MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »
Commandement du ministère de l'Intérieur dans le cyberespace

Revue de presse des cybermenaces

Centre d'analyse des cybermenaces

#02 – Février 2026

A retenir

Le mois de janvier met en évidence des cybermenaces toujours plus diffuses et structurées. Plusieurs **organismes français** (OFII, France Éducation international, La Poste, FFT) ont été touchés, exposant des **millions de données personnelles**, souvent *via* des **prestataires compromis**. La réponse pénale se renforce : la **BL2C a interpellé** à Aubervilliers un jeune de 18 ans, soupçonné d'avoir volé et revendu les données d'un million d'adhérents de la **FFT**. Le Tribunal judiciaire de Paris a **condamné** un **informaticien** de 27 ans à **30 mois de prison (dont six fermes)** pour une cyberattaque contre **Hospi Grand Ouest**.

Chiffres du mois

1,15 milliard d'euros, il s'agit du total des **amendes RGPD** infligées par les autorités européennes en 2025. Plus de **330 sanctions** visant surtout le traitement des données, notamment dans les médias et télécoms. Surfshark

282 millions de dollars de cryptoactifs ont été **dérobés** le 10 janvier 2026 à une personne victime d'escroquerie. L'attaquant aurait usurpé l'identité d'un service légitime pour prendre le contrôle du portefeuille. Il a ensuite changé les fonds dans d'autres cryptoactifs, notamment en **monero** (XMR). Cryptoast

Principales cyberattaques

Le 1er janvier 2026, **La Poste** a subi une nouvelle cyberattaque perturbant l'**accès à plusieurs services en ligne**, dont le suivi des colis, le coffre-fort numérique **Digiposte** et les paiements *via* l'application de La Banque Postale. L'attaque ne semble pas avoir affecté les transactions par carte ou les retraits d'espèces. L'incident survient quelques jours après une attaque *DDoS* revendiquée par le groupe hacktiviste pro-russe *NoName057(16)* pendant les fêtes de Noël. Cette nouvelle attaque n'a cependant **pas encore été revendiquée**. Usine Digitale

L'**Office français de l'immigration et de l'intégration** a fait l'objet d'un **vol de fichiers** comprenant deux millions de lignes de données personnelles (notamment des identités, des coordonnées complètes et des motifs de séjour en France). Ces données sont récentes et ont été mises en vente sur un **forum** cybercriminel le 1er janvier 2026. L'auteur de l'annonce a diffusé un **échantillon** en guise de preuve. Selon l'OFII, les informations auraient été dérobées à la suite de la **compromission d'un prestataire externe**. 01Net

La société **Ledger**, spécialisée dans la sécurisation des cryptoactifs, a subi un incident similaire. Son **prestataire, Global-e** a été touché par un incident de sécurité, et des attaquants ont ainsi pu accéder à des données personnelles de clients de la plateforme Ledger. Parmi les données dérobées figurent des identités, des coordonnées et des informations sur leur commande. Ces informations pourraient permettre des attaques par **hameçonnage ciblé**, voire des **atteintes physiques** sur des détenteurs de cryptoactifs. Ledger 01Net

Entre le 9 et le 12 janvier 2026, la **plateforme GAEL** de l'établissement France Éducation international a été piratée à partir de deux comptes compromis. L'attaque a exposé les données personnelles de **5 millions de candidats** aux diplômes DELF-DALF : état civil, coordonnées complètes, ville et pays de naissance, ainsi que langue maternelle. L'**accès au service a été suspendu** pour sécuriser les données archivées depuis 2005. France Éducation international

La **Fédération française de tennis** (FFT) déclare avoir été victime d'une compromission ayant entraîné la consultation par les attaquants de certaines données personnelles (nom, prénom, coordonnées, type de licence) des licenciés. La FFT a informé la CNIL et l'ANSSI, et a déposé plainte. FFT

Check Point analyse une vague d'attaques ciblant les **projets liés aux cryptoactifs**. Le maliciel ***GoBruteForcer*** a exploité un réseau de **50 000 serveurs** Linux compromis pour scanner des plages d'adresses IP et tenter de se connecter en forçant des identifiants faibles ou générés par défaut avec un LLM. Check Point Bleeping Computer

Pour aller plus loin…

[Chambre du commerce et de l'industrie] « Le baromètre des dirigeants français 2026 » - D'après l'étude, 80 % des dirigeants interrogés ne considèrent pas le risque cyber comme un risque majeur, ce qui soulève des interrogations quant à une éventuelle sous-évaluation de ce risque dans un contexte de conflits hybrides.

[Elastic Security Labs] « Global Threat Report » - Les résultats de l'étude montrent une augmentation significative des logiciels malveillants destinés à voler des informations, avec plus de 25 % des malwares détectés. Ces données sont ensuite fournies à des réseaux d'intermédiaires spécialisés dans la vente d'accès.

Faits marquants

Un homme de 18 ans, résidant à Aubervilliers, a été **interpellé** le 6 janvier 2026 par la **Brigade de lutte contre la cybercriminalité** (BL2C). Il est soupçonné d'avoir participé au **vol de données** et à la **revente** de près d'un million d'adhérents de la **FFTir**. L'intrusion serait survenue entre les 18 et 19 octobre 2025. Ces informations, diffusées sur Telegram et sur des forums cybercriminels, ont servi à commettre une **série d'agressions et de vols d'armes à feu** en France, notamment à Limoges, Nice et Paris. L'enquête se poursuit pour identifier les autres membres du réseau et les acheteurs de ces données. FranceInfo Liberation

Ce 12 janvier, un informaticien de 27 ans a été **condamné** à 30 mois d'emprisonnement (dont six mois fermes) par le Tribunal judiciaire de Paris. Il était poursuivi pour la **cyberattaque** menée en octobre 2024 contre son employeur, **Hospi Grand Ouest**, groupe mutualiste gérant onze établissements de santé dans l'ouest de la France. Le Télégramme Ouest France

Informations sur la menace

Des chercheurs de la société de cybersécurité *Resecurity* ont attiré des membres du groupe cybercriminel ***Scattered Lapsus$ Hunters*** dans un ***honeypot*** (ou pot de miel). Il s'agit d'un système informatique leurre, conçu pour reproduire de fausses données sensibles et attirer les acteurs malveillants, dans le but d'étudier leurs méthodes et de les identifier. En utilisant de **fausses données**, les chercheurs ont incité les cybercriminels à révéler des informations sur leurs serveurs, leur permettant de documenter plus de 188 000 requêtes et d'**identifier des adresses IP** liées à leurs infrastructures. Les données recueillies ont été **transmises aux autorités** pour faciliter une enquête judiciaire. Security Week

Le groupe de rançongiciel ***LockBit 5.0*** marque son retour dans la sphère cybercriminelle en décembre 2025 en revendiquant plus de **110 attaques** sur son blog. Cependant, ce constat est **à nuancer**. Plusieurs dizaines d'entités s'avèrent être des victimes déjà ciblées sous *LockBit 3.0* voire d'autres groupes de rançongiciels tels que *Qilin*, *TheGentlemen*, *RaLord*, etc. **Seules 48 revendications apparaissent inédites**. Des annonces ont été retirées du blog de *LockBit*, supposant d'éventuels paiements de rançon. De plus, l'analyse des données montre que la majorité des incidents remontent en réalité à l'été et à l'automne 2025. LeMagIT

Une campagne d'attaque de type ***clickfix*** cible le secteur de l'**hôtellerie-restauration** en Europe via des postes utilisant le système d'exploitation Windows. Les établissements visés reçoivent un **courriel piégé** provenant du site d'hébergement booking.com, **relatif à une annulation de réservation**. Le montant exigé est élevé afin d'inciter la victime à cliquer sur le lien. Cette action provoque un affichage bleu typique d'un dysfonctionnement du système d'exploitation Windows (aussi appelé « écran bleu de la mort »). Ce faux affichage propose alors des manipulations à réaliser par la victime afin de rétablir le système, alors qu'un maliciel est installé. Celui-ci permet d'enregistrer les fenêtres s'affichant sur l'écran, de rechercher des mots de passe, des données clients, ou de tenter de se latéraliser sur le réseau de l'établissement. Securonix 01Net

Une nouvelle campagne exploitant le *malware* **GlassWorm** cible les utilisateurs de **macOS** et vise leurs **cryptoactifs**. Les attaquants distribuent des **versions compromises d'applications légitimes** pour dérober les actifs numériques. Cette campagne souligne l'intérêt croissant des cybercriminels pour l'écosystème Apple, traditionnellement jugé plus sûr, en exploitant la confiance des utilisateurs envers leurs outils de gestion de crypto-actifs. Bleeping Computer

Depuis le 12 janvier 2026, la plateforme ***Penguin*** industrialise les escroqueries à la fausse romance. Cette technique consiste à mettre la victime en confiance lors d'une **relation sentimentale fictive** pour l'inciter à investir massivement avant de disparaître. *Penguin* fournit des **kits prêts à l'emploi**, permettant à des cybercriminels peu qualifiés de mener ces **fraudes à grande échelle**. GBHackers

Anticipation / Réglementation

La Commission nationale de l'informatique et des libertés (**CNIL**) a publié, le 16 janvier 2026, une recommandation sur le **consentement** dit « **multi-terminaux** » dans la publicité en ligne. En effet, les usages numériques reposent aujourd'hui sur de plus en plus de comptes utilisateurs qui sont accessibles depuis plusieurs appareils (ordinateur, smartphone, tablette, télévision connectée, etc.).

Cette diversité entraîne une multiplication des demandes de consentement aux **cookies**. Désormais, lorsqu'un utilisateur est connecté à son compte, son choix concernant les cookies peut s'appliquer à **l'ensemble de ses appareils**. CNIL