Simjacker : la vulnérabilité des cartes SIM refait le buzz

« *Comment savoir si la carte sim* [sic] *de mon smartphone possède ou non la suite 'S@T Browser' ?* »

La question est apparue ce week-end sur le forum Orange. Elle fait suite au buzz qu'a suscité Simjacker.

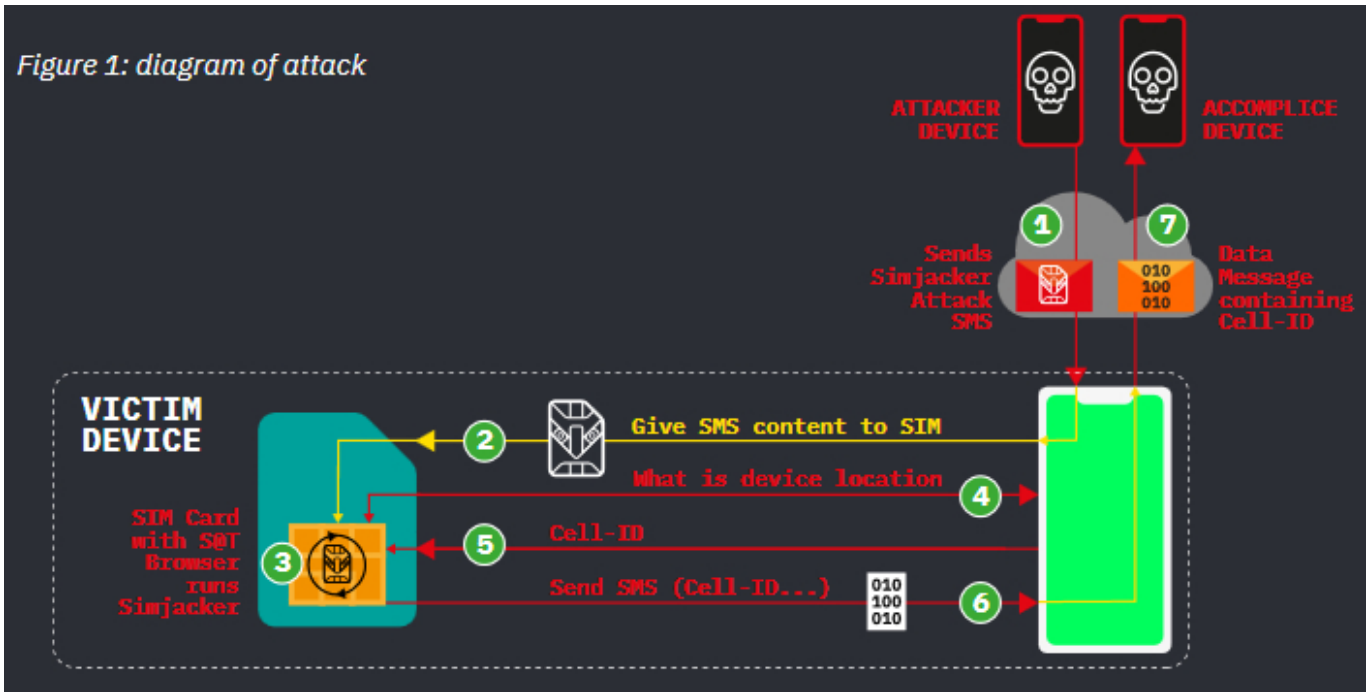
L'éditeur irlandais AdaptiveMobile Security a ainsi nommé cette vulnérabilité qu'il dit exploitée depuis au moins deux ans à des fins de surveillance.

S@T Browser en est la pierre angulaire.

Ce navigateur internet est embarqué dans certaines cartes SIM pour permettre l'accès à des services complémentaires. Typiquement, la consultation du crédit restant sur un forfait.

La SIM Alliance, à l'origine de S@T Browser, n'en a plus actualisé les spécifications depuis 2009. Pour autant, d'après AdaptiveMobile Security, la navigateur reste utilisé dans « au moins 30 pays » réunissant « plus d'un milliard d'habitants »*.

Autant de victimes potentielles de Simjacker.
L'attaque consiste à envoyer un SMS contenant du code malveillant que S@T Browser fera exécuter sur la carte SIM.



L'usage principal constaté vise à récupérer la localisation et l'identifiant (IMEI) des appareils visés, puis à transmettre ces données à un numéro de téléphone. Le processus est invisible pour l'utilisateur ciblé.
Il est possible de déclencher bien d'autres actions : passer des appels, lancer une session de

navigation internet, désactiver la SIM…

AdaptiveMobile Security voit dans Simjacker un successeur des attaques qui touchaient traditionnellement SS7. Cet ensemble de protocoles (« système de signalisation ») sert à établir une interopérabilité entre les services de téléphonie.

** Vulnérabilité également observée sur des objets connectés équipés de cartes SIM.*

Photo d'illustration © A Jackson – Shutterstock.com