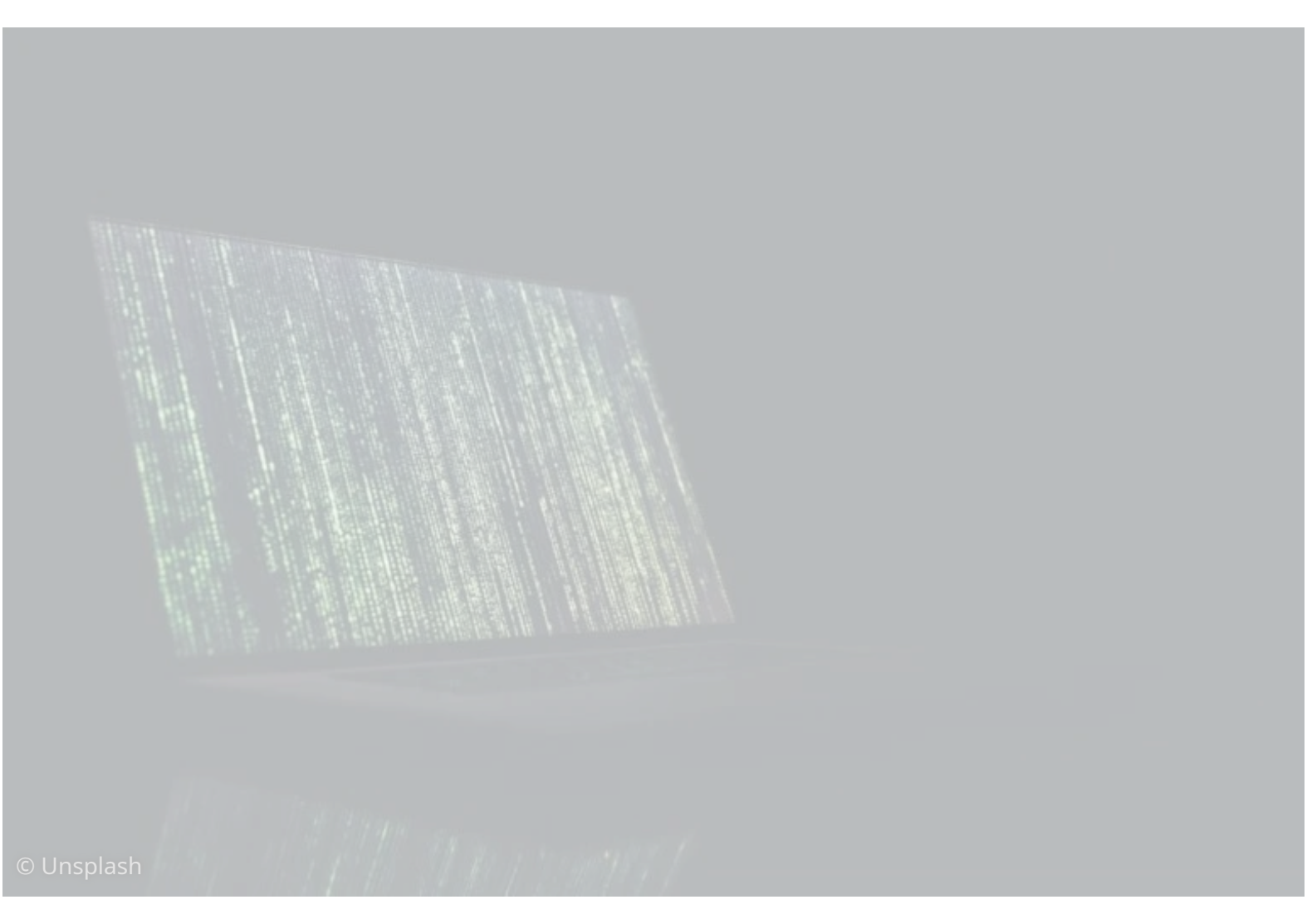
1 milliard de données sensibles exposées sur Internet par une plateforme de vérification d'identité négligente

Publié le 19 février 2026 à 13:13


© Unsplash

Une base de données appartenant à IDMerit, spécialiste de la vérification d'identité (KYC) pour les banques et les fintechs, a été exposée sur Internet sans aucune protection. Un milliard de fiches personnelles sensibles s'est retrouvé à la merci des cybercriminels. C'est un véritable kit d'usurpation d'identité pour les pirates, alertent les chercheurs.

L'équipe de recherche de Cybernews a découvert une nouvelle base de données exposée sur Internet sans la moindre sécurité. Dénichée en novembre, cette instance MongoDB, à savoir une base de données NoSQL open source, ne dispose d'aucune protection. Il n'est pas nécessaire de s'identifier et de rentrer un mot de passe pour accéder aux informations stockées sur l'instance.

Selon les investigations menées par Cybernews, l'instance appartient à **IDMerit**, un spécialiste de la vérification d'identité pour les banques, les fintechs et les services financiers. Au sein de la base de données, on trouve une montagne d'informations récoltées dans le cadre de procédures de Know Your Customer (KYC).). Principalement utilisé dans les secteurs financiers et bancaires, le KYC sert à vérifier l'identité des internautes. Son objectif premier est de prévenir les activités illégales, comme le blanchiment d'argent, la fraude ou le financement du terrorisme. Un formulaire KYC est obligatoire pour de nombreuses entités financières, telles que les plateformes de cryptomonnaies.

À lire aussi : Les données de 1,2 million de comptes bancaires français ont été piratées

Un milliard de données sensibles exposées sur Internet

Le répertoire pèse près d'un téraoctet et totalise environ **3 milliards d'enregistrements**, dont un milliard de fiches contenant des données personnelles sensibles. On y trouve aussi des informations techniques moins sensibles, comme des logs, ces fichiers qui enregistrent tout ce qu'il s'est passé sur un système. Ils peuvent comprendre des horodatages, des adresses IP ou encore la description des événements.

Ce sont surtout les données personnelles compromises qui inquiètent les chercheurs. Parmi les informations exposées, et qui étaient entre les mains d'IDMerit, on trouve le nom complet, l'adresse postale, le code postal, la date de naissance, le numéro d'identification national, le numéro de téléphone, l'adresse e-mail, le genre, les métadonnées de télécommunications, et tous les profils de réseaux sociaux. Le répertoire comprenait aussi un identifiant interne qui indique si la donnée provient elle-même d'une fuite de données antérieure, ou si son profil a été enrichi à partir d'une base déjà compromise. En clair, il apparaît qu'IDMerit (ou un prestataire) aurait **croisé ses données KYC** avec des bases d'informations issues d'autres violations pour enrichir les profils de ses clients.

À lire aussi : Fuite de données en France – 40,3 millions de comptes français piratés en 2025, le cauchemar continue

Un vrai « kit d'usurpation d'identité »

C'est une véritable mine d'or pour les cybercriminels, surtout pour ceux qui orchestrent des arnaques en ligne et des attaques de phishing. Les chercheurs parlent d'un véritable *« kit d'usurpation d'identité clé en main »* qui permet par exemple d'ouvrir un crédit à votre nom ou de détourner vos comptes en ligne.

Les investigations révèlent que les données concernent des individus en provenance du monde entier. Les victimes sont réparties dans **26 pays différents**. Les États-Unis arrivent en tête, avec plus de 203 millions d'enregistrements, suivis du Mexique (124 millions) et des Philippines (72 millions). En Europe, l'Allemagne, l'Italie et la France sont particulièrement touchées, avec chacune plus de 50 millions de fiches exposées.

Dans la foulée de leur triste découverte, les chercheurs sont entrés en contact avec IDMerit. Alertée par les chercheurs, l'entreprise a pris toutes les mesures nécessaires pour sécuriser les données en sa possession. L'accès public est fermé, mettant un terme à la fuite d'informations. Par prudence, Cybernews a publié les résultats de ses recherches des mois plus tard, en février 2026. Les experts expliquent ne **pas avoir trouvé de preuve d'exploitation malveillante**. Les chercheurs rappellent qu'Internet est balayé en permanence par des bots qui traquent précisément ce type de bases ouvertes et mal sécurisées. Il est tout à fait possible que les données aient été aspirées par des cybercriminels.

Les personnes dont les données étaient détenues par IDMerit risquent de se retrouver dans le viseur des hackers. Parmi les clients d'IDMerit, on trouve énormément de banques, de fintechs et d'assureurs qui ne souhaitent pas afficher leurs sous-traitants de conformité. C'est pourquoi la liste des clients de l'entreprise américaine n'est pas publique.

> *« Du point de vue d'un attaquant, la base de données contient des identifiants à haut risque : de nombreuses régions incluent des numéros d'identification nationaux, des dates de naissance complètes et des données de contact, qui sont des ingrédients de choix pour le vol d'identité », souligne le rapport.*

Les prestataires KYC dans le viseur des cybercriminels

Ce n'est pas la première fois qu'un prestataire spécialisé dans la vérification d'identité met en danger les données en sa possession. Il y a quelques semaines, SumSub, une plateforme de vérification d'identité et de lutte contre la fraude, a été piratée, laissant des données personnelles entre les mains de cybercriminels.

Ces incidents illustrent à quel point la sécurité de la vérification d'identité en ligne est fragile. Les utilisateurs sont en effet obligés de confier leurs papiers, leur adresse et leur numéro de téléphone à une banque, une application de paiement ou une plateforme crypto, mais la sécurité de leurs données dépend ensuite d'une multitude de prestataires, tels que SumSub ou IDMerit.

Cette affaire souligne *« à quel point les fournisseurs d'identité tiers sont devenus une infrastructure essentielle et peuvent constituer des points de défaillance catastrophiques »*, explique Cybernews. Ces prestataires sont des cibles de choix pour les criminels au vu des données sensibles qui sont collectées.

Source : *Cybernews*

Florian Bayard

#ARNAQUE BANCAIRE #CYBERATTAQUE #FUITE DE DONNÉES #KYC #VOL DE DONNÉES

Sur le même sujet

Énième fuite de données en France : le syndicat CFDT a été piraté, les informations des adhérents volées

Les données de 1,2 million de comptes bancaires français ont été piratées

Cyberattaques chinoises : des espions ont exploité une faille Dell sans se faire remarquer pendant 18 mois

Meilleur antivirus 2026 : quel est le meilleur choix ?

Quel est le meilleur VPN ?

Comparatif des meilleurs stockages cloud en 2026 : lequel choisir ?

Comment accéder au Dark Web ? Tutoriel en 3 étapes

Meilleur gestionnaire de mots de passe 2026, le comparatif

Meilleur VPN gratuit : 7 services à choisir + 2 à fuir

Les dernières actualités

Gemini 3.1 Pro : Google déploie un modèle plus à l'aise avec les problèmes complexes

Pour « sauver » les Européens de la « censure » de Bruxelles, l'administration Trump développerait un portail VPN

YouTube teste un bouton Gemini pour « discuter » avec les vidéos

La PS5 à 149 euros pour toute souscription à cette offre Bbox chez Bouygues

« Ces tâches seront automatisées par une IA » : Microsoft annonce la fin de plusieurs métiers d'ici 18 mois

Mauvaise nouvelle chez Free qui augmente le prix de son forfait Série Free

LES TESTS À LA UNE

Welcome

We and our 262 **partners** wish to store and access information on your devices (such as cookies and pixels), and collect personal data on this site to process it along with both known and future information (such as identifiers, browsing history, preferences, purchases, phone number, postal, IP and email addresses, precise geolocation, etc.).

This is used to develop and provide you with services, content, commercial offers, and advertisements across your various devices and screens (including by email, mail, texts, phone, audio, and video), to personalize and measure them, and to conduct audience research and analysis.

You can "accept all" and withdraw your consent at any time via the "cookies" footer link. You can also "set detailed preferences" to object to more limited processing activities. These choices remain valid for 6 months.

powered by Sirdata

Set your choices

Accept all