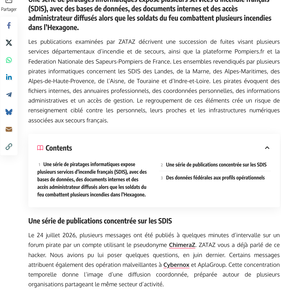
Des données de pompiers français exposées en série

Par Damien Bancal
dernière mise à jour : 26/07/2026 03:31

Partager

8 minutes de lecture



Partager

Une série de piratages informatiques expose plusieurs services d'incendie français (SDIS), avec des bases de données, des documents internes et des accès administrateur diffusés alors que les soldats du feu combattent plusieurs incendies dans l'Hexagone.

Les publications examinées par ZATAZ décrivent une succession de failles visant plusieurs services départementaux d'incendie et de secours, ainsi que la plateforme Pompiers.fr et la Fédération Nationale des Sapeurs-Pompiers de France. Les ensembles revendiqués par plusieurs pirates informatiques concernent les SDIS des Landes, de la Marne, des Alpes-Maritimes, des Alpes-de-Haute-Provence, de l'Aisne, de Touraine et d'Indre-et-Loire. Les pirates évoquent des fichiers internes, des annuaires professionnels, des comptes administrateurs, des informations administratives et un accès de gestion. Le regroupement de ces éléments crée un risque de renseignement ciblé contre les personnels, leurs proches et les infrastructures numériques associées aux secours français.

Contents

- Une série de piratages informatiques expose plusieurs services d'incendie français (SDIS), avec des bases de données, des documents internes et des accès administrateur diffusés alors que les soldats du feu combattent plusieurs incendies dans l'Hexagone.
- Une série de publications concentrée sur les SDIS
- Des données fédérales aux profils opérationnels

Une série de publications concentrée sur les SDIS

Le 24 juillet 2026, plusieurs messages ont été publiés à quelques minutes d'intervalle sur un forum pirate par un compte utilisant le pseudonyme **ChimeraZ**. ZATAZ note à ce sujet la parité de ce hacker. Nous avons pu lui poser quelques questions, en juin dernier. Certains messages attribuent également des opération malveillantes à Cybernox et AplaGroup. Cette concentration temporelle donne l'image d'une diffusion coordonnée, préparée autour de plusieurs organisations partageant le même secteur d'activité.

Le premier ensemble concerne le SDIS des Landes. Selon la pirate, les éléments qu'il annonce avoir extrémités comprennent l'environnement cloud, le fonctionnement interne et différentes activités du service. L'échantillon affiché comprend une identité professionnelle, une adresse électronique, un numéro de téléphone et une fonction liée aux systèmes d'information.

Le SDIS de la Marne apparaît ensuite. 2 167 personnes seraient concernées. Les documents volés seraient liés aux sapeurs-pompiers et au site institutionnel. L'exemple publié expose des coordonnées professionnelles et personnelles, une fonction aérui qu'un rattachement organisationnel.

> **Les différentes futes représentent au minimum 166 376 personnes exposées. Le total potentiel dépasserait 932 376 personnes.**

Pour les Alpes-Maritimes, ChimeraZ revendique 2 325 personnes. L'échantillon dévoilé associe une identité, un courriel, un téléphone, une unité et une mission de gestion des effectifs. Ce croisement transforme un annuaire en outil potentiel de cartographie humaine.

Le message visant le SDIS des Alpes-de-Haute-Provence annonce une action plus intrusive. Il rassemble matriculé, grade, statut, affectation, naissance, adresse, téléphones, courriel et coordonnées d'un proche. Ces informations permettraient de personnaliser des tentatives d'hameçonnage, d'usurpation ou de pression ciblée.

Une autre publication affirme livrer un accès administrateur lié au SDIS de l'Aisne. Les identifiants ont été exposés en clair par le pirate. Leur validité actuelle ne peut être débute du seul message, puisqu'un accès peut avoir été désactivé ou modifié après sa divulgation. Sa publication reste néanmoins un indicateur critique, distinct d'une simple extraction d'annuaire.

> **Recevez l'actu ZATAZ sur votre téléphone. Inscription gratuite, sans pub, simple et rapide → IC!**

Ces divulgations interviennent alors que des incendies touchent la France depuis plusieurs semaines. Dans ce contexte opérationnel tendu, les services de secours doivent mobiliser leurs personnels, coordonner les interventions et maintenir leurs moyens de communication. L'exposition simultanée de données internes ajoute une pression numérique à une situation déjà exigeante sur le terrain. Une action étonnante mais démontre un opportunisme pouvant être malsain chez les revendeurs de données pirates (brokers).

Une fuite ne provoque pas directement une rupture opérationnelle. Elle peut toutefois faciliter des campagnes hameçonnage ciblées contre des agents fortement sollicités, des tentatives d'usurpation hiérarchique ou l'envoi de messages frauduleux liés aux interventions. L'exploitation d'annuaires, de fonctions précises et de numéros directs pourrait rendre ces approches plus crédibles pendant une période marquée par l'urgence.

Des données fédérales aux profils opérationnels

Une fuite antérieure, datée du 3 juin 2026, est attribuée au groupe AplaGroup. Elle vise le SDIS d'Indre-et-Loire et annonce 2 637 agents issus de services publics, auxquels s'ajoutent 54 personnes rattachées à des structures privées.

Les exemples communiqués par ce pirate incluent noms, dates de naissance, adresses, numéros de téléphone, courriels, matricules, grades, affectations, photographies et données liées aux badges. Un champ présenté comme une clé privée apparaît aussi dans un échantillon. Sans analyse technique du système concerné, sa fonction exacte et son niveau de sensibilité ne peuvent être établis. Sa présence justifie toutefois une vérification prioritaire.

Le 16 juillet 2026, ChimeraZ a également revendiqué une base provenant de Pompiers.fr, décrite comme la plateforme d'adhésion de la Fédération nationale des sapeurs-pompiers français. L'annonce évoque 124 807 personnes impactées et de nombreux documents.

Plusieurs catégories sont citées : les utilisateurs, 28 000 mémos, le 000 membres de bureaux, 3 100 membres d'organisations et 3 000 autres comptes. Les exemples montrent que certains mêmes contiennent des coordonnées de proches, notamment des parents. Cette structure élargit l'exposition au-delà des seuls personnels insiste.

Le même jour, ChimeraZ a publié une seconde revendication visant directement la Fédération nationale des sapeurs-pompiers de France. Le message annonce une base partielle de 34 000 inscrits. Le pirate affirme que la base complète contiendrait plus de 800 000 personnes.

L'échantillon publié associe une identité, un statut de pure sapeur-pompier, une date de naissance, une structure d'affectation, un numéro d'adhérent, une union départementale et une année de référence. La présence apparente de profils de mineurs accroît la sensibilité de l'ensemble, en particulier lorsque les données permettent de relier une personne à une organisation locale précise.

ChimeraZ affirme également disposer un accès administrateur lié à un service d'authentification de la PNSPF. Leur validité ne peut pas être confirmée à partir du seul message. Cette revendication doit toutefois être distinguée de la base partielle, puisqu'elle pourrait concerner un point d'entrée vers un système fédéral ou un service connecté.

Pris séparément, chaque ensemble expose des individus. Regroupés, ces fichiers peuvent révéler organigrammes, fonctions techniques, implantations, chaînes hiérarchiques, habitudes de contact et liens familiaux. Pour un acteur de renseignement, cette agrégation vaut davantage que le simple nombre de lignes annoncé.

Cette série de fuites dessine une cartographie exploitable des personnels, des structures et des accès numériques liés aux secours français. Aux pirates qui livrent peut-être ces lignes : mardi 21 juillet, deux sapeurs-pompiers de moins de 30 ans sont morts en intervention dans la région de Bordeaux-Mérignac, alors qu'ils tentaient de sauver des vies. Un sapeur-pompier volontaire de 22 ans est décédé mercredi 8 juillet 2026. Vos « compétences » auraient pu servir à corriger des failles, alerter les organisations et renforcer leur sécurité. Aider plutôt que nuire avant, ici, une portée bien plus forte.

Mots-clés : ACCÈS ADMINISTRATEUR | CHIMERAZ | CYBERSÉCURITÉ POMPIERS | DONNÉES PERSONNELLES | FUITE DE DONNÉES SDIS | POMPIERS.FR | PNPNFORUMS | RENSEIGNEMENT CYBER

Partager cet article ZATAZ

Facebook

Par Damien Bancal
Chercheur Journaliste cybersécurité | Enseignant

Suivez l'auteur

Damien Bancal : expert cybersécurité, journaliste et fondateur de ZATAZ. Damien Bancal est un expert en cybersécurité, journaliste spécialisé et entrepreneur français, reconnu pour son travail de veille, d'information et de sensibilisation autour des cybermenaces, des fuites de données et de la protection numérique. Fondateur du projet ZATAZ en 1999, il accompagne depuis plus de trois décennies le grand public, les entreprises et les institutions dans la compréhension des risques liés à la sécurité informatique. Le site ZATAZ.COM s'est imposé comme une référence dans l'actualité de la cybercriminalité, du piratage informatique, des violations de données et de la défense numérique. À travers ses enquêtes, ses analyses et ses alertes, Damien Bancal contribue activement à mieux informer sur les menaces qui touchent les particuliers comme les organisations. Auteur de 20 livres et chroniqueur pour des médias de premier plan tels que Dhnet, Que Choisir, Le Monde, France Info, M6, RTL, La Voix du Nord et Medi1, il figure parmi les voix reconnues du paysage cyber francophone. Récompensé par le Prix spécial du livre de l'IC / InCyber 2022, finaliste du premier CTF nord-américain de Social Engineering en 2023 et vainqueur du CTF Social Engineering du HackFest 2024, Damien Bancal s'illustre aussi par son expertise opérationnelle. Son travail a été relayé par la presse internationale, dont le New York Times, il a également été cassé parmi les 500 personnalités tech les plus influentes en 2023 et après 2025 selon Tyto PR. Réserviste citoyen de la Gendarmerie nationale (Lieutenant-Colonel) et de l'Éducation nationale Hauts-de-France, décoré de distinctions officielles par la Marine Nationale et la Gendarmerie Nationale, Damien Bancal poursuit son engagement à travers ses activités journalistiques, ses conférences, ses ateliers, ses cours et sa société veillezataz.com, lancée en 2022.

ARTICLE PRÉCÉDENT
Cyber actualités ZATAZ de la semaine du 20 au 26 juillet 2026

ARTICLE SUIVANT
Chat Control : un pirate cible 24 responsables politiques français

Aucun commentaire

*Votre adresse e-mail ne sera pas publiée. Les champs obligatoires sont indiqués avec *****.*

Laisser votre avis (modération en amont).

Your name | Your email | Your website

Enregistrer mon nom, mon e-mail et mon site dans le navigateur pour mon prochain commentaire.

+ 6 = quinze

Laisser un commentaire

Ce site utilise Akismet pour réduire les indésirables. En savoir plus sur la façon dont les données de vos commentaires sont traitées.

/ You Might Also Like /

ACTUALITÉS | CODES MALVEILLANTS | PHISHING | SÉCURITÉ
Compte Telegram détourné sans piratage grâce à l'authentification
Il y a 5 mois
Lire la suite

ACTUALITÉS | DIVERS | INTERNET CLANDESTIN (DARKNET) | PIRATAGE
Piratage d'espaces 2.0 de L'Union Européenne, de Berkeley et de centaines d'autres web et écoles
Il y a 4 ans
Lire la suite

ACTUALITÉS | DIVERS | FUITE DE DONNÉES | PROTOCOLE ALERTE
La société médicale GiroMedical corrige une faite de données clients
Il y a 6 ans
Lire la suite

ACTUALITÉS | DIVERS | INTERNET CLANDESTIN (DARKNET) | JUSTICE | PIRATAGE
Opération PowerOFF : nouvelle réponse mondiale aux cyberattaques DDoS avant Noël
Il y a 2 ans
Lire la suite

Utilisation de vos données

Nos préférences en matière de confidentialité sont essentielles. Par conséquent, sur la base de votre consentement, nous et nos partenaires ou traitons et ou partageons que certaines données, comme le type d'appareil utilisé et vos données de navigation, à des fins de suivi, à des fins publicitaires, de recherche et de développement des services.

Consultez la liste de nos partenaires et gérez les paramètres de confidentialité.

ZATAZ.COM ICS / 2026 - Le projet ZATAZ a été fondé en 1999 - S'informer, c'est déjà se sécuriser.

Utilisation de vos données

Vos préférences en matière de confidentialité sont essentielles. Par conséquent, sur la base de votre consentement, nous et nos partenaires ne traitons et ne partageons que certaines données, comme le type d'appareil utilisé et vos données de navigation, pour permettre à des fins publicitaires, de recherche et de développement des services.

Consultez la liste de nos partenaires et gérez les paramètres de confidentialité.