TrueCrypt n’est pas mort, l’audit bouge encore

TrueCrypt n’est pas mort, l’audit bouge encore

Les développeurs chargés d’auditer la sécurité de TrueCrypt ont donné quelques nouvelles de leur avancement. Le développement du logiciel de chiffrement avait été interrompu brusquement durant l’été 2014, soulevant de nombreuses inquiétudes quant à la fiabilité du programme.

L’affaire TrueCrypt fait partie des mystères de la cybersécurité: en mai, le site web distribuant le logiciel annonçait la fin du développement, ajoutant que TrueCrypt n’était « plus sûr » et que les utilisateurs qui décidaient de s’appuyer dessus s’exposaient « à des failles de sécurité non comblées.»
Une nouvelle version du logiciel était distribuée par la même occasion, fortement déconseillée par la plupart des experts en cybersécurité. Un coup dur : TrueCrypt était l’un des projets considérés comme les plus solide en matière de protection des données et, aux dernières nouvelles, donnait encore du fil à retordre aux analystes de la NSA selon des documents datés de 2012.

Doutes et remises en question
Un audit de TrueCrypt avait néanmoins été initié en 2013, en s’appuyant sur un crowdfunding réalisé auprès de la communauté afin de financer un examen en profondeur du code source du logiciel. Si celui-ci avait été lancé bien avant l’arrêt brutal du développement, ses résultats sont aujourd’hui très attendus par les utilisateurs de TrueCrypt. Mais depuis juin 2014, aucune nouvelle n’avait émané du projet, suscitant les interrogations de la communauté.
Sentant monter l’inquiétude, Matthew Green, le chercheur à l’origine du projet d’audit a posté une mise à jour faisant le point sur l’avancement des travaux du groupe. Et c’est bien la moindre des choses : le financement de cet audit a été réalisé sur une opération de crowdfunding, qui avait rassemblé 70.000 dollars au mois de décembre 2013. Compte tenu de la somme récoltée auprès de donateurs et de l’actualité inquiétante du développement de Truecrypt, l’initiative menée par Matthew Green et Kenn White est surveillée de très près.
L’annonce de l’arrêt du développement a d’ailleurs suscité de nombreuses interrogations au sein du groupe chargé de l’audit du code : « L’annonce de l’abandon du projet par l’équipe de Truecrypt nous a poussé à reconsidérer notre approche. Etait-ce vraiment la bonne manière d’utiliser nos ressources ? Ne devrions-nous pas nous pencher au contraire sur les forks de Truecrypt qui émergeaient alors ? »
Matthew Green explique que le projet d’audit a donc connu une longue période de remise en question, mais que le projet est aujourd’hui à nouveau sur les rails, au travers d’un partenariat avec la société NCC Group North America, qui reprend en charge la poursuite de l’audit. Celui-ci entre dans sa seconde phase, après la publication d’une première partie qui avait noté quelques vulnérabilités mais aucune backdoor sérieuse au sein du code de la dernière version de TrueCrypt jugée fiable, la version 7.1a du logiciel.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/chiffrement-truecrypt-n-est-pas-mort-l-audit-bouge-encore-39815118.htm
Par Louis Adam