## 🔍 Synthèse de veille — 19 au 26 mai 2026

**Thèmes : CVE | Phishing | Ransomware | Vulnérabilité zero-day**

---

### 🌓 CVE — Vulnérabilités critiques de la semaine

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

Drupal a publié le 20 mai 2026 un correctif d'urgence pour une vulnérabilité d'injection SQL classée de sévérité maximale dans son cœur. 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, une injection SQL arbitraire pouvant aller jusqu'à l'exécution de code à distance selon la configuration. Selon les données de la semaine, plus de 15 000 attaques ont été détectées dans les 48h suivant la publication. Donneespersonnelles

**CVE-2026-34926 — TrendAI Apex One (21 mai) — Exploitée 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 KEV le 21 mai. SecurityWeekCVEfeed

**CVE-2026-2005 — pgcrypto PostgreSQL (25 mai) — PoC public**

Un exploit de type preuve de concept pour CVE-2026-2005 remet en lumière une vulnérabilité critique vieille de vingt ans dans l'extension pgcrypto de PostgreSQL, permettant une élévation de privilèges et l'exécution de commandes arbitraires. DCOD

**CVE-2026-46333 — Noyau Linux (25 mai) — 9 ans non détectée**

Des chercheurs ont révélé une vulnérabilité du noyau Linux restée indétectée pendant neuf ans, référencée CVE-2026-46333 (CVSS 5,5), liée à une mauvaise gestion des privilèges pouvant permettre une élévation de privilèges locale. DCOD

**Contexte CERT-FR — Bulletin ACT-022 (18 mai) :** Le CERT-FR a émis des avis sur PHP, Spring, Mozilla, VMware, Microsoft Edge, Azure Linux, PostgreSQL PgBouncer, CPython, Traefik, LibreNMS, Apple, SPIP, Siemens, Schneider Electric, SAP, Nextcloud, Centreon et HPE Aruba Networking. CERT-FR

**Signal IA :** Le fondateur de Linux alerte sur l'explosion de rapports de bugs générés par l'IA rendant la liste de sécurité Linux « ingérable », en raison de doublons massifs et de signalements non vérifiés sans preuve de concept solide. DCOD

## 🎣 Phishing — Campagnes de la semaine

### Ghostwriter / UAC-0057 (Biélorussie) — Ciblage des gouvernements ukrainiens (21 mai)

Le groupe Ghostwriter a été observé utilisant des leurres liés à Prometheus, une plateforme d'apprentissage ukrainienne, pour cibler des organisations gouvernementales. L'activité implique l'envoi d'emails de phishing via des comptes compromis. L'email contient une pièce jointe PDF avec un lien menant au téléchargement d'une archive ZIP contenant un fichier JavaScript (OYSTERFRESH), qui déploie une charge OYSTERBLUES dans le registre Windows. Dans son avis du 21 mai 2026, le CERT-UA a averti que UAC-0057 avait mis à jour sa boîte à outils de malwares. The Hacker NewsSOC Prime

### Coupe du Monde FIFA 2026 — Vague de phishing (20-26 mai)

Depuis novembre 2025, une hausse continue des enregistrements de domaines contenant les mots-clés "Fifa" ou "World Cup" est observée. En février 2026, leur nombre a plus que quadruplé en deux mois. Des cybercriminels proposent des maillots et souvenirs avec des rabais allant jusqu'à 80%, ou incitent à acheter de faux billets VIP. CTM360 observe une forte augmentation des enregistrements de domaines thématiques, avec avril seul représentant plus de 2 700 nouveaux domaines. ICTjournalThe Hacker News

### Tycoon 2FA — Évolution post-démantèlement (semaine du 19 mai)

Bien que démantélé, les opérateurs Tycoon 2FA ont adopté une nouvelle variante exploitant le flux OAuth 2.0 Device Authorization Grant. L'utilisateur pense approuver l'accès pour un lecteur de messagerie vocale, mais autorise en réalité l'émission d'un token vers un appareil contrôlé par l'attaquant. "Il n'y a pas de proxy, pas de fausse page Microsoft — tout se passe sur l'infrastructure Microsoft légitime." KnowBe4

### Phishing Ledger — Lettres papier postales (26 mai)

Des escrocs envoient par courrier de fausses lettres Ledger à des utilisateurs en Italie, contenant des codes QR qui incitent les utilisateurs de portefeuilles crypto à révéler leurs phrases de récupération. Une attaque hybride offline/online particulièrement inédite et convaincante. DCOD

### Phishing Uniswap — 400 000 $ vidés (26 mai)

Un site de phishing se faisant passer pour Uniswap a vidé des wallets, les attaquants détenant près de 400 000 dollars. L'alerte demande aux traders de vérifier les URL et d'utiliser uniquement les liens officiels. BeInCrypto

## Ransomware — Incidents et tendances

### Qilin attaque Semgrep (22 mai)

Le 22 mai 2026, le groupe Qilin a revendiqué publiquement une attaque contre Semgrep, une société américaine spécialisée dans la sécurité du code (analyse statique, détection de vulnérabilités dans les pipelines CI/CD). Le groupe a publié un avis d'extorsion indiquant que des données sensibles seraient divulguées sans négociation. La cible est particulièrement sensible : un outil DevSecOps compromis peut exposer les pipelines de sécurité de milliers de clients. DeXpose

### The Gentlemen — Fuite interne analysée (semaine 19 mai)

ZATAZ propose une chronologie du cas The Gentlemen. Une attaque menée en avril 2026 contre un cabinet britannique de conseil logiciel montre que le groupe a d'abord compromis cette société, puis réutilisé les informations volées pour frapper l'un de ses clients en Turquie, pratiquant une double extorsion. The Gentlemen se classe 2e groupe le plus actif de 2026, avec environ 130 victimes revendiquées. ZATAZRansom-ISAC

### Gunra — Émergence d'un nouveau RaaS

Le ransomware Gunra évolue rapidement vers une opération de cybercriminalité plus structurée et dangereuse, après être passé d'un système de stockage basé sur Conti à son propre modèle de Ransomware-as-a-Service. DCOD

### Tendance Q1 2026 — Reconsolidation de l'écosystème

2 122 victimes ont été publiées sur des sites de fuite de données en Q1 2026, faisant de ce trimestre le deuxième plus haut jamais enregistré. Le TOP 10 des groupes représente désormais 71,1 % de toutes les victimes, la concentration la plus élevée depuis Q1 2024. Qilin reste en tête pour le troisième trimestre consécutif. Industrial Cyber

## Vulnérabilités zero-day

### YellowKey — CVE-2026-45585 (divulgué 13 mai, mitigation 20 mai)

Le 13 mai 2026, Chaotic Eclipse a publié un exploit pour YellowKey et GreenPlasma, ciblant BitLocker et l'escalade de privilèges Windows. Le chercheur, ayant préalablement tenté une divulgation via le MSRC Microsoft, a calé la publication juste après le cycle Patch Tuesday, laissant les organisations sans correctif officiel. ThreatLocker

L'attaque YellowKey cible le Windows Recovery Environment (WinRE). Un attaquant avec accès physique ou local place des fichiers FsTx spécialement conçus sur une clé USB ou la partition EFI. Après redémarrage en WinRE en maintenant CTRL, un shell obtient un accès sans restriction au volume protégé par BitLocker, sans nécessiter la clé de chiffrement. Microsoft travaille sur un correctif permanent mais fournit en attendant des instructions de mitigation étape par étape. Daily Security ReviewHelp Net Security

### GreenPlasma — Escalade de privilèges SYSTEM (13 mai)

La seconde vulnérabilité, GreenPlasma, est une faille d'escalade de privilèges Windows affectant le framework CTFMON sur Windows 11 et Windows Server 2022/2026. L'exploit permet de créer des objets de section mémoire arbitraires dans des répertoires accessibles en écriture par SYSTEM, permettant potentiellement une élévation de privilèges jusqu'au niveau SYSTEM. Pas de CVE officiel, pas de patch. L'escalade de privilèges facilite le vol d'identifiants, le mouvement latéral, l'interférence avec les outils de sécurité et le déploiement de ransomware. Security AffairsThreatLocker

### Pwn2Own Berlin 2026 — 47 zero-days découverts

Pwn2Own Berlin 2026 a révélé 47 zero-days et distribué 1,3 million de dollars de primes. Les vulnérabilités couvrent navigateurs, systèmes d'exploitation, logiciels d'entreprise et solutions de virtualisation, et ont été transmises aux éditeurs pour correction dans le cadre du programme de divulgation coordonnée. Ayinedjimi-consultants