La famille Tempora vient d’installer un **thermostat connecté (voir ressource 1)** pour mieux gérer la température de leur maison et réaliser des économies d’énergie. Cependant, ils sont préoccupés par la sécurité de leurs données personnelles et la protection de leur vie privée. Ils souhaitent comprendre comment utiliser cet appareil de manière sécurisée.

**Exemple de l’attaque du botnet Mirai**

Le botnet Mirai est un exemple frappant d’échec dans la sécurisation des objets connectés. En 2016, Mirai a infecté des centaines de milliers d’objets connectés, notamment des caméras de surveillance et des **routeurs[[1]](#endnote-1)**, en utilisant des identifiants par défaut qui n’avaient pas été changés par les utilisateurs. Les appareils infectés ont été utilisés pour lancer une attaque massive, perturbant de nombreux sites web à travers le monde.

* **Hypothèses pour sécuriser ses données personnelles lors de l’utilisation d’objets connectés :**

1. **Un routeur** est un équipement informatique qui permet de relier des réseaux entre eux. Il achemine les données entre des équipements appartenant à des réseaux différents [↑](#endnote-ref-1)