🔍 Synthèse de veille cybersécurité — 19 au 26 mai 2026

💻 Cyberattaques majeures de la semaine

FR Campagne ChimeraZ : le tourisme français en crise — 14-17 mai

L'événement majeur de la période est une série de trois attaques enchaînées en moins de 72 heures par un même pirate, opérant sous le pseudonyme ChimeraZ, qui a exploité la même faille technique chez trois grands acteurs du tourisme hexagonal.

Gîtes de France a confirmé le dimanche 17 mai avoir été victime d'un vol de données affectant près de 389 000 clients, perpétré la veille le 16 mai. Il s'agit du troisième coup porté en trois jours après Pierre et Vacances-Center Parcs le vendredi, puis Belambra le samedi. Economiematin

Pour Belambra, la base revendiquée inclurait environ 360 000 données liées à des mineurs et enfants enregistrés dans les réservations, couvrant une période d'environ six mois entre novembre 2025 et mai 2026. FrenchBreaches

Pour Gîtes de France, ChimeraZ revendique avoir exfiltré des données couvrant plus de trois décennies, de 1995 à 2026. Les informations compromises englobent les noms et prénoms, adresses postales, numéros de téléphone, adresses électroniques, ainsi que les dates, durées et montants des réservations. Ce dernier point est particulièrement préoccupant : connaître les dates de séjour revient à savoir quand un foyer est vide. Social Mag

Au total, en l'espace de 72 heures, trois cyberattaques ont compromis les données de 5,3 millions de Français. Selon le fondateur de French Breaches, le cybercriminel aurait déclaré avoir agi pour « gagner en visibilité et montrer à quel point la France est une passoire en matière de cybersécurité ». TourMaGLes Smartgrids

FR McDonald's France — Credential stuffing (21 mai)

McDonald's France a été touché par une fuite de données liée à son programme de fidélité. Plusieurs clients ont vu leurs comptes fidélité utilisés sans autorisation. Les fraudeurs auraient exploité les points cumulés pour obtenir des remises sur leurs achats. Plus un message contient d'éléments vrais, plus il paraît crédible : un pirate qui connaît une enseigne fréquentée, une adresse mail et un identifiant fidélité peut fabriquer un courriel de phishing beaucoup plus convaincant. EconomiematinZATAZ

🌐 APT chinois — Serveur Exchange entreprise énergétique

Des pirates informatiques affiliés à l'État chinois ont compromis un serveur Microsoft Exchange chez une importante entreprise énergétique, réutilisant à plusieurs reprises ce même point d'entrée pour mener des opérations. DCOD

🌐 Campagne Mini Shai-Hulud — Supply chain open source (26 mai)

Une campagne nommée Mini Shai-Hulud a compromis des dizaines de projets open source, contaminant en cascade les développeurs et entreprises qui les intègrent, illustrant la portée systémique des attaques sur la chaîne d'approvisionnement logicielle. DCOD

⚠ Zero-days & vulnérabilités critiques

CVE-2026-45585 « YellowKey » — Bypass BitLocker (19 mai)

Microsoft travaille sur un correctif pour CVE-2026-45585 (alias "YellowKey"), une vulnérabilité permettant de contourner la protection BitLocker et d'accéder aux données des utilisateurs. La vulnérabilité a été divulguée publiquement une semaine avant l'avis de Microsoft par un chercheur sous le pseudonyme Nightmare Eclipse, apparemment par frustration face à la gestion des rapports de bugs. Help Net Security

YellowKey permet à un attaquant disposant d'un accès physique au PC d'ouvrir un shell sans restriction dans l'environnement de récupération Windows (WinRE), ce qui donne accès au disque chiffré sans saisie d'identifiants ni installation logicielle. L'avis Microsoft cible Windows 11 versions 24H2, 25H2 et 26H1, ainsi que Windows Server 2025. Un PoC public est disponible. Aucun patch définitif n'est encore disponible. Testdisquedur

CVE-2026-34926 — TrendAI Apex One (21 mai, exploité activement)

La vulnérabilité CVE-2026-34926 est une faille de traversée de répertoires dans le serveur Apex One on-premise. Un attaquant peut modifier une table clé du serveur pour injecter du code malveillant à déployer sur les agents des installations affectées. TrendAI a observé au moins une tentative d'exploitation in-the-wild. La CISA a ajouté la vulnérabilité à son catalogue des vulnérabilités exploitées connues (KEV), avec une alerte publiée le 21 mai. SecurityWeekCVEfeed

CVE-2026-9082 — Drupal Core SQLi (20 mai)

Drupal a publié le 20 mai 2026 un correctif d'urgence pour une vulnérabilité d'injection SQL classée de sévérité maximale dans son cœur, identifiée CVE-2026-9082. La faille touche l'API d'abstraction de base de données sur les sites utilisant PostgreSQL et permet, par requête malveillante envoyée par un utilisateur anonyme, l'injection SQL arbitraire. Les conséquences peuvent aller de la divulgation d'information à l'exécution de code à distance selon la configuration. Donneespersonnelles

---

🔄 Mises à jour de sécurité & correctifs

ANSSI — Référentiel PACS v2.0 (21 mai)

L'ANSSI a publié le 21 mai 2026 la version 2.0 du référentiel d'exigences applicable aux Prestataires d'Accompagnement et de Conseil en Sécurité (PACS). La version 2.0 actualise les exigences sur la compétence des consultants, les règles de confidentialité des informations client, la traçabilité des interventions et l'indépendance vis-à-vis des éditeurs et intégrateurs.

Pour les entités NIS2, recourir à un PACS qualifié facilite la démonstration de diligence (Art. 21). Donneespersonnelles

TrendAI Apex One — Bulletin mai 2026 (21 mai) : 8 CVE au total (34926 à 34930 + 45206 à 45208). Versions corrigées : SP1 CP Build 18012 ou Build 17079 (on-prem) ; agent build 14.0.20731 (SaaS).

Protection des données

Vague ChimeraZ — Obligations RGPD en cascade FR

Les trois organisations (Pierre & Vacances, Belambra, Gîtes de France) ont notifié la CNIL et déposé plainte. Ces attaques illustrent la vulnérabilité croissante du secteur touristique face aux cybermenaces. Les spécialistes rappellent que les entreprises du tourisme sont particulièrement exposées en raison de la multiplicité des partenaires, plateformes de réservation et systèmes interconnectés. Ici

LookUp / Telegram — Suspect français arrêté (22 mai) FR

Un suspect français a été interpellé dans un dossier mêlant Telegram, crypto-actifs et 79 millions d'entrées. Telegram inquiète également : un audit confirme un risque de suivi passif via une clé d'authentification, malgré les démentis de l'entreprise. ZATAZ

Sécurité informatique — Opérations & tendances

Opération Saffron — Démantèlement de First VPN (19-20 mai)

L'opération baptisée « Saffron », amorcée en 2021 avec le soutien d'Europol et d'Eurojust, visait le service VPN connu sous le nom de firstVPNservice. Les autorités françaises et néerlandaises ont démantelé le service lors d'une action coordonnée ayant permis de saisir l'infrastructure, de fermer des serveurs utilisés dans 27 pays et d'accéder aux données de nombreux utilisateurs. Begeek

Le FBI a confirmé qu'au moins 25 groupes de ransomware distincts — dont Avaddon — utilisaient First VPN pour dissimuler leurs opérations de reconnaissance, d'intrusion et d'infrastructure de commande-contrôle. 506 utilisateurs identifiés, 83 paquets de renseignement distribués aux agences partenaires dans le monde. Pour l'écosystème ransomware, c'est un coup significatif porté au modèle de confiance qui rend les opérations criminelles possibles. Tech TimesStateofsurveillance

CA Botnet Kimwolf — Arrestation (Ottawa, 21 mai)

Les autorités américaines et canadiennes ont annoncé le 21 mai l'arrestation à Ottawa d'un homme de 23 ans, soupçonné d'avoir construit et exploité Kimwolf, un botnet IoT de classe Mirai qui a infecté près de deux millions d'appareils. La propagation reposait sur des

identifiants par défaut jamais changés et sur des vulnérabilités non corrigées dans des firmwares en fin de support. Donneespersonnelles

IA offensive — Un seuil franchi

Des chercheurs de Google signalent que des pirates exploitent déjà l'intelligence artificielle pour concevoir des failles inconnues, des portes dérobées Android et des attaques automatisées contre la chaîne logicielle visant notamment les plateformes de développement GitHub et PyPI. DCOD