Les raisons de l'arrêt de TrueCrypt toujours mystèrieuses

Que s'est-il passé autour de **TrueCrypt**? L'équipe de développement du logiciel multiplateforme (Windows, OS X, Linux) de chiffrement des disques durs a annoncé, fin mai, mettre fin à ses travaux. Raison officielle: **l'application serait truffée de failles de sécurité**.

« L'utilisation de TrueCrypt n'est pas sûre car il peut contenir des vulnérabilités non corrigées », peut-on désormais lire sur la page d'accueil du projet. Une justification des plus étonnantes alors que TrueCrypt a obtenu à deux reprises la **certification de l'Anssi** (Agence nationale de la sécurité des systèmes d'information) en France pour les versions 7.1a en octobre 2013 et 6.0 en décembre 2008. *« Au jour où ces certifications ont été émises, le produit répondait aux caractéristiques de sécurité spécifiées dans les rapports [réalisés par la société Amossys] »*, indique l'Anssi. Et dans son audit, la firme de sécurité Isec Partners concluait en février 2014 à l'**absence de backdoor** et autre code malveillant.

Une version vulnérable… qui ne justifie pas tout

Aujourd'hui, TrueCrypt est en version 7.2. **Une version il est vrai exploitable par un pirate pour accéder aux données** (via un débordement de mémoire physique). Mais les failles sont loin d'être critiques avec une gravité de 2/4 selon les équipes de Vigilance, notamment. Et même si l'évolution de TrueCrypt est impactée par des bugs, la présence de failles de sécurité et leurs corrections constituent, avec l'enrichissement du produit, la base du cycle de vie d'une solution informatique. Il est donc étonnant de justifier l'arrêt d'un projet par la seule présence de vulnérabilités.

L'équipe derrière l'application ajoute laconiquement que *« le développement de TrueCrypt a été arrêté en mai 2014 après la fin du support de Windows XP [en avril, NDLR] »*. Lancé en 2004 sur les bases du logiciel E4M, TrueCrypt s'inscrivait à l'époque comme l'une des seules solutions de chiffrement de disques, répertoires et fichiers pour Windows XP. Il est vrai que, avec l'arrivée de Vista, Microsoft a introduit son propre outil de chiffrement, BitLocker, également adopté par ses successeurs Windows 7 et 8.x. **Une offre qui rendrait caduque celle de TrueCrypt**. L'équipe de TrueCrypt invite ainsi ses utilisateurs à adopter et migrer une solution de cryptage supporté par la plate-forme de l'utilisateur.

Pression sur les développeurs

On peut aussi s'interroger sur les pressions que les développeurs auraient pu recevoir de la part d'agences gouvernementales qui se cassent les dents sur la puissance de TrueCrypt comme en témoigne l'affaire **Daniel Dantas**. Arrêté pour fraudes financières, ce banquier brésilien avait chiffré ses disques dur avec le logiciel gratuit. Ni l'INC (l'institut de criminologie brésilien), ni le FBI venu à la rescousse, n'avaient réussi à déchiffrer les contenus des disques. Il est vrai que l'affaire remonte à 2008 et semble éloignée de la récente décision. Mais, selon **Matthew Green**, un expert en cryptographie, l'arrêt du projet TrueCrypt serait la réponse de ses concepteurs, jusqu'alors

restés anonymes, face à **un potentiel chantage**. *« Une alternative est que quelqu'un était sur le point de désanonymiser les développeurs de TrueCrypt et c'est leur réponse »*, a-t-il déclaré dans un Tweet du 29 mai. La véritable raison de l'arrêt de TrueCrypt risque de rester encore longtemps aussi obscure que les disques qu'il chiffrait…

Lire également
OpenSSL encore touché par des failles de sécurité