THALES
Building a future we can all trust

Le Nouveau Visage des Cybermenaces en 2025

Cybersecurity Premium Services

www.thalesgroup.com

THALES
Building a future we can all trust

Paysage de la menace cyber 2025

Analyse des tendances

www.thalesgroup.com

Introduction & Chiffres Clés (Le Choc)

Volume total : 51 863 vulnérabilités en 2025

+41,3% par rapport à 2024

Rapidité d'attaque : « Weaponization »

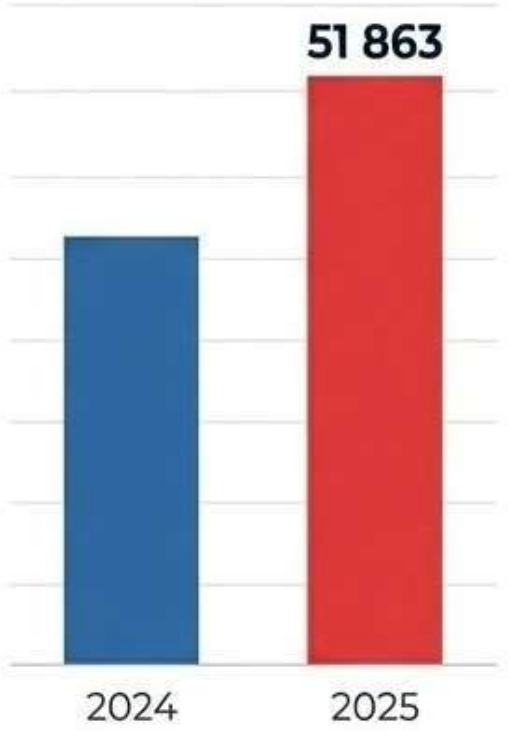
La militarisation des failles en moins de 24h

Ransomware: 7 701 incidents recensés

Les attaques mondiales par rançongiciel ont augmenté de 32 % en 2025.

Tendance majeure : Passage du **chiffrement pur à l'extorsion de données seule** (sans blocage des système)

Croissance des vulnérabilités



Evolution technique : De l'IA au supply Chain

> Exploitation des « Edge Devices »

Ciblage massif des VPN et pare-feux (ex : CVE-2025-61882 sur Oracle)

> L'IA offensive

Première campagne d'espionnage à grande échelle orchestrée par l'IA en septembre 2025 (automatisation de la reconnaissance)

> Supply Chain

Attaques via les écosystèmes Open Source (npm, PyPi)

> Living-off-the-land

Utilisation d'outils système légitimes et d'outils RMM pour rester furtif.

Le Top3 des Groupes de Ransomware (H2 2025)

Groupe	Volume d'attaques	Particularité
Qilin	708	Leader incontesté, très actif sur le secteur manufacture.
Akira	415	Très présent dans le secteur du conseil et de la finance.
Inc Ransom	250	Forte présence en Australie et sur les services.

Analyse par Secteurs Critiques

Industrie (Manufacturing) : Cible n°1 mondiale (2801 attaques).
Menace croissante sur les systèmes industriels (OT/ICS)

Santé : Espionnage par des groupes étatiques (Chine/Russie) notamment sur des données de R&D; vol d'identifiants Cloud

Finance : Retour des malwares ATM et ciblage des crypto-monnaies par la Corée du Nord (Lazarus)

Télécoms : Espionnage des infrastructures 5G et exploitation des protocoles historiques (TETRA)

Défense : Attaque de grande ampleur (Rootkits kernel, persistance Cloud par des acteurs étatiques)

Zoom Géographique : Focus France & Europe

France

- 175 attaques via des ransomware

- **L'ANSSI constate une hausse de 15% en 2025 par rapport à 2024, avec plus de 4 300 incidents, avec un ciblage prioritaire des secteurs du transport, de l'énergie et de la défense.**
- Qilin domine (40% des attaques au S2)
- Hausse massive du hacktivisme et des fraudes QR Code/SMS

Benelux

- Belgique très ciblée sur l'e-commerce
- Luxembourg plus épargné mais touché par le hacktivisme pro-russe

Espagne

- Fort taux de cybercriminalité
- 248 fuites de données sur le Dark Web

Que nous devons conclure ?

1

La fin du périmètre traditionnel

Les identités Cloud et les API sont les nouvelles frontières.

2

Urgence du Patching

Le délai de 24h impose une automatisation de la veille vulnérabilités.

3

Hygiène Identity-Centric

La compromission d'identifiants est le vecteur principal en 2025.


THALES
Building a future we can all trust
Prediction
www.thalesgroup.com

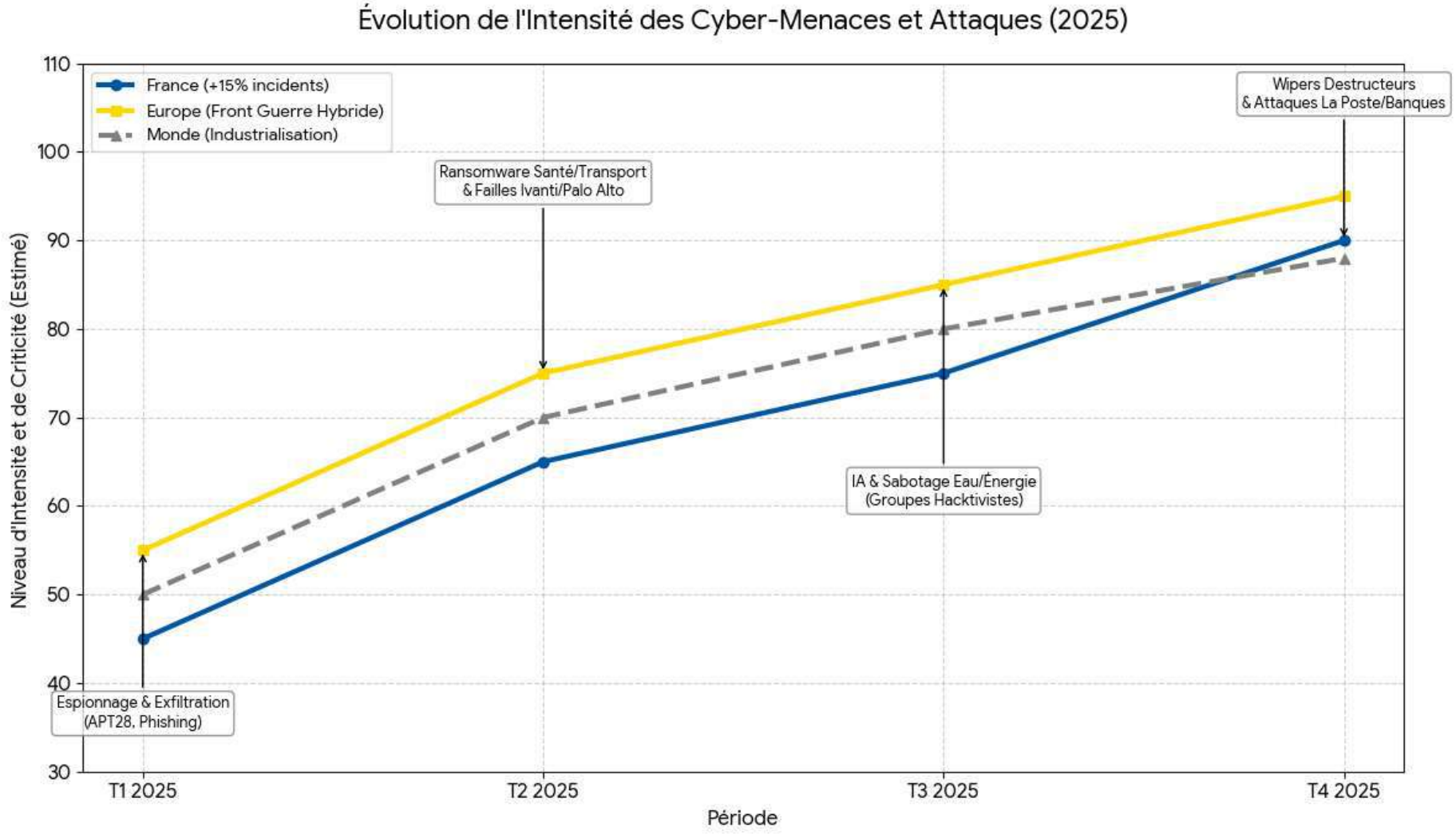
L'IA un axe de cybermenace

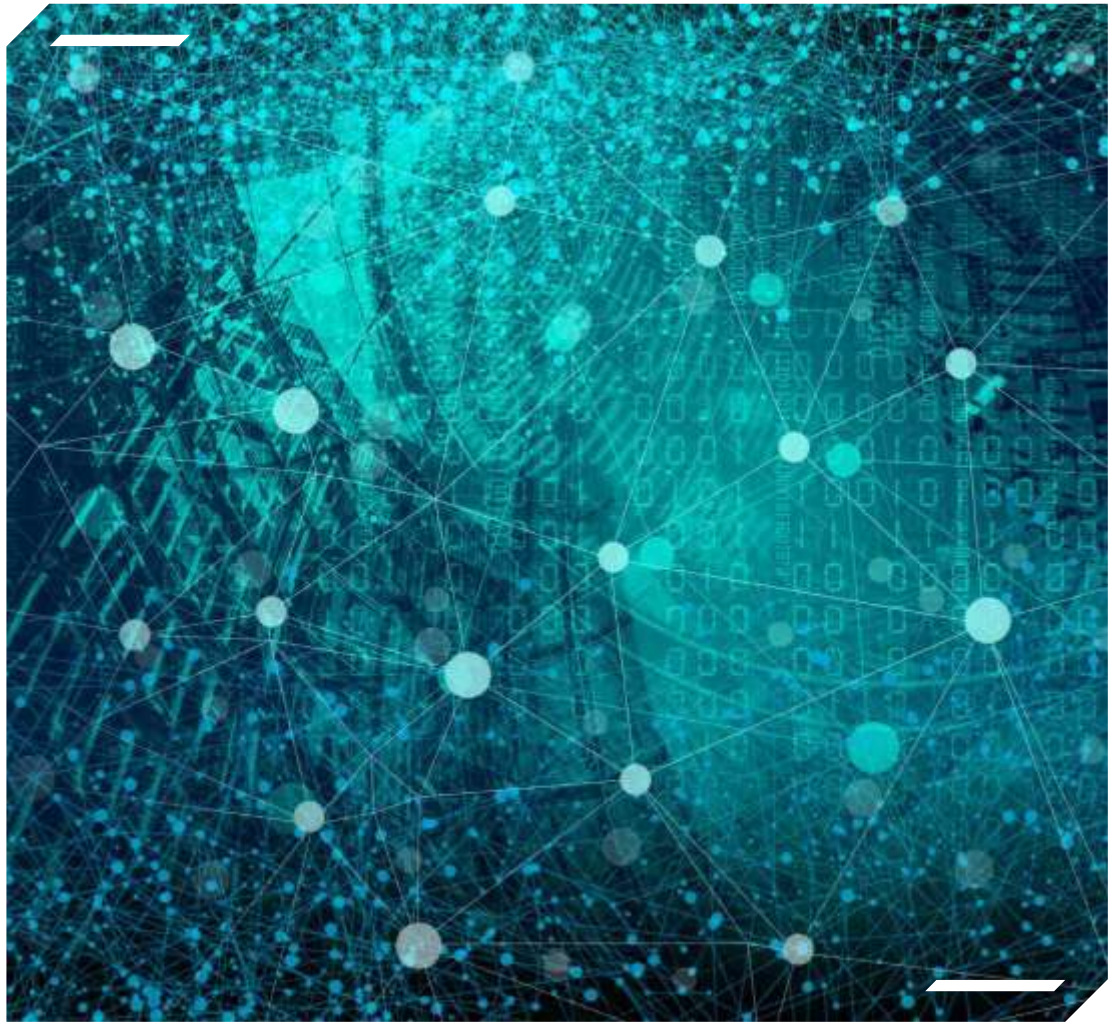
- L'IA rend les cyberattaques beaucoup plus sophistiquées.
- Les cybercriminels industrialisent massivement l'utilisation de l'IA.
- Le phishing est devenu hyper-personnalisé et sans erreur.
- Les malwares polymorphes échappent aux antivirus traditionnels.
- Les agents autonomes malveillants ont confirmé leur montée en puissance.

Hacktivisme : Nouvelle Cyber-Guerre

- L'IA rend les cyberattaques beaucoup plus sophistiquées.
- La distinction entre cybercriminalité et opérations militaires s'estompe.
- Les infrastructures critiques sont désormais ciblées pour de la déstabilisation.
- Les groupes d'hacktivistes ont un fort soutien étatique.
- Les tactiques incluent des attaques DDoS et des campagnes de désinformation.

Augmentation des attaques sur les CNI





La désinformation: nouvelle cyber guerre moderne

Automatisation de la désinformation

Les fermes à trolls modernes exploitent l'IA générative pour diffuser massivement des récits polarisants et trompeurs.

Impact sur les populations civiles

La désinformation vise à semer le doute, la peur et l'incertitude parmi les populations civiles pendant les conflits.

Campagnes ciblant les tensions mondiales

Des campagnes de désinformation émergent lors de crises maritimes ou sur les infrastructures mondiales, affectant la perception et la stabilité publique.

Conclusion : Défis de 2026

L'IA comme arme d'infiltration

L'intelligence artificielle est utilisée pour orchestrer des infiltrations à grande échelle, menaçant la sécurité de nombreuses entreprises.

Nécessité d'une coordination internationale

Face à ces attaques sophistiquées, la coopération entre pays devient vitale, notamment à travers des initiatives comme le EU Cyber Blueprint.

Renforcer la résilience par l'IA

Le développement de systèmes résilients pilotés par l'IA est indispensable pour anticiper et contrer efficacement ces nouvelles menaces.

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com