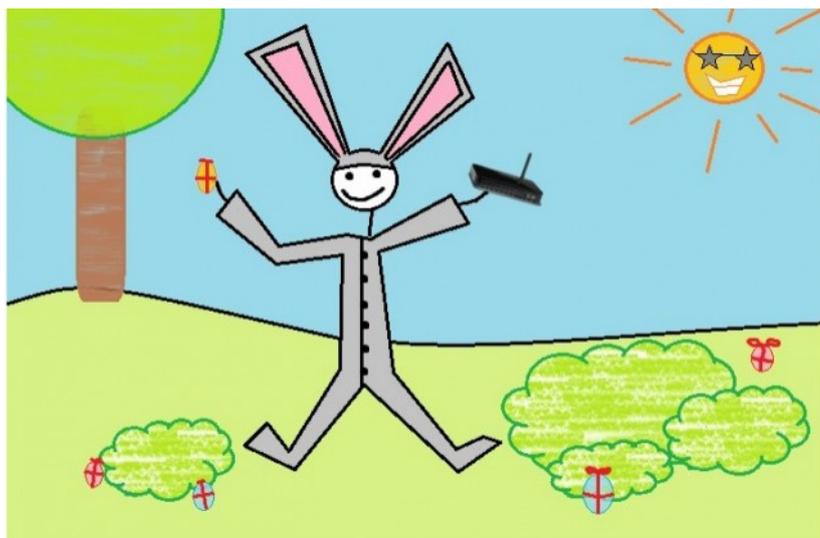# Easter egg: DSL router patch merely hides backdoor instead of closing it

By *Rianne Schestowitz*
Created *22/04/2014 - 11:35am*
Submitted by Rianne Schestowitz on Tuesday 22nd of April 2014 11:35:15 AM Filed under Hardware [1] Security [2] Legal [3]

First, DSL router owners got an unwelcome Christmas present. Now, the same gift is back as an Easter egg. The same security researcher who originally discovered a backdoor in 24 models of wireless DSL routers has found that a patch intended to fix that problem doesn?t actually get rid of the backdoor?it just conceals it. And the nature of the ?fix? suggests that the backdoor, which is part of the firmware for wireless DSL routers based on technology from the Taiwanese manufacturer Sercomm, was an intentional feature to begin with.

Back in December, Eloi Vanderbecken of Synacktiv Digital Security was visiting his family for the Christmas holiday, and for various reasons he had the need to gain administrative access to their Linksys WAG200G DSL gateway over Wi-Fi. He discovered that the device was listening on an undocumented Internet Protocol port number, and after analyzing the code in the firmware, he found that the port could be used to send administrative commands to the router without a password.

After Vanderbecken published his results, others confirmed that the same backdoor existed on other systems based on the same Sercomm modem, including home routers from Netgear, Cisco (both under the Cisco and Linksys brands), and Diamond. In January, Netgear and other vendors published a new version of the firmware that was supposed to close the back door.

[4]

Hardware Security Legal

Source URL: http://www.tuxmachines.org/node/65163

Links:
[1] http://www.tuxmachines.org/taxonomy/term/39
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] http://www.tuxmachines.org/taxonomy/term/106
[4] http://arstechnica.com/security/2014/04/easter-egg-dsl-router-patch-merely-hides-backdoor-instead-of-closing-it/