

Android 4.2 inefficace contre 85% des malwares

L'ouverture de la plate-forme Android et ses risques de sécurité induits s'inscrivent souvent comme un frein à son adoption au sein des entreprises. [L'étude](#) de **Xuxian Jiang**, professeur au département informatique de l'université de New York (NCSU), enfonce un peu plus le clou.

L'enseignant s'est penché sur le nouveau système de vérification d'application introduit avec le récent [Android « Jelly Bean » 4.2](#). Google laisse entendre que le nouveau filtre permet de repérer les applications malicieuses que l'utilisateur tente d'installer, quelle que soit leur provenance (du magasin Play comme d'un autre « store »).

Une vraie passoire

Sur le papier, un système imparable pour utiliser son smartphone ou sa tablette en toute tranquillité. Hélas, en usage réel, le service basé sur une vérification en ligne des fichiers d'installation se révèle être une vraie passoire. Sur les 1260 échantillons d'applications malicieuses que le chercheur a installées sur une tablette Nexus 10 sous Android 4.2, seuls 193 ont été détectés comme dangereux. Soit environ 15% d'efficacité.

Xuxian Jiang a approfondi son étude en voulant comparer l'efficacité du service de Google avec les antivirus du marché. Il s'est alors appuyé sur le service en ligne Virus Total (acquis par Google en septembre 2012) auquel il a soumis un échantillon pour chacune des 49 familles de virus étudiés. Le résultat est sans appel avec des taux de 51% à 100% d'efficacité pour les antivirus du marché (Avast, AVG, TrendMicro, Symantec, BitDefender, ClamAV, F-Secure, Fortinet, Kaspersky, Kingsoft) contre un peu plus de 20% pour le système de Jelly Bean.

Le projet Android Malware Genome

Les échantillons en question proviennent du projet [Android Malware Genome](#) qui vise à collecter les agents Android malveillants dans une base de données mise à disposition. Elle est notamment utilisée dans le cadre de projet de recherche universitaire, par des éditeurs, mais aussi des industriels (Nokia, Qualcomm, Samsung, AT&T...). Mais visiblement pas par Google.

Et Xuxian Jiang de noter que Virus Total n'est pas intégré à l'outil de sécurité d'Android 4.2. Il ne reste plus qu'à espérer qu'il le sera bientôt. Dans tous les cas, l'offre de sécurité de Google reste largement perfectible.

Table 2: The detailed comparison with ten representative anti-virus engines

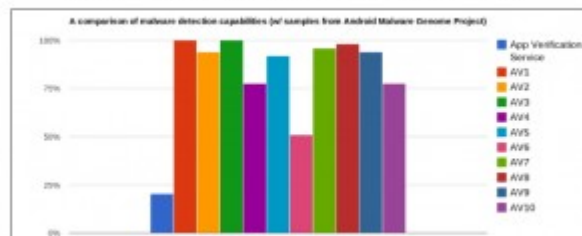


Figure 3: The comparison between the new app-verification service (in Android 4.2) and ten other representative anti-virus engines

Voir aussi

[Quiz Silicon.fr – 4 ans d'Android !](#)