Comment les hackers transforment en profits des mots de passe volés

La vaste majorité de leurs vols de données et des cyber crimes commis par les hackers à travers le monde sont motivés par l'argent. Mais une fois qu'un hacker à dérobé des données privées telles que des numéros de sécurité sociale, des mots de passe ou des numéros de cartes de crédit, comment transforme-t-il ces informations en monnaie sonnante et trébuchante ?

Comprendre le modus operandi des hackers après une attaque réussie est non seulement intéressant mais peut aussi aider à minimiser les dommages résultant du vol de données. Les informations qui suivent sont une vue générale des étapes les plus courantes qu'empruntent les hackers pour monétiser leur butin. Elles ne s'appliquent donc pas à tous les cas, et pas non plus, bien sûr aux cyber attaques menées par des états nations dont les motivations sont autres que financières.

Une fois qu'une attaque a réussi et que le criminel détient les données donc, le plus probable est qu'il empruntera les étapes suivantes, que l'on pourrait appeler « Checklist Post Attaque » du hacker.

1. Inventaire des données volées – Les hackers examineront les fichiers de données volés pour identifier des identifiants d'authentification, des informations personnelles telles que noms, adresses et numéros de téléphone, et des informations financières telles des coordonnées de cartes de crédit.
2. Vente d'informations personnelles – Ensuite, le hacker réunira les informations personnelles récoltées telles que noms, adresses, numéros de téléphone et adresses email et les vendra, typiquement en vrac. Plus ces informations seront récentes, plus elles auront de la valeur. D'après le titre en ligne Quartz, une fiche complète d'informations personnelles sur un individu incluant numéro d'identification, adresse, date de naissance et si possible coordonnées de carte de crédit vaut entre 1 et 450$.
3. Recherche des informations les plus intéressantes – Les hackers vont alors examiner plus avant les identifiants d'identification qu'ils détiennent et rechercher les comptes potentiellement les plus lucratifs. Les adresses correspondant à des organisations gouvernementales et militaires ont une grande valeur, de même que les adresses email et mots de passe de grandes entreprises. Les employés réutilisant souvent les mêmes mots de passe plusieurs fois, les hackers peuvent utiliser ces identifiants pour cibler d'autres entreprises. Par exemple, Dropbox a subi une attaque en 2012 utilisant des identifiants volés lors de l'attaque du réseau LinkedIn plus tôt la même année. Un hacker pourra mener lui-même une telle attaque, ou vendre les identifiants à d'autres hackers sur le dark web à un prix beaucoup plus élevé.
4. Vente des coordonnées de cartes de crédit – Les informations financières telles que les numéros de cartes de crédit sont rassemblées et vendues par lots. Un individu possédant les connaissances appropriées peut facilement acheter des coordonnées de cartes de crédit par groupes de dix ou de cent. Généralement, un « broker » achète ces coordonnées, puis les revend à un « carder » qui utilise un processus en plusieurs étapes pour éviter d'être détecté. Dans un premier temps, les « carders » achètent des cartes cadeaux dans des boutiques ou sur Amazon.com, puis utilisent ces cartes pour acheter des produits de consommation. Ils les revendent ensuite via des canaux légitimes tels que eBay ou via un site sur le dark web.
5. Vente en vrac – Quelques mois après, le hacker rassemblera les identifiants d'identification qui lui restent et les revendra en vrac à prix cassé. A ce stade, la plupart d'entre eux n'ont plus aucune valeur, les entreprises concernées ayant très probablement découvert l'attaque et pris des mesures pour y remédier.

Pour les non-initiés, le dark web est un ensemble de réseaux chiffrés qui ont été intentionnellement rendus invisibles sur le web et ne peuvent être accédés qu'avec des logiciels spécifiques. La plupart du

temps l'expression « dark web » s'applique à des contenus hébergés sur le réseau Tor, un système de relais qui dissimule les adresses IP. Utiliser Tor ou un réseau similaire (il en existe d'autres mais Tor est le plus populaire) empêche une personne surveillant votre navigation Internet de savoir quels sites vous visitez, et empêchent les sites web de déterminer votre position. En raison de cet anonymat garanti, le dark web héberge un grand nombre de sites illégaux. La vente de données volées a lieu généralement sur des sites du dark web.

Que pouvez-vous donc retirer de tout ceci en tant que consommateur ?

Premièrement, assurez-vous que vous utilisez des mots de passe différents pour chacun de vos comptes en ligne. Ainsi, même si l'un d'entre eux est compromis, les autres resteront sûrs. Deuxièmement, agissez rapidement si vous suspectez que vos données personnelles ont été volées. Si vous possédez un compte dans une entreprise qui a signalé une attaque, changez votre mot de passe immédiatement. Vous pouvez vérifier si un de vos comptes a été volé sur haveibeenpwned, un site web tenu par un analyste de sécurité de Microsoft qui traque les informations liées aux vols d'identifiants. Vous ne pouvez pas toujours éviter que vos données soient dérobées, mais en réagissant rapidement vous pouvez en minimiser les conséquences.

Pascal Le Digol, Country Manager France WatchGuard