Piratage du site des impôts : les hackers s'expriment... Ce que doivent savoir les victimes

Alors que les victimes du piratage de la DGFiP qui a touché près 680 000 personnes sont informées des risques de la fuite de leurs données et que le gouvernement prend des mesures de sécurité, les hackers se sont exprimés.

"Nous nous excusons, parce que ce qui est arrivé est insupportable pour les Français". Le ministre de l'Action et des Comptes publics a présenté des excuses, le mardi 18 août, près d'une semaine après la revendication du piratage informatique et du vol de données qui a ciblé la Direction générale des finances publiques (DGFiP). Ce n'est pas une, mais trois attaques successives qui ont permis à des pirates de subtiliser des données en juin, en juillet et en août, a précisé la directrice générale des finances publiques, Amélie Verdier, en conférence de presse le 18 août. Elle a fait le point sur chaque piratage tandis que le parquet de Paris a annoncé l'ouverture d'une enquête pour "extraction frauduleuse de données" et "association de malfaiteurs".

Au total, 678 000 particuliers et professionnels ont été victimes du piratage et du vol de données sur le site des impôts, dont 350 000 contribuables. Toutes les personnes concernées doivent être prévenues par la DGFiP, qui a commencé à envoyer des courriers aux intéressés le lundi 17 août. Ce dernier précise le type de données consultées, volées et, si nécessaire, les précautions à prendre. Le processus est encore en cours car "ce n'est pas facile de recouper les profils concernés et de les alerter de manière individuelle, ça prendra du temps", a prévenu une source ministérielle auprès du Parisien.

Quelles données ont été volées ?

La première attaque informatique survenue fin juin a été la plus importante et a touché le système d'information du fisc. Diverses données ont pu être consultées, extraites et mises en vente par les pirates sur le dark web. La DGFiP a précisé qu'il pouvait s'agir de "l'identifiant fiscal, de l'état civil, des coordonnées postales, téléphoniques et électroniques, de la situation fiscale, du revenu fiscal de référence, du nombre de personnes à charge, du nombre de parts et du taux de prélèvement à la source", notamment pour les particuliers. Pour les professionnels, les données volées sont "moins sensibles". Il s'agit du numéro SIREN, de l'adresse de l'entreprise ou de celle du mandataire, a détaillé l'administration fiscale.

La deuxième attaque menée en juillet a permis, elle, de voler des données cadastrales extraites du Serveur professionnel de données cadastrales (SPDC), dont les informations relient les parcelles et leurs adresses à leur propriétaire. Les cybercriminels ont revendiqué le vol de données de deux millions de personnes, mais la DGFiP a indiqué le 18 août avoir, pour l'heure, identifié "maximum à 433 485 particuliers et 1 082 professionnels" concernés.

L'administration financière a également évoqué une "troisième fuite" concernant les données liées aux successions, mais celle-ci a rapidement été "coupée" et "n'est vraiment pas du tout de la même ampleur" que les deux autres piratages a souligné la patronne de DGFiP, Amélie Verdier.

Malgré ces trois piratages et le vol de données sensibles, les cybercriminels n'ont pas réussi à s'introduire "dans un compte fiscal, ni d'un particulier ni d'un professionnel" et aucune des attaques "n'a permis de récupérer des codes d'accès au compte sécurisé d'un contribuable", a assuré la directrice générale de la DGFiP.

Comment le site des impôts et à la DGFiP ont-ils pu être piratés ?

Le piratage de la DGFiP est le fruit d'une "attaque plus sophistiquée que ce qu'on avait vu par le passé", a fait savoir Amélie Verdier. Les cybercriminels auraient évité de procéder à des requêtes massives, plus facilement détectables par les systèmes de surveillance de l'administration. Ils semblent plutôt avoir compromis le compte d'un agent de l'administration en profitant d'une faille de sécurité et en détournant les identifiants de l'employé en question. Cet accès a été "fermé immédiatement" après la découverte de la compromission, mais les investigations ont "échoué à repérer ce qu'il s'est passé". Le fisc n'a été informé du vol de données qu'au moment de la revendication des faits par les hackers.

C'est le groupe ZeroBytes, qui dit être composé de deux hackers français, qui a revendiqué les attaques menées contre le DGFiP. Le groupe qui communique sur X et même à la presse promet de ne pas s'arrêter là. "Les impôts, ce n'était que le début", a-t-il annoncé sur le réseau social le 16 août. Il a d'ailleurs évoqué le piratage de données de l'Education nationale. ZeroBytes semble se concentrer sur les services de l'Etat, mais s'en prend aux données de milliers de personnes. Pour quel motif ? L'argent comme il l'explique à BFMTV : le duo trouve des failles des sécurité, les exploite pour accéder à des données et les vendre au plus offrant sur le dark web. Les services publiques semblent ciblés pour leur facilité à être piratés, selon ZeroBytes : "Leur service était mal sécurisé, c'est tout".

Des mesures, un plan de sécurisation et une augmentation du budget

Le piratage de la DGFiP a poussé le gouvernement à tenir une cellule interministérielle le 17 août. A l'issue, le ministre des Comptes publics David Amiel a reconnu que les "systèmes d'information comportent des faiblesses", malgré les "plus de 100 emplois" dédiés à cybersécurité et les "plus de 5 300 informations de la DGFiP" cités par Amélie Verdier. Le ministre a ensuite évoqué un plan d'action pour renforce la sécurité en plusieurs phases, dont "la lutte contre la compromission des comptes des agents" et un renforcement "de la formation cyber des agents". La sécurisation des comptes des agents doit être renforcée avec, entre autres, des "token USB" qui permettent de se connecter à un compte personnel de manière sécurisée. Par ailleurs, les "campagnes internes d'hameçonnage seront intensifiées" pour éviter que les agents se fassent piéger par du "phishing".

L'Etat s'était déjà penché sur la question de la sécurité et avait annoncé en avril 2026 la mise en place d'un plan de sécurisation numérique de l'État prévoyant la création de l'autorité de gouvernance "Ariane", un investissement de 200 millions d'euros dans la cybersécurité et l'IA, ainsi que l'obligation pour chaque ministère d'allouer 5 % de son budget au cyber dès 2027. Des

mesures qui pourraient être réhaussées après le piratage. L'hypothèse d'un doublement du budget informatique annuel - évalué à 489,9 millions d'euros en 2025 - serait sur la table, avance RMC, qui estime que le milliard d'euros pourrait ainsi être atteint.