# Exploiting the geographical distribution of a security issue in the Netherlands

**Introduction:**

Recently, more than 300,000 home and small-office (SOHO) routers have been compromised by hackers. If you are an UPC Netherlands subscriber, you have a big chance to be a victim of this kind of router takeover.

**30 November 2013:**

I discovered a vulnerability (CSRF or sea-surf) in the Cisco EPC3925 router. It is the router actually used by UPC Netherlands subscribers (www.upc.nl). I decided to keep the discovery private, in order to present it for the first time during a security conference. So the issue was submitted to the HackInTHeBox call for papers.

**16 December 2013:**

Jeroen, an information security consultant, published in the wild the same security issue about the Cisco EPC3925 router. He was the first one providing the exploit code to change username and password to administer the router itself.

**3 March 2014:**

BBC warns the world about more then 300,000 home routers have been hacked (http://www.bbc.com/news/technology-26417441).

Team Cymru (it is a Celtic word, pronounced *kum-ree)* is the white hat hackers team that discovered the security issue, reporting that router and firewall from the following vendors are vulnerable to the attack:

- D-Link
- Micronet
- Tenda
- TP-Link
- Other unnamed vendors

**How safe is your router?**

If you are an UPC Netherlands subscriber, it is highly probable you have a Cisco EPC3925 router, and it means that you may have been hacked too, and you are a happy owner of one of the 300,000 home routers reported by the BBC.

Hacking a router represents the deepest and almost perfect attack to your security:

- it compromises the security of all the internet connections you could have at home: your computer, your mobile phone, your smart television.
- it is difficult to discover: no antivirus or firewall can detect it.

The best way to compromise you privacy, is to change the DNS settings of your router. In this way all the internet connection are redirected and intercepted (man in the middle attack). Actually Cisco EPC3925 routers are vulnerable to a CSRF attack that allows the user to change any setting in the router (my first exploit code, was about the Wi-Fi password/network name). Including the DNS settings.

Exploiting the geographical distribution of a security issue.

It is really interesting how an attacker could easily use the previous information to carry out a wide scale attack in the Netherlands.

The exploit code to infect a router is just a link in a web page. If the user clicks the link, the router is compromised.

The exploit code just will work for a specific router (in this case the Cisco EPC3925), highly distributed in the Netherlands.

In order to increase the chances of success, the attacker just has to “infect” with the malicious link pages written in Dutch (Dutch forums, websites, mailing lists). Another way to localize the attack would be to use targeted media advertisement systems, like Google Adsense, or Facebook. Imagine a banner advertising a free subscription to a gym in your area,  a free ticket for the Cinema, all targeted just for Dutch users.

Even better, using banners advertising discounts or offers for Dutch UPC subscribers will increase the attack effectiveness :)

You can contact me at: info@studio-sg.net