PIXELS
CYBERCRIMINALITÉ

Hackeurs de Big Mac : comment des pirates informatiques font leur beurre avec des points McDonald's

Certains trafiquants numériques ont trouvé une nouvelle façon de s'enrichir : usurper les points de fidélité des clients de la chaîne de fast-food. Une combine symptomatique d'une petite délinquance informatique, discrète et rentable.

Par Gabriel Thierry

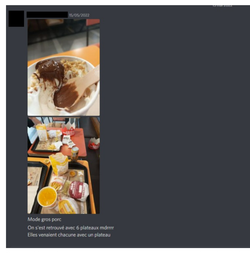
Publié le 21 mai 2022 à 08h00

Article réservé aux abonnés

BLAKE PATTERSON CC BY 2.0

« *Mode gris pore : on s'est retrouvé avec six plateaux vide.* » Sur ce serveur Discord, populaire plate-forme de tchat, les commentaires sont enthousiastes. On y achète en effet des sandwichs McDonald's à prix cassé : pour 5 dollars, soit 4,75 euros, on peut repartir d'un restaurant hexagonal avec un menu Best of, facturé en ce moment entre 7 et 9 euros. Une aubaine pour ces internautes français qui mettent en avant leurs rigoles, comme dans cette vidéo postée par un adolescent se rendant à toutinette dans un restaurant pour tester le service.

S'ils sont nombreux à s'inquiéter dans leurs échanges d'une éventuelle arnaque, peu cherchent à en savoir plus sur les origines de ce trafic. Pourtant, sans surprise, la vente de ces burgers à prix d'ami est bien une fraude, caractéristique d'une petite délinquance numérique qui, bien que courante, passe en partie sous les radars. « *Ce qui peut apparaître comme un événement de faible intensité peut en réalité faire partie d'un phénomène de masse avec des préjudices globaux élevés* », relevait ainsi en 2019 le ministère de l'intérieur dans un rapport.



Capture d'écran d'un internaute montrant son repas après avoir acheté des sandwichs bradés.

Bourrage d'identifiants

Cette vente sous le manteau de sandwichs McDonald's repose sur le piratage informatique des comptes fidélité, auxquels on peut souscrire lorsque l'on est client régulier. A chaque euro dépensé, votre compte est crédité d'un point. Ce qui permet ensuite d'obtenir des produits gratuits, d'une boisson à un dessert, en passant par l'inévitable Big Mac, payables en caisse grâce à un code-barres à présenter. « *Je perdais mon solde de points, des personnes s'en servaient pour avoir des commandes gratuites* », regrette ainsi auprès du *Monde* Anaïs, une jeune femme des Yvelines *déçue d'avoir « cotisé pour rien »*. Interrogée, McDonald's France affirme de son côté toujours veiller à rétablir, après vérifications, les points de clients lésés.

Tout commence par des fuites de données (…) qui alimentent des (…) couples identifiants-mots de passe partagés sur des forums

Pour faire main basse sur ces points, les hackeurs malveillants utilisent une recette éprouvée : le bourrage d'identifiants. Tout commence par des fuites de données, comme celle qui avait affecté le service d'édition de PDF Lumin, en 2019. Elles alimentent des « combo-lists », des fichiers d'agrégats qui ne gardent que les couples identifiants-mots de passe partagés sur des forums. Les pirates parient ensuite sur le fait que ces couples ont été utilisés ailleurs, comptant sur la trop grande propension des internautes à renseigner le même mot de passe pour différents comptes.