Android : Check Point alerte sur des SMS contrefaits pour dérober des emails

Qui est exposé à l'attaque ?

Toute personne connectée à un réseau cellulaire peut devenir la cible de ce type d'attaque de phishing, ce qui signifie que vous n'êtes pas obligé d'être connecté à un réseau Wifi pour que vos données personnelles soient extraites de manière illicite par des cybercriminels.

Quel est le type d'attaque ?

Les pirates conçoivent des messages SMS sur mesure, pour intercepter la totalité du trafic de messagerie à destination et en provenance des appareils mobiles, en les déguisant en messages innocents de « mise à jour des paramètres réseau » émanant de leur opérateur de télécom tel que T-Mobile, Verizon ou AT&T.

Comment fonctionne l'attaque ?

Un seul message SMS suffit pour obtenir un accès complet aux emails.
Le destinataire du message SMS ne peut vérifier si les paramètres suggérés proviennent de son opérateur ou d'un imposteur.
Plus dangereux encore, n'importe qui peut acheter un dongle USB à 10 € et lancer une attaque de phishing à grande échelle. Aucun équipement spécial n'est requis pour mener à bien l'attaque.

Ce type de cyberattaque est unique car il ne nécessite aucune connexion Wifi, ce qui rend les emails des utilisateurs Android vulnérables à tout moment de la journée ou tant qu'ils sont connectés au réseau de leur opérateur.

Comment se déroule l'attaque ?

Le vecteur d'attaque repose sur un processus appelé provisionnement OTA (Over-the-Air), utilisé habituellement par les opérateurs de téléphonie mobile pour déployer des paramètres spécifiques à leur réseau sur les nouveaux téléphones rejoignant leur réseau.

Cependant, Check Point Research a démontré que n'importe qui peut envoyer des messages de provisionnement OTA pour accéder à des emails. Ainsi, un opérateur de télécom envoie généralement un message de bienvenue dès qu'il détecte un nouvel appareil sur son réseau. Le message des opérateurs est utilisé pour déployer des paramètres spécifiques à leur réseau, tels

que l'adresse du centre de service MMS.

Quelle(s) parade(s) contre cette attaque ?

Samsung a inclus un correctif pour cette vulnérabilité dans sa version de maintenance de sécurité du mois de mai (SVE-2019-14073).
LG a publié son correctif en juillet (LVE-SMP-190006).
Huawei a annoncé son intention d'inclure des correctifs de l'interface utilisateur pour OMA CP dans la prochaine génération des smartphones de la série Mate ou de la série P.
Sony a refusé de reconnaître la vulnérabilité, affirmant que ses appareils étaient conformes à la spécification OMA CP. L'OMA suit ce problème sous la référence OPEN-7587.

« Nous ne devrions plus faire confiance aux messages des opérateurs de téléphonie mobile, et réfléchir à deux fois avant d'installer quoi que ce soit de recommandé via des messages. L'installation d'un proxy WAP via le message d'un opérateur permet l'interception de la totalité du trafic de messagerie d'une cible dans le monde entier. » indique Check Point.