Attention au whaling, ce phishing qui cible les équipes dirigeantes

	**Attention au whaling, ce phishing qui cible les équipes dirigeantes**

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.
Si vous travaillez dans la finance ou la comptabilité et si vous recevez un email de votre patron vous demandant de transférer des fonds vers un compte externe, mieux vaut réfléchir à deux fois avant d'obtempérer. Selon le cabinet de sécurité Mimecast, ces attaques de phishing très élaborées, dites whaling attacks, qui ciblent des cadres ou des directeurs d'entreprises, mais aussi des personnalités du monde politique ou des personnes célèbres, sont en hausse. Pour camoufler la provenance de e-mails, les pirates utilisent des noms de domaine usurpés ou très proche de domaines familiers du destinataire. Tout est fait pour ce dernier croit que les messages proviennent bien de son directeur financier ou du directeur général.

Le nom de domaine est usurpé dans 70% des attaques

55 % des 442 professionnels IT interrogés par Mimecast ce mois-ci ont déclaré que leur entreprise avait constaté une augmentation du volume de ces « chasses à la baleine » au cours des trois derniers mois, comme l'a déclaré le cabinet de sécurité. Les entreprises visées sont localisées aux États-Unis, au Royaume-Uni, en Afrique du Sud et en Australie. « L'usurpation de nom de domaine est la stratégie la plus courante, puisqu'elle est utilisée dans 70 % des attaques », a précisé le cabinet de sécurité. La majorité des faux messages sont signés du CEO, mais près de 35 % des entreprises ont vu passer des emails signés par le directeur financier. « Les messages conçus pour des attaques de whaling peuvent être plus difficiles à détecter, car ils ne contiennent pas de lien hypertexte ou de pièce jointe malveillante, et comptent uniquement sur l'ingénierie sociale pour tromper leurs cibles », explique Orlando Scott-Cowley, un stratège de la cybersécurité chez Mimecast. « Souvent, des sites comme Facebook, LinkedIn et Twitter fournissent aux attaquants les détails dont ils ont besoin pour préparer ces attaques », a encore déclaré Mimecast.

Informer est la première chose à faire

Alors, que faire ? Mimecast a quelques suggestions. D'abord informer les dirigeants, les équipes de management et de la comptabilité sur ce risque. Ensuite, réaliser des tests sur l'entreprise en montant de fausses attaques de whaling pour évaluer la vulnérabilité des employés. Une autre solution consiste à marquer les emails provenant de l'extérieur du réseau de l'entreprise, ou encore à créer des alertes pour signaler des noms de domaine qui ressemblent étroitement à celui de votre entreprise. « Les barrières pour bloquer l'entrée de ces attaques sont à niveau dangereusement bas », a déclaré Orlando Scott-Cowley. « Étant donné que la pêche est très bonne pour les cybercriminels, il est probable que le volume et la fréquence de ce type d'attaques augmentent », a mis en garde Mimecast.

Réagissez à cet article