Synthèse de veille du 19 au 27 mai 2026

Thème 1 · Cyber-sécurité

CVE et vulnérabilités critiques

CVE-2026-34926 sur TrendAI Apex One, publiée le 21 mai, exploitation active confirmée

TrendAI (anciennement Trend Micro) a dû sortir un correctif en urgence pour son produit Apex One, une solution de protection des postes très utilisée dans les entreprises françaises. La faille est de type path traversal : un attaquant authentifié peut sortir du dossier autorisé, accéder à des fichiers système critiques, modifier une table clé du serveur et injecter du code malveillant qui se déploie ensuite sur tous les postes connectés. La CISA a confirmé une exploitation active dans la nature et l'a ajoutée à son catalogue KEV le jour même. Concrètement, si une entreprise utilise Apex One sans avoir appliqué le patch, l'attaquant peut prendre le contrôle de tout le parc informatique via l'outil censé le protéger.

Sources : SecurityWeek, CISA KEV, donneespersonnelles.fr

CVE-2026-41091 et CVE-2026-45498 sur Microsoft Defender, publiées le 22 mai, zero-day

Deux failles zero-day découvertes simultanément dans Microsoft Defender, l'antivirus intégré à Windows. La première permet à un attaquant d'obtenir les privilèges SYSTEM, soit le niveau d'accès maximal sur une machine Windows. La seconde peut provoquer un déni de service. Zero-day signifie que ces failles étaient déjà exploitées dans la nature avant que Microsoft en soit informé. Les deux ont été ajoutées au catalogue KEV de la CISA avec obligation de patch sous 48 heures pour les agences fédérales américaines.

Sources : integrity360.com, CISA KEV

YellowKey, CVE-2026-45585, divulguée le 13 mai, mitigation partielle le 20 mai

BitLocker est le système de chiffrement du disque dur intégré à Windows. YellowKey est une faille qui permet de contourner complètement ce chiffrement sans avoir la clé. L'attaque cible le Windows Recovery Environment, l'environnement de réparation accessible au démarrage : en plaçant des fichiers spéciaux sur une clé USB ou la partition EFI, puis en redémarrant en maintenant CTRL, l'attaquant obtient un accès total au volume chiffré. Elle nécessite un accès physique ou local à la machine. Le chercheur Chaotic Eclipse a délibérément publié l'exploit juste après le Patch Tuesday de Microsoft, laissant les organisations sans correctif officiel pendant plusieurs jours. Microsoft a fourni des instructions de mitigation en attendant un patch permanent.

Sources : ThreatLocker, Daily Security Review, Help Net Security

GreenPlasma, escalade de privilèges SYSTEM sur Windows, divulguée le 13 mai, sans patch

Divulguée en même temps que YellowKey par le même chercheur, GreenPlasma cible le framework CTFMON sur Windows 11 et Windows Server 2022 et 2026. Une escalade de privilèges permet à un utilisateur ordinaire de devenir SYSTEM, le compte le plus puissant du système. En pratique cela facilite le vol d'identifiants, les déplacements latéraux dans le réseau, la désactivation des outils de sécurité et le déploiement de ransomware. Ce qui est particulièrement préoccupant : aucun CVE officiel n'a été attribué et il n'existe aucun correctif à ce jour.

Sources : Security Affairs, ThreatLocker

Pwn2Own Berlin 2026, 47 zero-days découverts cette semaine

Pwn2Own est une compétition internationale de hacking éthique organisée deux fois par an. L'édition berlinoise 2026 a mis en lumière 47 failles zero-day en quelques jours sur des navigateurs, systèmes d'exploitation, logiciels d'entreprise et solutions de virtualisation. 1,3 million de dollars de primes ont été distribués aux chercheurs. Toutes les vulnérabilités ont été transmises aux éditeurs dans le cadre d'une divulgation coordonnée. Pour rappel : en 2026 le délai médian entre la publication d'un CVE critique et son exploitation active est passé sous les 5 jours.

Sources : IT-Connect, ayinedjimi-consultants.fr

Phishing

Vague de phishing autour de la Coupe du Monde FIFA 2026, active depuis novembre 2025

Avec la Coupe du Monde qui approche, les cybercriminels multiplient les arnaques thématiques. Depuis novembre 2025 une hausse continue d'enregistrements de domaines contenant les mots-clés FIFA ou World Cup est observée : leur nombre a quadruplé entre décembre et février, avec plus de 2 700 nouveaux domaines créés en avril seul. Les techniques utilisées sont variées : faux sites de vente de maillots avec 80% de remise, faux billets VIP, fausses plateformes de streaming. Ces sites collectent les données bancaires des victimes puis disparaissent.

Sources : CTM360, The Hacker News, ICT Journal

Tycoon 2FA, nouveau contournement de double authentification, semaine du 19 mai

Tycoon 2FA est un kit de phishing vendu en service qui permettait de contourner la double authentification. Bien que démantelé, ses opérateurs ont relancé une nouvelle variante exploitant le flux OAuth 2.0 Device Authorization Grant, un mécanisme légitime conçu pour les appareils sans clavier comme les TV ou imprimantes. L'attaque fonctionne ainsi : la victime pense autoriser l'accès à un lecteur de messagerie vocale, mais autorise en réalité l'émission d'un token vers un appareil contrôlé par l'attaquant. Ce qui la rend difficile à détecter c'est qu'il n'y a aucun proxy ni fausse page Microsoft : tout se passe sur l'infrastructure officielle de Microsoft.

Source : KnowBe4

Phishing Ledger par lettres postales avec QR code, signalé le 26 mai

Ledger est un fabricant français de portefeuilles physiques pour cryptomonnaies. Des escrocs envoient de vraies lettres papier à des utilisateurs en Italie, probablement depuis une base de données issue d'une fuite Ledger de 2020. Les lettres contiennent un QR code qui renvoie vers un faux site demandant la phrase de récupération du portefeuille. Quiconque la saisit perd l'intégralité de ses cryptomonnaies. L'originalité ici c'est l'aspect hybride : le courrier physique inspire confiance et contourne tous les filtres anti-phishing numériques.

Source : DCOD

Thème 2 · Fuites de données et failles applicatives

Ransomware

Qilin attaque Semgrep, revendiqué le 22 mai

Semgrep est un outil d'analyse statique de code open source très utilisé dans les pipelines DevSecOps pour détecter automatiquement des vulnérabilités avant mise en production. Le groupe Qilin, numéro 1 mondial du ransomware depuis trois trimestres consécutifs, a revendiqué l'attaque avec menace de publication de données sensibles. La cible est particulièrement stratégique : compromettre un outil d'analyse de sécurité peut exposer les pipelines CI/CD et les bases de code de milliers d'entreprises clientes. Qilin pratique la double extorsion, c'est-à-dire le chiffrement des données couplé à la menace de publication pour forcer le paiement.

Sources : DeXpose, Ransom-ISAC

The Gentlemen et la double extorsion via sous-traitant, analysée cette semaine

The Gentlemen est le deuxième groupe ransomware le plus actif de 2026 avec environ 130 victimes revendiquées. L'analyse de leur attaque d'avril 2026 illustre une tactique de plus en plus courante : ils ont d'abord compromis un cabinet britannique de conseil logiciel, puis ont réutilisé les accès et informations volées pour frapper l'un de ses clients en Turquie. Ce schéma d'attaque par la chaîne d'approvisionnement rend la défense périmétrique classique insuffisante car c'est le prestataire de confiance qui devient le vecteur d'intrusion.

Sources : ZATAZ, Ransom-ISAC

Bilan ransomware Q1 2026, reconsolidation de l'écosystème

2 122 victimes ont été publiées sur des sites de fuite en Q1 2026, ce qui en fait le deuxième trimestre le plus élevé jamais enregistré. Le phénomène marquant est que le top 10 des groupes représente désormais 71% de toutes les victimes, la concentration la plus forte depuis début 2024. L'écosystème se reconsolidie après les démantèlements de 2024 et 2025 : moins de groupes mais plus professionnels, organisés en véritables franchises RaaS avec recrutement d'affiliés, support aux victimes et portails de négociation dédiés.

Source : Industrial Cyber

Fuites de données

Fuite de données d'assurance santé confirmée le 23 mai

Une fuite confirmée cette semaine exposant des données particulièrement sensibles : numéro de sécurité sociale, nom de l'assureur, numéro de contrat, dates de couverture et rang de naissance. Ces informations suffisent pour usurper une identité, monter des fraudes à l'assurance ou construire des campagnes de phishing ultra-ciblées. Le numéro de sécurité sociale est une donnée critique car il ne change jamais et ouvre l'accès à de nombreux services publics.

Source : bonjourlafuite.eu.org

Fuite de documents RH et professionnels confirmée le 21 mai

Une fuite exposant des documents administratifs très sensibles : bulletins de salaire, avis d'imposition, IBAN, justificatifs professionnels. Ce type de données permet des virements frauduleux par modification d'IBAN, des arnaques à l'embauche ou des demandes de crédit frauduleuses. Dans un contexte de développement logiciel, ce type de fuite illustre concrètement les conséquences d'une API mal sécurisée ou d'une injection SQL sur un portail RH.

Source : bonjourlafuite.eu.org

McDonald's France, risque sur le programme de fidélité, semaine du 19 mai

Une fuite chez un prestataire de service client expose les données du programme de fidélité McDonald's France. Ce cas illustre un problème récurrent en 2026 : le maillon faible est souvent le sous-traitant et non l'entreprise principale. Les données exposées comme les adresses email, l'historique d'achats et les coordonnées permettent des campagnes de phishing ciblées au nom de la marque. ManoMano en janvier et The Gentlemen en mai ont suivi exactement le même schéma.

Source : datasecuritybreach.fr

Bilan France au T1 2026

La France est désormais le deuxième pays le plus touché au monde par les violations de données avec 23,5 millions de comptes compromis et plus de 300 services impactés depuis janvier. Les incidents majeurs du trimestre : Cegedim Santé avec 15 millions d'assurés touchés et des données médicales exposées, l'URSSAF avec 12 millions de personnes concernées, et Free et Free Mobile avec une amende record de 42 millions d'euros pour la fuite d'octobre 2024 ayant compromis 24 millions de contrats et les IBAN associés. La CNIL durcit son application du RGPD : les inspections se multiplient sur les PME et les sanctions ne sont plus réservées aux grands groupes.

Sources : CNIL, SYLink, FrenchBreaches, i-leadconsulting.com

Sources principales : ANSSI · CERT-FR · CISA KEV · IT-Connect · datasecuritybreach.fr · donneespersonnelles.fr · integrity360.com · ZATAZ · Industrial Cyber · DeXpose · KnowBe4 · Security Affairs · ThreatLocker · bonjourlafuite.eu.org