TrueCrypt : Retour sur une mort prématurée

par Régis SENET

Joe Pemberton

TrueCrypt ne « crypt » plus depuis la fin du mois de Mai 2014. Nous vous proposons une rapide « analyse post-mortem » d'un des plus célèbres logiciels grand public de chiffrement des données.

> Qu'est ce que TrueCrypt ?

Avant de nous lancer dans de vastes explications, voici un bref rappel sur ce qu'est (qu'était ?) TrueCrypt. Il s'agit d'un logiciel gratuit, multi plateforme (Windows, Mac et Linux) permettant de faire du chiffrement de données à la volée.

Il permet de créer un disque virtuel chiffré contenu à l'intérieur d'un fichier et de le monter comme un disque physique. Il est également possible de chiffrer entièrement une partition ou un périphérique externe. Le chiffrement est automatique, en temps réel et transparent pour l'utilisateur. Toute donnée stockée dans un volume TrueCrypt sera entièrement chiffrée, incluant les noms des fichiers et les répertoires.

Trois algorithmes de chiffrement sont disponibles afin d'assurer la sécurité des données : AES, Serpent et Twofish. De nombreuses combinaisons sont également disponibles (AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish_AES et Twofish-Serpent). Celles-ci permettent de prévenir une potentielle faiblesse dans l'un des algorithmes, aux dépens de la vitesse de lecture et d'écriture. En effet, chaque bloc de données est chiffré individuellement.

Parallèlement, ou conjointement, à l'utilisation d'un mot de passe, il est possible d'utiliser un fichier jouant le rôle de clef secrète pour le chiffrement des données. Ces fichiers ne subiront aucune modification par TrueCrypt. Bien sûr, ces fichiers sont sensibles aux changements : si les 1024 premiers kilos bytes sont modifiés, il ne sera alors plus possible de déchiffrer vos données. Il est donc impératif d'utiliser des fichiers n'ayant pas pour vocation à être modifiés (Images, PDF, etc.).

« Avant sa rapide et brutale disparition, TrueCrypt était considéré comme robuste. De nombreux audits furent effectués ... aucun réel problème de sécurité n'a pu être identifié »

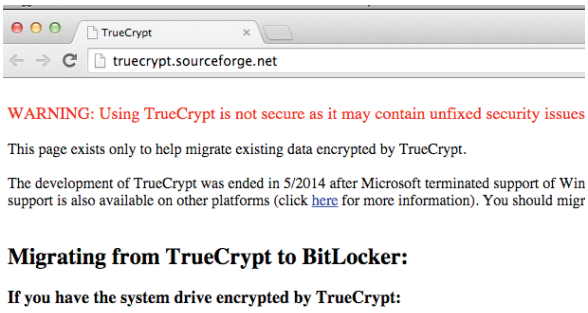
TrueCrypt est également connu pour ses possibilités de déni plausible. Le déni plausible consiste en l'incapacité de prouver qu'un conteneur caché et chiffré existe au sein d'un conteneur chiffré. Ce second volume chiffré est accessible à l'aide de son propre mot de passe (et non accessible à l'aide du mot de passe du volume principal). Son existence ne peut alors être prouvée, ou plutôt, ne peut être niée.

Avant sa rapide et brutale disparition, TrueCrypt était considéré comme robuste. De nombreux audits furent effectués afin d'éprouver sa sécurité et ils furent tous unanimes : aucun réel problème de sécurité n'a pu être identifié (Voir 1, 2 et 3).

> 28 mai 2014, nous avons perdu TrueCrypt

Le 28 mai 2014, une tempête a soufflé dans la sphère informatique. Les développeurs de TrueCrypt abandonnent le projet ! En effet, le site TrueCrypt.org a été modifié afin de rediriger vers une page rudimentaire hébergée sur truecrypt.sourceforge.net.

Ce nouveau site avertit les internautes de l'existence potentielle de failles de sécurité (WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues). Ces failles seraient liées à la fin du support de Windows XP par Microsoft survenue trois semaines auparavant. Le site propose en tant qu'alternative un tutoriel sur le logiciel de chiffrement propriétaire de Windows : BitLocker.



Plusieurs points rendent la microsphère des spécialistes en sécurité informatique perplexes face à cette annonce :

➕La nouvelle page, plus que rudimentaire, pousse les utilisateurs d'un projet Open Source à se rapprocher d'un logiciel propriétaire Microsoft, connu pour sa proximité avec les services de renseignements américains.

➕La totalité des versions de TrueCrypt a été supprimée du site. Seule la version 7.2 (mise en ligne le jour même) subsiste. Cette dernière passant d'une taille de 3.3Mo à 2.5Mo (4).

➕Enfin, les développeurs ont déclaré que leur logiciel n'était plus fiable et l'ont abandonné, du jour au lendemain, après dix années de développement et de maintenance.

Tout le monde s'est accordé sur le fait que cette disparition est étrange, rapide et que quelque chose de louche traîne là-dessous. Oui, mais quoi ? De nombreuses hypothèses existent :

Le projet TrueCrypt a été piraté

Une page faite à la va-vite, une annonce (passer sur BitLocker) tellement improbable qu'elle en est risible, une nouvelle version déchiffrant mais ne chiffrant plus... TrueCrypt a été piraté !!

Oui mais...

➕Sourceforge déclare qu'aucun de leur voyant permettant de détecter une intrusion ne s'est affolé. (6)

➕ La nouvelle version de TrueCrypt a été signée avec les mêmes clés que les autres versions.

➕ Plusieurs semaines plus tard, les développeurs auraient pu se manifester pour annoncer l'imposture, mais ne l'ont pas fait.

Le projet TrueCrypt comporte réellement de grosses vulnérabilités

De nombreux audits sont actuellement en cours sur le logiciel de chiffrement. L'un d'entre eux était il sur le point de trouver une importante vulnérabilité affectant l'ensemble des versions ?

Les développeurs n'ont d'ailleurs pas répondu favorablement à la demande des internautes désireux de disposer du code afin de pouvoir « forker » TrueCrypt. Officiellement, il serait préférable de repartir de zéro plutôt que de reprendre le logiciel.

Oui mais ...

➕L'apparition de failles critiques est quotidienne. Certains logiciels régulièrement impactés (Microsoft, Oracle, Adobe, etc.) devraient-ils faire comme TrueCrypt ? Ceci est un autre débat !

➕La présence d'une faille, même critique, ne signifie pas obligatoirement l'arrêt du développement d'un projet. TrueCrypt aurait pu s'en sortir mais a préféré saborder son projet ainsi que l'ensemble des versions précédentes sans donner la possibilité à la communauté de lui venir en aide.

Les services de renseignements s'en sont mêlés !

L'arrêt aussi brutal d'un logiciel vieux de dix ans reste un mystère pour de nombreuses personnes et la théorie du complot refait son apparition.

TrueCrypt commençait à revenir régulièrement dans des affaires ou les forces de l'ordre et les services secrets américains étaient mêlés (Edward Snowden, Daniel Dantas, etc.). Agacé par ces échecs à répétitions, il est probable que les services de renseignement américains (ou autre, ne soyons pas sectaires) aient réussi à découvrir l'identité des développeurs, qui étaient jusqu'ici restés anonymes.

Toujours selon cette théorie conspirationniste, la nouvelle page du site fait penser à un « Warrant Canary ». Ce procédé permet aux éditeurs d' « annoncer » qu'ils se sont fait approcher par les services de renseignement sans avoir le droit légalement de l'avouer publiquement (article 18 U.S.C 2709 du Patriot Act).

Cette affaire ressemble étrangement à l'affaire Lavabit, également utilisé par Edward Snowden, dont le projet avait été

sabordé d'une manière similaire.

Rajoutons à cela certains faits marquants :

➕ Demande aux utilisateurs de migrer vers une technologie « NSA compliant »

➕ Sur la page du site, on peut lire « WARNING: Using TrueCrypt is Not Secure As » Si l'on souhaite avoir plus de détails, il est possible de lire la totalité de la phrase : Using TrueCrypt is not secure as it may contain unfixed security issues

Si l'on extrait les premières lettres (uti nsa im cu si) nous obtenons « Si je veux utiliser la NSA » en latin ou encore, si l'on reprend le W du début (Wuti nsa im cu si) nous obtenons (j'espère que vous le savez), « la NSA voit tout le monde » en albanais. CQFD !

« Alors que les jours passants décrédibilisent de plus en plus l'hypothèse de la compromission du compte, nous sommes toujours dans l'attente de l'audit en cours qui pourra peut-être répondre à certaines de nos questions. »

Marre de mettre toujours en doute l'honnêteté de la NSA ? Cela se comprend. Après tout, ce n'est peut-être pas eux. N'oublions pas que la version 7.2 de TrueCrypt est la dernière version en date et que 7 et 2 correspondent respectivement à G et B. Il n'y a plus aucun doute, les services de renseignements anglais sont également dans le coup !

> Des alternatives à TrueCrypt ?

Depuis l'arrêt brutal de TrueCrypt, les alternatives fleurissent un peu partout dans le monde :

➕ des forks (Ciphersed.org, TrueCrypt.ch, VeraCrypt,) ;

➕ des logiciels compatibles (TcPlay, Luksus, etc.) ;

➕ ou encore des logiciels embarqués aux systèmes d'exploitation (Windows avec BitLocker, Mac avec FileVault ou encore Linux avec LUKS).

Le site Truecrypt.ch se présente ainsi comme une plateforme ayant pour ambition de récolter le maximum d'informations sur l'arrêt de TrueCrypt. Le site met à disposition les dernières versions valables de TrueCrypt. De plus, le site évoque clairement la possibilité d'un fork, qui reprendrait le code source de TrueCrypt toujours disponible sur Github.

Le développement de ce fork, basé en Suisse pour éviter toute influence américaine, serait moins opaque que celui de l'équipe originale.

Néanmoins, avant de commencer à travailler sur ce fork, l'équipe préfère attendre les résultats de l'audit de sécurité initié par l'OpenCryptoAudit. Une première partie des résultats a déjà été publiée et n'a pas permis d'identifier de faille critique dans le code source de l'ancienne version de TrueCrypt. Une version finale de l'audit devrait être disponible dans les prochains mois.

> Conclusions

Toutes les cartes ne sont pas encore jouées concernant TrueCrypt.

Alors que les jours passants décrédibilisent de plus en plus l'hypothèse de la compromission du compte, nous sommes toujours dans l'attente de l'audit en cours qui pourra peut-être répondre à certaines de nos questions.

Au cas où cet audit ne permettrait pas d'identifier de faille de sécurité critique, nos regards recommenceraient à se tourner vers les services de renseignements. Nous commençons à bien les connaître avec les nombreuses informations divulguées par les documents dérobés par Snowden.

Références

➕ **[1]** http://www.ssi.gouv.fr/IMG/cspn/dcssi-cspn_2008-03fr.pdf

➕ **[2]** http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/

➕ **[3]** https://madiba.encs.concordia.ca/~x_decarn/truecrypt-binaries-analysis/

➕ **[4]** https://github.com/warewolf/truecrypt/compare/master...7.2#diff-9fc90217decda8d7d16d55ffaf7401c0R2295

➕ **[5]** http://beta.slashdot.org/story/203553

➕ **[6]** https://news.ycombinator.com/item?id=7813121