Tuesday, March 24. 2009

Botnets ... based on routers - revisited

While waiting for my tea water to boiling, i had an idea: Perhaps it´s much easier to hack a router to a botnet drone than i initially thought. I think it´s consensus, that Windows based PC are still easily infectable with bots. But the PC are under steady control by their users. As tight as the firewalls of these routers are to the outside, as open they are to the inside. I think it would be nice idea, to target the Windows PC at first, infect the router from there (it´s easy to find the router ... it´s the default router). Perhaps by an exploit for the remote administration software or just by router passwords stored in the browser password chain. After infecting the router, the bot could remove itself from the Windows PC without leaving traces. An bot detection tool can´t find something on the PC and it doesn´t check the router for an infection. Well ... you can think about Trusted Execution or TPMs what you want ... but there are valid use cases outside DRM.

It´s a little bit like tonsillectomy by opening the chest, but sometimes it´s easier this way ... especially when the patient don´t want to open the mouth

Posted by Joerg Moellenkamp in English, Security at 09:15