Bitdefender : La hausse de malwares AndroÃ¯d, affecte la vie privÃ©e.
MobilitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 15/4/2013 11:30:00

Bitdefender attire notre attention sur la hausse du nombre dâ□□adwares et deÂ malwares AndroÃ¯d, rÃ©sultat : Notre vie privÃ©e en est de plus en plus affectÃ©e.

Parce que les adwares (logiciels espions publicitaires) recueillent plus de donnÃ©es sur les appareils des utilisateurs que ce dont ils ont rÃ©ellement besoin et que les dÃ©veloppeurs ajoutent souvent plus dâ□□un composant adware (framework adware) au sein de leurs applications, la vie des utilisateurs devient de moins en moins privÃ©e au profit des dÃ©veloppeurs et des publicitaires. De plus en plus de tierces parties ont dÃ©sormais accÃ¨s Ã lâ□□historique de navigation des utilisateurs, Ã leurs numÃ©ros de tÃ©lÃ©phone, Ã leurs adresses e-mail et Ã tout ce qui est nÃ©cessaire pour crÃ©er des profils complets et personnalisÃ©s.

Câ□□est dâ□□autant plus inquiÃ©tant que les adwares ciblant les appareils Android ont augmentÃ© de 61% au niveau mondial, entre septembre 2012 et janvier 2013 et que les malwares ont progressÃ© dans le mÃªme temps de 27%, allant jusquâ□□Ã une hausse de 37% pour les chevaux de Troie selon une Ã©tude des Laboratoires Bitdefender.

Lâ□□adoption dâ□□Android a rÃ©guliÃ¨rement progressÃ© au cours des cinq derniers mois, de mÃªme que le nombre de dÃ©tections de malwares et dâ□□adwares. Il nâ□□est ainsi plus rare de dÃ©nicher des malwares et des adwares Android aussi bien sur les marchÃ©s dits Â« alternatifs Â» que sur la plate-forme officielle Google Play .

Lâ□□augmentation la plus importante pour les adwares (+34,47%) a Ã©tÃ© enregistrÃ©e entre novembre et dÃ©cembre 2012, certains dÃ©veloppeurs ayant profitÃ© des fÃªtes de fin dâ□□annÃ©e pour tenter de gÃ©nÃ©rer des revenus supplÃ©mentaires en misant sur le fait que les nouveaux utilisateurs ignorent le fonctionnement des adwares.

Les chevaux de Troie ont connu une augmentation lente mais constante de septembre 2012 Ã janvier 2013 puis ont lÃ©gÃ¨rement dÃ©cru en fÃ©vrier 2013 (-2,22%).

Les adwares devenant plus intrusifs et programmÃ©s plus prÃ©cisÃ©ment pour rÃ©cupÃ©rer autant dâ□□informations sensibles que possible, la diffÃ©rence est plus tÃ©nue que jamais entre les logiciels lÃ©gitimes et les applications qui se rÃ©vÃ¨lent en rÃ©alitÃ© Ãªtre des malwares. Des adwares virulents portent ainsi de plus en plus prÃ©judice Ã la vie privÃ©e des utilisateurs en recueillant et utilisant des informations personnelles Ã leur insu.

Bien que les adwares ne soient pas fondamentalement malveillants, ils peuvent recueillir des numÃ©ros de tÃ©lÃ©phone, des coordonnÃ©es et des adresses e-mail, qui sont transmis Ã des tiers ou vendus au plus offrant. Le marchÃ© noir valorise Ã©normÃ©ment ces donnÃ©es qui peuvent Ãªtre utilisÃ©es Ã des fins marketing pour crÃ©er des profils dâ□□utilisateurs.

Puisque la plupart des utilisateurs utilisent leurs appareils personnels Ã des fins professionnelles, il est logique que lâ□□accÃ¨s aux fichiers confidentiels et sensibles soit souvent autorisÃ© via ces appareils. Ce nâ□□est donc pas seulement un problÃ¨me de risques vis-Ã -vis de leurs donnÃ©es personnelles, mais cela concerne Ã©galement les informations critiques des entreprises elles-mÃªmes. Des politiques de BYOD strictes doivent offrir une protection efficace Ã la fois contre les malwares et contre les adwares sous Android, puisquâ□□ils ont tous les deux un impact direct sur la prÃ©servation de la confidentialitÃ© des donnÃ©es.

La principale famille de chevaux de Troie sâ□□intitule Â« FakeInst Â», elle escroque les utilisateurs en leur demandant de payer des applications qui sont normalement gratuites. Si les utilisateurs acceptent, lâ□□application envoie des messages SMS Ã des numÃ©ros surtaxÃ©s, faisant ainsi grimper leur facture tÃ©lÃ©phonique.

Parmi les adwares agressifs, la famille Android.Adware.Plankton est la plus prÃ©sente puisque les dÃ©veloppeurs utilisent le framework intÃ©grÃ© Ã lâ□□appli pour monÃ©tiser leur dÃ©veloppement. Les adwares peuvent Ã©galement recueillir des informations personnelles telles que des adresses e-mail et des numÃ©ros de tÃ©lÃ©phone. Plus il y a de frameworks associÃ©s Ã une application, plus celle-ci devient intrusive puisquâ□□elle diffuse les donnÃ©es Ã plusieurs tiers.

La tendance Ã la hausse de ces deux types de dÃ©tection indique que les pirates sont Ã la recherche dâ□□argent et de moyens dâ□□en obtenir en vendant les donnÃ©es personnelles des utilisateurs. Lâ□□argent est le moteur du dÃ©veloppement de ces deux catÃ©gories.

La solution Bitdefender Mobile Security pour Android bloque les menaces susceptibles de compromettre les donnÃ©es des utilisateurs. Comprenant un scanner en temps rÃ©el et Ã la demande, Bitdefender Mobile Security vous signale les applications potentiellement malveillantes avant que vous ne les exÃ©cutiez. Elle est la solution idÃ©ale pour bloquer les malwares et protÃ©ger vos donnÃ©es contre les adwares intrusifs et agressifs.

Bitdefender Mobile Security est disponible sur Google Play.

Pour retrouver Bitdefender