

Router hijacking

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-09/0259.html>

From: Nick (*kewlest_at_yahoo.com*)

Date: 09/09/04

Date: Wed, 08 Sep 2004 15:24:41 -0700

Hi

I had a belkin's router with a simple packet filtering firewall. I had switch off remote access/configuration – that is, it won't(shouldn't) allow any connections to port 80 that comes from the external interface.

One day, I found a open TCP port (Virtual Server/port forwarding) to my housemate's machine that we hadn't set up! I checked my housemate's machine for any process listening on that port...none!

I closed the port / changed the password and it didn't happen again. But I wonder how it happened in the first place? Any ideas?

My router also used to get a couple of port scans that it used to log.

But that's it!

I recently came across a similar complaint at some other newsgroup too.

Only way that I can think of, is that my friend downloaded some spyware with a keylogger – got the login/passwd info (though I doubt it since he hardly used to login himself) and tried to login and add the entry (the author must know exact http packets that were exchanged with the router). Or a bug in belkin's router that I am not aware of!

–N