	**BoxCryptor**	
	Outil de chiffrement pour Dropbox, Google Drive et autres services de stockage dans le Cloud	
	System Requirements: Windows, Mac, Linux, iOS et Android.	
	Développé par:	Secomba
Existe en trois versions : une avec version gratuite et deux versions à 34,99€ et 79,99€.	**Personne à contacter**	Julien.Cathalo@smals.be

Fonctions

BoxCryptor est un logiciel de chiffrement conçu pour les utilisateurs de services de stockage dans le Cloud comme Dropbox, Google Drive, SkyDrive ou Box.net. BoxCryptor permet de protéger ainsi la confidentialité des données stockées dans le Cloud. Le chiffrement empêche à la fois le fournisseur Cloud et des attaquants externes d'accéder au contenu des données. Utiliser Dropbox seul n'offre pas une sécurité suffisante car les clés de chiffrement sont gérées par le fournisseur.

Le principe de fonctionnement de BoxCryptor est simple. Il consiste à chiffrer un répertoire local. Si l'utilisateur le souhaite, il peut utiliser un service de stockage dans le Cloud qui synchronise automatiquement ce répertoire avec un répertoire en ligne. Mais ce n'est pas obligatoire : BoxCryptor peut donc aussi être simplement utilisé pour chiffrer des données de son disque dur.

Lors de l'installation de BoxCryptor, l'utilisateur peut créer un nouveau répertoire ou utiliser un répertoire existant. Si Dropbox, Google Drive ou SkyDrive sont déjà installés sur la machine, le programme trouve le répertoire correspondant et propose de l'utiliser. L'utilisateur choisit une lettre de disque virtuel à l'installation (ce disque sera par la suite monté automatiquement au démarrage de l'ordinateur). Ensuite l'utilisateur doit choisir un mot de passe et peut sauvegarder son fichier de configuration. Ces deux étapes sont importantes : d'une part, le choix d'un mot de passe faible impliquera un faible niveau de sécurité. D'autre part, si le mot de passe est oublié ou le fichier de configuration perdu, les données chiffrées seront impossibles à déchiffrer et donc perdues.

Lors de l'installation, BoxCryptor génère aléatoirement une clé de 256 bits, utilisée pour chiffrer les données (avec l'algorithme AES-256, standard), et stockée dans le fichier de configuration encodée avec le mot de passe.

L'utilisateur peut ensuite travailler avec le lecteur virtuel comme n'importe quel espace de stockage.

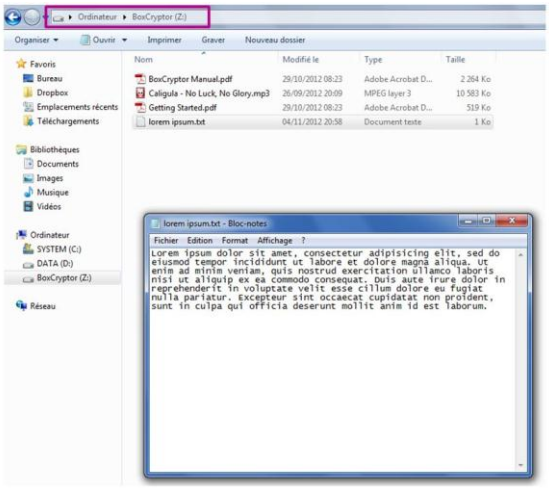
Conclusions et Recommandations

BoxCryptor s'adresse à des utilisateurs privés qui utilisent un service de stockage dans le Cloud et veulent ajouter une couche de sécurité à leurs données. La force de BoxCryptor réside dans sa simplicité d'utilisation ; les utilisateurs plus avancés préfèreront utiliser TrueCrypt (cfr. Quick Review), qui est plus complexe et un peu plus lourd à l'utilisation (n'ayant pas été conçu pour cet emploi) mais offre de meilleures garanties de sécurité.

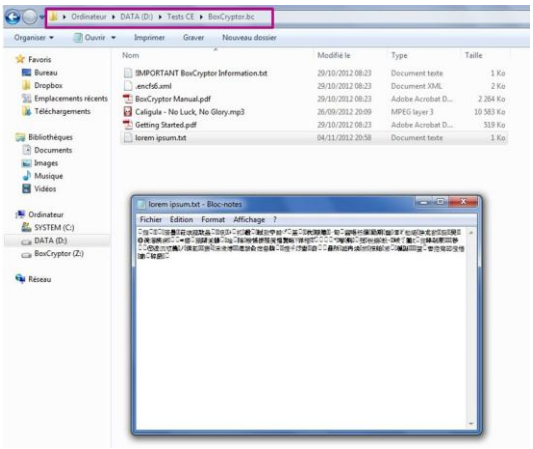
Tests et Résultats

Les tests ont été effectués avec la version gratuite de BoxCryptor sur un PC avec Windows Vista. Les tests ont été effectués avec différents types et tailles de fichier. Dans la suite nous montrons l'exemple d'un simple fichier texte (extension .txt) qui permet bien d'illustrer le fonctionnement du logiciel et du chiffrement.

On travaille ici dans le lecteur virtuel Z. Le fichier texte est lisible et éditable normalement.



Ici, on travaille dans le répertoire local BoxCryptor. C'est ce répertoire qui est synchronisé avec Dropbox ou équivalent. Notons la présence du fichier de configuration (encfs6.xml). Le fichier texte apparaît, mais son contenu est chiffré. Le nom du fichier est en clair ; notons que la version payante de BoxCryptor permet de chiffrer aussi les noms des fichiers.



Les données sont chiffrées à la volée. Le développeur annonce un débit de chiffrement et de déchiffrement de 50 Mo/sec. En pratique, lors du test (effectué sur un disque dur classique), le débit en écriture et en lecture a été suffisant pour travailler de façon normale.