MINIONS: MitigatINg IOt-based DDoS attacks via DNS

Elsa Turcios Rodríguez (TUD) & Carlos Hernandez Ganan

Summary: Consumer IoT devices may suffer malware attacks, and be recruited into botnets or worse. There is evidence that generic advice to device owners to address IoT malware can be successful, but this does not account for emerging forms of IoT malware. This presentation summarizes different field studies conducted during MINIONS project on the removal of IoT malware by consumers. Our findings demonstrate the critical nature of interventions from outside for malware and in particular persistent IoT malware, since automatic scan of an AV tool or a power cycle, like we are used to for Windows malware and Mirai infections, will not solve persistent IoT malware infections.
Summary of MINIONS: This project aims at MitigatINg IOt-based DDoS attacks via DNS and is a project in collaboration of New York University with Delft University of Technology, Delft. The main goal is to evaluate IoT botnet countermeasures for in-home networks and Internet of Things (IoT) devices, primarily from attacks using Domain Name System (DNS).