Le malware Backoff a pris Home Depot dans ses filets

Backoff, l'hécatombe continue ? En tous cas, **plusieurs banques américaines pensent que les magasins Home Depot**, une chaîne de magasins omniprésente aux Etats-Unis, sont la source d'une nouvelle fuite massive de données bancaires. Hier matin, sur les sites underground, un nouveau lot de numéros de cartes de débit et de crédit a en effet été mis en vente. La chaîne de distribution enquête sur le sujet, avec l'aide des banques et des autorités américaines, ont expliqué hier les porte-parole de la société à nos confrères d'outre Atlantique.

Selon Brian Krebs, qui tient un blog spécialisé sur la sécurité, plusieurs signes laissent à penser qu'on a affaire au **gang de hackers russes et ukrainiens** déjà à l'origine des attaques contre d'autres distributeurs américains, dont celle contre la chaîne de grande distribution Target. Le serveur utilisé pour mettre en vente les données dérobées est par exemple identique.

Politique et bonnes affaires

Les hackers semblent également vouloir **faire passer un message politique**. Les numéros de cartes américaines dérobés sont regroupés dans deux fichiers, appelés « American Sanctions » 1 et 2, tandis que les numéros de cartes européennes figurent dans un fichier nommé « European Sanctions ». L'opération ressemble donc à une **mesure de rétorsion** prise à l'encontre des Etats-Unis et de l'Union européenne après les sanctions décidées contre Moscou. Même si elle a, en réalité, probablement été lancée pour des motifs purement mercantiles.

En effet, selon le même Brian Krebs, plusieurs banques estiment que les vols de numéros de cartes chez Home Depot ont démarré fin avril ou début mai 2014. Soit avant les sanctions décidées à l'encontre de Moscou. S'il s'avérait qu'une large part des magasins de la chaîne (2 200 aux Etats-Unis et près de 300 au dehors) ait été piratée, ce vol de données pourrait **dépasser en taille celui dont a été victime Target** (40 millions de numéros de cartes dérobés).

En début de semaine, Kaspersky Labs livrait des prévisions très noires concernant le butin de Backoff, ce **malware qui cible les lignes de caisse** pour exfiltrer des données bancaires et dont serait également victime Home Depot. La société estimait que le bilan sera encore plus lourd que les 1 000 entreprises touchées, première estimation donnée la semaine dernière par le ministère de l'Intérieur américain. Rappelons que Backoff cible les terminaux point de vente et utilise une faiblesse de sécurité du processus d'autorisation des paiements par carte bancaire à piste magnétique pour extorquer un maximum d'informations.

A lire aussi :

Sécurité de l'information : les entreprises dépensent toujours plus

Piratés, les magasins Target font face à une kyrielle de procès