Billet

Une arrestation et après ? Il faudra bien tirer les leçons de la cyberattaque massive qui a visé le fisc

Corinne Bouchouchi

Publié le 7 septembre 2026 à 17h00 ,
mis à jour le 7 septembre 2026 à 17h02
Lecture : 3 min. Abonné

Un hacker récidiviste de 18 ans a été arrêté à Paris et placé en détention dans le cadre de l'enquête sur le vol des données de quelque 678 000 contribuables. Une indéniable réussite policière qui n'efface pourtant pas le goût amer du fiasco.

Sébastien Lecornu peut respirer : l'Office anti-cybercriminalité (Ofac) a réussi un coup de maître en permettant l'arrestation, dès le 18 août, de l'un des membres du collectif dissimulé sous le pseudonyme de ZeroBytes pour revendiquer les attaques du fisc (révélées le 13 août), mais aussi de l'Education nationale (revendiquées le 18 août). Annoncée vendredi 4 septembre, cette première mise en examen est une victoire après un été tumultueux.

A lire aussi

Décryptage Piratage du fisc : un hacker de 18 ans mis en examen et placé en détention

provisoire

Selon le communiqué du parquet de Paris, qui s'est saisi de l'enquête *« en toute discrétion »* dès le 31 juillet avant de la confier naturellement à l'Ofac, le suspect, domicilié en région parisienne, est un récidiviste tout juste âgé de 18 ans. Un mineur de moins de 16 ans avait également été interpellé et placé en garde à vue, mais si le majeur a été placé deux jours plus tard en détention provisoire, le plus jeune a, lui, été rapidement libéré. Dort donc aujourd'hui en prison un dénommé « ChatNoir » (le pseudonyme du hacker selon une information du « Monde »), dont le profil laisse imaginer un de ces jeunes geeks avides de challenges et/ou d'argent facile.

La suite des investigations *« pour identifier et interpeller les autres personnes mises en cause »*, a précisé le parquet, permettra, on l'espère, d'en apprendre un peu plus sur ces « ZeroBytes » qui ont mis à nu des centaines de millions de Français cet été… Mais pas de dormir sur nos deux oreilles, rassurés d'avoir confié nos données à des ministères ou administrations bien protégés. Car la célérité policière ne doit pas faire oublier le volet politique de l'affaire et l'identification des responsabilités de chacun. Un terrain sur lequel le gouvernement est clairement attendu.

Interrogée au lendemain des annonces par France-Inter, Amélie Verdier, directrice générale des Finances publique (DGFip), était visiblement mal à l'aise pour aller au-delà de la contrition, admettant que la confiance avec les Français a été *« entamée »*. Et si la patronne des finances ne dément pas un manque de moyens certain – le nombre d'agents dans les services informatiques serait passé de 130 000 il y a vingt ans à 93 000 aujourd'hui, et seuls 50 s'occupent de cybersécurité ! –, c'est pour souligner aussi que son administration a contribué aux économies générales par solidarité…

Où sont les responsables ? L'exemple Target versus l'Etat français

« Y a-t-il eu un manque d'attention ? C'est sûr. Un manque de focalisation sur certains secteurs alors que Sébastien Lecornu, après l'attaque de l'Agence nationale des Titres sécurités (ANTS) en avril, avait demandé à ses ministres "un sursaut" *? L'enquête de l'Anssi* [Agence nationale de la Sécurité des Systèmes d'Information, NDLR] *le dira »*, prévient Pierre Delort, président de l'Association nationale des Directeurs des Systèmes d'Information (Andsi), sans plus s'avancer. L'ingénieur, qui est aussi professeur invité à Mines Paris-PSL, sait pourtant de quoi il parle, lui qui a été directeur des systèmes d'information, entre autres, de l'Inserm et de Réseau ferré de France. S'il admet qu'aucun système ne sera jamais inviolable, il ne transige pas avec les responsabilités des dirigeants : *« J'espère que l'enquête de l'Anssi déterminera des responsabilités personnelles »,* insiste-t-il.

A lire aussi

Entretien Piratage du fisc : « La cybersécurité est le canari dans la mine, c'est le premier sujet qui va nous exploser à la figure »

Abonné

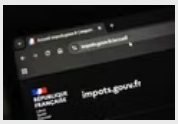
Sa référence ? L'affaire du groupe Target, un cas d'école en matière de cybersécurité. Pour mémoire, fin 2013, le géant américain de la grande distribution subit une attaque de grande ampleur. Des dizaines de millions de coordonnées de paiement sont volées. Le mode opératoire : un vol d'accès via un sous-traitant mal protégé, suivie d'une diffusion interne en cascade en raison d'un manque de segmentation du réseau et d'alertes ignorées ou traitées trop tardivement…

De la même façon, en 2025, c'est par la messagerie de l'ordinateur personnel d'un agent du ministère de l'Agriculture que des pirates seraient entrés dans les systèmes du ministère de l'Intérieur. Dans le cas du fisc, les accès VPN utilisés par les agents des impôts pour travailler à distance auraient permis à ZeroBytes de siphonner les données de 678 000 Français. Ce qui signifie qu'il y avait une faille humaine, s'est empressé de se défausser sur LCI Sébastien Lecornu le 29 août :

« Si je reprends un parallèle avec une maison, ce n'est pas un problème de solidité des volets, de vos fenêtres, de votre porte ou de votre système d'alarme. C'est bien ce qui me met en colère dans ce qui s'est passé, c'est que globalement, on avait une maison qui était bien fermée, avec une porte blindée, bien fermée, serrures deux points.

Malheureusement, la clé a été mise sous le paillasson et il a été dit dans tout le quartier que la clé était là. Cela s'appelle un problème d'hygiène numérique. »

A lire aussi



« Je récolte la colère populaire » : dans l'affaire du piratage du fisc, une action collective salutaire

Abonné

A la suite de la cyberattaque de Target, le PDG (Gregg Steinhafel) et la directrice des systèmes d'information (CIO) ont dû démissionner. Et surtout, l'affaire a marqué un tournant dans la gestion de telles crises au sein des grands groupes, observe Pierre Delort : *« Ça a été un point d'inflexion. Après Target, la cybersécurité est devenue un sujet de conseil d'administration. Ce n'était plus seulement l'affaire d'informaticiens au fond du couloir qui vous embêtent avec vos mots de passe à changer et vous coûtent cher. C'était le conseil d'administration qui était responsable. »* Le gouvernement tirera-t-il les mêmes leçons pour ses administrations ? Interrogée sur France-Inter sur son éventuelle démission, la directrice de la DGFip a, quant à elle, choisi d'éluder : *« Ma responsabilité première est d'organiser la réponse à la crise. »*

Par Corinne Bouchouchi