

13/09/2011

www.enisa.europa.eu

La sécurité des app-stores – Cinq ‘lignes de défense’ – Nouveau rapport de l’Agence européenne pour la cyber-sécurité ENISA

L’ENISA publie aujourd’hui un nouveau rapport sur la [Sécurité des app-stores où elle encourage l’adoption d’une stratégie de base comptant «cinq lignes de défense»](#) contre les logiciels malveillants.

L’industrie du smartphone, dont la croissance est explosive, a une façon spécifique de proposer des logiciels aux utilisateurs : les *app-stores* (ou boutiques d’applications). Les app-stores populaires regroupent des centaines de milliers d’applications aux multiples utilités (des services bancaires en ligne aux insectifuges), et celles des plus populaires (ex. : l’Apple App-store, l’Android Market de Google) sont téléchargées des milliards de fois.

Malheureusement, les app-stores n’ont jamais échappé à l’attention des cybercriminels. Au fil de l’année 2011, [de nombreuses applications malveillantes ont été découvertes](#), ciblant une variété de modèles de smartphones. Le Dr. Marnix Dekker et le Dr. Giles Hogben, auteurs du rapport, ont déclaré : «*En utilisant des applications malveillantes, les criminels peuvent facilement tirer parti de la vaste quantité de données privées traitées sur des smartphones telles que les e-mails professionnels confidentiels, les données d’emplacement, les appels téléphoniques, les SMS et ainsi de suite. Les consommateurs ne s’en rendent pas vraiment compte.*»

«Cinq lignes de défense» pour sécuriser les app-stores

En partant d’un modèle de menace pour les app-stores, le document identifie ce qu’il appelle «**les cinq lignes de défense**» devant être mises en place pour sécuriser les app-stores face aux logiciels malveillants : **critiques des applications, réputation, anti-démarrage, sécurité des appareils et prisons**. «*Ce rapport offre une analyse très pratique et technique des menaces des logiciels malveillants pour les app-stores en moins de 20 pages. L’Agence a fait un choix excellent de techniques de sécurité, et les recommandations sont prêtes à l’emploi*», a déclaré Raoul Chiesa, expert en matière de cybersécurité et pirate éthique italien.

Sans négliger les différences entre les divers modèles de smartphones et app-stores, l’ENISA recommande une approche à l’échelle de l’industrie pour faire face aux applications malveillantes et peu sûres. «*Le nombre d’attaques malveillantes dirigées vers les smartphones fait encore pale figure par rapport à celui des attaques dirigées vers les PC. Ce document est un plan qui nous montrera comment maintenir cette avance et accroître la sécurité à travers les app-stores*», a déclaré [le Professeur Udo Helmbrecht, Directeur Exécutif de l’ENISA](#).

Pour consulter [l’intégralité du rapport](#) :

Informations contextuelles : Les logiciels malveillants sévissant dans les app-stores ne constituent pas le seul risque pour les utilisateurs de smartphones ; l’ENISA a récemment publié [une présentation complète des risques pour les smartphones](#).

Pour tout entretien : Ulf Bergstrom, Porte-parole, ENISA, press@enisa.europa.eu, Mobile : +30-6948-460-143 ou Dr. Marnix Dekker, Expert, ENISA, marnix.dekker@enisa.europa.eu
Veuillez noter: traduction. La version anglaise est la seule version officielle.

www.enisa.europa.eu/media/enisa-en-francais/

www.enisa.europa.eu