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

#03 – Mars 2026

A retenir

Tant par leurs enjeux financiers, les techniques mises en oeuvre, que l'évolution constante des acteurs malveillants, les **cybermenaces ont continué de marquer l'actualité** au cours du mois de février 2026.

Les **fuites de données** occupent une place centrale, ciblant des institutions en France et au Mexique, au-delà des sociétés privées (télécommunications, défense...).

L'évolution des **groupes de rançongiciel**, les attaques sophistiquées par la **chaîne logistique** et les enjeux liés aux **cryptoactifs** marquent également l'actualité.

Chiffres du mois

900 millions. C'est le montant (en dollars) payé en 2025 à la suite d'attaques par rançongiciel. Malgré une hausse de 50 % des attaques entre 2024 et 2025. On observe une baisse continue de ce montant, qui était de 1,2 milliard en 2023. Chainalysis

1,8 million. C'est le montant en dollars perdu à la suite d'une erreur de configuration d'un *smart contract* (concernant le prix de l'ether) sur le protocole de finance décentralisé Moonwell. Le paramétrage avait été généré par l'outil IA Claude Opus 4.6. Cybernews

Principales cyberattaques

Le **10 février 2026**, l'acteur malveillant *Spirigatito* revendique sur *BreachForums* la possession de données attribuées à **Safran**, avant de les rendre publiques une semaine plus tard. Il demeure impossible de confirmer leur authenticité ou leur lien avec l'incident évoqué par Safran : deux jours après, la société a précisé qu'une fuite de données avait bien eu lieu, mais était liée à un accident chez un fournisseur tiers, démentant toute compromission. L'Usine Digitale

Le **19 février**, le ministère de l'Économie a annoncé que les données associées à 1,2 million de comptes bancaires ont été siphonnées par un acteur malveillant. Ce dernier est parvenu à s'introduire dans le **fichier des comptes bancaires (FICOBA)** grâce aux authentifiants compromis d'un fonctionnaire « disposant d'accès dans le cadre de l'échange d'informations entre ministères ». ZDNet

Une **campagne d'attaque sur la chaîne logistique** des développeurs combine stéganographie et typosquatting : les attaquants sont capables d'activer des **chevaux de troie d'accès à distance** (*Remote Access Trojans* ou RAT) **à partir d'images PNG déployées depuis un paquet logiciel NPM malveillant**. L'écosystème *Node Package Manager* (NPM) regroupe certaines des bibliothèques JavaScript les plus utilisées. GB Hackers

Entre décembre 2025 et janvier 2026, l'**agent conversationnel Claude Opus aurait été détourné** pour dérober plus de 150 Go de données fiscales et d'état-civil gérées par les autorités mexicaines. L'outil IA de la société *Anthropic* aurait permis de trouver des vulnérabilités dans les réseaux publics, de rédiger des scripts pour les exploiter, et d'automatiser le vol de données. Bloomberg

Dans un communiqué publié **mercredi 25 février**, l'**Olympique de Marseille** dit avoir été ciblé par une **intrusion dans ses systèmes d'information**. Le club de football a également précisé renouveler l'ensemble des billets vendus avant la cyberattaque et signaler cette intrusion à la CNIL, avant de porter plainte. L'Équipe

L'**opérateur téléphonique néerlandais ODIDO** a subi une **exfiltration de données personnelles relatives à plus de 6 millions de ses clients**, dont des numéros de téléphone, des adresses postales et des IBAN. L'intrusion à l'origine de la compromission des systèmes d'information aurait été détectée au début du mois de février. Solutions Numériques

Pour aller plus loin...

[CYFIRMA] « *Energy and utilities Q1 : industry report* » analyse des cybermenaces observées dans les secteurs de l'énergie et du service public sur les trois derniers mois. Le rapport souligne une **hausse marquée des campagnes APT (43 % des attaques observées, contre 13 % précédemment)**, principalement attribuées à des acteurs chinois et russes, ainsi qu'une **recrudescence des rançongiciels (+64 % de victimes**, avec une diversification géographique notable).

[Allianz Risk] Selon le dernier baromètre publié par l'assureur Allianz, **les cyberattaques représentent la première menace pour les entreprises**. L'étude concerne 97 pays, avec 338 experts interrogés sur leur cartographie des risques cyber.

[OpenAI] Escroqueries à la fausse romance, usurpations d'identité de services financiers, opérations d'influence, vols de données... : dans un rapport publié le 25 février, **OpenAI documente les détournements dans l'utilisation de son agent conversationnel ChatGPT**. La société spécialisée dans l'IA annonce en outre avoir suspendu plusieurs comptes liés aux autorités chinoises, suspectés de conduire des opérations d'influence avec l'IA.

Le fait marquant

Dans un communiqué de presse publié le 18 février, **INTERPOL** revient sur **l'opération Red Card 2.0**. Celle-ci a été menée avec les autorités britanniques et les Etats suivants : Angola, Bénin, Cameroun, Côte d'Ivoire, Tchad, Gabon, Gambie, Ghana, Kenya, Namibie, Nigeria, Rwanda, Sénégal, Ouganda, Zambie et Zimbabwe. Menée du 8 décembre 2025 au 30 janvier 2026, elle ciblait les **réseaux criminels africains commettant des escroqueries à l'investissement**, aux paiements mobiles et aux applications de prêt en ligne. **651 personnes ont été arrêtées et 4,3 millions de dollars ont été saisis, ainsi que 2 341 terminaux**. Interpol

Informations sur la menace

Dans une publication du 2 février, **Notepad++** revient sur un incident de sécurité ayant compromis ces logiciels entre juin et décembre 2025 : des paquets binaires malveillants auraient pu **infecter les clients via le mécanisme de mises à jour automatiques**. La société suspecte un Etat étranger d'avoir parrainé les attaquants et recommande de mettre à jour le logiciel à la version v8.9.1 Notepad++

Depuis fin 2025, une campagne mondiale d'espionnage cyber, baptisée **« *Shadow Campaigns* »**, cible massivement les **administrations** (ministères des finances, sécurité intérieure…) et **infrastructures critiques.** Attribuée à un groupe asiatique (TGR-STA-1030), cette opération a compromis des entités gouvernementales dans 37 pays et mené des reconnaissances actives sur des infrastructures de 155 États. Les techniques employées (hameçonnage ciblé, exploitation de vulnérabilités) révèlent une sophistication technique élevée. Palo Alto

La **saisie par les autorités fin janvier du forum RAMP**, plateforme majeure pour les cybercriminels spécialisés en rançongiciels, a provoqué des perturbations dans la sphère clandestine. **Prodaft, société de cybersécurité, a récupéré des données sur 7 709 utilisateurs**, incluant messages privés, fichiers échangés, historiques de recherche et informations de connexion. L'initiative vise à **éclaircir des enquêtes jusqu'alors non résolues**, tandis que certains membres du forum collaborent volontairement, accentuant l'anxiété au sein de la communauté criminelle. Le Mag IT

En **janvier 2026**, le groupe de **rançongiciel *0APT*** a émergé en revendiquant plus de **200 victimes en quelques jours**, dont des organisations de haut niveau. Halcyon et GuidePoint révèlent de nombreuses incohérences (noms d'entreprises génériques, fichiers vides, absence de communication directe avec les victimes, disparition plusieurs semaines puis réapparition avec une liste réduite de cibles…). ***0APT* se prévaudrait d'attaques fictives pour extorquer des victimes mal informées, réextorquer d'anciennes cibles, ou attirer des affiliés**. Il n'aurait pas démontré de capacité réelle à chiffrer ou à exfiltrer des données. Halcyon GuidePoint

Identifié en décembre 2023, **Dragonforce** a rapidement évolué vers un modèle d'affiliation (RaaS). Combinant **héritage technique** (codes de *LockBit* et *Conti*) et **innovation continue** (plateforme RansomBay), il constitue une menace majeure dans l'écosystème du rançongiciel. Avec 363 victimes revendiquées, dont une majorité depuis 2025, le groupe se positionne comme un **carrefour criminel multi-services** : génération de **payloads**, **gestion des victimes**, **diffusion de données**, et même **harcèlement téléphonique des cibles**. Sa stratégie repose à la fois sur la **collaboration** (*Qilin*, *Scattered Spider*) et **l'affrontement avec d'autres groupes malveillants** (*RansomHub*, *BlackLock*). GB Hackers

Un **ex-employé de Revolut** a utilisé ses anciens accès toujours valides pour récupérer les **données personnelles d'un client investisseur en cryptoactifs**. Il a ensuite contacté la victime et plusieurs membres de sa famille pour réclamer une **rançon en cryptoactifs** sous peine de divulgation de leurs informations personnelles. Une enquête interne a permis d'identifier le maître-chanteur et d'ouvrir une enquête judiciaire. 01Net

Un maliciel nommé **Keenadu** a été **inséré sur des milliers de téléphones** à leur sortie d'usine par un prestataire de la chaîne d'approvisionnement. Keenadu agit comme une **porte dérobée sur les systèmes Android**. Une fois installé, il télécharge des fichiers .apk qui octroient de multiples permissions non souhaitées. Ce maliciel **transforme notamment le smartphone infecté en bot cliquant sur des publicités, générant ainsi des revenus par rebond**. 01Net

Un ensemble de **30 extensions malveillantes du navigateur Chrome** ont été installées à plusieurs centaines de milliers de reprises. Ces extensions se présentent comme des **assistants IA permettant de dérober des authentifiants, des courriels et des données de navigation sur Internet**. Bleeping Computer

Anticipation / Réglementation

L'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** met à jour sa **politique open source**, soulignant sa volonté de **promouvoir l'innovation technologique et la transparence**. Quatre grands axes sont abordés : la publication et la contribution à des logiciels en source ouverte, la structuration de l'écosystème et l'utilisation de ces logiciels par l'ANSSI. Source