May 2014 until the last one in July 2015, the number of vulnerable boxes in the Czech Republic decreased from 5,368 in May 2014 to the current 1,561 (July 2015) — a decline by almost 71%. Globally, the decrease was from 1,225,514 (in May 2014) to the current 330,397, which is 73%. The following graph shows that most countries show a significant decline since the first counting. However, there are also isolated regions where the number of vulnerable devices has grown. Fortunately the numbers are not big and occurrence of new vulnerable boxes can be attributed to stock sellouts of routers with old firmware and some degree of carelessness and ignorance.



(http://blog.nic.cz/wp-content/uploads/2015/07/delta-20150716.png)

Change in the number of vulnerable routers from May 2014 to July 2015. Green = decrease, red = increase

Despite the intensive awareness campaign among professionals and the general public, the problem with the boxes vulnerable to the “rom-0” bug has not disappeared completely even in the Czech Republic. We can only hope that router manufacturers and network operators learn their lesson, which will not only significantly reduce the probability of a similarly dangerous and easily exploitable bug in the future, but also bring about mechanisms to solve such situations. The CZ.NIC project Turris (https://www.turris.cz/cs/), which introduced routine automatic updates, became a pioneer in this field. The updates not only distribute security patches, but can also add new features and radically improve performance throughout the life cycle of home routers.

Author: Tomáš Hlaváček (http://en.blog.nic.cz/author/thlavacek/)

Leave a comment

Name*:

Email*:
(to not be shown)

Your comment:

Previous: New Features in Knot DNS 2.0 (http://en.blog.nic.cz/2015/08/02/new-features-in-knot-dns-2-0/)

Next: Knot recursive fortnightly, August 11th 2015 (http://en.blog.nic.cz/2015/08/11/knot-recu

Categories: Domains (http://en.blog.nic.cz/category/domains/) (1) , Knot DNS (http://en.blog.nic.cz/category/
mojeID (http://en.blog.nic.cz/category/mojeid/) (2) , Programming (http://en.blog.nic.cz/category/programming/) (1)
Security (http://en.blog.nic.cz/category/security/) (18) , Turris (http://en.blog.nic.cz/category/turris/) (7) ,
Unclassified (http://en.blog.nic.cz/category/unclassified/) (6)

Archi