Piratage Anthem : voici venu le temps du phishing

	Piratage Anthem : voici venu le temps du phishing

Victime d'une importante cyber-attaque, l'assureur américain Anthem invite ses clients à ignorer les e-mails qui leur seraient envoyés en son nom.

Victime d'une attaque informatique qui a potentiellement exposé les données personnelles de 80 millions d'individus, Anthem est passé en mode gestion de crise.
La compagnie américaine d'assurances santé mène actuellement l'enquête avec les autorités sur place. Elle a également sollicité la firme Mandiant (filiale de FireEye) pour pratiquer un audit de son système d'information et adopter les solutions de protection ad hoc.
Depuis le lancement de l'alerte mercredi dernier, de nouveaux éléments ont été révélés… sans qu'Anthem en soit systématiquement à l'origine. On a ainsi appris, d'une source dite « proche du dossier » par la presse américaine, que les données subtilisées par les pirates n'étaient pas chiffrées.
Sur la liste figurent, selon les déclarations officielles de l'assureur, des noms, des dates de naissance, des numéros de téléphone et de Sécurité sociale, des adresses postales et électroniques, ainsi que des éléments relatifs à l'activité salariée de clients, comme leur niveau de revenus.
Il n'existe toujours pas de preuves que des informations bancaires et médicales aient été dérobées. Mais celles-ci pourraient l'être d'une façon détournée ; en l'occurrence, par des campagnes de hameçonnage (phishing). Les clients d'Anthem commencent effectivement à recevoir des e-mails d'apparence légitime qui les invitent à cliquer sur un lien pour bénéficier d'un suivi de leurs encours de crédit.
Problème : si l'entreprise a bel et bien annoncé son intention de fournir gratuitement ce service à toutes les victimes collatérales de la cyber-attaque, elle n'a pas encore adressé de communication officielle. Bilan : les e-mails reçus ces derniers jours ne sont qu'un scam visant à récupérer de précieuses données auprès des utilisateurs insuffisamment vigilants.
Voilà Anthem contraint d'user de pédagogie. La société cotée en Bourse – sur le NYSE – a ouvert une rubrique dédiée dans la foire aux questions du site AnthemFacts, créé pour centraliser les dernières nouvelles relatives à la cyber-attaque. Elle enjoint ses clients à ne cliquer sur aucun lien, à ne pas ouvrir les éventuelles pièces jointes, à ne renseigner aucune information sur le site Web qui s'ouvrirait éventuellement et à ne pas répondre au mail.
Pour l'heure, il reste difficile de déterminer s'il s'agit d'une campagne de phishing ciblée ou si ces envois de mails sont l'œuvre de pirates qui ont visé large en espérant toucher des souscripteurs aux assurances santé d'Anthem. Ce qui laisse supposer que les données volées sont bel et bien activement exploitées, ce sont plutôt ces appels téléphoniques invitant les clients à fournir leur numéro de carte bancaire et/ou de Sécurité sociale.
Le bilan pourrait être lourd : près de 40 millions de clients revendiqués à fin 2014… et autant d'anciens souscripteurs. Une affaire d'une telle envergure que le Département des services financiers de New York envisage aujourd'hui un audit global de toutes les compagnies d'assurance. L'agence fédérale compte intégrer ces contrôles « réguliers et ciblés » dans sa feuille de route. Elle projette aussi de durcir les obligations auxquelles les institutions sont soumises en matière de sécurité informatique.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itespresso.fr/piratage-anthem-temps-phishing-88038.html
Pat Clément BOHIC