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

#07 – Juillet 2026

A retenir

La mise à disposition de données volée sur des forums cybercriminels occupe encore l'essentiel de l'actualité du mois écoulé (messagerie Tchap, Fédération Sportive de la Police Nationale, plateforme e-pulsy et Assurance Maladie).

L'OFAC a procédé à sept interpellations d'individus soupçonnés de faire partie du groupe malveillant *DumpSec*.

Afin de réduire la dépendance technologique de l'Union Européenne, la Commission européenne instaure un principe de priorité au logiciel libre.

Chiffres du mois

250 000, c'est le nombre de cartes nationales d'identité et de passeports français que l'acteur malveillant ChimeraZ a mis en vente sur un forum cybercriminel.

Ces documents proviendraient à l'origine de scans envoyés lors des phases de vérifications d'identités sur des services en ligne, compromis par la suite. Les fichiers auraient été compilés et croisés par l'acteur qui en a probablement conçu une base de données. Utilisés à mauvais escient, ces documents peuvent notamment servir à souscrire des crédits bancaires, à transmettre des courriels d'hameçonnage ou acheter des cartes SIM anonymes. Siècle Digital

Principales cyberattaques

Un compte utilisateur de la messagerie Tchap a été compromis par usurpation, exposant les données de 73 467 agents de l'administration. L'attaquant a pu accéder aux conversations publiques non chiffrées, révélant noms, prénoms, adresses e-mail et entités d'appartenance. Les échanges privés restent protégés par le chiffrement. L'incident a été détecté et le compte bloqué La compromission d'un seul compte a permis l'exposition de l'ensemble des salons publics auxquels il a accès. DINUM

La Fédération Sportive de la Police Nationale a été la cible d'un vol de données revendiqué par l'acteur *misere*. Les données contiendraient l'identité, date de naissance, grade, matricule et affectation sur la période comprise entre 2012 et 2026. 70 000 licenciés et adhérents seraient concernés. En outre, l'attaquant affirme avoir dérobé environ 180 000 certificats médicaux, 380 000 licences sportives et un million de convocations. La Fédération a confirmé l'attaque.
01Net

La plateforme de e-santé Pulsy, qui centralise les échanges de données médicales pour la région Grand Est, a été la cible d'un vol de données survenu le 18 juin 2026. Ces données ont ensuite été mises en vente sur une plateforme cybercriminelle. D'après l'auteur de l'annonce, deux fichiers ont été mis à disposition, comportant respectivement 5 677 450 et 180 609 lignes pour un volume supérieur à 35 Go. Cependant, le directeur de Pulsy remet en cause ces volumes qu'il considère impossibles à extraire sur la durée de l'attaque estimée à trois heures. Ouest France

Un acteur, sous le pseudonyme *Lagui,* revendique le 2 juin 2026 une base attribuée au Dossier Médical Partagé. L'Assurance Maladie dément toute extraction massive : absence de données médicales, NIR mal formés, IBAN atypiques. L'hypothèse retenue est un fichier recomposé à partir d'anciennes fuites françaises. cyberattaque.org

Pour aller plus loin …

[Recorded Future] Recorded Future publie un rapport sur les risques liés à la coupe du monde de football au Canada, aux Etats-unis et au Mexique (escroqueries liées à la contrefaçon de marques officielles, avec hameçonnage augmenté par l'IA comme méthode privilégiée). Le volume global d'authentifiants de cartes bancaires volées devrait être supérieur au précédentes éditions.

[Group-IB] Group-IB détaille le 11 juin 2026 le démantèlement de SniperDz, plateforme d'Hameçonnage-en-tant-que-Service active depuis 2015 et associée à plus de 20 000 domaines visant une trentaine de marques (PayPal, Netflix, Steam).

Faits marquants

Des chercheurs de SafeBreach ont démontré qu'il était possible de manipuler l'assistant vocal Google Gemini via des notifications de messagerie. En exploitant une faiblesse structurelle de l'IA, des attaquants peuvent injecter des instructions cachées dans des messages (WhatsApp, Signal) pour tromper l'assistant. Celui-ci peut alors interpréter ces instructions comme légitimes, permettant des actions non autorisées comme l'usurpation de contacts ou le déclenchement d'actions à distance. Cette technique d'injection de prompt indirect contourne les protections classiques en exploitant la différence entre ce que voit l'utilisateur et ce que traite le modèle. SafeBreach

L'Office anti-cybercriminalité (OFAC) annonce le 12 juin 2026 l'interpellation de sept personnes, dont des mineurs, à Lille, Marseille, Strasbourg, Poitiers, Bordeaux et Limoges. Le groupe, qui revendiquait publiquement ses attaques sur BreachForums sous le nom *DumpSec*, aurait visé plus de 1 500 entités, dont l'Assemblée nationale, Leroy Merlin, le Crous et l'UNSS, pour plusieurs dizaines de millions de données exfiltrées. L'OFAC avait infiltré le collectif plusieurs mois en se faisant passer pour des acheteurs. Enquête ouverte en novembre 2025 après une attaque visant une entreprise rennaise. Génération NT

Informations sur la menace

Le Commandement central des États-Unis (Centcom) a confirmé que des acteurs malveillants exploitent des données de localisation commerciales pour surveiller et cibler le personnel militaire américain dans des zones de conflit actives, notamment dans le Golfe. Ces données, collectées par des applications et des fournisseurs de services, sont vendues à des tiers à des fins publicitaires. Cette exploitation permet aux adversaires d'identifier les regroupements de troupes et leurs habitudes, facilitant ainsi des attaques par missiles, drones ou engins explosifs improvisés. Cybercs ecurity News

Des escrocs utilisent le système de paiement Wero pour tenter d'arnaquer les vendeurs sur leboncoin.fr et Facebook Marketplace. Au motif de sécuriser la vente, l'escroc propose de virer la somme demandée par le vendeur via un virement Wero nécessitant uniquement le numéro de téléphone de la victime. L'escroc transmet au vendeur une fausse capture d'écran censée attester le virement, ainsi qu'un SMS contenant un lien cliquable pour valider le paiement et le transfert des fonds. Le lien renvoie vers une fausse page Internet Wero invitant la victime à renseigner ses données personnelles et bancaires. Ouest France

Le *Steam Workshop* est régulièrement exploité par des pirates via des fonds d'écran malveillants pour *Wallpaper Engine*. En détournant la fonctionnalité d'exécution de code légitime, les attaquants injectent des programmes malveillants, qui s'exécutent derrière l'affichage du fond d'écran. L'objectif principal reste le vol des comptes *Steam* pour revendre les identifiants ou propager la contamination. Cette campagne a ainsi distribué divers maliciels, dont des rançongiciels et des voleurs d'identifiants. 01Net

Des victimes de violations de données ont reçu des courriels prétendant provenir des associations « Ligue de défense des données personnelles », la « Ligue de protection des données personnelles » ou l'« Association de protection des données personnelles ». Ces organismes affirment être en mesure d'intervenir auprès des forums sur lesquels les données personnelles sont habituellement échangées pour les faire supprimer. Les courriels mentionnent également le numéro de téléphone de la CNIL, alors que la Commission réfute tout lien avec ces initiatives. La CNIL préconise la plus grande prudence face à ces services proposant la suppression de données volées. CNIL

Anticipation / Réglementation

La Commission européenne publie une stratégie open source élevant le logiciel libre au rang d'instrument de politique industrielle. Le projet de règlement Cloud and AI Development Act (CADA) instaure un principe de priorité au logiciel libre dans la commande publique de cloud et d'IA, avec obligation de réutilisation des codes achetés avec des fonds publics. Cette mesure vise à réduire la dépendance technologique de l'UE, qui dépense 264 milliards d'euros annuellement en solutions propriétaires. Conseil national du logiciel libre – CNLL

L'Autorité des Marchés Financiers alerte les sociétés de gestion de portefeuille, les prestataires de services de financement participatif et les prestataires de services sur crypto-actifs et les appelle à renforcer leur résilience opérationnelle cyber (règlement européen DORA) et faire face aux menaces liées à l'intelligence artificielle. Autorité d es Marchés Financiers

La Région Sud a adopté le 26 juin 2026 une nouvelle stratégie de cybersécurité visant à protéger 10 000 entreprises et collectivités par an. Face aux menaces ciblant particulièrement les TPE/PME, ce plan renforce la prévention et consolide le CSIRT régional. L'objectif est d'assurer la compétitivité économique du territoire en vue des futurs défis, dont les Jeux d'hiver 2030. Var Actu