Passware Kit Forensic déchiffre les mots de passe cryptés par TrueCrypt

TrueCrypt est une solution de chiffrement des disques *open source*, disponible pour Windows, Mac OS X et Linux. La dernière mouture en date a été téléchargée près de **1,3 million de fois**. Cet outil très complet pourra même chiffrer la partition système d'une machine fonctionnant sous Windows.

La nouvelle version de Passware Kit Forensic permet dorénavant **de retrouver les mots de passe** permettant d'accéder aux données protégées par TrueCrypt (une fonction uniquement disponible sous Windows). Cet outil spécialisé dans la récupération des mots de passe (et vendu au prix d'or de 795 dollars) ajoute donc une nouvelle corde à son arc. Rappelons qu'il a également été le premier à pouvoir afficher le mot de passe des disques chiffrés à l'aide de **BitLocker**, l'outil de chiffrement de Windows.

Officiellement, cette solution est destinée principalement aux forces de l'ordre. Toutefois, la découverte d'un mot de passe TrueCrypt nécessite que le volume protégé soit ouvert, bref, que l'utilisateur ait saisi le mot de passe permettant d'accéder aux données. En aucun cas il ne permet d'accéder aux données d'un volume dont l'accès n'a pas été déverrouillé au préalable. Bref, il n'est **d'aucune utilité pour les forces de police**, qui auront plus vite fait de demander le mot de passe à l'utilisateur de la machine. Par contre, cet outil sera très efficace pour ceux qui souhaitent **subtiliser** le mot de passe **sans que le propriétaire des données en soit averti**. Bref, des pirates.

Alertés de la sortie de cet outil, les auteurs du logiciel se veulent confiants. Passware Kit Forensic n'exploite aucune faille, mais se borne à **retrouver le mot de passe d'un volume dans la mémoire vive de l'ordinateur**. Si aucun logiciel de sécurité n'est à l'abri d'une telle technique, il convient de rappeler quelques règles de bon sens: fermer un volume protégé dès qu'il n'est plus nécessaire (ce qui supprime le mot de passe de la mémoire), et chiffrer le disque où le fichier d'échange et les informations de mise en veille prolongée sont stockés.