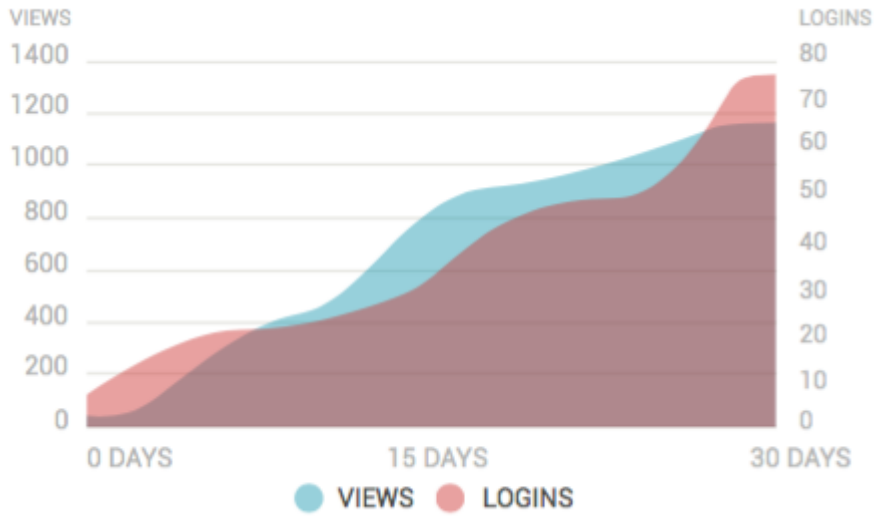
Que se passe-t-il après un vol de données ?

BitGlass, éditeur de solution CASB (Cloud Access Security Broker), est devenu un spécialiste des « honeypot », des pièges pour les cybercriminels afin d'analyser et de comprendre la vitesse et le processus de propagation des données dérobées dans le cyberespace. En avril dernier, BitGlass avait réalisé un premier tour de chauffe en créant et marquant un fichier contenant des données fictives pour démontrer la rapidité à laquelle des informations sensibles peuvent être diffusées sur le Dark Web. Nous nous étions fait l'écho des résultats de cette expérience dans cet article.

Le spécialiste vient de récidiver avec un second cas d'école, baptisé Projet Cumulus : un identifiant d'un employé d'une banque fictive, un portail web de cet établissement bancaire et un compte Google Drive avec les données d'une carte de crédit et d'autres informations professionnelles. L'éditeur a ensuite laissé « fuiter » des accès (login/mots de passe) à Google Apps sur le Dark Web. Voilà le décor planté !

Réutilisation des mots de passe à proscrire

Et les résultats ne se sont pas fait attendre. En moins de 24 heures, BitGlass a recensé 5 tentatives de connexions sur le compte bancaire de la victime et 3 sur son compte Google Drive. Les fichiers ont, eux, commencé à être téléchargés au bout de 48 heures après la publication des accès sur le Dark Web. Au bout d'un mois, ces accès ont été consultés plus de 1400 fois et 1 hacker sur 10 a tenté sa chance pour se connecter sur le compte Google.



Plus inquiétant, 94% des pirates qui ont eu accès à Google Drive en ont profité pour se connecter à d'autres comptes de la victime, réseaux sociaux, comptes bancaires. Pour se faire, ils ont réutilisé les accès trouvés sur le Dark Web, démontrant ainsi le problème de la réutilisation des mots de passe. Un pirate a même réussi à casser et voler un fichier chiffré contenant des informations sensibles.

Tor devient la norme

Autre enseignement intéressant, la mondialisation et l'anonymisation des connexions frauduleuses. Les cybercriminels sont originaires de plus de 30 pays dont 34,85 % provenaient de Russie, 15,67 % des États-Unis et de 3,5 % de la Chine.

Mais surtout 68% des connexions étaient réalisées par l'intermédiaire du réseau Tor. Une proportion beaucoup plus importante que lors de la première expérience constate BitGlass. Cela signifie que les pirates sont de plus en plus conscients des questions de sécurité. Les jeunes pirates sont incités à utiliser Tor en complément d'un VPN pour s'assurer d'un anonymat sécurisé.

A lire aussi :

Experian : les données piratées de T-Mobile déjà sur le Dark Web ?

Les sites cachés Tor exposés grâce au serveur Apache