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

Par Jacqueline Sala

Focus Cybersécurité. Mars 2026 "Attaques protéiformes, exploitation précoce des vulnérabilités et pression accrue sur les organisations : un mois de cristallisation de la cybermenace". Yannick Pech

Lemois de mars 2026 confirme latendance amorcée en débutd'année: lacybersécurité entre dansunephase de pression constante et multidimensionnelle. Entre l'exploitation active de vulnérabilités critiques, la multiplication des campagnes de ransomwares et la poursuite des fuites de données, les organisations publiques comme privées font face à une menace toujours plus structurée et protéiforme. Dans ce contexte où acteurs étatiques et criminels intensifient leurs opérations, les autorités renforcent leurs alertes. La gestion des accès, la sécurisation des infrastructures exposées et la maîtrise des dépendances technologiques constituent définitivement des enjeux cruciaux.

VULNÉRABILITÉS CRITIQUES : EXPLOITATION RAPIDE ET SURFACE D'ATTAQUE ÉTENDUE

Le mois de mars a été marqué par la publication et **l'exploitation rapide de plusieurs vulnérabilités critiques**, notamment dans des solutions largement déployées (**VPN**, équipements réseau, **logiciels collaboratifs** et **outils open source**). Le délai entre la divulgation d'une faille et son exploitation active continue de se réduire drastiquement.

Certaines vulnérabilités ont été **exploitées avant même la publication de correctifs** complets, illustrant une capacité accrue des attaquants à surveiller les failles émergentes et à industrialiser leur exploitation. Les infrastructures exposées sur l'Internet — notamment les équipements mal configurés ou non mis à jour — restent des cibles privilégiées.

Cette dynamique renforce **l'importance d'unegestion proactive des vulnérabilités** : inventaire précis des actifs, priorisation des correctifs, supervision continue et réduction de la surface d'exposition : désactivation des services inutiles (ports logiciels), segmentation réseau.

FACE À CES FAILLES CRITIQUES, L'ANSSI TIRE LA SONNETTE D'ALARME

Le 11 mars, l'agence a publié son panorama de la cybermenace 2025. Il révèle une année marquée par une **persistance de la menace à un niveau très élevé**, comparable à celui de 2022.

Voici les points-clés relevés :

Bilan chiffré (Année 2025)

- **Incidents recensés :** 831 (niveau de menace « très élevé », comparable à 2022).
- **Événements traités :** 3 580 (baisse de 20 % par rapport au précédent).
- **Tendance majeure :** recul des rançongiciels classiques au profit de l'**exfiltration pure de données** (espionnage).

Acteurs malveillants et géopolitique

- **Principales menaces : Russie** et **Chine** (espionnage stratégique, pré-positionnement).
- **Floutage des frontières :** effacement progressif entre cybercriminels et acteurs étatiques (partage d'outils, spécialisation des rôles).
- **Alerte rouge :** attaques destructrices coordonnées contre les **infrastructures électriques polonaises** fin 2025, signalant un scénario de guerre hybride que la France essaie d'anticiper.

Secteurs ciblés

- **Priorité absolue :** télécommunications (équipements mobiles), réseaux diplomatiques, énergie.
- **Méthode :** espionnage de longue haleine et collecte de renseignement stratégique (APT).

Évolution des tactiques

- **Ingénierie sociale :** passage du *phishing* classique au *spear phishing* via ***deepfakes*** ; généralisation de l'**usurpation d'identitéde prestataires** de confiance.
- **Outillage :** détournement massif d'outils légitimes (PowerShell, cloud) et utilisation de l'**IA générative** pour automatiser les attaques et créer du contenu trompeur.
- **DDoS :** attaques fréquentes mais peu techniques, visant surtout à **nuire à laréputation** des victimes.

Recommandations-clés

- Accélérer l'application des correctifs de sécurité (vulnérabilités critiques).
- Renforcer la détection des comportements anormaux (usage d'outils légitimes).
- Préparer des exercices de crise pour des scénarios de perturbation d'infrastructures vitales.
- Former les utilisateurs aux nouvelles menaces (*deepfakes*, hameçonnage ciblé dit *spear phishing/whaling*).

LE MODÈLE ÉCONOMIQUE DU RANSOMWARE : UNE PRESSION TOUJOURS FORTE, DES ATTAQUES PLUS CIBLÉES

Les attaques par rançongiciel se maintiennent à un niveau élevé en mars, avec une évolution notable : les groupes cybercriminels privilégient de plus en plus des attaques ciblées à forte valeur, plutôt que des campagnes massives indiscriminées.

Le mois de mars confirme ainsi la professionnalisation du modèle du rançongiciel et la mise en exergue de deux *ransom gangs* en particulier :

- le **groupe Clop** : après 334 attaques en novembre 2025, intensification des campagnes contre les organisations publiques françaises, hôpitaux et services municipaux ;
- **LockBit** et nouvelles souches opportunistes : ciblage accru des entreprises françaises ;
- **demandes de rançons élevées** : montants multimillionnaires, perturbations opérationnelles significatives.

L'ANSSI a émis des alertes renforcées, et coordonné les efforts de réponse à travers le pays.
Les **modes opératoires** observés confirment plusieurs tendances :

- **double extorsion** systématique (chiffrement + menace de divulgation des données) ;
- **exfiltration préalable des données** pour maximiser la pression ;
- ciblage de **secteurs critiques ou peu matures** (collectivités, PME, santé, éducation).

Par ailleurs, la fragmentation de l'écosystème *ransomware* se poursuit, avec une multiplication de groupes plus petits mais très actifs, rendant la menace plus diffuse et difficile à anticiper.

FUITES DE DONNÉES : UNE EXPOSITION CONTINUE DES ORGANISATIONS FRANÇAISES

Dans la continuité de janvier et février, le mois de mars reste marqué par un flux constant de fuites de données. Citons en particulier bien qu'américain le cas du *leak* d'Anthropic du 31 mars dont on peut considérer qu'il s'est déroulé en deux temps. Déjà concernée en 2025 par ce type d'erreur humaine, Anthropic a accidentellement rendu publique une partie du code source (500 000 lignes, fichier source-map exposé) de son interface en ligne de commande (CLI), « Claude Code ». Au-delà du nouveau coup porté à l'image de la startup américaine, des références internes aux projets des futurs modèles d'IA baptisés « Mythos » et « Capybara » ont été divulgués, ainsi que des indices sur la feuille de route technique de l'entreprise.

En somme, des informations commercialement sensibles. Dans un deuxième temps, prise de court par les évènements du fait d'un partage viral sur X, l'entreprise a vu son dépôt officiel sur GitHub être concurrencé par des *repos* malveillants largement indexés par le moteur Google. Notamment « claw-code », devenu le dépôt à la croissance la plus rapide de l'histoire de la plateforme d'informatique. Ainsi, en proposant des *forks* (logiciels dérivés) du code d'Anthropic, des pirates ont piégé les curieux en surfant sur l'engouement suscité par ce type de *leaks*. Ces chevaux de Troie comportaient notamment des *infostealers*. Au-delà de ces compromissions, les pirates ont par ailleurs mis la main sur des pièces de code très instructives leur permettant de monter en compétences pour piloter des agents IA par leurs propres moyens.

D'une manière générale en France, les incidents liées à des fuites concernent une grande diversité d'acteurs : entreprises de services, structures locales, associations, plateformes numériques. Les données exposées incluent :

- informations d'identité (noms, prénoms, dates de naissance) ;
- coordonnées (adresses, numéros de téléphone) ;
- données professionnelles ou administratives ;
- documents justificatifs (pièces d'identité, contrats…).

Ces fuites, souvent liées à des erreurs de configuration, des accès insuffisamment sécurisés ou des compromissions de comptes, alimentent un écosystème criminel structuré, où les données sont revendues, agrégées et exploitées pour des attaques secondaires. Le phénomène devient structurel : il ne s'agit plus d'incidents isolés, mais d'une exposition permanente des données, qui fragilise la confiance dans les services numériques.

Le ministère de l'Éducation nationale ciblé : Due à un compte usurpé, la fuite de données a compromis les dossiers personnels (identifiants, coordonnées) de 243 000 enseignants-stagiaires. L'incident a déclenché un plan de sécurisation annoncé par le ministère pour les mois à venir, soulignant la vulnérabilité persistante des structures éducatives face aux compromissions d'identité.

COMPTES COMPROMIS ET HAMEÇONNAGE : LE FACTEUR HUMAIN TOUJOURS CENTRAL

Les campagnes de *phishing* et de compromission de comptes continuent de représenter un vecteur d'entrée majeur pour les attaquants. En mars, plusieurs alertes ont mis en évidence des campagnes particulièrement sophistiquées, combinant :

- usurpation d'identités professionnelles crédibles ;
- utilisation de données issues de fuites précédentes ;
- scénarios personnalisés (factures, notifications administratives, accès cloud…).

La compromission de comptes (messagerie, accès SaaS, comptes administrateurs) reste l'un des points d'entrée les plus fréquents dans les incidents majeurs. Une fois l'accès obtenu, les attaquants peuvent se déplacer latéralement, exfiltrer des données ou préparer une attaque plus large. Cela confirme un énième fois que la cybersécurité ne repose pas uniquement sur des outils techniques, mais aussi voire surtout sur des pratiques organisationnelles : authentification multifactorielle, sensibilisation des utilisateurs, surveillance des comportements anormaux...

DÉPENDANCES NUMÉRIQUES ET CHAÎNES DE SOUS-TRAITANCE : UN RISQUE AMPLIFIÉ

Les incidents observés en mars mettent également en lumière un point critique : la dépendance aux prestataires et aux services tiers. De nombreuses compromissions trouvent ainsi leur origine dans la chaine logistique :

- un fournisseur de service mal sécurisé ;
- un accès tiers compromis ;
- une intégration technique insuffisamment contrôlée.

Cette dépendance complexifie la gestion des risques : une vulnérabilité chez un prestataire peut impacter simultanément plusieurs organisations clientes. La sécurisation des chaînes de sous-traitance devient donc un axe stratégique majeur nécessitant audits, contractualisation renforcée et exigence de transparence.

PERSPECTIVES

doivent désormais composer avec un environnement où les attaques sont continues, les vulnérabilités rapidement exploitées et les données régulièrement exposées.

Face à cette réalité, trois priorités s'imposent :

- renforcer la gestion des vulnérabilités et des accès ;
- sécuriser les relations avec les prestataires et l'écosystème en général ;
- développer une culture de cybersécurité à tous les niveaux de l'organisation.

La capacité à anticiper, détecter et réagir rapidement devient un facteur-clé de résilience dans un paysage numérique de plus en plus instable.

RÉSUMÉ

1. **Vulnérabilités critiques :** exploitation rapide et surface d'attaque toujours étendue. Le *time-to-exploit* (TTE) se raccourcit : les failles sont exploitées dès leur publicisation voire avant leur caractérisation et assignation formelles dans les systèmes de *scoring* (CVE/EPSS/CVSS). 2. **Panorama de la cybermenace 2025 de l'ANSSI :** une année tendue, au niveau de 2022. Les rançongiciels reculent au profit de l'exfiltration de données pure. Les acteurs étatiques (Russie, Chine) dominent, floutant les frontières avec le cybercrime, et ciblent télécoms, énergie et diplomatie via des APT. Les attaques utilisent *deepfakes*, outils légitimes détournés, IA générative, et aussi DDoS visant la réputation. 3. **Ransomwares :** attaques ciblées et généralisation de la double extorsion (chiffrement + fuite de données), professionnalisation accrue visant hôpitaux, collectivités et entreprises françaises pour des rançons très élevées. L'ANSSI renforce les alertes, tandis que la fragmentation des groupes rend la menace plus diffuse et complexe à contrer. 4. **Fuites de données :** exposition continue des organisations (entreprises, collectivités, ministère de l'Éducation nationale), souvent par erreurs techniques ou humaines (*leak* Anthropic) ou usurpation de comptes. Ces fuites alimentent un écosystème criminel et fragilisent la confiance numérique. 5. ***Phishing* et compromissions de comptes :** facteur humain toujours déterminant. Le *spear phishing* devient la norme en combinant usurpation d'identités et données volées. MFA, sensibilisation et détection précoce amélioreraient la résilience. 6. **Sous-traitance et dépendances :** un maillon faible de plus en plus exploité. Les compromissions via fournisseurs ou accès tiers soulignent le risque systémique des dépendances numériques : une faille chez un prestataire peut affecter des dizaines d'organisations.

SOURCES PRINCIPALES UTILISÉES

VeilleCyber.fr - flux et alertes cybersécurité - mars 2026
https://veillecyber.fr

BonjourLaFuite - Suivi des fuites de données - mars 2026
https://bonjourlafuite.eu.org

CERT-FR - Bulletins d'alertes et vulnérabilités - mars 2026
https://www.cert.ssi.gouv.fr/

ANSSI - Panorama de la cybermenace 2025 - mars 2026
https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2025/

Zataz - Cyber actualités et ransomware 2025-2026 - mars 2026
https://www.zataz.com

Numerama - Les futurs projets d'Anthropic dévoilés par erreur/L'appât était parfait… - mars 2026
https://www.numerama.com/tech/2222683-fuite-claude-code-2026-les-futurs-projets-danthropic-devoiles.html ; https://www.numerama.com/cyberguerre/2225831-lappat-etait-parfait-certains-ont-profite-autrement-du-leak-de-claude-code.html

Zscaler Blog - Anthropic Claude Code Leak - 1er avril 2026
https://www.zscaler.com/blogs/security-research/anthropic-claude-code-leak

Le Monde Informatique - Analyses et incidents cyber - mars 2026
https://www.lemondeinformatique.fr

A PROPOS DE L'AUTEUR

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).*

06/04/2026