Cyberattaque contre le Ministère de l’Intérieur : un suspect récemment « condamné pour des faits similaires » interpellé… il a 22 ans et vit chez sa mère (MàJ : Le suspect, Melvin L., avait participé au harcèlement de Mila)

18/12/2025 à 21h09



18/12/2025

C’est dans une petite commune du Limousin (Haute-Vienne) que des dizaines de policiers surarmés des Brigades de recherches et d’intervention (BRI), plus habitués à traiter des grands bandits que des hackers blafards, sont venus l’interpeller, ce mercredi après-midi, au domicile de sa mère. Âgé de 22 ans, Melvin L., alias « SSRQM » (entre autres), est soupçonné, selon nos informations, d’être impliqué dans l’embarrassant piratage dont a été victime le ministère de l’Intérieur.

Ainsi, Melvin L. est actuellement mis en examen et renvoyé dans une affaire de « swatting » – canulars en ligne – dans l'attente d'être jugée. Dans le cadre d'investigations sur du cyberharcèlement dont avait été victime l'influenceuse et militante anti-islam Mila, les enquêteurs avaient découvert que le jeune pirate présumé avait inventé et fourni un dispositif technique ayant permis à certains internautes d'agir.

Un rôle qui rappelle une autre affaire pour laquelle il a été jugé en avril dernier avec un cercle de geeks particulièrement surprenants. Il est question d'une cyberescroquerie appelée « Sim Swap ». Concrètement, l'arnaque consiste à prendre possession de lignes téléphoniques de citoyens en faisant des déclarations fallacieuses de portabilité. Grâce à cela, les pirates peuvent ensuite détourner les systèmes de double authentification par SMS qui permettent de se connecter, par exemple, à des comptes bancaires, de cryptomonnaies ou de trading. Dans cette affaire, un groupe de jeunes hackers désinvoltes a utilisé ce procédé pour siphonner plusieurs dizaines de milliers d'euros sur le compte de victimes françaises et usurpé leurs lignes téléphoniques.

[…]

Le Parisien

Un homme âgé de 22 ans a été interpellé mercredi et placé en garde à vue dans le cadre de l'enquête ouverte après le piratage des serveurs du ministère de l'Intérieur, a annoncé la procureure de Paris, Laure Beccuau. (…)

Le suspect « est déjà connu des services de justice pour avoir été condamné pour des faits similaires en 2025 », a précisé la procureure dans un communiqué. Le jeune homme, qui vivait chez sa mère, a été interpellé par la Brigade de recherche et d'intervention (BRI) en Haute-Vienne. (…)

Le Parisien

17/12/2025

«Quelques dizaines de fichiers» confidentiels ont été «extraits» lors de l’attaque informatique qui a touché Beauvau, a indiqué mercredi le ministre de l’Intérieur Laurent Nunez.

«*Quelques dizaines de fichiers*» confidentiels ont été «*extraits*» lors de l’attaque informatique qui a touché Beauvau, a indiqué mercredi le ministre de l’Intérieur Laurent Nunez.

«On ne connaît pas encore l’ampleur de la compromission, on ne sait pas ce qui a été extrait : à date, quelques dizaines de fichiers ont pu être sortis du système mais on parle de millions de données»

Le Figaro

> *Cette seule maigre "preuve" que donnait les cybercriminels qui revendiquent la cyberattaque sur le ministère de l'intérieur… □□*
>
> *Tout laisse à penser -et donc confirmer les nouvelles déclarations de Laurent Nuñez ce matin- qu'ils ont eu accès aux mots de passe, hélas en clair,… https://t.co/J4li3qC6Jg pic.twitter.com/n8LkeBH3vP*
>
> *— SaxX ¯_(□)_/¯ (@_SaxX_) December 17, 2025*



16/12/2025

L’inquiétude grandit autour de l’attaque informatique visant le ministère de l’Intérieur dans la nuit du 11 au 12 décembre. Alors que le ministre Laurent Nuñez assurait vendredi qu’aucune “compromission grave” n’avait été détectée, le collectif de hackers revendiquant l’opération affirme au contraire détenir des informations d’une ampleur exceptionnelle. Le partage public de ces données, une fois leur ultimatum expiré le 20 décembre, pourrait représenter un tournant majeur pour la sécurité nationale.

Dès samedi, le groupe pirate a indiqué sur BreachForums être en possession de fichiers issus du Traitement des antécédents judiciaires (TAJ), du Fichier des personnes recherchées (FPR), mais aussi de la Direction générale des finances publiques et de la Caisse nationale d’assurance vieillesse. Sollicité par Le Parisien et d’autres médias, le ministère “ne confirme pas” cette étendue — sans l’infirmer. Selon ces pirates, des données concernant victimes, témoins, criminels et particuliers seraient mêlées dans une fuite massive.

Dans leurs messages successifs, les hackers affirment avoir

examiné pendant plusieurs semaines les boîtes mail d'enquêteurs de la Police nationale et de la Gendarmerie, ce qui leur aurait permis d'exfiltrer "suffisamment de données" avant d'être repérés. "La vérité que nous pourrions révéler sur l'ampleur réelle de cette fuite – qui touche à la fois les criminels et les victimes – choquerait la France et compromettrait gravement de nombreuses personnes", écrivent-ils.

Le spécialiste en cybersécurité Clément Domingo, alias SaxX, estime que la vente ou la publication des informations piratées serait "critique" et que cette fuite "mettrait la sécurité nationale en péril". L'enquête a été confiée à l'Office anticybercriminalité (OFAC). Les pirates menacent encore de vendre les données ou de les diffuser intégralement, un scénario qu'ils qualifient d'"impact sans précédent pour la France".

Journaldugeek

> *Piratage Ministère de l'Intérieur : nouveau message des cybercriminels hier nuit…*
>
> *3 points à retenir :*
>
> *Les Shiny Hunters -ce groupe de 5 jeunes adolescents arrêté par la France en juin 2025- se désolidarisent de ce groupe cybercriminel qui revendique la… https://t.co/bp7s6js47r pic.twitter.com/D16ylDYXAv*
>
> *— SaxX ¯_()_/¯ (@_SaxX_) December 16, 2025*

> *SCANDALE D'ÉTAT – Le ministère de l'Intérieur a été la cible d'une cyberattaque et les données du Traitement des antécédents judiciaires auraient été dérobées. C'est GRAVISSIME*
>
> *Vendredi matin, Laurent Nuñez affirmait tranquillement sur*

RTL qu’un assaillant avait pu… pic.twitter.com/R9liX4IOAO

— Ilan Gabet (@Ilangabet) December 15, 2025

Laurent Nunez indique avoir « décidé de renforcer ses mesures de cybersécurité, notamment par l’analyse proactive des serveurs et des boîtes de messagerie [et] la mise en œuvre systématique de la double authentification ».

DONC LA DOUBLE AUTHENTIFICATION N’ÉTAIT PAS SYSTÉMATIQUE… pic.twitter.com/W66j9iapG1

— Ilan Gabet (@Ilangabet) December 16, 2025