Sécurité : un code USSD réinitialise le Samsung Galaxy S3

Ravi Borgaonkar a fait son petit effet lors de sa démonstration baptisée « Dirty use of USSD Codes in Cellular Network » (usage néfaste des codes USSD sur les réseaux mobiles) et présentée à l'Ekoparty de Buenos Air.

À partir d'un simple lien, l'expert en sécurité rattaché à l'université technologique de Berlin a effacé tout le contenu du téléphone le reconfigurant par défaut comme s'il sortait d'usine, rapporte *lTespresso.fr*.

Pour parvenir à ce résultat, le chercheur a utilisé une instruction USSD, ces codes à base d'un enchaînement de caractères et de chiffres (type *#06#) utilisés par les constructeurs pour effectuer des opérations locales (de maintenance, d'accès aux informations, etc.).

Dans le cadre de la démonstration, le chercheur a envoyé un SMS avec un lien renvoyant vers une page web animée d'un iframe ou d'un script qui envoie le code USSD de Samsung (*2767*3855# en l'occurrence) et déclenche la réinitialisation de l'appareil, **ici un Galaxy S3**, à sa valeur d'usine.

Les terminaux Samsung Android concernés

Selon lui, il est possible de transmettre cette instruction potentiellement dommageable par SMS (en mode Wap Push pour intégrer un lien cliquable), par QRcode ou encore par NFC (near field communication), lequel ouvre directement la page web sans contrôle de l'utilisateur.

La vulnérabilité toucherait les smartphones Samsung équipés de l'interface **TouchWiz**. Notamment le récent Galaxy S3 mais aussi potentiellement les modèles S, S II, S III, Note, Ace, S Advance, Beam. Mais pas le Galaxy Nexus. Les tablettes Galaxy Tab seraient également affectées. Mais pas la Nexus 7 de Google/Asus sous Jelly Bean.

Android 4 affecté

La faille pourrait en fait toucher Android 4.0 dans son ensemble. L'utilisateur **David Rogers** confirme sur Twitter que les HTC One X et XL sont également concernés par le problème.

En attendant une mise à jour (de Google ou des constructeurs), Collin Mulliner annonce la disponibilité du correctif TelStop disponible sur Google Play. Autre astuce évoquée, utiliser Google Chrome pour la navigation ou bien mettre à jour son système sous Android 4.1 Jelly Bean, quand c'est possible.

Voir aussi
Quiz Silicon.fr – Connaissez-vous les OS mobiles ?