Bitly : encore une faille attribuÃ©e Ã des comptes utilisateurs compromis
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 19/5/2014 11:30:00

Suite Ã la faille de sÃ©curitÃ© qui a rÃ©cemment touchÃ© Bitly, le fournisseur de service de rÃ©ductions de liens a rapidement sensibilisÃ© ses utilisateurs sur le fait que des identifiants aient pu Ãªtre compromis. Il les invitait donc Ã rÃ©initialiser leurs mots de passe. De nouvelles informations relatives aux vecteurs de l'attaque ont depuis Ã©tÃ© divulguÃ©es.
Bitly a en effet rÃ©vÃ©lÃ© sur son **blog*** qu'un compte utilisateur compromis serait Ã l'origine de cette faille : Â« Nous avons effectuÃ© un audit de l'historique de sÃ©curitÃ© de notre code source hÃ©bergÃ© qui contient les identifiants d'accÃ¨s aux sauvegardes des donnÃ©es stockÃ©es hors site et avons dÃ©couvert un accÃ¨s non autorisÃ© sur le compte d'un employÃ©. Â»

Olivier MÃ©lis, Country Manager France chez CyberArk a fait les commentaires suivants :

Â« *Nous savons depuis un moment que les comptes Ã privilÃ¨ges, dont les identifiants de connexion des comptes administrateurs font partie, sont un outil puissant pour les cybercriminels souhaitant hacker un systÃ¨me cible. Par consÃ©quent, ces derniÃ¨res annÃ©es, ces identifiants sont devenus le vecteur d'attaque classique dans la plupart des intrusions subies par de grandes entreprises.*

La faille subie par Bitly est un nouvel exemple de dommages qui peuvent Ãªtre causÃ©s par un abus de ces identifiants Ã hauts-pouvoirs qui restent trop souvent sans surveillance ou sont peu sÃ©curisÃ©s au sein des organisations, malgrÃ© les risques Ã©levÃ©s qu'ils prÃ©sentent.

Les organisations doivent prendre conscience des menaces rÃ©elles que les comptes Ã privilÃ¨ges non surveillÃ©s prÃ©sentent pour une entreprise. Afin de suivre le rythme des risques en Ã©volution, les organisations doivent s'assurer qu'un systÃ¨me est mis en place pour surveiller et enregistrer tous les accÃ¨s et activitÃ©s liÃ©s aux comptes privilÃ©giÃ©s avec la possibilitÃ© d'intervenir et d'interrompre toute session Ã l'activitÃ© inhabituelle ou suspecte si nÃ©cessaire.

Comme annoncÃ© trÃ¨s rÃ©cemment par Symantec, l'Ã¨re du pÃ©rimÃ¨tre de sÃ©curitÃ© n'est plus, l'anti-virus est mort ! Il est donc essentiel Ã prÃ©sent de protÃ©ger les entreprises de l'intÃ©rieur. Les dirigeants devraient imaginer la situation de la maniÃ¨re suivante : si l'assaillant se

trouve dÃ©jÃ Ã l'intÃ©rieur du rÃ©seau, sera-t-il bloquÃ© par des portes fermÃ©es Ã chaque tournant ou aura-t-il la libertÃ© de se promener Ã l'intÃ©rieur du rÃ©seau et d'atteindre le cÅ□ur de l'entreprise? Par expÃ©rience, le dernier cas reste malheureusement le plus actuel pour le moment. Â»