# Scanning for TR-069 is neither Cyber nor War

Posted on **November 30,2016** by **lynx**

The Deutsche Telekom was in the news. The reason was a major malfunction of routers at the end of the last mile. Or something like that. As always theories and wild assumptions are the first wave. Apparently a modified Mirai botnet tried to gain access to routers in order to install malicious software. The attacks lasted from Sunday to Monday and affected over 900,000 customers. These routers often are the first point of contact when it comes to a leased line. Firewalls and other security equipment usually comes after the first contact with the router. There are even management ports available, provided the ISP has no filters in place. The TR-069 (Technical Report 069) specification is one management interface, and it has its security risks.

Now that the dust has settled the Deutsche Telekom and politicians are quick to point out that „Cyber“ is going on, a „Cyber NATO“ is needed, the law needs to be amended (because once you have a law against something, It™ will never ever happen again), someone needs to take the blame, and more meaningless phrases are needed to not address the problem at hand. Golem.de has published a good summary and a comment on these remarks (in German). A detailed in-depth analysis showed that no TR-069 exploit was working on the targets. Instead the devices just failed to work. Which is very different from warfare or any other targeted attack.

Let's face it. Most devices out there (Internet of Things or not) can be fried by using the ISIC (IP Stack Integrity Checker) tool for a couple of minutes. You should try this at home. There is not war, and there is no „cyber“ going on. It's just the missing defence-in-depth concept at work.

Posted in:Discussion,High Entropy,Internet | Tagged:Defence,Design,Infrastructure,IoT,Malware | With 3 comments