L’ancienne faille dans SS7 braque des comptes bancaires par SMS

Les anciennes vulnérabilités ont la vie dure. En 2014, des chercheurs allemands rendaient publics leurs travaux montrant des faiblesses dans le réseau 3G et en particulier dans le protocole SS7, le système de signalisation des communications mobiles. Les failles se trouvent notamment dans les fonctions qui permettent de basculer le signal d’une antenne cellulaire à l’autre lors d’un déplacement de l’utilisateur. Selon les chercheurs, des pirates suffisamment qualifiés pourraient ainsi détourner les appels vers leurs propres systèmes pour écouter ou enregistrer les communications avant de les rediriger vers le destinataire final. Un exemple classique d’attaque de type Man in The Middle (homme du milieu).

A l’époque, on pensait que ce type de piratage était le fait de gouvernements. Et bien les pirates s’y sont mis également. Selon *Süddeutsche Zeitung*, l’opérateur mobile 02-Telefonica a confirmé que plusieurs de ses clients ont vu leurs comptes bancaires siphonnés. L’attaque a été menée en 2 étapes. Après l’installation d’un malware sur les PC des clients pour récupérer les identifiants, mots de passe et numéro de téléphone portable, les attaquants ont exploité la faille dans SS7 pour intercepter les codes envoyés par SMS dans le cadre de l’authentification à double facteur pour valider les demandes de transfert d’argent.

SS7 faillible, mais incontournable

Dans le cadre de cette affaire, aucun détail n’a été fourni sur les équipements utilisés pour intercepter les appels. Ce dernier peut être acquis pour moins de 1000 euros et ainsi accéder aux réseaux SS7 des opérateurs mobiles, précise les experts en sécurité.

Face à ces attaques, plusieurs voix s’élèvent contre le maintien de SS7 comme système de signalisation dans les réseaux mobiles. Un représentant du Congrès américain va saisir la FCC (le gendarme américain des télécoms) de la question en estimant que « *les comptes de millions d’individus protégés par une authentification à double facteur, comme les comptes bancaires sont vulnérables* ».

Le remplacement de SS7 est envisagé dans le cadre des travaux sur les réseaux 5G. Le protocole se nomme Diameter, mais petit hic, la commission de sécurité de la FCC y a trouvé des failles de sécurité.

A lire aussi :

Des failles très indiscrètes trouvées sur les réseaux 3G

Faille SS7 à la télé

crédit photo © LDprod – shutterstock