Bitdefender : Ces applications iPhones qui ne nous veulent pas que du bien
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 25/7/2012 11:00:00

Une Ã©tude rÃ©alisÃ©e par Bitdefender, Ã©diteur de solutions de sÃ©curitÃ©, a rÃ©vÃ©lÃ© que quasiment une application iOS sur cinq pouvait accÃ©der au rÃ©pertoire de votre iPhone, tandis que 41% dâentre elles pouvaient savoir oÃ¹ vous vous trouvez et que plus dâune sur trois stockait vos donnÃ©es sans les crypter.

Des milliers dâapplications iPhone seraient capable dâutiliser vos contacts ou de vous localiser Ã votre insu, selon une Ã©tude de Bitdefender

Lâ Ã©tude qui portait sur plus de 65 000 applications largement distribuÃ©es sur lâApp Store a rÃ©vÃ©lÃ© que des dizaines de milliers dâentre elles exploitaient des informations sur les contacts, suivaient lâemplacement des utilisateurs et accÃ©daient Ã des donnÃ©es sans avoir la permission explicite de ces mÃªmes utilisateurs.

Alors que de nombreuses applications utilisent clairement ces privilÃ¨ges pour fonctionner, dâautres nâont aucune raison Ã©vidente dâutiliser les donnÃ©es quâelles recueillent, quâelles proviennent du rÃ©pertoire des utilisateurs ou du suivi de la localisation. Par dÃ©faut, les applications de lâApp Store demandent uniquement la permission pour accÃ©der Ã des services liÃ©s Ã la localisation gÃ©ographique, et non lorsquâelles accÃ¨dent au rÃ©pertoire ou Ã dâautres fonctions.

Lâanalyse de Bitdefender portait sur 65 000 des applications les plus populaires de lâApp Store et a dÃ©montrÃ© que seulement 57,5% dâentre elles cryptaient les donnÃ©es des utilisateurs. Environ 41,4% des applications analysÃ©es peuvent localiser les utilisateurs, ce qui signifie que la plupart des possesseurs dâiPhone sont susceptibles dâavoir au moins une application sur leur appareil capable de savoir oÃ¹ ils se trouvent.

Le suivi gÃ©ographique exploitÃ© par des publicitÃ©s contextuelles, basÃ©es sur la localisation des utilisateurs, est trÃ¨s controversÃ©, bien quâassez courant. Ce type dâinformations peut Ãªtre vendu aux entreprises, pour les aider Ã Ã©laborer des campagnes marketing plus efficaces.

Lâ□□Ã©tude de Bitdefender ne porte pas sur lâ□□ensemble des applications disponibles sur lâ□□App Store et il est donc possible que les nombres et les proportions varient lors de lâ□□extrapolation Ã lâ□□ensemble de lâ□□App Store.

Lâ□□Ã©tude a Ã©galement rÃ©vÃ©lÃ© que 18,6% des applications peuvent accÃ©der au rÃ©pertoire de lâ□□utilisateur, ce qui inclut lâ□□accÃ¨s Ã toutes les informations sur ses contacts. La seule raison valable pour quâ□□une application accÃ¨de au rÃ©pertoire dâ□□un utilisateur est lors dâ□□un transfert de contact ou un rapprochement de donnÃ©es entre des contacts de rÃ©seaux sociaux et des numÃ©ros dÃ©jÃ enregistrÃ©s dans le rÃ©pertoire. Il est peu probable que presque 20% des applications aient besoin des informations du rÃ©pertoire pour fonctionner. Il y a donc de grandes chances pour que de nombreuses applications accÃ¨dent au rÃ©pertoire Ã lâ□□insu des utilisateurs.

Bitdefender a dÃ©tectÃ© que 30,7% des applications analysÃ©es peuvent afficher des publicitÃ©s et que 16,4% peuvent se connecter Ã Facebook. Dâ□□autres fonctions comprennent le suivi de lâ□□utilisation via Flurry analytics, Google Analytics ou Mobclix analytics. Certaines applications utilisent les trois logiciels dâ□□analyse. Des centaines dâ□□applications analysÃ©es utilisent Ã©galement un UDID (Unique Device Identifier) de lâ□□iPhone, permettant dâ□□identifier le possesseur, alors que des centaines dâ□□autres utilisent la voix sur IP en tÃ¢che de fond, le suivi de lâ□□utilisation dâ□□Open Feint et plus encore.

Â« *Il est inquiÃ©tant de constater que les donnÃ©es stockÃ©es sur iOS ne sont que trÃ¨s peu cryptÃ©es, et que le suivi de la localisation est si prÃ©sent. Sans information sur ce Ã quoi peut concrÃ¨tement accÃ©der une application, il est difficile de contrÃ´ler les informations que les utilisateurs divulguent* Â» dÃ©clare **Catalin Cosoi**, Directeur de recherche en sÃ©curitÃ© des Laboratoires Bitdefender. Â« *Nous observons une situation inquiÃ©tante de faible cryptage des donnÃ©es, une prÃ©valence du suivi de la localisation et un accÃ¨s silencieux, injustifiÃ©, au rÃ©pertoire* Â».

Du coup ces donnÃ©es personnelles peuvent Ãªtre utilisÃ©es pour Ã©tablir des schÃ©mas de comportements y compris pour du profilage pour des activitÃ©s de marketing. Des algorithmes de recueil de donnÃ©es et des schÃ©mas dâ□□utilisation sont parfois utilisÃ©s pour obtenir bien plus dâ□□informations, notamment lâ□□identitÃ© de lâ□□utilisateur. Il nâ□□existe pas, Ã ce jour, de base de donnÃ©es mise Ã disposition du public pour la sensibilisation et lâ□□Ã©ducation des utilisateurs au sujet de ces problÃ¨mes de confidentialitÃ©.