Cyberdefense

Communiqué de presse
Paris, le 4 décembre 2025

Security Navigator 2026 : Le cybercrime s'industrialise et devient un des épicentres des équilibres géopolitiques. Un front commun doit se structurer.

Orange Cyberdefense, l'un des leaders européens des services de cybersécurité, dévoile aujourd'hui les conclusions de son enquête internationale annuelle Security Navigator. Fruits, entre autres, de l'analyse de plus de 139 000 incidents de sécurité entre octobre 2024 et septembre 2025 et de divers travaux de recherches reposant sur sa base de données de renseignement cyber propriétaire et des sources OSINT, Open Source Intelligence, il compte parmi ses enseignements :

- La cyber-extorsion a explosé à l'échelle mondiale, avec un triplement des victimes depuis 2020, atteignant 19 000 sociétés dans notre base ;
- Les augmentations des victimes de ce type d'attaques sont criantes et significatives pour certains segments comme les PME qui représentent 2/3 des entreprises impactées, notamment, vecteur d'attaques sur la *Supply Chain ;* mais aussi pour les secteurs critiques comme la finance et les assurances avec +71%, la santé et les transports avec respectivement +69 et +67% d'augmentation des structures touchées.
- La cybersécurité redessine les équilibres géopolitiques à l'image de la manipulation de l'information. La convergence d'intérêts des groupes paraétatiques, des hacktivistes et des organisations mafieuses numériques renforce le phénomène de balkanisation de l'espace cyber. Ils œuvrent pour saper la confiance dans nos démocraties, et désormais, nos économies via des attaques cognitives comme la désinformation.
- L'industrialisation du marché de la cybercriminalité s'appuie aussi sur un nouveau modèle « Crime as-a-service » et sur l'intégration croissante de l'IA pour faciliter les attaques ;
- Malgré cela, la coopération judiciaire internationale et les partenariats public-privé s'avèrent de plus en plus efficaces pour démanteler les réseaux de cybercriminels. Un front commun public/privé est plus que nécessaire.

L'industrialisation du marché du cybercrime accentue l'explosion de la cyber-extorsion

Depuis 2020, le nombre de victimes de cyber extorsion (Cy-X) a triplé, avec une hausse de **44,5 %** en 2025 dans le monde. Les petites et moyennes entreprises (1-249 employés) subissent 2/3 des attaques avec des croissances significatives en Europe (+91 % en Allemagne, +54 % en France). La cyber extorsion se globalise avec 35 nouveaux pays ajoutés à notre étude. Le nombre de victimes s'amplifie notamment en Afrique (+47% de victimes), en Amérique latine (+60%) et en Asie (+82%) et impacte les secteurs critiques : +69% dans la santé, +71% dans la finance et l'assurance ou encore la distribution (+80%) par exemple.

Le phénomène de fragmentation du paysage de la cybercriminalité s'accélère. La dissolution de groupes comme LockBit ou Black Basta a laissé place à une multitude d'acteurs, chacun opérant à une échelle comparable. La liste des acteurs malveillants actifs a presque triplé, passant de 33 à 89.
La cybercriminalité s'était professionnalisée, elle s'est, maintenant, industrialisée s'appuyant sur un modèle « Crime-as-a-Service ».

> **Charl van der Walt, Head of Security Research, Orange Cyberdefense,** souligne : *"Alors que les attaquants se répartissent entre différentes zones géographiques et tailles d'entreprises, il est clair que la perception traditionnelle de la « chaîne d'approvisionnement » en tant que chaîne linéaire est obsolète. En réalité, nous vivons dans un réseau dense d'interdépendance où une seule faiblesse peut permettre une compromission massive. Les petites entreprises et les services essentiels sont devenus des vecteurs privilégiés pour amplifier les conséquences économiques et sociales des attaques. Si les défenses traditionnelles et l'application progressive de la loi sont nécessaires, elles ne suffisent pas à contrecarrer les adversaires agiles qui exploitent cette interdépendance de la société. "*

La convergence entre cybercrime organisé, acteurs étatiques et hacktivistes redessine les tendances de la géopolitique contemporaine.

Le phénomène de balkanisation du cyberespace se manifeste par une division du monde cyber en blocs géopolitiques. Comme révélé dans notre Security Navigator 2025, la frontière entre ces acteurs continue de s'estomper, notamment avec la montée en puissance des hacktivistes, souvent alignés, idéologiquement, avec des États complices. Ils mènent des campagnes de déstabilisation, d'attaques DDoS, de manipulation de systèmes critiques.

L'objectif principal de ces opérations n'est plus seulement la perturbation technique, mais aussi la désinformation, la manipulation de l'opinion et la déstabilisation psychologique. Une véritable stratégie d'attaques cognitives qui démontre l'intrication des différents acteurs. Les hacktivistes

se professionnalisent et exploitent les solutions de cybercriminalité sur étagère « bot as-a-service » pour mener ces campagnes de déstabilisation.

La désinformation complète l'arsenal et devient un des marqueurs de l'évolution de la cybercriminalité et de la géopolitique contemporaine, visant également les entreprises des secteurs critiques. La diffusion de fausses informations, la manipulation de l'opinion publique via des campagnes de désinformation, ou encore la mise en scène de cyber-attaques spectaculaires, alimentent une guerre hybride où la frontière entre cybercriminalité, espionnage et propagande s'estompe.

Par ailleurs, les acteurs étatiques continuent d'investir le cyberespace pour mener leurs opérations de cyberespionnage et sabotage dans un contexte géopolitique sous tension. Ils utilisent des groupes criminels comme des proxies ou des extensions de leur stratégie géopolitique, notamment pour déstabiliser des adversaires ou collecter des renseignements sensibles. Par exemple, les campagnes de Salt Typhoon, attribuées à la Chine, ciblent des infrastructures critiques dans plus de 80 pays, exploitant des vulnérabilités dans des équipements de télécommunications et des réseaux de fournisseurs tiers. Ces opérations illustrent l'intégration de la cyberattaque dans les stratégies géopolitiques des États.

Notre analyse inédite conclut à la montée en puissance des actions de coopération judiciaire internationales et souligne l'efficacité de la lutte contre les organisations cybercriminelles.

La collaboration internationale se renforce avec la participation active de 74 acteurs privés, sous l'égide, entre autres d'Europol, Interpol, ou l'alliance Five Eyes.
L'analyse de 418 actions de law enforcement (2021-2025) fait ressortir une augmentation constante de ces opérations qui aboutissent en majorité à des arrestations (29%), des démantèlements (17%) et des mises en examens (14%).

Une coopération qui fonctionne.

- La coopération entre agences publiques et acteurs privés est essentielle. La majorité des opérations impliquent des partenaires privés, notamment dans la dissuasion et le démantèlement d'infrastructures criminelles.
- La coordination internationale a permis de démanteler des réseaux, de saisir des serveurs, de poursuivre les cybercriminels, et de renforcer la dissuasion.
- La réussite de ces opérations montre que la collaboration public-privé est une arme efficace pour faire face à la multiplication des attaques et à la montée en puissance des groupes cybercriminels.

Pour Hugues Foulon, CEO d'Orange Cyberdefense : *« Loin d'être une fatalité, les conséquences de la balkanisation du cyberespace doivent nous servir d'opportunité pour renforcer la coopération, la transparence et la résilience. La lutte contre le cybercrime organisé passe par une alliance mondiale, publique et privée, pour faire face à une menace qui ne connaît pas de frontières. Orange Cyberdefense est prêt à partager le fruit de son renseignement cyber pour renforcer notre bouclier numérique. ”*

A propos d'Orange Cyberdedense

Orange Cyberdefense est le premier partenaire européen pour les services de cybersécurité, s'appuyant sur plus de 30 ans d'expertise développée au sein du groupe Orange. La filiale fournit de manière indépendante des solutions de services de sécurités managés, de conseil et d'intégration alimentées par ses capacités de renseignement cyber souverain. Elle soutient les organisations afin d'anticiper, de prévenir et de répondre aux cyber-menaces à tout moment. Nos services tirent leur force de la recherche et du renseignement, ce qui nous permet d'offrir à nos clients une connaissance inégalée des menaces actuelles et émergentes. Avec plus de 3 200 experts pluridisciplinaires dans 12 pays et 36 centres de détection répartis dans le monde entier, nous savons comment relever les défis mondiaux et locaux de nos clients grâce à notre ancrage local fort. Nous considérons la cybersécurité comme un enjeu humain et une question sociétale. Nous contribuons donc à construire une société numérique plus sûre en plaçant l'Homme au cœur de nos actions. https://www.orangecyberdefense.com/fr