Google Play : pourquoi le nombre de adware explose

PHA. C'est l'acronyme utilisé par Google pour « potentially harmful apps », soit les « applications potentiellement nuisibles ».

Cette année, ils sont en augmentation de 100% sur le Google Play, et c'est Google lui-même qui le reconnaît dans son rapport annuel sur la sécurité sur Android. Faut-il s'en inquiéter ?

La réponse est « non » pour Google qui rappelle que le taux d'installation d'applications « vérolées » est de 0.04%, contre 0,02% en 2017. Cela reste donc très minime, et le géant du web en profite donc pour vanter la sécurité de sa boutique d'applications, mais aussi son blocage de malwares externes avec 1.6 milliard de tentatives d'intrusions bloquées.

55 % des logiciels malveillants sont des adwares

Surtout, Google justifie ce chiffre par la prise en compte des adwares jusque là absents de son rapport. Ce type de malware, qui consiste à forcer l'utilisateur à cliquer sur une publicité, représente 55% de tous les logiciels malveillants présents sur les applications, et ils sont loin devant les Cheveux de troie (16%).

Selon Google, si on enlève les adwares, présents essentiellement aux Etats-Unis, au Brésil et au Mexique, le taux de malware a baissé de 31% en un an.

Simbad, un adware dans plus de 200 applications

La semaine dernière, l'éditeur Check Point révélait que plus de 200 applications distribuées sur Google Play contenaient Simbad, un logiciel malveillant masqué en plateforme publicitaire pour leurrer les développeurs.

Son action : créer une porte dérobée dans l'application infectée afin de pouvoir installer d'autres malware sans être repéré par les systèmes d'analyse de Google Play. Une fois installé sur un mobile, l'adware supprime l'icône de l'application et s'exécute en arrière-plan

Check Point a communiqué la liste des applications infectées à Google qui les a retirés de Google Play, mais ne peut pas les dé-sinstaller sur les terminaux.

Parmi celles-ci figurent dix jeux qui à eux seuls totalisent 55 millions de téléchargements. Une fois

que le malware récupère ses instructions du serveur de commande et de contrôle, il va visiter en arrière-plan une série d’adresses Web diffusant des publicités afin de générer des revenus.