MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

Revue de presse des cybermenaces

Centre d'analyse des cybermenaces

#05 – Mai 2026

A retenir

Au cours du mois d'avril, l'actualité a été marquée par une vaste opération internationale coordonnée par Europol contre les services de **DDoS à la location**, ainsi que par des condamnations historiques liées aux centres d'arnaques cambodgiens.

Parallèlement, la menace se complexifie avec l'usage de **l'IA générative** pour réaliser des fraudes aux colis sophistiquées. Enfin, une série d'attaques massives a provoqué la fuite d'un nombre important de données personnelles, frappant notamment **l'ANTS** et **le ministère de l'Éducation nationale.**

Chiffres du mois

293 millions de dollars. C'est le montant total des cryptoactifs dérobés lors d'une attaque attribuée au groupe nord-coréen ***Lazarus***. L'attaque ciblait la plateforme de finance décentralisée **KelpDAO**. La vulnérabilité exploitée a permis le détournement de 116 500 RSETH. Enderi

ZachXBT, un détective spécialisé dans l'analyse transactionnelle de blockchain, a aidé la plateforme d'échange Binance à geler plus de **800 000$ de fonds illicites** extorqués à l'influenceur français TeufeurS. Journalducoin

Principales cyberattaques

Le ministère de l'**Éducation nationale** confirme la cyberattaque survenue fin 2025, entrainant la fuite de données **personnelles d'élèves**. Les informations compromises incluent prénom, nom, identifiant, établissement, classe, adresse mail et code d'activation. L'intrusion a été réalisée via l'usurpation d'un compte administrateur sur le service ÉduConnect. Le nombre exact de victimes est en cours d'évaluation. Le Telegramme Numerama

L'exploitant de salles de sport néerlandais **Basic-Fit** annonce être victime d'une cyberattaque affectant un million de membres notamment aux Pays-Bas et dans plusieurs autres pays européens, dont la France. Les données exfiltrées incluent noms, adresses, e-mails, numéros de téléphone, dates de naissance et coordonnées bancaires. Aucun mot de passe ni pièce d'identité n'a été compromis. Le nombre de victimes en France n'a pas été précisé. Basic-Fit FranceInfo

Une cyberattaque a touché la plateforme **AlumnForce** de l'**université d'Angers**, exfiltrant 127 400 fiches contenant des données personnelles d'étudiants, enseignants et personnels administratifs. Les informations compromises incluent nom, e-mail, téléphone, adresse et éléments du parcours académique et professionnel. La présidence de l'université a déposé plainte le 15 avril 2026. La plateforme **ip'Oline**, utilisée pour la gestion des alumni, a été le point d'entrée de l'intrusion. Ouest France FranceInfo

Coopérative U (anciennement Système U) a informé ses clients avoir subi une cyberattaque et un **vol de données personnelles**. Parmi les informations dérobées figurent l'identité, l'adresse e-mail, l'adresse postale, le numéro de téléphone et le numéro de carte de fidélité. 01net

12 millions de comptes seraient concernés par la fuite de données ayant affecté **l'ANTS** (organisme chargé notamment d'éditer les cartes nationales d'identité et permis de conduire). Les données contiendraient l'identifiant de connexion, la civilité, l'identité, l'adresse e-mail, la date de naissance et l'identifiant unique du compte. **L'enquête a été confiée à l'Office Anti-Cybercriminalité (OFAC)**. Le Figaro

Une nouvelle version du logiciel espion **SparkCat** cible de nombreuses applications sur l'app store d'Apple, à la recherche de photographies divulguant la phrase de récupération d'un portefeuille de cryptoactifs. Chacune des 26 applications frauduleuses identifiées se fait passer pour une application de portefeuille de cryptoactifs connue. Parmi elles : **Metamask, Ledger, Trust Wallet, Coinbase**. Kaspersky

Pour aller plus loin …

[Infoguard] – **Infoguard** publie un rapport d'analyse d'un incident impliquant le rançongiciel *DragonForce*, révélant la mise en place de techniques de persistance par le biais de l'interpréteur python.
[IC3] – **Rapport IC3 2025 du FBI** : La référence annuelle sur la cybercriminalité aux États-Unis aborde les points suivants : pertes par typologie, place de l'IA et des cryptomonnaies, sectorisation des rançongiciels.
[Paloalto] – **Unit 42** fait la cartographie des groupes hacktivistes iraniens (*Handala*, *Cyber Islamic Resistance*, *Dark Storm Team*) et l'observation de leurs tactiques DDoS et wiper post-conflit.

Faits marquants

Une opération internationale menée sous l'égide d'**Europol** a ciblé les services de ***DDoS-for-hire*** (DDoS à la location), entraînant l'arrestation de quatre personnes, la fermeture de **53 domaines et l'émission de 25 mandats de perquisition**. Plus de 75 000 utilisateurs ont reçu des avertissements écrits ou par courriel. L'action, menée le 13 avril 2026 par 21 pays, s'appuie sur la saisie de bases de données contenant plus de **3 millions de comptes criminels**. Les pays participants incluent des États membres de l'Union européenne, les États-Unis, le Royaume-Uni, le Japon, l'Australie et le Brésil. Les efforts conjoints de l'UE, des États-Unis, du Japon et de l'Australie ont permis de localiser et de neutraliser des serveurs critiques en Pologne et en Thaïlande, portant un coup d'arrêt aux capacités techniques de ces réseaux de cyber-extorsions. Europol

La **justice cambodgienne** a franchi un cap historique en condamnant à la **réclusion à perpétuité des gestionnaires de centres d'arnaques en ligne**. Ces individus dirigeaient des opérations de séquestration visant à forcer des victimes à orchestrer des escroqueries sentimentales et financières mondiales. Cette décision marque une **rupture jurisprudentielle** majeure dans une zone géographique identifiée par l'ONU comme l'**épicentre de la cybercriminalité liée à la traite d'êtres humains**. Ce verdict sévère vise à dissuader les syndicats du crime qui exploitent la misère humaine pour alimenter des fraudes technologiques toujours plus sophistiquées. BitDefender

Le **20 avril 2026**, les **autorités françaises ont interpellé en Vendée un individu de 21 ans** agissant sous le pseudonyme ***HexDex***. Accusé d'avoir piloté de nombreuses cyberattaques et orchestré des **fuites de données sensibles**, il ciblait prioritairement des **administrations publiques et des fédérations sportives**. Le parquet de Paris a ouvert une procédure pour atteintes graves aux systèmes de traitement automatisé de données. Lors de sa garde à vue, le suspect a reconnu son identité numérique. Son matériel informatique ainsi que son compte sur le forum cybercriminel Darkforum ont été saisis. L'individu a depuis été **mis en examen et placé en détention provisoire**, tandis que les enquêteurs tentent désormais de déterminer l'étendue des préjudices financiers subis par les victimes. Le Monde

Informations sur la menace

Les **escroqueries** fondées sur des livraisons de colis fictives, initialement basées sur des **images de livreurs générées par intelligence artificielle**, évoluent vers une **approche multi-canaux** plus sophistiquée : les victimes reçoivent d'abord un **message vocal personnalisé**, également **produit par IA**, **imitant une voix légitime** (ex : service client d'un transporteur), puis un **SMS** contenant une **image de livreur falsifiée** et un **lien malveillant dirigeant vers un site** conçu pour collecter les données bancaires — numéro de carte, date d'expiration et cryptogramme. Aucun débit n'est effectué à ce stade ; au contraire, **la victime est ensuite contactée par téléphone par un « conseiller bancaire » frauduleux**, qui, sous prétexte de bloquer une fraude, l'incite à effectuer des virements ou transferts à distance via des applications bancaires, vidant ainsi intégralement son compte. 01net

Une **fausse application imitant Ledger Live** a été disponible sur le Mac App Store pendant une semaine, **dérobant 9,5 millions de dollars en cryptomonnaies à plus de cinquante utilisateurs**. L'application nommée **Leva Heal Limited**, reproduisait l'interface officielle de Ledger et apparaissait dans les résultats de recherche. Les victimes ont été incitées à saisir leur phrase de récupération lors de l'installation, permettant le transfert immédiat de leurs fonds. Le réseau de transactions transiterait par KuCoin et un service de mixage nommé AudiA6. L'application n'était pas distribuée par Ledger, qui publie sa solution uniquement sur leur site officiel. **Apple a retiré la fausse application du Mac App Store**. Numerama

Le groupe ***Akira***, apparu en 2023, a publié **84 victimes pour le seul mois de mars 2026**, plus du double de février et son deuxième record mensuel historique. Disposant d'une chaîne d'attaque optimisée capable de passer de l'accès initial au chiffrement complet en moins de quatre heures, le groupe cumule plus de **1 400 victimes revendiquées et 245 millions de dollars de paiements depuis sa création**, avec une concentration marquée sur la France (53 % des détections sur 2024). Cyberscoop

Anticipation / Réglementation

Lors du **Forum InCyber début avril**, le **GDI Patrick Touak a exposé la stratégie du ministère de l'Intérieur**, plaçant la souveraineté numérique au cœur de la continuité de l'État. Ce plan s'appuie sur des **outils souverains** (Cloud, système Néo) et une réponse globale : **formation accrue**, **hygiène numérique stricte** et **judiciarisation systématique** des attaques par les services spécialisés pour protéger les institutions. Gendarmerie

Cliquez ici pour vous abonner :

TLP:CLEAR