

Tuesday, October 4, 2016

The "Enemy inside" ... now at your home

Given the news about the DDoS attacks carried out by "Internet of Things devices" that were in the news last week like in "Brace yourselves—source code powering potent IoT DDoSes just went public" i just thought: "It's finally there, the time has come". The thing i speculated about in a coffee kitchen 2005, wrote about it in 2009 in "Botnets ... based on routers" and "Botnets ... based on routers - revisited" respectively 2014 in "Enemy Inside".

We have 1.4 billion devices out there running Android all running the same OS. We have roughly 1 billion iOS devices all running a different OS, but all running the same different OS. Both with significant compute power per device. We have 10 million Raspberry Pi out there. The variant 3 is quite powerful. I don't know how many routers, TV sets, fridges, running a modified general-purpose OS.

You could joke that we are just one really bad zero-day and enough criminal energy away from a Terminator 3-style scenario. The bright side: We are still protected by a lack of updates in technology from the full T3 scenario as described in "CNN: The U.S. is still using floppy disks to run its nuclear program" . By the way, this is the only case where i 'm against updates. This code and hardware did not killed us for the past decades. Keep it this way. Still bad enough: Given failing TVs, lack of Netflix and porn , no smartphone to stare at and the necessity to talk with each other ... people will go on a rampage anyway and behave like post nuclear armageddon zombies.

Posted by Joerg Moellenkamp in English, Security at 20:29