The internet of things – by Bernard Collin

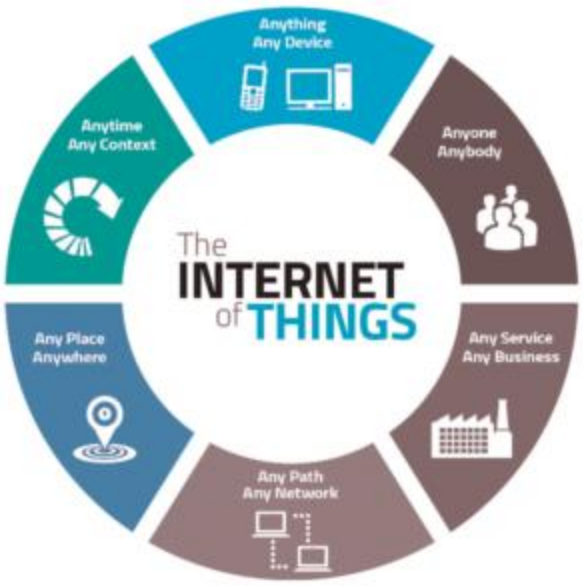
September 2017

Article by Bernard Collin, CEO of SafeComs Network Security Consulting Co., Ltd. in the magazine “EXPAT LIFE in Thailand” about the Internet of Thing (IoT).

“Conversation on the IoT (internet of things) is rising as it becomes a more broad and social consideration. It has a wide reach, and it also shows that people need to be more aware of their personal impact. What might look like a minor problem hides a greater trouble.”

The internet of things is any, and every device connected in some way to a network and open to the internet. A home system designed to allow you to set the house to wake up the lights and run the heating/air conditioning ready for your arrival home. A sound system connected wirelessly through your home Wi-Fi, a baby monitor you can check from the office. But the term simply applies to any and every device meant to automatically connect to the internet and accomplish a task with little to no oversight.

This is where the problems start, these devices are crafted for simple use and convenience which then become points of weakness. Not designed for high security but simply task completion, many of the devices have now been breached and exploited. The activity isn’t specifically because it targets you, in fact,
that the device is “yours” is incidental, it’s just another bot to them. The devices are not breached to spy on you and aren’t designed to break down and try to ransom the device back to you (See the previous article on Ransomware).



Without your knowledge or consent, any device connected to your internet connection can be used by criminal organizations and general mischief makers against networks and websites. Shutting down a business ability to connect to the internet or simply wielded as a hammer against single uses they have found offends them. People are selling time and activity on your home devices against others, a device you paid for and pay to keep running, on an internet connection you pay for upkeep.

What can we do to combat this new botnet problem?
For one, we should make sure that device creators take their responsibility on creating secure devices more seriously, but on a more personal angle, anyone who likes to add gadgets and devices to their own home should either consider adding security layers to their connection to the internet.

Security is a personal responsibility these days, and being aware of how your devices are being used and exploited is something each household should be concerned about. These are your devices, and you should be certain they aren’t being exploited by others for their own ends.