Les Honeywords : des faux mots de passe pour piéger les hackers

Aujourd'hui il est possible de piéger les pirates informatiques. Les RSSI (Responsables de la Sécurité des Systèmes d'Information) ont désormais la capacité de se doter de leurres pour éliminer les vols de mots de passe grâce aux « honeywords ». Ce sont de faux mots de passe qui déclenchent des alarmes dans le système chaque fois que des pirates tentent d'accéder à des comptes.

Ronald Rivest, professeur de la faculté des sciences informatiques Vannevar Bush du MIT, est l'un des inventeurs de la technique des « honeywords ». Cet outil arrive au moment où le vol de mots de passe atteint des proportions épidémiques. Le cabinet Hold Security a découvert que pas moins de 360 millions d'identifiants de compte récemment volés étaient disponibles sur le marché noir. La société a contribué l'an dernier à déceler des atteintes à la sécurité des données chez Adobe, où 2,9 millions d'identifiants avaient été volés.

« Honeywords » - les faux mots de passe : comment ça fonctionne ?

Ronald Rivest, professeur de la faculté des sciences informatiques Vannevar Bush du MIT, est l'un des inventeurs de la technique des « honeywords ». Elle fonctionne comme suit :Des faux mots de passe dits « honeywords », sont stockés au même endroit que les mots de passe réels d'un utilisateur. Si des mots de passe sont volés ou si des fichiers sont craqués, le voleur ne sait pas quel mot de passe associé au compte est le bon. Si le pirate tente d'utiliser l'un des faux mots de passe pour commettre une intrusion, un message d'alerte se déclenche pour avertir le service informatique que quelqu'un tente de s'introduire dans le réseau.Les « honeywords » n'empêchent pas une intrusion, mais ils permettent de détecter une attaque en temps réel et donc d'optimiser la réactivité des services informatiques.

Les « honeywords », c'est simple et sans contrainte

L'avantage des « honeywords » c'est qu'aucun changement n'est opéré côté utilisateur final, et qu'aucune formation n'est nécessaire. L'utilisateur se connecte comme d'habitude, et si son mot de passe correspond, l'accès lui est accordé normalement.Côté Back Office, cependant, un programme serveur auxiliaire dénommé Honeychecker aide à reconnaître les faux mots de passe et à donner l'alerte en cas d'attaque. Concrètement, le système d'authentification de l'entreprise stocke une matrice qui lie un ensemble de mots de passe à un utilisateur. Le logiciel Honeychecker stocke l'index du mot de passe correct de l'utilisateur. Honeychecker est installé en aval dans le centre des opérations de sécurité et ne participe pas à l'authentification proprement dite. Son rôle consiste uniquement à vérifier que le mot de passe n'est pas un honeyword. Si Honeychecker est hors ligne ou défaillant, l'utilisateur peut quand même se connecter, bien que les capacités de détection d'infraction soient alors perdues.Les « honeywords » établissent un juste équilibre entre la facilité de déploiement et la sécurité.