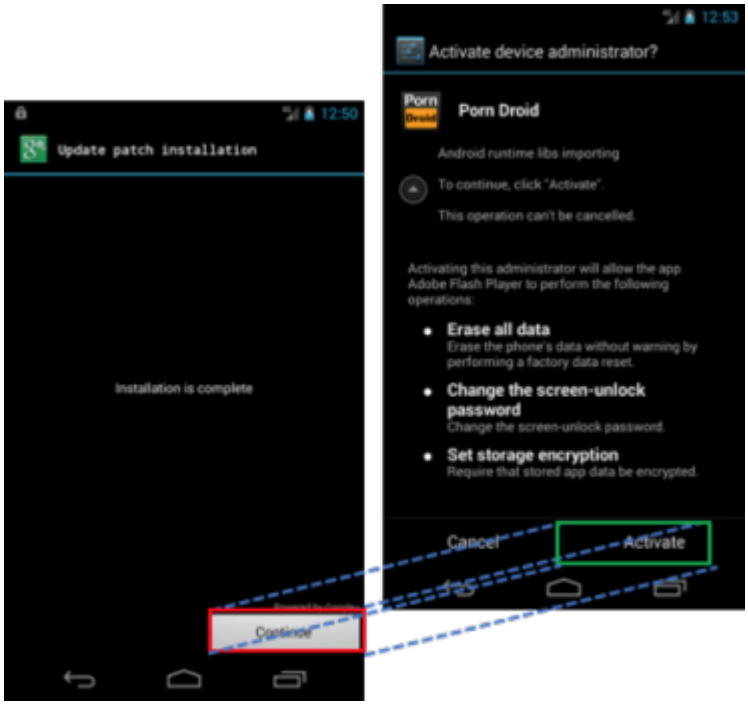
Android: une faille redoutable peut enclencher une attaque par recouvrement

A l'exception de Android 8.0 « Oreo » (du nom de la nouvelle génération de l'OS mobile de Google pas encore distribuée sur les terminaux), toutes les versions d'Android sont sensibles à la vulnérabilité critique dénichée par Palo Alto Networks.

« Certains malware exploitent quelques vecteurs [de la vulnérabilité] mais l'unité 42 de Palo Alto n'a pas connaissance d'attaques en cours à ce jour », souligne Christopher Budd, le responsable communication de l'éditeur de solutions de sécurité IT, dans une contribution blog.

Qui plus est, la nouvelle faille classée comme très dangereuse (« new high-severity vulnerability ») a été corrigée dans le correctif mensuel livré par Google début septembre. Encore faut-il que les fabricants et opérateurs de l'écosystème Android appliquent le patch par mise à jour de l'OS si l'utilisateur ne s'en charge pas lui-même.

La faille permet de mener des attaques dites «overlay» où une fausse page s'affiche sur l'écran en lieu et place de l'affichage légitime pour tromper l'utilisateur et le pousser à installer des malwares à son insu.



Par exemple, une application invite l'utilisateur à «Continuer» pour appliquer une mise à jour alors qu'elle cache en fait l'installation du malware Porn Droid, comme le montre les captures d'écran ci-contre.

Une fois la sombre application installée, celle-ci peut prendre le contrôle total du smartphone affecté, que ce soit pour dérober des données, installer un ransomware (ou tout autre logiciel malveillant), espionner les communications et saisies à l'écran, voire complètement bloquer l'appareil.

Toast mis en cause

Si les attaques par recouvrement ne sont pas nouvelles sur Android, leur succès nécessitait jusqu'à présent deux conditions : demander explicitement l'autorisation « draw on top » (afficher par dessus) à l'utilisateur lors de son installation; et être installés à partir de Google Play.

Mais, selon Palo Alto, la vulnérabilité « overlay » permet de contourner ces barrières si l'application est téléchargée depuis un store alternatif ou une page web.

La firme californienne n'entre pas dans les détails de la faille. Mais laisse entendre que celle-ci vient de Toast, le système d'affichage des notifications d'Android.

« Contrairement à d'autres types de fenêtres dans Android, Toast ne requiert pas les mêmes autorisations, et donc les facteurs atténuants appliqués aux attaques de superposition précédentes ne s'appliquent pas ici », indique Christopher Budd.

Qui plus est, il est possible d'utiliser Toast pour créer une fenêtre qui occupe l'intégralité de l'écran et se faire passer pour une application légitime.

Pour éviter de tomber dans le piège que pourraient dresser des personnes malintentionnées en exploitant la faille en question, mieux vaut mettre à jour Android avec les derniers correctifs. Et, surtout, installer uniquement des applications issues de Google Play.

Même si le magasin applicatifs de Mountain View est loin d'être parfaitement sécurisé, *« l'équipe de sécurité Android surveille activement les applications malveillantes et les excluent du store en priorité »*, assure Palo Alto Networks.

Lire également
SonicSpy contamine plusieurs milliers d'apps Android
SpyDealer, le malware qui espionne de fond en comble des smartphones Android
2 milliards de terminaux sous Android !