

Jeudi 26 janvier 2012

Une vague de grippe asiatique contamine les smartphones Android avec des applications indésirables

Les attaquants publient des applications légitimes qui sont ensuite remplacées par des malwares une fois qu'elles ont obtenu des évaluations positives

Les versions alternatives de l'Android Market ont toujours constitué un des vecteurs privilégiés pour la diffusion des applications malveillantes, en particulier dans des régions comme l'Asie, où les utilisateurs n'ont pas accès à la plateforme officielle.

C'est également ce procédé qui a été utilisé par les cyber-escrocs lors de leur dernière campagne afin de convaincre les utilisateurs d'installer des applications connues sur le véritable Android Market. Ces applications en apparence légitimes, ont été en réalité modifiées afin de lancer des services additionnels en plus de l'application originale.

En résumé, l'application Android originale téléchargée à partir d'un emplacement tiers contient la véritable application ainsi qu'un service incluant un cheval de Troie (généralement nommé « GoogleServicesFrameworkService »), qui est lancé dès que l'application hôte est démarrée.

Identifié par Bitdefender sous le nom d'Android.[Trojan.FakeUpdates.A](#), ce [malware](#) se connecte au serveur C&C et récupère une liste de liens dirigeant vers différents fichiers APK. Il télécharge ensuite chaque APK de la liste puis affiche la notification suivante dans la barre d'état : « 您好,已经获取最新更新,请点击安装 » (« Pour accéder aux dernières mises à jour, cliquez sur Installer »). Cette approche trompe l'utilisateur, puisqu'il ne peut pas savoir d'où provient le message.

Ce cheval de Troie requiert un large panel de privilèges lors de l'installation, afin de s'assurer le contrôle complet du Smartphone lorsque cela s'avèrera utile. En fonction de l'APK à télécharger et à installer, l'application peut requérir jusqu'à 10 autorisations avant l'installation et la plupart des utilisateurs les accorderont sans se poser de questions, puisqu'ils pensent qu'il s'agit d'une mise à jour d'une application qu'ils ont déjà installée.

La publication d'applications Android sur des plateformes Android Market tierces ne constitue pas une nouveauté en tant que telle, mais cette approche se distingue par le modus operandi des attaquants : ces derniers publient une application totalement légitime sur le Market visé, la laissent recueillir des évaluations positives et gagner la confiance des utilisateurs pendant quelques jours, puis remplacent l'APK par un fichier contenant un cheval de Troie, afin d'atteindre leurs buts malveillants. Il est également important de noter que la plupart des applications repackagées que nous avons analysées ont des taux de détection assez faibles, et qu'elles présentent donc un réel danger, même pour les utilisateurs de Smartphones qui disposent d'une solution de sécurité mobile.

Android.Trojan.FakeUpdates.A représente une menace immédiate pour les utilisateurs de Smartphones puisqu'il peut télécharger et installer tous types d'applications ou de services, depuis des versions d'essai de logiciels dans des campagnes « pay-per-install » jusqu'à des [spywares](#) et autres chevaux de Troie.

Afin de protéger votre vie privée et de maintenir votre appareil dans le meilleur état possible, nous vous recommandons de ne PAS installer d'applications demandant plus de permissions que celles utilisées normalement. De même, installer une solution de sécurité pour mobile performante vous permettra de prévenir ce type d'attaques.

Bitdefender Mobile Security est disponible sur Android Market et sur les sites de téléchargement au prix public conseillé : de 7,45€ TTC. Pour plus d'informations sur Bitdefender Mobile Security : <http://www.bitdefender.fr/solutions/mobile-security-android.html>

Pour retrouver Bitdefender en ligne et rester au fait de l'actualité des e-menaces, inscrivez-vous à nos fils d'information :

- [Flux RSS](#)
- [Facebook](#)
- [Twitter](#)
- [La communauté MalwareCity](#)

Article réalisé grâce aux informations techniques fournies par Vlad Ilie, spécialiste des Laboratoires Antivirus Bitdefender.

Tous les noms de produits ou d'entreprises mentionnés dans ce document le sont à titre purement informatif et sont la propriété, et éventuellement les marques, de leurs propriétaires respectifs.

À propos de Bitdefender®

Bitdefender est une entreprise internationale qui développe, édite et commercialise des solutions de sécurité dans plus de 100 pays. Sa technologie proactive, en évolution permanente, protège aujourd'hui plus de 400 millions de particuliers et d'utilisateurs professionnels dans le monde et est reconnue et certifiée par les organismes de tests indépendants comme l'une des plus efficaces et rapides du marché.

Depuis 2001, Bitdefender confie, pour la France et les pays francophones, l'édition et la commercialisation de ses solutions à la société Editions Profil.

Pour plus d'informations sur les produits Bitdefender : www.bitdefender.fr

Pour retrouver toutes les infos presse, surfez sur la rubrique [Centre de Presse](#).

À propos d'Editions Profil

Editions Profil est une société française indépendante créée en 1989 qui développe, édite et commercialise des solutions de sécurité et de filtrage de contenus numériques adaptées aux particuliers et aux entreprises. Ses produits phares sont édités sous les marques Bitdefender et Profil Technology.

Plus d'informations sur www.editions-profil.eu



Editions Profil édite et commercialise les solutions Bitdefender pour la France et les pays francophones.