Monday, March 23. 2009

Botnets ... based on routers

With a sharp tongue, you could state: Microsoft already proofed that cloud computing is a economic success. The large botnets in the Internet are nothing else than clouds, even with SaaS (no, not software as a service, spam/scam as a service). And you can make really a money by owning a botnet. Well ... I hope that the discovery of DroneBL doesn´t lead to a much larger wave of BotNets.

The worst managed computer system in the common household is often not the Windows PC .... it´s the small Linux computer that got ubiquitous since DSL or cable internet is something normal. Most people configure them once, put them somewhere in a closet and forget them. So it was just a matter of time before someone would have created a botnet consisting out of this small routers. DroneBL writes about such a botnet.

When you really think about it: These small routers are a perfect target. They run 24h/7days a week. Most people don´t really look at them, so they can´t detect strange traffic patterns by looking at the blinkenlights. Furthermore the once you have an exploit for a certain type of router, it´s highly probable that you can exploit a vast amount of systems. Depending on the type of the router, there is a large population of identical system. Just a thought game: Let´s assume, you find an exploit for a brand of routers distributed by almost all ISP in a country to their end customers. This would be a hell of a botnet. Millions of members Obviously the first action of such an exploit would be the deactivation of online router software update and the redirection of any request to the support website. It would be really hard to get rid of this bot.

I hope the developers of the OS of such small router boxes are aware of their responsibility ... an error could be an really nasty home run for the dark side.

Posted by Joerg Moellenkamp in English, Security at 20:26