The Internet of Things (IoT) revolution promises to make our lives easier by providing cheap and always connected smart embedded devices, which can interact on the Internet and create added values for human needs. But all that glitters is not gold. Indeed, the other side of the coin is that, from a security perspective, this IoT revolution represents a potential disaster. This plethora of IoT devices that flooded the market were very badly protected, thus an easy prey for several families of malwares that can enslave and incorporate them in very large botnets. This, eventually, brought back to the top Distributed Denial of Service (DDoS) attacks, making them more powerful and easier to achieve than ever. This paper aims at provide an up-to-date picture of DDoS attacks in the specific subject of the IoT, studying how these attacks work and considering the most common families in the IoT context, in terms of their nature and evolution through the years. It also explores the additional offensive capabilities that this arsenal of IoT malwares has available, to mine the security of Internet users and systems. We think that this up-to-date picture will be a valuable reference to the scientific community in order to take a first crucial step to tackle this urgent security issue.