MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Commandement du ministère de l'Intérieur dans le cyberespace

Revue de presse des cybermenaces

Centre d'analyse des cybermenaces

#04 – Avril 2026

A retenir

Ce mois est marqué par une **persistance des fuites de données massives** touchant aussi bien le secteur public que privé. La **finance décentralisée** reste une cible de choix. Les **techniques d'ingénierie sociale se sophistiquent**, mêlant **IA générative** et ***smishing***. Les **vulnérabilités *zero-day*** continuent d'alimenter l'écosystème de la surveillance commerciale.

En réponse, les autorités intensifient leurs efforts avec le déploiement du portail **17Cyber** et plusieurs **opérations judiciaires d'envergure** menées par **Europol**.

Chiffres du mois

373 000. C'est le nombre de noms de domaines associés à des contenus d'abus sexuels sur mineurs fermés à la suite d'une opération conjointe de 23 pays (dont la France), menée par Europol du 9 au 19 mars 2026. Europol

Le 10 mars, **10 938 cryptoactifs** représentant des ether sous-jacents (wstETH) ont fait l'objet d'une liquidation sur le réseau de finance décentralisée (DeFI) AAVE. En cause : une erreur dans la mise à jour d'un oracle censé empêcher la manipulation du prix des actifs. La perte s'élève à environ 28 millions USD. Rekt

Principales cyberattaques

En janvier 2026, la plateforme **Hubee** (gérée par la direction interministérielle du numérique) a été piratée, compromettant les données de **70 000 dossiers RSA** (160 000 documents). Les informations exposées (noms, numéros de sécurité sociale, coordonnées, dates de droits) peuvent servir à du ***phishing*** ou de l'**usurpation d'identité**. La CAF confirme que les **données bancaires et mots de passe ne sont pas touchés**, mais **appelle les allocataires à la vigilance**. La CNAF précise que son système n'a pas été piraté et informe individuellement les victimes, sans préciser leur nombre. Le Monde Informatique

L'équipementier **Michelin** confirme une **fuite de données** liée à l'exploitation d'une **faille *zero-day*** dans Oracle E-Business Suite. L'attaque, revendiquée par le groupe ***Cl0p*** (associé à *FIN11*), a conduit à la publication de plus de **315 Go de fichiers**. Michelin assure qu'aucune donnée sensible n'a été compromise et que ses systèmes mondiaux n'ont pas été affectés. Securityweek

Vivaticket a subi une attaque par **rançongiciel** revendiquée par ***RansomHouse***. Des données personnelles de visiteurs (identité, courriel, adresse, identifiants) ont été extraites. Parmi les partenaires concernés : le musée du **Louvre**, le musée **d'Orsay**, la **BNF**, **Notre-Dame de Paris** ou la **Tour Eiffel**. 01net

Une campagne d'hameçonnage contre la **Fédération Française de Rugby** a permis l'exfiltration de données de **530 000 licenciés (identité, numéro de licence, club, historique)**. Près d'un **million de photos de joueurs**, dont des mineurs, et **948 scans de cartes d'identité** figureraient parmi les données compromises. 01net

Le 22 mars, le protocole de finance décentralisé **Resolv** a subi une **perte de l'équivalent de 25 millions de dollars américains**. **Sans contrepartie équivalente** déposée en amont, un attaquant a généré **80 millions de cryptoactif USR** (un cryptoactif stable synthétique du dollar, censé être à parité avec ce dernier). Journal du Coin

Spécialisée en cybersécurité, la société **CodeWall** affirme s'être **introduite dans la plateforme IA du cabinet de conseil McKinsey**, nommée « **Lili** ». C'est l'agent IA de CodeWall qui aurait sélectionné McKinsey parmi plusieurs cibles, **accédant ensuite à 46,5 millions de messages, 728 000 documents, et à 70 000 comptes utilisateurs** de collaborateurs de la cible. Codewall

Pour aller plus loin…

[ANSSI] L'**ANSSI** dresse le **bilan 2025 des menaces**, soulignant l'**effacement des frontières entre cybercriminalité et opérations étatiques**, et appelant à une vigilance accrue face aux **menaces ciblées**.

[Google] « *Look What You Made Us Patch: 2025 Zero-Days in Review* » - L'analyse recense **90 failles *zero-day* exploitées en 2025**. Les **entreprises deviennent la cible principale (48 % des cas)**, tandis que les navigateurs voient leur exposition diminuer. États et acteurs commerciaux ciblent désormais **systèmes** et **équipements réseau**, révélant une évolution des stratégies d'intrusion.

[Snyk] Spécialisée en cybersécurité, la société **Snyk** analyse la **compromission de LiteLLM**. Cette bibliothèque Python populaire et utilisée par les grands modèles de langage (LLM) a subi une attaque par la chaine logistique le 19 mars. La campagne a été minutieusement préparée par le groupe cybercriminel ***PCPTeam***, en **substituant un logiciel malveillant aux paquets logiciels légitimes**.

TLP:CLEAR

Les faits marquants

Europol a démantelé *LeakBase*, un **forum cybercriminel**, comptant **142 000 utilisateurs et spécialisé dans le commerce de données piratées (mots de passe, identifiants)**. Actif depuis 2021, il proposait des fuites récentes ou anciennes, avec un système de crédits et de réputation pour renforcer la confiance entre criminels. Les 3 et 4 mars, une opération mondiale a conduit à des arrestations, des perquisitions et à la fermeture du site, remplacé par une page d'avertissement. **Europol a joué un rôle central, au côté de 14 pays, analysant des millions de données** pour identifier les suspects et relier les preuves numériques. L'opération, menée *via* le J-CAT, vise aussi à dissuader de futures activités illégales et à informer sur les risques de la cybercriminalité. Europol

Deux suspects, âgés de 17 et 20 ans, ont été arrêtés pour le piratage de l'OFII, impliquant la fuite de données administratives. L'un d'eux, actif sous le pseudo « ***marak*** » sur des forums cybercriminels, revendiquait la vente de plusieurs bases de données piratées (K-CHESS, ANPS, VERYCHIC, OTACOS, etc.). Mis en examen pour accès frauduleux et association de malfaiteurs, leur profil numérique révèle une activité intense depuis fin 2025. Mis en examen pour accès frauduleux, extraction de données et association de malfaiteurs, leur arrestation met en lumière l'ampleur de leurs activités illicites. FrenchBreaches

Informations sur la menace

Check Point a publié un rapport révélant plusieurs vulnérabilités dans **Claude Code**. Ces failles ont notamment permis l'**exécution de code à distance** et l'**exfiltration de clés API**. Les **fichiers de configuration de projet**, apparemment anodins, constituaient en réalité une **couche d'exécution exploitable**. Le simple clonage d'un dépôt malveillant pouvait suffire à déclencher l'attaque. Une première vulnérabilité (CVE-2025-59536, CVSS 4.0 : 8.7) permettait de contourner le consentement utilisateur dans le protocole MCP en initialisant des services sans autorisation préalable. Une seconde (CVE-2026-21852, CVSS 4.0 : 5.3) redirigeait le trafic API authentifié vers un serveur contrôlé par l'attaquant, exposant les clés dès l'ouverture du projet. Check Point

Les **campagnes d'arnaques par SMS** évoluent avec l'intégration d'**images générées par intelligence artificielle** pour renforcer leur crédibilité. Les attaquants utilisent ces visuels pour simuler des preuves (colis, documents, amendes) et inciter les victimes à cliquer sur des liens frauduleux. Cette combinaison de *smishing* et d'IA **augmente l'efficacité des tentatives d'hameçonnage et complique leur détection** par les utilisateurs. Numerama

Un virus de type **cleptogiciel** vendu sur les forums cybercriminels depuis décembre **vise** le navigateur **Google Chrome**. Nommé ***VoidStealer***, il permet de récupérer la **clé maîtresse v20_master_key** stockée dans le navigateur. Elle permet aux attaquants de déchiffrer l'ensemble des données protégées et d'accéder aux sessions actives des comptes de la victime, **sans même avoir besoin** d'**authentifiants** ou de **contournement** de la **MFA**. Le maliciel profite du court laps de temps lors duquel la clé maîtresse est stockée dans un registre du processeur pour l'intercepter et la copier dans sa propre mémoire, ce qui lui permet ensuite de déchiffrer les cookies et autres informations stockées dans le navigateur. 01net

Une **nouvelle technique d'escroquerie** visant les utilisateurs de la plateforme **Leboncoin** a été mise au jour. La victime reçoit un appel téléphonique depuis un numéro débutant par 09. Une **voix préenregistrée se faisant passer pour le service support** alerte que la messagerie Leboncoin de la victime est actuellement indisponible car elle serait bloquée par des spams. Cette dernière est alors invitée à contacter le service technique sur un numéro distinct. L'interlocuteur à ce numéro réclame alors la somme de 37€ pour débloquer la messagerie. Presse Citron

À partir d'avril 2026, l'**Assurance maladie** adopte une **nouvelle charte graphique** pour ses courriels afin d'en améliorer la **lisibilité** et de **faciliter l'identification des messages officiels** face à la recrudescence des tentatives d'hameçonnage. Parmi les changements : le logo repositionné en haut à gauche, des intertitres en bleu et un bloc en bas de message renvoyant vers les services en ligne. L'organisme rappelle que **seules les adresses en @ameli.fr ou @assurance-maladie.fr sont légitimes** et qu'aucune donnée bancaire ou médicale ne sera jamais demandée par courriel. Ameli

Google Threat Intelligence Group analyse la chaîne d'exploitation ***DarkSword***, un **logiciel espion exploitant six vulnérabilités *zero-day* sur iOS**. Utilisé depuis novembre 2025 par plusieurs éditeurs de logiciels de surveillance commerciaux et des acteurs étatiques présumés, il a ciblé des utilisateurs en Arabie Saoudite, en Turquie, en Malaisie et en Ukraine. Apple a depuis corrigé l'ensemble des failles, notamment dans iOS 26.3 et iOS 18.7.3. Google

Anticipation / Réglementation

Déployé publiquement par les autorités début mars 2026, « **17Cyber.gouv.fr** » est le **nouvel outil de l'État pour assister les victimes de cybermalveillance**. Géré par la **Gendarmerie nationale, la Police nationale et Cybermalveillance.gouv.fr**, ce portail gratuit, disponible 24h/24 et 7j/7 propose un diagnostic en ligne et un accompagnement par chat avec des agents dédiés. GendInfo