Veille Newsletter
www.veillemag.com
Le magazine des professionnels de l'information stratégique

Par Jacqueline Sala

Focus Cybersécurité. Avril 2026. La cybersécurité bascule dans l'ère de l'urgence permanente. Yannick Pech

Avril2026a confirmé unetendancelourde :lacybersécuritén'estplus unequestion de "si",maisde "quand". Entrel'exploitation immédiate de vulnérabilités zero-day, la multiplication des attaques sur la chaîne logistique (supply chain), et l'émergence de menaces autonomes pilotées par l'IA, les organisations – publiques comme privées – subissent une pression sans précédent. En France, notamment, c'est l'escalade, avec une recrudescence d'incidents touchant des infrastructures publiques critiques, confirmant la vulnérabilité des systèmes de l'État. Dans le même temps, la DINUM a fait savoir qu'elle allait migrer ses postes Windows sous Linux : un signal encourageant qui cache néanmoins bien des défis opérationnels à relever.

VULNÉRABILITÉS CRITIQUES : L'EXPLOITATION EN QUASI-TEMPS RÉEL DEVIENT LA NORME

Avril 2026 a été marqué par le déploiement d'une vague de correctifs importants et, comme en miroir, des exploitations zero-day en série, avec un time-to-exploit (TTE) de plus en plus court (parfois moins de 24h après la divulgation).
Pour se faire une idée du phénomène, on peut consulter le site web : **https://zerodayclock.com/**

- Microsoft : 165 failles corrigées en un seul Patch Tuesday

- CVE-2026-32201 (SharePoint Server, CVSS 6.5) : **exploitée activement**, permet l'**usurpation d'identité** et l'accès à des données sensibles. Liée à des campagnes de **ransomware et cyberespionnage** (chaîne d'exploitation *ToolShell*).
- CVE-2026-33824 (Windows IKE, CVSS 9.8) : **exécution de code à distance** (RCE) sans authentification, via des paquets UDP malveillants. **Critique pour les infrastructures réseau**
- CVE-2026-33826 (Active Directory, CVSS 8) : **prise de contrôle totale d'un domaine** possible via une faille RPC. **Menace directe pour les identités**
- CVE-2026-33825 (Defender, CVSS 7.8) : **élévation de privilèges**, exploitée pour désactiver les outils de sécurité et déployer des malwares.

→ **Impact** : Les RSSI doivent **prioriser les correctifs** et **renforcer la surveillance** des comportements anormaux (ex. : utilisation suspecte de PowerShell ou d'outils légitimes).

- Cisco et Fortinet : des failles critiques dans les équipements réseau

• CVE-2026-20147/20180/20186 (Cisco ISE, CVSS 9.9) : **exécution de code à distance** dans les solutions d'**authentification et gestion des accès** exploitée par des groupes APT.
• CVE-2026-35616 (FortiClientEMS, CVSS 9.8) : **contournement de sécurité et exécution de code arbitraire**. Utilisée dans des attaques ciblant les **administrateurs système**
• CVE-2026-20133 (Cisco Catalyst SD-WAN, CVSS 7.5) : **atteinte à la confidentialité des données**, exploitée activement.

→ Risque : les **équipements réseau mal configurés** restent des **portes d'entrée privilégiées** pour les attaquants.

- **Open source et supply chain : l'attaque par les dépendances**

• **Compromission du paquet npm *Axios*** : des versions malveillantes (v1.14.1 et v1.30.4) ont été publiées, permettant l'**exfiltration de données** ou l'**exécution de code arbitraire**. **Impact potentiel : des milliers de projets Node.js**
• **Vulnérabilités dans Traefik** (CVE-2026-41174, 39858, etc.) : **contournement de politique de sécurité** avec des **PoC publics disponibles**
• **GLPI** (CVE-2026-26026, CVSS 9.1) : **exécution de code à distance** via une faille SQLi. **Ciblage des outils de gestion IT**.

Enjeu : la **chaîne logistique logicielle** confirme son statut de **vecteur d'infiltration privilégiée** comme l'avait anticipé l'ANSSI en 2025.

RANSOMWARES ET EXTORSION : LA PROFESSIONNALISATION SE POURSUIT

Les ransomgangs **ciblent toujours plus des organisations critiques** (santé, énergie, administrations) avec des **demandes de rançon multimillionnaires** et des **techniques de double extorsion** (chiffrement + menace de divulgation).

- Nouvelles souches et cibles prioritaires

• **Attaque contre l'Agence nationale des titres sécurisés (ANTS)** : fuite massive de données, impactant des **millions de citoyens français**.
• **Booking.com, McGrawHill, Medtronic** : des **fuites de données sensibles** (coordonnées clients, dossiers médicaux) ont été revendiquées par des groupes comme **Interlock** (exploitant la CVE-2026-20131 dans Cisco).
• **Vercel** : **compromission de son infrastructure** (19 avril), avec **accès non autorisé à des dépôts clients**. Les attaquants ont tenté de **monétiser les données volées** sur des forums illégaux.

Tendances :

• **double extorsion systématique** (chiffrement + fuite).
• **ciblage des PME et collectivités** (moins matures en cybersécurité).
• **fragmentation des groupes** : multiplication de petits acteurs **agiles et difficiles à tracer**.

FOCUS | PIRATAGE DE L'ANTS : 11,7M DE COMPTES COMPROMIS ET UN ADOLESCENT INTERPELLÉ

Le 15 avril 2026, l'Agence nationale des titres sécurisés (ANTS), désormais rebaptisée *France Titres*, a subi une intrusion informatique majeure qui a secoué l'administration française. L'attaque a permis l'exfiltration de données sensibles liées à la gestion des titres d'identité, des passeports et des permis de conduire.

L'ampleur de la fuite : si le chiffre officiel communiqué par le ministère de l'Intérieur établit la compromission de **11,7 millions de comptes personnels**, des sources de la communauté cybernétique et des veilleurs du Darkweb chiffrent à **19 millions d'enregistrements**. Les données exposées incluent des informations d'identification nominative, des adresses électroniques, des dates de naissance et potentiellement des numéros de titres en cours de validité. Cette exposition ouvre la voie à des campagnes de *phishing* ultra-personnalisées et des tentatives d'usurpation d'identité.

L'enquête et la capture d'un mineur de 15 ans : contrairement aux hypothèses initiales évoquant un groupe criminel organisé ou une attaque étatique sophistiquée, l'enquête menée conjointement par la police judiciaire et la gendarmerie nationale a rapidement orienté les investigations vers
le profil d'un **mineur de 15 ans** comme principal suspect de cette cyberattaque, pseudo-nommé *breach3d*. Le prévenu aurait exploité une faille de configuration dans les systèmes d'authentification du portail *ants.gouv.fr*. Techniquement, il s'agit probablement soit d'une faille *path traversal* (qui permet de lire des fichiers arbitrairement sur le serveur qui exécute une application en contournant la hiérarchie des répertoires : code et données ; identifiants d'accès aux systèmes back-end ; fichiers sensibles de l'OS) ; soit une vulnérabilité IDOR pour *insecure direct object reference*, qui apparaît lorsqu'une application utilise un identifiant fourni par l'utilisateur pour accéder à un objet interne sans vérifier qu'il y soit autorisé (interversion manuelle d'IDs utilisateurs via l'URL). Ce problème s'inscrit dans la catégorie plus large du contrôle d'accès défaillant, mais il se distingue par la difficulté de l'éliminer complètement, notamment avec des applications modernes basées sur des API.

Cette arrestation soulève plusieurs questions :

• **la vulnérabilité des infrastructures publiques :** comment une administration centrale de l'État a-t-elle pu être compromise par un adolescent, suggérant des lacunes potentielles dans les tests d'intrusion ou la surveillance des accès ?
• **le profil des attaquants :** cet incident illustre la survivance ou la recrudescence des *script kiddies* : jeunes talents autodidactes capables de causer des dommages systémiques majeurs, parfois sans intention malveillante initiale, mais par curiosité ou défi technique.
• **la réponse judiciaire :** la procédure engagée contre un mineur pour un crime de cette ampleur (atteinte aux STAD) pose la question de la

proportionnalité des sanctions dans un cadre de cybersécurité nationale.

Conséquences immédiates : suite à l'incident, le site de l'ANTS a été placé en maintenance préventive dès le 24 avril 2026 pour sécuriser les accès et auditer l'ensemble des bases de données. Les citoyens concernés ont reçu des notifications personnalisées les invitant à modifier leurs mots de passe et à surveiller leurs comptes. Des campagnes de sensibilisation ont été lancées pour alerter le public sur les risques de *phishing* utilisant les données volées, notamment des faux courriels imitant l'administration pour demander des frais de renouvellement de titre.

Cet épisode confirme que la cybermenace ne se limite pas aux grands groupes criminels internationaux : elle peut provenir de toute personne disposant de compétences techniques (mêmes basiques), quel que soit son âge, rendant la vigilance et la mise à jour constante des systèmes d'information indispensables pour toutes les administrations.

Cette attaque soulève *in fine* plusieurs enjeux majeurs :

- **sensibilité des données concernées** : les informations liées aux titres d'identité, passeports et permis de conduire constituent un socle d'identité individuelle critique.
- **risque de fraude secondaire** : usurpation d'identité, escroqueries ciblées, campagnes de *phishing* exploitant des données précises et crédibles pour tromper les victimes.
- **crédibilité des infrastructures publiques et doute sur les capacités de l'Etat à se sécuriser lui-même** : l'ANTS représente l'un des piliers numériques de l'État ; toute faille repose constamment le débat sur la résilience des SI publics et la nécessité d'une souveraineté numérique renforcée.

FUITES DE DONNÉES : L'EXPOSITION PERMANENTE DES ORGANISATIONS

Avril 2026 a vu une **recrudescence des *leaks***, souvent liées à des :

- **erreurs de configuration** (ex. : bases de données cloud exposées) ;
- **compromissions de comptes** (*phishing*, usurpation d'identité, gestion des mdp défaillante) ;
- **attaques sur la supply chain** (ex. : fournisseurs de services)

- Cas emblématiques :

- Hong Kong Hospital Authority : **56 000 dossiers patients exposés** (2 avril), suite à une cyberattaque ciblée ;
- BePrime (Mexique) : **fuite de données clients** (Starbucks, Iberdrola, etc.) due à un **compte admin sans MFA** (authentification forte/ multifactorielle) ;
- Ministère de l'Intérieur français : **nouvelles fuites** (suite à des compromissions de comptes), confirmant la **vulnérabilité persistante des administrations**

Conséquences :

- **alimentation de l'écosystème criminel** (revente de données, attaques secondaires) ;
- **perte de confiance** dans les services numériques (santé, éducation, administrations).

PHISHING ET INGÉNIERIE SOCIALE : L'HUMAIN RESTE LE MAILLON FAIBLE

Les campagnes de ***phishing* ciblé** (*spear phishing*, *whaling*) et de **compromission de comptes** se **sophistiquent** :

- **utilisation de *deepfakes*** (voix, vidéos) pour tromper les victimes ;
- **usurpation d'identités professionnelles** (ex. : faux emails de prestataires de confiance) ;
- **exploitation de données issues de fuites précédentes** (ex. : fuites LinkedIn, Adobe).

- Exemples marquants :

- **attaque contre un détachement militaire français** : compromission de comptes via un **faux ordre de mission** ;
- **campagnes de *phishing* ciblant les RSSI** : utilisation de **fausses alertes de sécurité** pour inciter à cliquer sur des liens malveillants.

Recommandations :

- **authentification forte** obligatoire.
- **sensibilisation renforcée** aux nouvelles techniques (*deepfakes spear phishing*).
- **surveillance des comportements anormaux** (ex. : connexions depuis des pays inhabituels).

GÉOPOLITIQUE ET CYBERMENACE : LA GUERRE HYBRIDE S'INTENSIFIE

Les **acteurs étatiques** (Russie, Chine, Iran) **intensifient leurs opérations** :

- **Attaques destructrices** : utilisation de ***wipers*** (ex. : attaque contre **Stryker Corporation**, 200 000 appareils « effacés » dans 79 pays), associées aux bombardements physiques (Etats du Golfe arabo-persique)
- **Cyberespionnage** : ciblage des **télécoms, énergéticiens et entités diplomatiques** (ex. : APT chinois UNC3886 contre les opérateurs télécoms

de Singapour) ;

- **Prépositionnement** : **infiltration silencieuse** des infrastructures critiques en vue de futures attaques.

Alerte ANSSI : la France anticipe des **scénarios de guerre hybride** (ex. : attaques coordonnées contre les **réseaux électriques**).

BILAN CHIFFRÉ DU MOIS

Catégorie	Avril 2026	Évolution vs. 2025	Source
Vulnérabilités critiques	165 (Microsoft + autres éditeurs)	+150%	CERT-FR, ANSSI
Incidents de cybersécurité	~1 200 (ANSSI)	**+100%** (vs 2025)	ANSSI
Fuites de données	30+ (majeures)	**Stable** (mais volume de données en hausse)	ZATAZ, Le Monde Informatique
Attaques par *ransomware*	50+ (ciblées)	**+20%**	CM-Alliance
Exploitations *zero-day*	10+ (dont SharePoint, IKE, Axios)	**+200%**	CERT-FR, Microsoft

SOUVERAINETÉ NUMÉRIQUE : LA DINUM VEUT PASSER À LINUX

La Direction interministérielle du numérique (DINUM) a officialisé le 8 avril 2026 sa décision de migrer ses postes Windows vers Linux, en commençant par ses 250 agents et invitant chaque ministère à se préparer.

Le choix s'est porté sur **NixOS**, une distribution originale et intéressante qui garantit la reproductibilité des postes grâce à une **configuration déclarative**. Deux versions émergent de cette base technique : **Sécurix**, dédié à la sécurité des administrateurs, et **Bureautix**, conçu pour la bureautique.

Derrière **l'effet d'annonce encourageant**, se cache une **réalité technique très ambitieuse**, car nécessairement inscrite dans un long-terme **rarement compatible avec le temps politique**. **L'hétérogénéité du parc informatique de l'Etat**, en miroir inversé avec l'avant-gardisme de la gendarmerie (GendBuntu, installé en 15 ans), constitue un défi majeur, sans compter **les coûts et le besoin de compétences métiers** spécifiques, comme l'a par exemple appris à ses dépens la ville de Munich en Allemagne. Le risque étant de voir fonctionner deux OS en parallèle, générant un effet contre-productif.

PERSPECTIVES : VERS UNE CYBERSÉCURITÉ PLUS RÉSILIENTE ?

Ce mois d'avril a montré que :

- **l'IA est un accélérateur de menaces** (automatisation et sophistication des attaques).
- **la supply chain reste le talon d'Achille** des organisations.
- **les acteurs étatiques et criminels collaborent** de plus en plus.

Pour les mois à venir, les experts anticipent :

- **une augmentation des attaques autonomes** (pilotées par IA).
- **un ciblage accru des infrastructures critiques** (énergie, santé, transports).
- **une régulation plus stricte** (NIS2, Cyber Resiliency Act).

→ Message-clé : **la cybersécurité doit devenir une priorité stratégique**, avec une **approche globale** (technique, organisationnelle, réglementaire).

POUR ALLER PLUS LOIN :

Le rapport IOCTA 2026 (Internet Organised Crime Threat Assessment) d'Europol alerte sur l'accélération de la cybercriminalité, propulsée par l'IA, le chiffrement de bout en bout et les proxys résidentiels qui créent un fossé technologique face aux enquêteurs.
Les fraudes en ligne se sont industrialisées grâce à l'automatisation et aux fermes de cartes SIM, tandis que le *ransomware*, toujours omniprésent, privilégie l'extorsion par fuite de données. L'infrastructure criminelle se fragmente et se spécialise, rendant le traçage financier via cryptomonnaies et mixers de plus en plus complexe.
Parallèlement, la pédocriminalité augmente avec la monétisation accrue des abus, l'utilisation massive d'applications chiffrées et la montée en puissance du contenu synthétique généré par IA. Europol conclut que la réponse nécessite une coopération privée/publique renforcée, et l'adoption urgente d'outils d'IA par les forces de l'ordre pour combler ce retard opérationnel.

SOURCES PRINCIPALES

- *ANSSI :* **Panorama de la cybermenace 2025**
- *CERT-FR :* **Bulletins d'actualité avril 2026**
- *Le Monde Informatique :* **Microsoft corrige 165 failles** / **Fuite ANTS**
- *Le Monde :* **Piratage de l'ANTS : un mineur appréhendé**
- *ZATAZ :* **Actualités cyber**
- *Cyberactualité.fr :* **Actualités avril 2026**
- *CM-Alliance :* **Major Cyber Attacks April 2026**
- *SharkStriker :* **Data Breaches April 2026**
- *Linuxfr.org :* **LaDINUM : passage de Windows à Linux**
- *Code.gouv.fr :* **NixOS et son écosystème**
- *IT-connect :* **DINUMpasse de Windows à Linux : les autres ministères doivent préparer leur plan**
- *01Net :* **Cybersécurité : les 10 menaces qui planent sur 2026**

A PROPOS DE...

Yannick PECH *est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, détenteur d'une certification de Pentester junior (eJPT) et de la certification EBIOS Risk Manager de l'ANSSI.*
Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur associé au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste à la Compagnie européenne d'intelligence stratégique (CEIS), consultant-analyste au CRR-FR (OTAN-France) et réserviste opérationnel-spécialiste de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie.
Il prépare actuellement la certification ISO-27001 (GRC/SMSI).

#Cybersecurity #ZeroDayExploits #RansomwareThreats #DataBreaches #SupplyChainSecurity #AIThreatLandscape #CriticalInfrastructureSecurity #CyberResilience #LinuxMigration #CyberDefense Strategy

04/05/2026