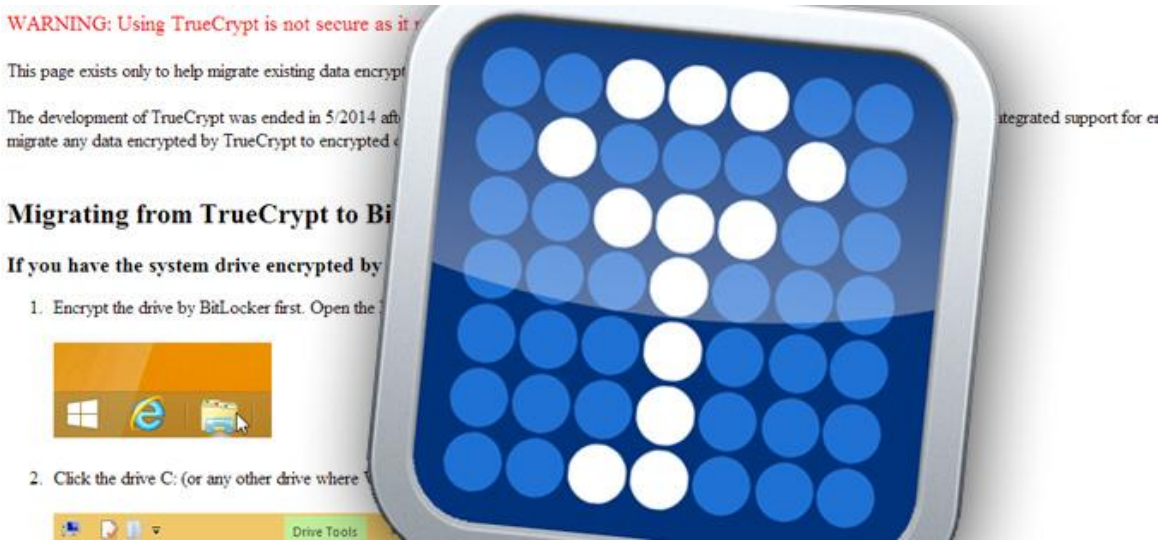
TrueCrypt ferme pour insécurité, et conseille de faire confiance à… Microsoft

Guillaume Champeau - 29 mai 2014

L'affaire semble tellement improbable que beaucoup ont du mal à y croire. L'équipe anonyme de développement de TrueCrypt, un logiciel open-source permettant de créer facilement un espace de stockage chiffré, a publié sur le site officiel un message d'avertissement et une nouvelle version de TrueCrypt, qui assurent que TrueCrypt n'est pas sûr. Ils conseillent d'utiliser BitLocker, la solution propriétaire de Microsoft.



C'est une petite bombe dans le monde de la cryptographie. Alors qu'il est considéré comme un outil de référence pour chiffrer des données, et alors que les premiers résultats d'un audit communiqués le mois dernier ont rassuré sur l'absence de backdoors, le logiciel TrueCrypt ne serait finalement pas sûr.

Depuis mercredi, le site du logiciel hébergé par Sourceforge affiche un message d'avertissement en lettres rouge : "ATTENTION : Utiliser TrueCrypt n'est pas sécurisé puisqu'il pourrait contenir des problèmes de sécurité non corrigés". Le message qui n'est accompagné d'aucune explication détaillée sur l'éventuelle faille ajoute que le site officiel n'existe plus que pour expliquer aux utilisateurs comment migrer les données chiffrées avec TrueCrypt vers d'autres solutions de cryptographie.

Microsoft en curieux recours

"Le développement de TrueCrypt s'est arrêté en mai 2014 après que Microsoft a arrêté le support de Windows XP", explique la page web. "Windows 8/7/Vista et supérieurs proposent le support intégré des disques et images virtuelles de disques chiffrés. De tels supports intégrés sont aussi disponibles sur d'autres plateformes. Vous devriez faire migrer toute donnée chiffrée avec TrueCrypt vers des disques ou images virtuelles de disques chiffrés supportés sur votre plateforme".

La page web de TrueCrypt conseille ainsi d'utiliser le système BitLocker de Microsoft, ce qui est surprenant tant les révélations d'Edward Snowden (qui conseillait TrueCrypt) sur les pratiques de la NSA ont ravivé les inquiétudes sur les liens incestueux entre l'agence de renseignement et les entreprises américaines, en particulier dans les algorithmes de cryptographie. De plus contrairement à TrueCrypt, le code source de BitLocker n'est pas disponible, ce qui permet d'autant moins de lui faire confiance.

L'annonce de la fin de TrueCrypt est un tel choc que la communauté semble douter de l'authenticité du message. Mais une nouvelle version 7.2 de TrueCrypt, qui ne permet plus que de déchiffrer les données pour effectuer leur migration, a bien été publiée sur Sourceforge avec la signature utilisée par les développeurs.

tenté de les contacter pour avoir des explications, mais sans grand espoir. Il soupçonne qu'ils aient pu subir des pressions et décider de fermer TrueCrypt :

« I THINK IT UNLIKELY THAT AN UNKNOWN HACKER (A) IDENTIFIED THE TRUECRYPT DEVS, (B) STOLE THEIR SIGNING KEY, © HACKED THEIR SITE. »

« — MATTHEW GREEN (@MATTHEW_D_GREEN) 28 MAI 2014 »

« AN ALTERNATIVE IS THAT SOMEBODY WAS ABOUT TO DE-ANONYMIZE THE TRUECRYPT DEVS AND THIS IS THEIR RESPONSE. »

« — MATTHEW GREEN (@MATTHEW_D_GREEN) 28 MAI 2014 »

WHO'S WHO

SUNRISE
Le calendrier de Microsoft

DATES

LIRE LA FICHE

MICROSOFT

Signaler une erreur dans le texte

CHIFFREMENT MICROSOFT NSA SÉCURITÉ TRUECRYPT 72

PARTAGER SUR LES RÉSEAUX SOCIAUX

Tweeter Partager Partager Partager reddit

Vous aimerez peut-être

Le meilleur de l'actu tech est aussi sur YouTube !

Microsoft attaque Washington pour lever le secret des requêtes gouvernementales

JUSTICE MICROSOFT SÉCURITÉ SURVEILLANCE VIE PRIVÉE

TrueCrypt conseillé par l'État islamique, ou l'impossible contrôle du chiffrement

CHIFFREMENT ETAT ISLAMIQUE TERRORISME TRUECRYPT

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

CHIFFREMENT IPHONE JUSTICE SÉCURITÉ VIE PRIVÉE

Chiffrement : l'Union européenne en ordre dispersé

Politique : les dernières actualités

Le Conseil constitutionnel dynamite le délit de consultation des sites terroristes

À San Francisco, les camions autonomes d'Uber sont testés en toute illégalité

Une procédure en ligne pour juger les délits mineurs est étudiée au Royaume-Uni

Wikipédia bannit le tabloïd Daily Mail de ses sources

Facebook muscle sa politique contre le ciblage publicitaire ethnique

L'ex-agent de la NSA risque la perpétuité pour avoir dérobé les secrets des États-Unis

La rédaction vous recommande