Des chercheurs élaborent un malware via l'interface utilisateur des apps mobiles

Des chercheurs des universités de Californie et du Michigan viennent de trouver une nouvelle méthode permettant à une application malveillante de dérober des informations personnelles sur un terminal mobile. Ils ont baptisé ce procédé » UI State Interference Attack ».

Un démonstrateur a été proposé sous **Android**, mais la technique employée serait transposable sur d'autres plates-formes mobiles, comme **iOS ou Windows Phone**. Les systèmes de protection des OS ne sont pas franchis et aucun mode 'root' n'est requis.

Voici le mode opératoire de cette attaque : imaginons que l'ouverture de la fenêtre de connexion de l'application eBay demande 13,5 Ko de mémoire vive. Le logiciel malveillant fonctionne en tâche de fond et surveille la mémoire consommée par le système (une information librement accessible). Lorsque cette dernière grimpe de 13,5 Ko, il affiche sa propre fenêtre de connexion – identique à celle de l'application eBay – par-dessus celle de ladite application. Et le tour est joué.

Une attaque presque indétectable

Une méthode simple et efficace. L'utilisateur emploie en effet l'application eBay officielle, sauf lorsqu'il saisit les identifiants de connexion. C'est à ce moment, et ce moment seul, que l'outil malveillant affiche une fenêtre par-dessus celle de l'application légitime.

Certes, le logiciel eBay ne reçoit pas ici la saisie de l'utilisateur, ce qui pourrait lui mettre la puce à l'oreille par la suite. Il suffit à l'outil malveillant de simuler une erreur de saisie, puis de retourner dans l'ombre et de ramener ainsi l'utilisateur sur la véritable page de connexion du logiciel. Imparable !

Concernant le logiciel malveillant, ce dernier ne demandera aucun droit suspect, si ce n'est un accès au réseau. Le code incriminé pourra donc sans peine être ajouté à celui d'un outil parfaitement anodin (jeu, utilitaire, etc.), sans que cette fonction cachée puisse être découverte par la suite.

Sur le même thème

Alerte : une mise à jour de sécurité provoque le plantage des PC Windows !
Google va renforcer la protection contre le téléchargement de logiciels malveillants
10 % des extensions dédiées à Chrome seraient malveillantes