Forum: Windows 10

Topic: combien de fois mot de passe erroné pour déverrouiller Windows 10?

Subject: Re: combien de fois mot de passe erroné pour déverrouiller Windows 10?

Publié par: Mouffi
Contribution le : 10/10/2020 23:46:18

Je vois que vous avez bien phosphoré et j'en ai appris beaucoup !

Citation :

RGSOFT a écrit:
Bonjour à tous,

je pense très utile.

https://docs.microsoft.com/fr-fr/windo ... n-is-better-than-password

RGSOFT
Comme l'a dit Sylvie, ce lien est effectivement très intéressant.

En synthèse de ce que j'ai pu trouver, est indiqué au chapitre "Que se passe-t-il si quelqu'un vole l'ordinateur portable ou le téléphone?" :
"Pour compromettre une information d'identification Windows Hello protégée par le TPM, un attaquant doit avoir accès à l'appareil physique, puis doit ... deviner son code confidentiel, et tout cela doit être fait avant que la protection contre le module de plateforme sécurisée verrouille l'appareil."
Ce qui renvoie donc à la page "Principes de base du module de plateforme sécurisée (TPM)", et en particulier le chapitre "Anti-marteau", dont le sous-chapitre "Protection TPM 2.0 contre le marteau".

Là, vu que "Windows 8 certification" est cité, on peut penser que la version TPM 2.0 doit être a minima celle implémentée dans Windows 10.
Pour être compréhensible il faut passer en anglais
et retraduire en français avec Google

Et on trouve alors la réponse à ma question :

"Pour les systèmes avec TPM2.0, le TPM est configuré par Windows pour se verrouiller après 32 échecs d'autorisation et oubliera un échec d'autorisation toutes les deux heures. Cela signifie qu'un utilisateur pourrait rapidement tenter d'utiliser une clé avec la mauvaise valeur d'autorisation 32 fois. Pour chacune des 32 tentatives, le TPM enregistre si la valeur d'autorisation était correcte ou non. Cela entraîne par inadvertance le TPM à entrer dans un état verrouillé après 32 tentatives infructueuses.

Les tentatives d'utilisation d'une clé avec une valeur d'autorisation pendant les deux heures suivantes ne renverraient ni succès ni échec; à la place, la réponse indique que le TPM est verrouillé. Après deux heures, un échec d'autorisation est oublié et le nombre d'échecs d'autorisation mémorisés par le TPM tombe à 31, de sorte que le TPM quitte l'état verrouillé et revient au fonctionnement normal. Avec la valeur d'autorisation correcte, les clés peuvent être utilisées normalement si aucune erreur d'autorisation ne se produit au cours des deux heures suivantes. Si une période de 64 heures s'écoule sans échec d'autorisation, le TPM ne se souvient d'aucun échec d'autorisation et 32 tentatives infructueuses peuvent se reproduire."

J'ai donc l'impression que toutes les 64 heures, le voleur peut tester à nouveau 32 codes et cela autant de fois que nécessaire, sans jamais faire de verrouillage définitif de la possibilité par code confidentiel/code PIN. (une confirmation serait bienvenue
). Ca a de quoi décourager mais après ce n'est qu'une question de temps ou de chance.
J'ai donc juste à espérer qu'il le connecte à internet, ce qui devrait le verrouiller de façon définitive, l'ayant fait à partir du compte Microsoft de ma fille.

Je rappelle que, pour moi, le problème est uniquement la compromission des MDP stockés par Chrome et accessibles en clair avec le code PIN, moyennant de rester hors connexion (voir mon premier post).
Bien entendu, il doit y avoir x possibilités de reconfigurer le PC ou de lire le SSD, mais dans ce cas, ça me semble improbable d'arriver à décrypter la liste des MDP.

En tout cas, un grand merci à vous tous et particulièrement RG Soft dont le lien m'a bien guidé dans ma recherche.
Toute info complémentaire sera bien évidemment bienvenue, car je crois que je vais maintenant essayer d'activer Bit Locker (mais pas présent en Home d'après ce que j'ai compris), et peut-être voir si je peux mettre au moins 6 chiffres pour ce "Code confidentiel"