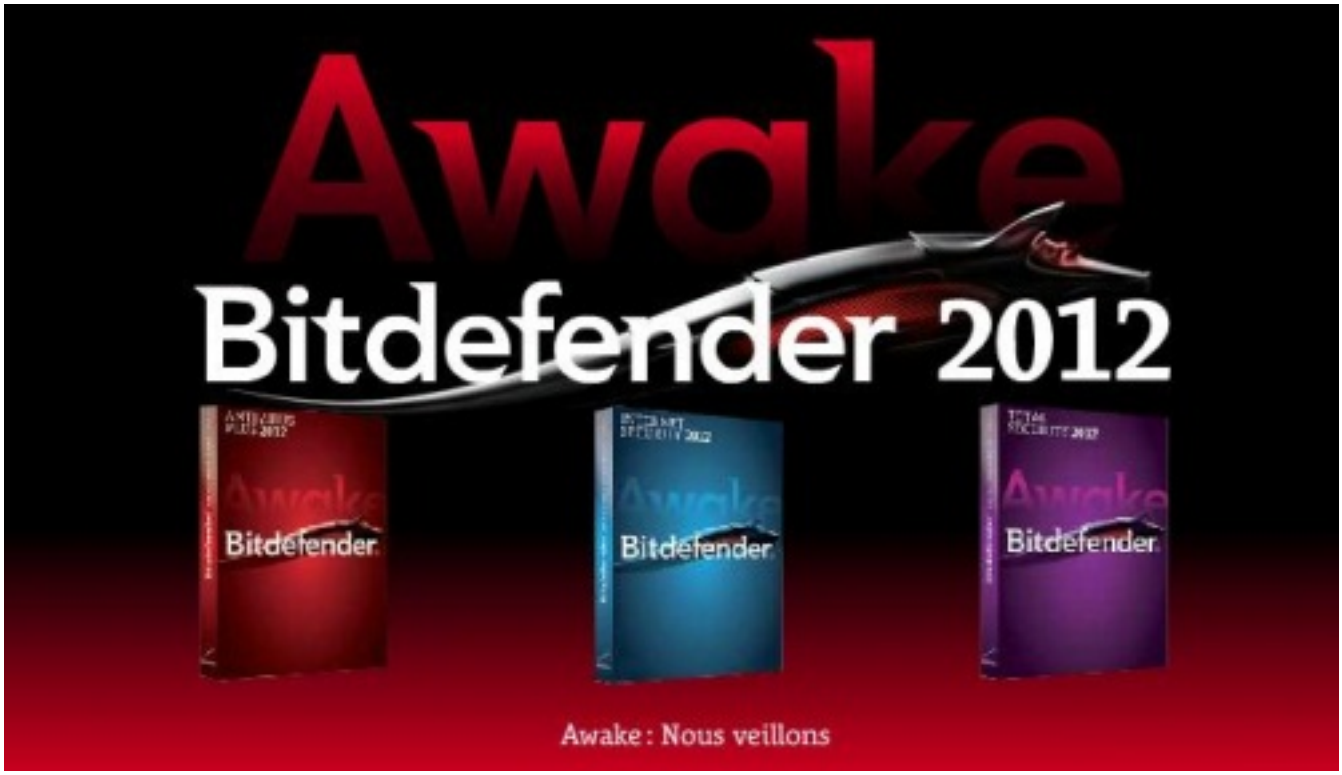
BitDefender : La grippe asiatique contamine les Smartphones Android
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 27/1/2012 14:00:00

Bitdefender constate que les attaquants publient des applications lÃ©gitimes qui sont ensuite remplacÃ©es par des malwares une fois quâ□□elles ont obtenu des Ã©valuations positives

Les versions alternatives de lâ□□Android Market ont toujours constituÃ© un des vecteurs privilÃ©giÃ© pour la diffusion des applications malveillantes, en particulier dans des rÃ©gions comme lâ□□Asie, oÃ¹ les utilisateurs nâ□□ont pas accÃ¨s Ã la plateforme officielle.

Câ□□est Ã©galement ce procÃ©dÃ© qui a Ã©tÃ© utilisÃ© par les cyber-escrocs lors de leur derniÃ¨re campagne afin de convaincre les utilisateurs dâ□□installer des applications connues sur le vÃ©ritable Android Market. Ces applications en apparence lÃ©gitimes, ont Ã©tÃ© en rÃ©alitÃ© modifiÃ©es afin de lancer des services additionnels en plus de lâ□□application originale.

En rÃ©sumÃ©, lâ□□application Android originale tÃ©lÃ©chargÃ©e Ã partir dâ□□un emplacement tiers contient la vÃ©ritable application ainsi quâ□□un service incluant un cheval de Troie (gÃ©nÃ©ralement nommÃ© Â« GoogleServicesFrameworkService Â»), qui est lancÃ© dÃ¨s que lâ□□application hÃ´te est dÃ©marrÃ©e.



IdentifiÃ© par Bitdefender sous le nom dâ□□Android.Trojan.FakeUpdates.A , ce malware se connecte au serveur C&C et rÃ©cupÃ¨re une liste de liens dirigeants vers diffÃ©rents fichiers APK. Il tÃ©lÃ©charge ensuite chaque APK de la liste puis affiche la notification suivante dans la barre dâ□□Ã©tat : Â« æ□¨å¥½,å·²ç»□è□·å□□æ□□æ□°æ□´æ□°,è¯·ç□¹å□»å®□è£□ Â» (Â« Pour accÃ©der aux derniÃ¨res mises Ã jour, cliquez sur Installer Â»). Cette approche trompe lâ□□utilisateur, puisquâ□□il ne peut pas savoir dâ□□oÃ¹ provient le message.

Ce cheval de Troie requiert un large panel de privilÃ¨ges lors de lâ□□installation, afin de sâ□□assurer le contrÃ´le complet du Smartphone lorsque cela sâ□□avÃ¨rera utile. En fonction de lâ□□APK Ã tÃ©lÃ©charger et Ã installer, lâ□□application peut requÃ©rir jusquâ□□Ã 10 autorisations avant lâ□□installation et la plupart des utilisateurs les accorderont sans se poser de questions, puisquâ□□ils pensent quâ□□il sâ□□agit dâ□□une mise Ã jour dâ□□une application quâ□□ils ont dÃ©jÃ installÃ©e.

La publication dâ□□applications Android sur des plateformes Android Market tierces ne constituent pas une nouveautÃ© en tant que telle, mais cette approche se distingue par le modus operandi des attaquants : ces derniers publient une application totalement lÃ©gitime sur le Market visÃ©, la laissent recueillir des Ã©valuations positives et gagner la confiance des utilisateurs pendant quelques jours, puis remplacent lâ□□APK par un fichier contenant un cheval de Troie, afin dâ□□atteindre leurs buts malveillants. Il est Ã©galement important de noter que la plupart des applications repackagÃ©es que nous avons analysÃ©es ont des taux de dÃ©tection assez faibles, et quâ□□elles prÃ©sentent donc un rÃ©el danger, mÃªme pour les utilisateurs de Smartphones qui disposent dâ□□une solution de sÃ©curitÃ© mobile.

Android.Trojan.FakeUpdates.A reprÃ©sente une menace immÃ©diate pour les utilisateurs de Smartphones puisquâ□□il peut tÃ©lÃ©charger et installer tous types dâ□□applications ou de services, depuis des versions dâ□□essai de logiciels dans des campagnes Â« pay-per-install Â» jusquâ□□Ã des spywares et autres chevaux de Troie.

Afin de protÃ©ger votre vie privÃ©e et de maintenir votre appareil dans le meilleur Ã©tat possible, nous vous recommandons de ne PAS installer dâ□□applications demandant plus de permissions que celles utilisÃ©es normalement. De mÃªme, installer une solution de sÃ©curitÃ© pour mobile performante vous permettra de prÃ©venir ce type dâ□□attaques.

Bitdefender Mobile Security est disponibilitÃ© sur Android Market et sur les sites de tÃ©lÃ©chargement au prix public conseillÃ© : de 7,45â□¬ TTC.

Pour plus dâ□□informations sur Bitdefender Mobile Security

Pour retrouver Bitdefender en ligne