

23 January 2008

By: Bogdan Botezatu, Hardware Editor



The best method to protect: unplug your network cable and lock the router's ports!  
Logitech

## **Keep an Eye on Your Router: It May Lead You On a Wrong Way!**

*So wrong that you won't even be able to find your money in the bank account*

If you thought that malware has made an obsession out of Windows-based operating systems only, you're wrong. A new type of criminal attack is committed to take over one of the most common hardware in a computer network: the router. According to the latest security reports, a new kind of attack tries to lure Internet users on spoofed banking pages, where they are faced with an exact clone of the login form. Although the majority of users have already "smoked" the hackers' spoofing tricks and tend to carefully type the legit address in the browser's address bar, the attack can take them by surprise. The attack changes a router's settings that deal with the domain name system server (the entity that translates domain names into the IP number mambo-jumbo - for instance, [www.softpedia.com](http://www.softpedia.com) translates into 64.225.158.189). basically, the attack would translate the domain name into an IP hosting a clone of the webpage, that tries to steal the user's banking credentials (such as username, password, PIN and credit card number). It is a common practice for cyber-criminals to use large numbers of rogue DNS servers to route people to fake versions of respectable websites. The most exposed pieces of hardware are home routers, that get hijacked through a technique known as cross-site request forgery. However, the attacker would need the router's administrative password, but that would be the easiest part, since the majority of home users won't bother changing the default password. These default credentials are public and can be found on the manufacturer's webpage. Some brands of routers have been penetrated even without entering an administrator password, so there is a high chance for the attack to succeed even though the password has been changed. Moreover, The Thomson / Alcatel routers are affected by an authentication bypass bug that lets non-administrators get into the router's settings panel. "Given the simplicity of the attack and the potential widespread implications, we always felt that it would simply be a matter of time before it happened," claims Symantec researcher Zulfikar Ramzan. "The building blocks have been out there for some time and anyone with sufficient familiarity could easily put them together."