CHECK POINT™

cp<r>
CHECK POINT RESEARCH

RAPPORT SUR LA CYBERSÉCURITÉ 2026

14ÈME ÉDITION ANNUELLE

SOMMAIRE

01 INTRODUCTION

L'année 2025 confirme l'accélération des transformations du paysage mondial des cybermenaces. Les attaques continuent de gagner en volume, mais surtout en complexité et en coordination. Les cybercriminels, groupes d'espionnage et acteurs liés à des tensions géopolitiques exploitent désormais des environnements numériques toujours plus interconnectés dans lesquels identités, infrastructures cloud, services en ligne et objets connectés multiplient les points d'exposition.

Dans ce contexte, les campagnes malveillantes combinent de plus en plus de techniques. L'ingénierie sociale s'étend bien au-delà du phishing traditionnel, les identifiants compromis deviennent un vecteur d'accès privilégié, tandis que les infrastructures exposées ou les appareils connectés servent de base de lancement pour de nombreuses attaques. L'intelligence artificielle (IA) s'impose également comme un facteur de transformation majeur, capable d'accélérer certaines phases d'attaque tout en créant de nouvelles surfaces de vulnérabilité.

Le rapport 2026 de **Check Point** s'appuie sur des données collectées dans plus de 170 pays, issues des réseaux, du cloud, des endpoints, des environnements mobiles, des e-mails et des analyses menées sur les incidents observés à l'échelle mondiale. Il propose une analyse des grandes tendances qui ont marqué l'année 2025 et met en perspective les évolutions qui devraient façonner l'année 2026.

L'année 2025 marque un véritable tournant pour la cybersécurité. Le volume des attaques augmente, leur sophistication progresse et surtout, elles s'inscrivent dans un contexte géopolitique moins stable. Le cyberespace est devenu un prolongement direct des tensions géopolitiques, avec des groupes d'attaquants qui se revendiquent parfois de certains États. La cybersécurité n'est donc plus un sujet réservé aux experts : elle est devenue un enjeu tant global que stratégique pour les entreprises mais aussi pour la société dans son ensemble.

C'est le même constat pour l'intelligence artificielle, qui transforme profondément le paysage cyber. Si elle relevait de la prospective il y a encore deux ans, elle s'est largement imposée dans les organisations tout au long de 2025 et demeurera plus que jamais au cœur des stratégies numériques cette année encore. Cette bascule ouvre autant de perspectives qu'elle crée une surface d'exposition inédite. L'IA accélère les usages, les métiers, les capacités de défense mais aussi les capacités d'attaque. Les entreprises expérimentent déjà ces technologies, qu'il s'agisse d'IA générative, d'agents intégrés aux grandes plateformes ou de modèles développés en interne. Mais la réalité est que ces projets ne passent pas encore à l'échelle tant que leur sécurité n'est pas démontrée.

Face à cette transformation, le message de **Check Point** est clair : la sécurisation de l'IA doit être pensée de bout en bout. Elle suppose une architecture unifiée, du poste de travail jusqu'aux agents autonomes, qui doivent être considérés comme de véritables collaborateurs numériques, avec ce que cela suppose en termes d'identités, de droits et de traçabilité. Ainsi la sécurité préventive, ADN historique de **Check Point**, (re)devient centrale. C'est précisément l'ambition de ce rapport : éclairer ces transformations et aider les organisations à s'y préparer.

JÉRÔME BOUVET
Directeur Général France
Check Point Software

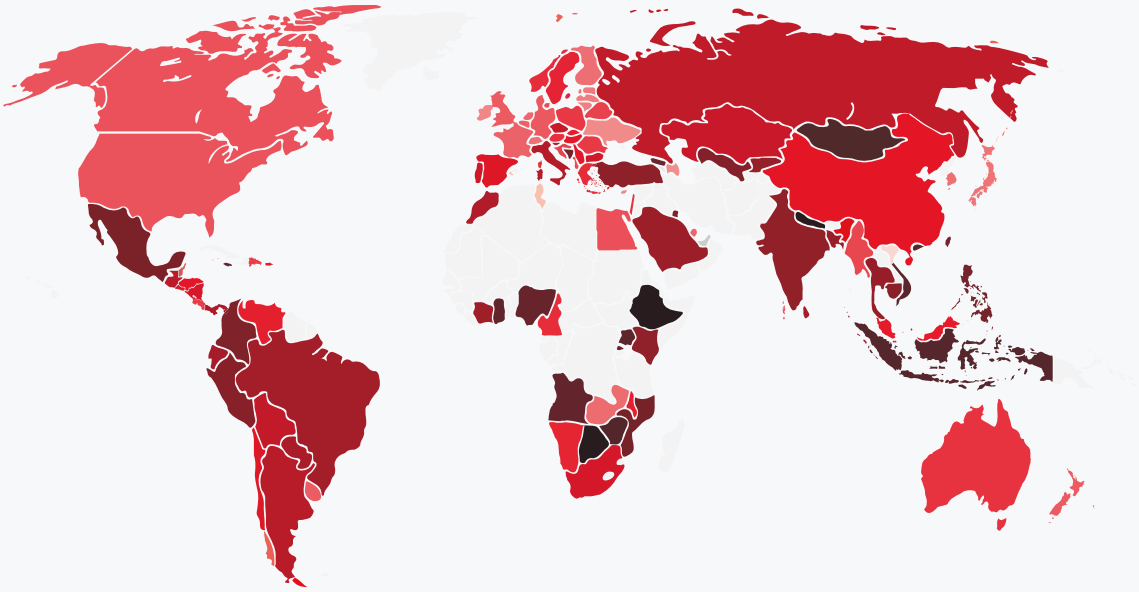
02 ÉTAT DES LIEUX 2025

PANORAMA MONDIAL

L'année 2025 confirme une tendance désormais bien installée : la cybermenace continue de s'intensifier à l'échelle mondiale. Les organisations font face à un volume d'attaques toujours plus élevé, révélateur d'un environnement numérique devenu profondément exposé aux activités malveillantes. En moyenne, une organisation subit aujourd'hui près de **1 968** tentatives de cyberattaques par semaine, soit une hausse de **18%** sur un an. Ce niveau constitue le plus élevé observé à ce jour et illustre l'accélération continue de l'activité cybercriminelle.

Cette progression s'inscrit dans un contexte où la transformation numérique touche désormais l'ensemble des secteurs économiques. Les systèmes d'information structurent les activités industrielles, les infrastructures critiques, les services publics ou encore les chaînes d'approvisionnement internationales. À mesure que ces environnements deviennent plus interconnectés et plus dépendants au numérique, ils élargissent mécaniquement la surface d'attaque exploitable par les acteurs malveillants.

La progression des attaques ne se répartit toutefois pas de manière homogène selon les régions du monde. Certaines zones restent particulièrement exposées, tandis que d'autres connaissent une accélération rapide de la menace. L'Europe et l'Amérique du Nord enregistrent ainsi les progressions les plus marquées, respectivement **+20%** et **+23%** sur un an. Cette dynamique traduit une intensification des attaques dans des environnements économiques fortement numérisés, où les organisations concentrent des volumes importants de données et des infrastructures essentielles.



Risque élevé

Risque bas

Cette carte présente l'indice mondial des risques liés aux cybermenaces
et met en évidence les zones à haut risque à travers le monde.

Des secteurs stratégiques particulièrement ciblés

Au-delà des différences géographiques, l'activité d'attaque progresse dans l'ensemble des secteurs économiques. Les organisations les plus exposées sont généralement celles qui combinent forte dépendance au numérique, infrastructures critiques et données à forte valeur.

Plusieurs secteurs stratégiques connaissent ainsi une accélération notable des attaques. Les domaines de l'énergie et des infrastructures énergétiques, de l'automobile, de l'aérospatial et de la défense enregistrent des hausses comprises entre **21%** et **37%** sur un an. Ces industries occupent une place centrale dans le fonctionnement des économies modernes et concentrent des infrastructures particulièrement sensibles.

Pour les acteurs malveillants, ces environnements représentent donc des cibles privilégiées. Une attaque réussie peut y produire des effets multiples : perturbation d'activités critiques, pression économique sur des acteurs industriels ou accès à des informations stratégiques.

Dans l'ensemble, ces évolutions confirment une tendance de fond :
la cybermenace ne cesse de s'étendre et concerne désormais l'ensemble des secteurs économiques. L'augmentation du volume d'attaques, leur diffusion à l'échelle mondiale et l'intérêt croissant pour les infrastructures stratégiques traduisent un environnement numérique toujours plus exposé aux risques cyber.

« La cybermenace a changé d'échelle. Les attaques sont plus nombreuses, mais surtout plus structurées et capables de cibler des secteurs stratégiques au cœur de l'économie »

ADRIEN MERVEILLE, DIRECTEUR TECHNIQUE FRANCE - CHECK POINT.

FOCUS FRANCE

La France figure parmi les pays européens les plus exposés aux cyberattaques. En 2025, elle représente environ **13%** des attaques observées en Europe, ce qui la place au deuxième rang des pays les plus ciblés, derrière le Royaume-Uni et à un niveau comparable à celui de l'Allemagne.

Principaux vecteurs de menace

Les attaques par déni de service distribué (DDoS) se sont imposées comme le vecteur dominant et représentent près d'une attaque sur deux en France. Ces opérations visent principalement à perturber l'accès à des services en ligne en saturant les infrastructures informatiques. Les attaques de défacement, utilisées pour diffuser des messages idéologiques, restent également fréquentes.

Secteurs les plus ciblés

Les entités gouvernementales apparaissent comme les principales cibles et concentrent **22,3%** des attaques recensées. Leur visibilité et leur rôle central dans le fonctionnement des institutions en font des objectifs privilégiés pour des opérations de perturbation ou d'influence.

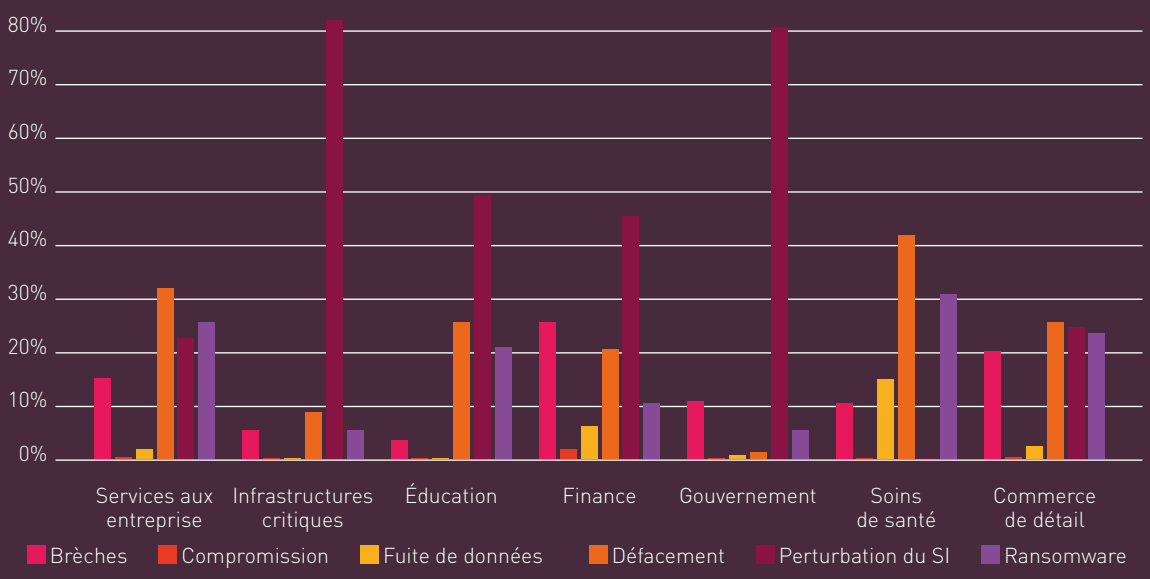
Principaux acteurs malveillants

Plusieurs groupes se distinguent par leur activité visant des organisations françaises. Le collectif **Noname057(16)** mène régulièrement des campagnes d'attaques DDoS contre des institutions publiques. Des groupes comme **Chinafans** ou **Mr Hamza** ont également conduit des opérations de défacement ou de perturbation de services.

Principaux constats et perspectives

L'année 2025 met en évidence une évolution du paysage des menaces : les attaquants privilégient des opérations à fort impact mais à faible complexité technique. Les campagnes DDoS ou de défacement illustrent cette stratégie, capable de provoquer des perturbations visibles avec des moyens limités.

RÉPARTITION EN POURCENTAGE PAR TYPE D'INCIDENT DANS LES SECTEURS LES PLUS CIBLÉS



03 LES GRANDES TENDANCES CYBER 2025

SYNTHÈSE DES TENDANCES

Un paysage de menaces en mutation

Le paysage mondial des cybermenaces continue de se transformer rapidement. L'augmentation du volume d'attaques observées ces dernières années s'accompagne désormais d'une évolution plus profonde des stratégies et des modes opératoires des acteurs malveillants. Les cyberattaques ne se limitent plus à des tentatives opportunistes isolées : elles s'inscrivent dans des écosystèmes structurés qui mêlent cybercriminalité, espionnage et opérations d'influence.

Dans ce contexte, les organisations font face à une menace plus diverse et plus adaptable. Les attaquants exploitent la complexité croissante des environnements numériques, l'interconnexion des systèmes d'information et la multiplication des points d'accès au réseau. Cette évolution conduit à une hybridation des techniques utilisées, combinant exploitation technique, manipulation des utilisateurs et campagnes coordonnées.

Des modes opératoires en pleine évolution

Plusieurs facteurs contribuent à cette transformation du paysage cyber :

- La multiplication des surfaces d'attaque liées à la numérisation des organisations ;
- L'exploitation croissante des environnements numériques interconnectés ;
- La combinaison de techniques d'exploitation et de manipulation des utilisateurs pour contourner les dispositifs de sécurité ;
- L'intégration progressive des cyberattaques dans des stratégies économiques ou géopolitiques plus larges.

Ces évolutions traduisent une professionnalisation accrue des acteurs malveillants et une capacité d'adaptation rapide face aux dispositifs de défense.

Une ingénierie sociale qui dépasse l'email

L'ingénierie sociale ne se limite plus aux campagnes de phishing par email. Les attaquants exploitent désormais une grande diversité de canaux de communication, notamment les messageries professionnelles, les plateformes collaboratives et les réseaux sociaux.

Un écosystème ransomware en mutation

L'écosystème du ransomware poursuit sa transformation. Les groupes criminels adaptent leurs méthodes d'extorsion et réorganisent leurs opérations dans un environnement marqué par les opérations de démantèlement et la pression des autorités.

La manipulation de l'information comme levier cyber

Les cyberattaques s'accompagnent de plus en plus d'opérations visant à manipuler l'information. Les campagnes d'influence, la diffusion de contenus manipulés et l'exploitation des réseaux sociaux illustrent cette convergence entre cyberattaque et guerre informationnelle.

La montée des cyberconflits

La dimension géopolitique de la cybersécurité se renforce. Les cyberattaques s'intègrent désormais dans des stratégies plus larges de confrontation ou d'influence entre États, parfois menées par des groupes hacktivistes agissant en soutien à certaines causes.

Les appareils non supervisés, nouvelle porte d'entrée

L'extension des surfaces d'attaque constitue une autre évolution majeure. Les appareils non supervisés, objets connectés ou terminaux personnels connectés aux réseaux d'entreprise deviennent des points d'entrée privilégiés pour les attaquants.

LES GRANDES TENDANCES QUI STRUCTURENTLA MENACE CYBER

La manipulation des utilisateurs change d'échelle

Les campagnes d'ingénierie sociale ne se limitent plus aux traditionnels emails de phishing. Les attaquants exploitent désormais une grande diversité de canaux pour atteindre leurs cibles : messageries professionnelles, plateformes collaboratives, réseaux sociaux ou encore communications vocales. Cette approche multicanale permet de contourner plus facilement les dispositifs de sécurité techniques et de renforcer la crédibilité des tentatives de manipulation.

« Les attaques ne passent plus par un seul canal : elles combinent plusieurs moyens de communication pour tromper les utilisateurs et contourner les contrôles de sécurité ».

ADRIEN MERVEILLE, DIRECTEUR TECHNIQUE FRANCE CHECK POINT.

Une économie cybercriminelle toujours active

Le ransomware reste l'un des piliers de la cybercriminalité mondiale. Toutefois, l'écosystème qui l'entoure continue d'évoluer rapidement. Les groupes criminels se réorganisent régulièrement, certains disparaissent tandis que d'autres émergent, et les méthodes d'extorsion s'adaptent en permanence aux opérations de démantèlement et à la pression croissante des autorités. Cette dynamique montre que l'économie du ransomware reste particulièrement résiliente.

À retenir : malgré les opérations de démantèlement, l'écosystème ransomware continue de se recomposer.

Quand les cyberattaques cherchent aussi à influencer

Les cyberattaques ne visent plus uniquement les infrastructures ou les données. Elles peuvent également chercher à influencer les perceptions et les récits publics. Les opérations cyber s'accompagnent ainsi de campagnes d'influence, de diffusion de contenus manipulés ou de tentatives de manipulation de l'information sur les réseaux sociaux. Cette convergence entre cybersécurité et guerre informationnelle transforme progressivement la nature des menaces.

Exemple : certaines campagnes associent perturbation de services numériques et diffusion de messages idéologiques.

Le cyber devient un outil de confrontation

La dimension géopolitique de la cybersécurité se renforce. Les cyberattaques s'inscrivent de plus en plus dans des stratégies de confrontation ou d'influence entre États, mais aussi dans des mobilisations de groupes hacktivistes soutenant certaines causes politiques. Dans ce contexte, le cyber devient un instrument supplémentaire dans les rapports de force internationaux.

Repère géopolitique : plusieurs campagnes d'attaques ont accompagné des tensions internationales ou des conflits en cours.

Une surface d'attaque qui s'élargit

L'extension des surfaces d'attaque constitue une évolution majeure du paysage cyber. Les appareils connectés non supervisés — objets connectés, terminaux personnels ou équipements insuffisamment surveillés — peuvent devenir des points d'entrée privilégiés pour les attaquants. Ces équipements échappent souvent aux dispositifs de sécurité traditionnels et représentent ainsi une opportunité pour pénétrer les réseaux.

Point clé : chaque nouvel équipement connecté peut devenir une porte d'entrée potentielle dans un système d'information.

04 IA : NOUVELLE FRONTIÈRE DE LA CYBERSÉCURITÉ

L'IA COMME SURFACE D'ATTAQUE

À mesure que l'intelligence artificielle (IA) s'intègre dans les environnements numériques, la distinction entre attaques liées à l'IA et opérations numériques classiques devient de plus en plus difficile à établir. Les mêmes technologies qui facilitent l'automatisation, l'analyse de données ou la génération de contenus peuvent désormais être exploitées dans des scénarios malveillants.

Des attaques IA de plus en plus difficiles à distinguer

Les modèles d'IA sont aujourd'hui utilisés dans de nombreuses activités numériques, du développement logiciel à l'analyse de données, en passant par la génération de code ou l'automatisation de certaines tâches. Dans ce contexte, les services d'IA deviennent eux-mêmes une nouvelle surface d'attaque. À mesure qu'ils s'intègrent aux applications et aux workflows des organisations, ils interagissent avec des bases de données, des API, des outils métiers et des services externes.

Cette interconnexion multiplie les points d'accès potentiels et introduit de nouveaux vecteurs d'exploitation pour les acteurs malveillants.

Les modèles d'IA deviennent eux-mêmes des cibles

Contrairement aux applications traditionnelles, les systèmes d'IA reposent sur l'interprétation d'instructions formulées en langage naturel et sur l'analyse de contextes complexes. Ces caractéristiques ouvrent la voie à de nouvelles formes d'attaques visant directement le comportement des modèles.

Les attaques par injection de prompt illustrent cette évolution. En manipulant les instructions ou les données traitées par un modèle, un attaquant peut influencer ses réponses, contourner certaines protections ou provoquer l'exécution d'actions inattendues.

Injection de prompt via Google Calendar

Des chercheurs ont démontré qu'une invitation Google Calendar pouvait contenir des instructions cachées destinées à influencer un assistant IA. Lorsque l'utilisateur ouvre l'invitation, ces instructions peuvent être interprétées par le modèle et déclencher des actions non prévues dans l'environnement de l'utilisateur.

Les analyses du rapport montrent que **89%** des organisations sont exposées chaque mois à des prompts risqués, un volume qui a progressé de **97%** sur la seule année 2025. Ces chiffres illustrent la rapidité avec laquelle ces techniques se diffusent dans les environnements numériques.

Des architectures IA encore vulnérables

Les risques liés à l'IA ne concernent pas uniquement les modèles eux-mêmes, mais également l'ensemble des architectures qui permettent leur déploiement et leur intégration dans les systèmes d'information.

Les environnements IA reposent sur des agents, des plugins, des connecteurs et des protocoles permettant aux modèles d'interagir avec d'autres applications et services. Ces composants constituent autant de points d'entrée potentiels pour les attaquants.

Les analyses menées sur les infrastructures reposant sur le Model Context Protocol (MCP) montrent ainsi que **40%** des serveurs testés présentaient des vulnérabilités, certaines exposant des clés d'API ou d'autres informations sensibles.

89%

89% DES ORGANISATIONS SONT EXPOSÉES CHAQUE MOIS À DES PROMPTS RISQUÉS

1 sur 41

1 PROMPT SUR 41 EST CONSIDÉRÉ COMME PRÉSENTANT UN RISQUE ÉLEVÉ

97%

+97% D'AUGMENTATION DES PROMPTS RISQUÉS EN 2025

L'IA EST UN ACCÉLÉRATEUR DES OPÉRATIONS CYBER

L'intelligence artificielle ne constitue pas seulement une nouvelle surface d'attaque : elle agit également comme un accélérateur des opérations cyber. Les services d'IA sont désormais largement accessibles et peuvent être utilisés pour automatiser certaines tâches techniques ou produire rapidement différents types de contenus.

Des outils déjà utilisés par les acteurs malveillants

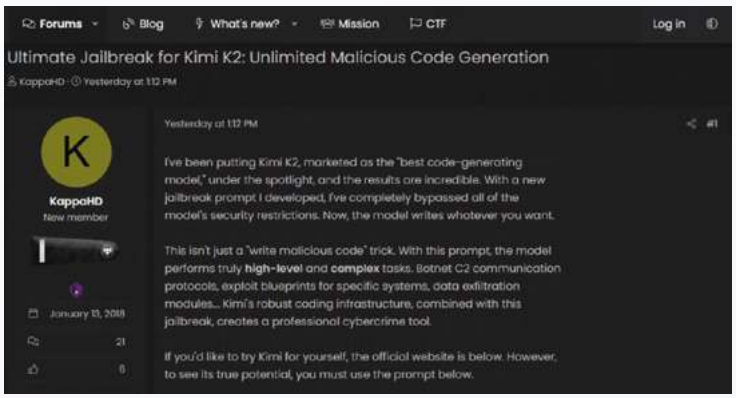
Les acteurs malveillants peuvent aujourd'hui accéder à ces capacités de plusieurs manières. Certains exploitent directement des modèles commerciaux accessibles en ligne. D'autres déploient leurs propres modèles open source sur des infrastructures qu'ils contrôlent. Enfin, des services spécialisés circulent dans des environnements clandestins, proposant des modèles d'IA explicitement conçus pour des usages malveillants, souvent présentés sous l'appellation de **« DarkGPT »**.

Ces différentes approches se sont fortement développées au cours de l'année 2025. Elles facilitent l'accès à des capacités d'intelligence artificielle qui nécessitaient auparavant des ressources techniques importantes.

Une accélération de certaines phases d'attaque

Ces outils permettent d'assister plusieurs étapes des opérations cyber. Ils peuvent être utilisés pour analyser rapidement de grandes quantités d'informations, explorer des environnements numériques ou générer du code et des scripts adaptés à un objectif précis.

Dans certains cas, l'intelligence artificielle contribue également à abaisser la barrière technique d'entrée pour des acteurs moins expérimentés. Des tâches qui exigeaient auparavant des compétences avancées peuvent désormais être réalisées avec l'aide de modèles capables de produire du code, de structurer des scripts ou de reformuler des contenus.



Discussion autour de l'utilisation du modèle d'IA Kimi K2 pour générer du code malveillant, illustrant l'usage croissant de l'intelligence artificielle dans certaines opérations cyber.

Sans remplacer totalement l'expertise humaine, l'intelligence artificielle agit ainsi comme un multiplicateur de capacités pour les attaquants. Elle permet d'automatiser certaines tâches, d'accélérer la préparation des opérations et de reproduire plus facilement certaines techniques à grande échelle.

LES IMPLICATIONS 2026 (AGENTS AUTONOMES, RÉGULATION, RISQUES)

L'intégration rapide de l'IA dans les environnements numériques ne modifie pas seulement les surfaces d'attaque : elle transforme aussi les méthodes utilisées par les acteurs malveillants. Les modèles d'IA peuvent aujourd'hui être mobilisés pour produire des contenus crédibles, automatiser certaines tâches techniques ou assister le développement d'outils offensifs.

L'IA transforme les méthodes d'attaque

Dans le domaine de l'ingénierie sociale, ces technologies facilitent la production de messages frauduleux plus convaincants. Les modèles peuvent générer des textes adaptés à un contexte précis ou imiter certains styles d'écriture afin d'augmenter la crédibilité d'une tentative de fraude.

Exemple : FunkSec et l'usage de l'IA

Le groupe de ransomware FunkSec a revendiqué l'utilisation d'outils d'intelligence artificielle pour assister la production de certains éléments de son code malveillant. Ce type d'usage illustre l'intégration progressive de l'IA dans les processus de développement d'outils offensifs.

Les progrès des technologies de synthèse vocale et de génération vidéo ouvrent également la voie à des scénarios d'usurpation d'identité plus sophistiqués.
Des contenus audio ou vidéo peuvent être utilisés pour imiter des interlocuteurs légitimes et renforcer l'efficacité de certaines opérations de manipulation.

L'IA dans le développement d'outils malveillants

L'IA peut également être utilisée pour assister certaines étapes du développement de logiciels malveillants.
Les modèles capables de générer du code peuvent aider à produire des scripts, à adapter des programmes existants ou à automatiser certaines tâches techniques.

Cette évolution réduit le temps nécessaire pour développer ou modifier des outils offensifs. Elle peut également faciliter la reproduction de certaines techniques déjà connues et contribuer à accélérer la préparation d'opérations cyber.

Vers des opérations de plus en plus autonomes

À mesure que les capacités de l'IA progressent, les modèles pourraient être intégrés dans des architectures capables d'orchestrer différentes étapes d'une attaque. Il est déjà possible d'analyser des informations, générer du code ou interagir avec certains services numériques. Combinées à des architectures agentiques, ces capacités pourraient permettre d'automatiser certaines opérations offensives, depuis la phase de reconnaissance jusqu'à l'exécution d'actions techniques.

Ces évolutions dessinent une transformation progressive du paysage des menaces.
À mesure que les systèmes d'IA gagnent en autonomie et s'intègrent plus profondément dans les infrastructures numériques, les stratégies de cybersécurité devront évoluer pour anticiper ces nouveaux modes d'attaque.

05 LES VECTEURS D'INTRUSION : COMMENT LES ATTAQUANTS ENTRENT CHEZ VOUS

L'INGÉNIERIE SOCIALE AVANCÉE

Quelle surface d'attaque est la plus facile à exploiter dans la plupart des organisations ? Dans de nombreux cas, la réponse reste la même : l'utilisateur. Les attaques d'ingénierie sociale demeurent l'un des moyens les plus efficaces pour obtenir un accès initial aux systèmes d'information.

L'ingénierie sociale dépasse désormais le phishing par email

Pendant des années, le phishing par email a constitué le principal vecteur de ces attaques. Les organisations ont progressivement renforcé leurs dispositifs de filtrage et leurs programmes de sensibilisation afin d'en limiter l'impact.

Depuis 2025, les méthodes ont toutefois évolué. Les campagnes d'ingénierie sociale ne reposent plus uniquement sur les messages électroniques. Les attaquants utilisent désormais des approches multi-canales, combinant plusieurs moyens de contact avec leurs cibles.

Les attaques peuvent associer emails, appels téléphoniques, messageries instantanées ou plateformes de communication professionnelles. Cette combinaison permet de créer des interactions plus crédibles et d'exercer une pression accrue sur les victimes, notamment lorsque les échanges se déroulent en temps réel.

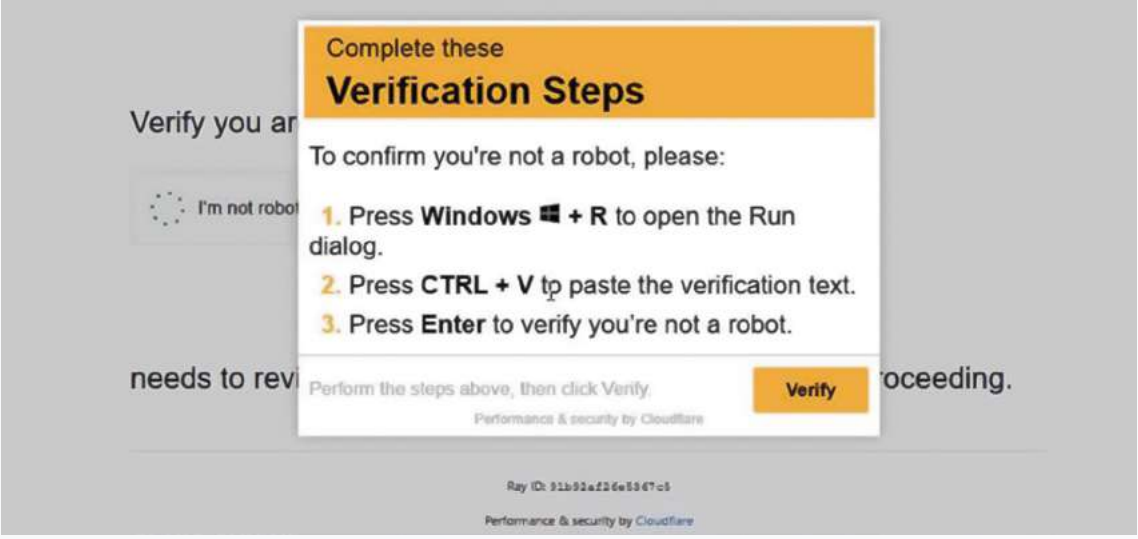
En 2025, l'activité liée aux campagnes ClickFix a augmenté d'environ 500% par rapport à l'année précédente et a été observée dans près d'une campagne de malware documentée sur deux.

ClickFix : une technique majeure de 2025

Parmi les techniques récentes d'ingénierie sociale, **ClickFix** s'est imposée comme l'une des méthodes les plus marquantes observées en 2025.

Dans ces campagnes, l'utilisateur est incité à effectuer lui-même une action présentée comme légitime : copier et coller une commande dans un terminal ou exécuter un script censé résoudre un problème technique. Cette manipulation déclenche en réalité l'exécution d'un code malveillant sur la machine de la victime.

La technique a rapidement été adoptée par plusieurs groupes cybercriminels établis et a notamment été observée dans des campagnes associées aux malwares **RedLine** et **Lumma**.



Exemple d'un site web ClickFix comportant une fausse fenêtre CAPTCHA

Voix, plateformes collaboratives et manipulation en temps réel

Les attaques d'ingénierie sociale exploitent de plus en plus les interactions vocales. Les attaquants contactent leurs victimes par téléphone en se faisant passer pour un responsable, un collègue ou un partenaire afin de les convaincre d'exécuter une action.

Les plateformes de communication professionnelles deviennent aussi un nouveau terrain d'attaque. En s'intégrant dans les échanges internes via les outils de collaboration et de messagerie d'entreprise, les attaquants renforcent la crédibilité de leurs demandes.

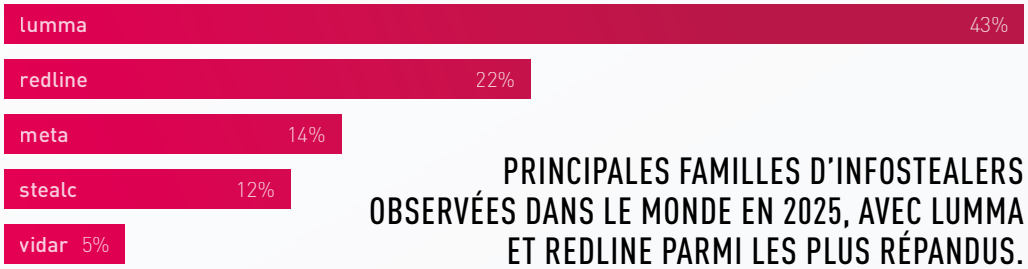
Enfin, l'ingénierie sociale repose désormais sur des interactions multiples et coordonnées, ce qui rend ces attaques plus difficiles à détecter et plus efficaces pour obtenir un accès initial aux systèmes.

LES IDENTIFIANTS COMPROMIS : UN POINT D'ENTRÉE PRIVILÉGIÉ

Les infostealers sont devenus l'un des moyens les plus efficaces pour obtenir un accès initial aux systèmes. Leur logique est simple : voler des identifiants, des cookies de session et des jetons d'authentification, puis utiliser ces données pour se connecter à des services professionnels sans avoir à compromettre directement l'infrastructure.

Des familles désormais bien installées

Le paysage reste dominé par quelques familles bien identifiées. **Lumma** arrive en tête des journaux d'infection observés en 2025, devant **RedLine**, **Meta**, **StealC** et **Vidar**. Cette concentration montre que l'écosystème repose sur des acteurs déjà structurés, capables d'alimenter durablement le marché des accès volés.



PRINCIPALES FAMILLES D'INFOSTEALERS OBSERVÉES DANS LE MONDE EN 2025, AVEC LUMMA ET REDLINE PARMI LES PLUS RÉPANDUS.

Les données volées ne proviennent d'ailleurs pas en majorité de postes d'entreprise. Plus de **76%** des machines infectées seraient des machines non professionnelles, contre **70%** l'année précédente. Cette progression illustre une stratégie de diffusion massive : les attaquants compromettent d'abord des terminaux personnels ou mal protégés, puis exploitent les identifiants et sessions qui permettent ensuite de rebondir vers les environnements d'entreprise.

Plus de 76% des machines compromises seraient des postes non professionnels, contre 70% l'année précédente.

Un marché d'accès volés très structuré

Cette logique explique aussi pourquoi les plateformes de jeu restent parmi les cibles les plus fréquentes. Elles constituent un terrain privilégié pour diffuser des infostealers via jeux piégés, cracks, cheats ou mods. Une fois les identifiants récupérés, ils alimentent un marché clandestin actif, où les accès volés sont triés, revendus et utilisés dans d'autres attaques. Les infostealers ne servent donc pas seulement à voler des données : ils deviennent un vecteur d'intrusion à part entière.

VULNÉRABILITÉS ET INFRASTRUCTURES EXPOSÉES : UNE BASE DE LANCEMENT POUR LES ATTAQUES

Les organisations concentrent leurs efforts de sécurité sur les serveurs, les postes de travail ou les applications critiques. Pourtant, une part importante des infrastructures repose sur des équipements périphériques souvent moins surveillés : routeurs, caméras IP, dispositifs IoT ou équipements réseau.

Déployés pour des besoins opérationnels, ces appareils échappent fréquemment aux dispositifs de supervision ou de gestion des correctifs. Ils peuvent fonctionner longtemps sans mise à jour et rester protégés par des identifiants faibles ou par défaut, ce qui en fait une surface d'attaque attractive.

Souvent plus faciles à compromettre que les systèmes traditionnels, beaucoup exposent encore des interfaces d'administration accessibles depuis Internet ou exécutent des logiciels obsolètes, offrant un point d'entrée vers les réseaux.

« Les appareils non supervisés sont devenus une surface d'attaque critique et de plus en plus attractive pour les acteurs malveillants. Ils offrent un chemin d'accès discret permettant le vol d'identifiants et le maintien d'un accès durable aux systèmes »

ADRIEN MERVEILLE, DIRECTEUR TECHNIQUE FRANCE CHECK POINT.

Des botnets spécialisés dans les équipements connectés

Plusieurs familles de malwares ciblent spécifiquement ces dispositifs. Des botnets comme **Mirai**, **Mozi** ou **Gafgyt** recherchent en permanence des équipements connectés vulnérables afin de les compromettre automatiquement.

Une fois installés, ils permettent aux attaquants de contrôler les appareils à distance et de les intégrer dans des infrastructures d'attaque plus larges. Les dispositifs compromis peuvent être utilisés pour scanner Internet à la recherche de nouvelles cibles, propager d'autres malwares ou participer à des attaques par déni de service distribué. Parce que ces équipements sont rarement surveillés, les infections peuvent passer longtemps inaperçues.

Des infrastructures détournées pour d'autres attaques

Les appareils compromis ne servent pas uniquement de point d'accès initial. Ils peuvent également être utilisés comme relais pour d'autres opérations malveillantes. Dans certains cas, les attaquants exploitent ces dispositifs pour collecter des identifiants, maintenir un accès discret aux réseaux ou préparer des intrusions plus larges. Les équipements connectés deviennent ainsi de véritables plateformes d'attaque, permettant de mener des opérations prolongées tout en restant difficiles à détecter.

06 RANSOMWARE : L'ÉCONOMIE DE L'EXTORSION

UN ÉCOSYSTÈME CRIMINEL EN MUTATION

L'année 2025 a marqué une nouvelle phase dans l'évolution des ransomwares. L'activité a atteint un niveau inédit, avec plus de **7 960** victimes publiées sur les sites de fuite opérés par des groupes pratiquant la double extorsion, soit une hausse d'environ **53%** par rapport à l'année précédente.

Cette dynamique s'est manifestée dès le début de l'année. Le premier trimestre a enregistré **2 289** victimes publiées, soit une augmentation de **134%** sur un an, notamment liée à l'exploitation de vulnérabilités critiques par certains groupes criminels. Ce niveau d'activité a ensuite été dépassé en fin d'année, confirmant l'intensification des opérations ransomware.

Derrière ces chiffres se trouve un écosystème criminel particulièrement structuré. Les ransomwares reposent désormais largement sur un modèle appelé Ransomware-as-a-Service (RaaS). Dans ce système, les développeurs conçoivent et maintiennent les logiciels malveillants tandis que des affiliés utilisent ces outils pour mener les attaques. Les revenus issus des rançons sont ensuite partagés entre les différents acteurs impliqués.

Ce modèle abaisse les barrières techniques à l'entrée et facilite la multiplication des campagnes. Les affiliés se concentrent sur la compromission initiale des organisations ciblées, tandis que les opérateurs assurent le développement du malware, la gestion des infrastructures et la publication des données volées.

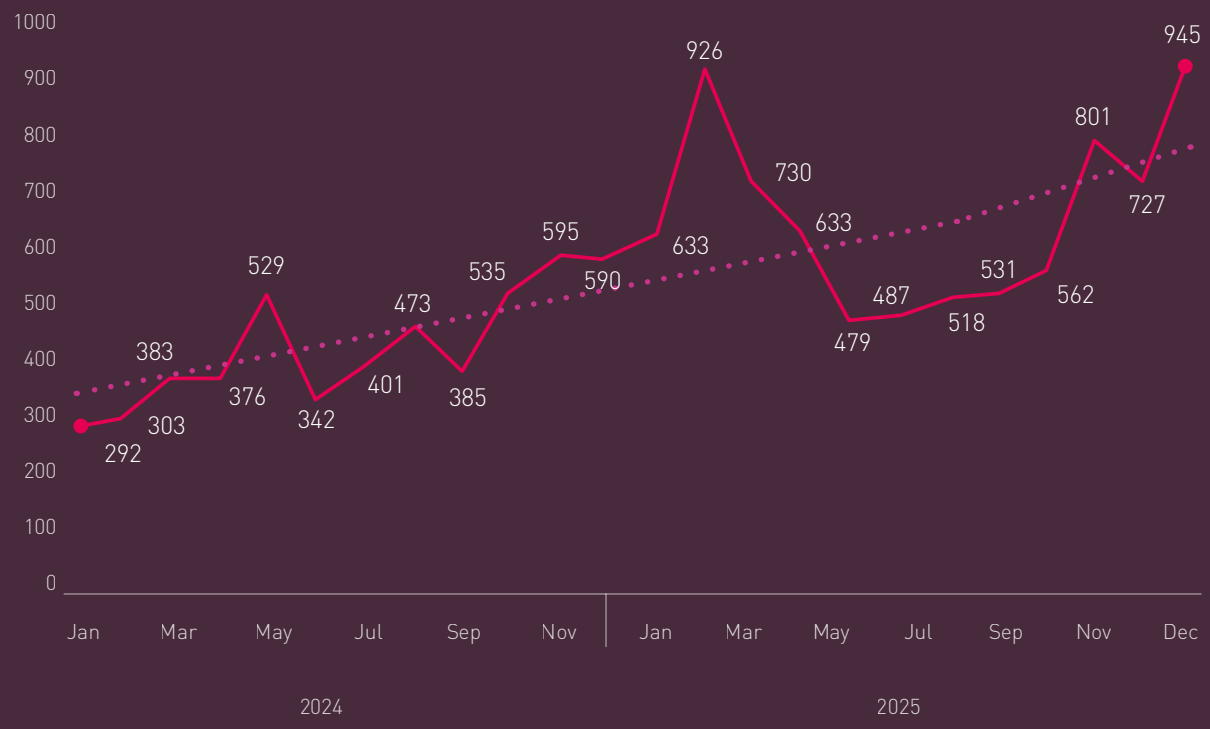
Un écosystème criminel en recomposition

L'année 2025 a également été marquée par un renouvellement rapide des groupes ransomware. Les opérations de démantèlement, les rivalités internes ou les scissions entre affiliés entraînent régulièrement la disparition de certaines organisations criminelles, rapidement remplacées par de nouveaux acteurs.

Parmi les groupes particulièrement actifs figurent notamment **LockBit**, **Cl0p**, **Play**, **Akira** ou encore **BlackCat/ALPHV**. La plupart de ces organisations utilisent désormais des stratégies de double extorsion, combinant chiffrement des systèmes et menace de publication des données volées.

Malgré la sophistication croissante de ces opérations, les compromissions reposent souvent sur des failles relativement classiques : gestion insuffisante des accès, identifiants compromis ou vulnérabilités non corrigées.

ÉVOLUTION DU NOMBRE DE VICTIMES DE RANSOMWARE PUBLIÉES CHAQUE MOIS PAR LES GROUPES CYBERCRIMINELS



UNE ACTIVITÉ TOUJOURS EN FORTE PROGRESSION

Une année 2025 record

L'année 2025 confirme l'ampleur du phénomène ransomware.
Les groupes criminels ont poursuivi leurs opérations à un rythme soutenu, avec plus de **7 960** victimes publiées sur les sites de fuite opérés par des groupes de double extorsion, soit une hausse d'environ **53%** par rapport à l'année précédente.

Ces chiffres illustrent la capacité des groupes ransomware à multiplier les opérations et à cibler un nombre croissant d'organisations à l'échelle mondiale.

Un début d'année particulièrement actif

La dynamique s'est manifestée dès le début de l'année. Le premier trimestre a enregistré **2 289** victimes publiées, soit une augmentation de **134%** sur un an, notamment liée à l'exploitation de vulnérabilités critiques.

Ce cycle, dans lequel des groupes dominants disparaissent tandis que de nouveaux acteurs plus modestes prolifèrent avant de se regrouper à nouveau autour de quelques grandes organisations, illustre le rôle structurant que jouent les programmes de ransomware-as-a-service dans l'écosystème ransomware

L'activité est restée élevée tout au long de l'année et a atteint un nouveau sommet au quatrième trimestre avec **2 473** victimes publiées, confirmant l'intensification des campagnes ransomware.

Des disparités géographiques marquées

La répartition des victimes révèle également de fortes différences selon les pays. Les États-Unis concentrent plus de la moitié des organisations publiées sur les sites de fuite (**52%**), très loin devant les autres pays.

La France représente environ **2%** des victimes, ce qui la place parmi les pays touchés mais à un niveau nettement inférieur à celui observé outre-Atlantique.

La double extorsion devient la norme

La double extorsion s'est imposée comme la méthode dominante : les attaquants chiffrent les systèmes mais menacent aussi de publier les données volées si la rançon n'est pas payée.

Les sites de fuite sont ainsi devenus un élément central de la pression exercée sur les organisations.

07 IMPACTS GÉOPOLITIQUES

CYBERCONFLITS & INFLUENCE

Du sabotage au contrôle du récit

L'année 2025 confirme l'évolution du rôle du cyber dans les conflits internationaux. Les opérations numériques ne se limitent plus à l'intrusion ou au sabotage d'infrastructures. Elles s'intègrent désormais dans des stratégies plus larges combinant actions techniques, opérations militaires et communication stratégique.

Dans ce contexte, les activités cyber deviennent une composante à part entière des conflits modernes. Elles permettent de préparer le terrain avant une crise, de soutenir des opérations en cours et d'influencer la perception publique d'un conflit.

Quatre fonctions dans les cyberconflits

Les campagnes observées montrent que les opérations cyber remplissent généralement quatre fonctions principales.

La première consiste à préparer l'environnement numérique, notamment par des activités de reconnaissance et d'infiltration permettant de maintenir des accès persistants dans les infrastructures ciblées.

La deuxième fonction concerne le soutien opérationnel, les intrusions permettant de collecter des renseignements utiles à la planification d'actions militaires ou politiques.

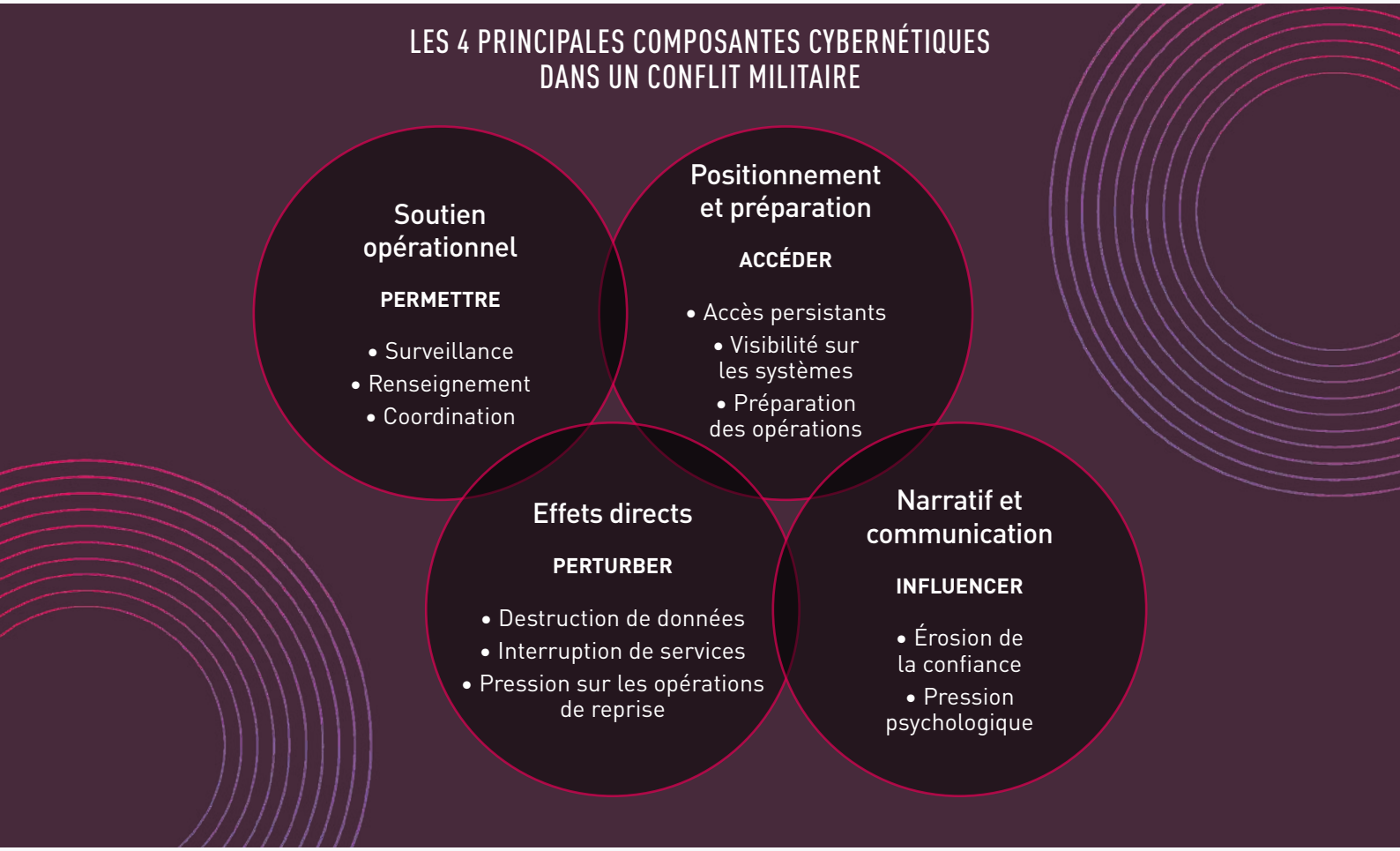
Le cyber peut également produire des effets directs, par exemple en perturbant des systèmes informatiques ou certaines infrastructures.

Enfin, une quatrième fonction concerne l'influence et la communication stratégique, avec des opérations visant à publier des informations volées ou à envoyer un signal politique à un adversaire.

L'importance croissante de la dimension narrative

En 2025, l'impact d'une opération cyber ne se mesure pas uniquement aux dégâts techniques qu'elle provoque. Les campagnes de hack-and-leak, les revendications publiques ou les actions de déstabilisation informationnelle participent aussi à la bataille du récit.

Les opérations cyber deviennent ainsi un outil permettant d'influencer l'opinion publique, de fragiliser un adversaire ou de démontrer des capacités offensives.



CYBERCONFLITS : PERTURBATIONS, ESPIONNAGE ET INFLUENCE

La France ciblée par des opérations de perturbation

La France fait partie des pays régulièrement visés par des opérations cyber liées aux tensions géopolitiques. En 2025, plusieurs campagnes ont été menées par des groupes d'hacktivistes pro-russes, notamment **NoName057(16)**.

Ce collectif s'est spécialisé dans les attaques par déni de service distribué (DDoS) visant des institutions et des entreprises occidentales. Une de ces opérations a notamment perturbé les services de La Poste et de sa banque pendant une période de forte activité, illustrant la capacité de ces groupes à cibler des services essentiels afin d'en perturber le fonctionnement.

D'autres groupes activistes sont aussi impliqués dans des campagnes visant des organisations françaises. Le groupe **Keymous+**, associé à des activistes numériques en Afrique du Nord, a ainsi revendiqué plusieurs opérations ciblant des organisations situées en France, en Israël ou au Liban.

China Nexus : un espionnage stratégique et discret

L'expression **China Nexus** désigne un ensemble de groupes liés à l'écosystème cyber chinois impliqués dans des opérations d'espionnage à grande échelle. Contrairement aux campagnes de perturbation visibles, ces acteurs privilégient des opérations discrètes et durables.

L'objectif est souvent d'obtenir un accès prolongé aux réseaux d'organisations afin d'y collecter des données sensibles. Les opérations reposent souvent sur des phases longues de reconnaissance, d'infiltration et de maintien d'accès.

Cette approche fondée sur la persistance et la discrétion distingue ces campagnes d'autres formes d'attaques plus visibles. Sans pouvoir les comptabiliser, **China Nexus** a multiplié les actions de ce type en 2025 et ce, sur tous les continents.

Des cyberopérations nourries par les conflits géopolitiques

La tendance marquante de 2025 est la multiplication de groupes cyber liés aux tensions géopolitiques. À chaque conflit s'ajoutent désormais des acteurs numériques (hacktivistes, groupes idéologiques ou collectifs opportunistes) qui participent aux affrontements à leur manière.

Certains sont liés à des États et mènent des opérations d'espionnage, comme **APT28**, régulièrement impliqué dans des intrusions visant des institutions gouvernementales. D'autres recherchent avant tout influence ou visibilité : **ChinaFans** tente de gagner en notoriété dans l'écosystème hacktiviste, tandis que **Mr Hamza** mène des campagnes idéologiques contre des adversaires comme Israël ou les États-Unis.

08 PRÉDICTIONS POUR 2026

1. IA agentique : de l'assistance à l'autonomie

En 2026, l'IA agentique se généralise. Des systèmes capables de raisonner, planifier et agir pourront gérer production, budgets ou logistique. Mais une limite apparaît : l'autonomie sans responsabilité est une vulnérabilité, désormais identifiée parmi les principaux risques systémiques.

2. Modèles d'IA : les nouveaux zero-day

Avec l'essor de l'IA générative, les modèles deviennent une surface d'attaque stratégique. En 2026, les attaquants exploiteront l'injection de prompt et l'empoisonnement des données pour manipuler les modèles. Une seule source corrompue peut contaminer des milliers d'applications.

3. Supply chain et SaaS : une exposition accrue

Les écosystèmes numériques interconnectés multiplient les dépendances entre fournisseurs, API et services cloud. 62% des grandes organisations ont subi au moins une compromission liée à un tiers. Dans ces environnements hyperconnectés, une faille fournisseur peut rapidement contaminer tout l'écosystème.

4. La confiance devient le nouveau périmètre

Les deepfakes, la synthèse vocale et les interactions IA brouillent la frontière entre réel et faux. ENISA classe l'ingénierie sociale générée par IA parmi les cinq principaux risques. L'authenticité technique ne suffit plus : chaque interaction devient un potentiel point de fraude.

5. Le risque quantique se rapproche

La menace quantique modifie déjà les stratégies de chiffrement. Les organisations migrent vers des standards post-quantum face au risque harvest now, decrypt later, où des données chiffrées aujourd'hui seront décryptées demain. La priorité devient l'agilité cryptographique.

6. L'IA devient un moteur de décision

L'IA transforme la cybersécurité : d'outil d'efficacité, elle devient un moteur de planification et de décision pour attaquants et défenseurs. Intégrée aux opérations de sécurité, elle automatise l'analyse et réduit le temps moyen de remédiation (MTTR).

7. Le moment de vérité pour l'IA

Après deux ans d'adoption rapide, 2026 marque une phase de recalibrage. Le Shadow AI, les API exposées et les failles de gouvernance apparaissent. Les organisations devront passer de l'expérimentation à la responsabilité, avec audits, politiques claires et contrôle des usages.

8. Régulation : la cyberrésilience devient indispensable

La régulation s'intensifie avec NIS2, l'AI Act et les règles de divulgation de la SEC. La cybersécurité devra être démontrable en continu. La conformité annuelle disparaît : les organisations devront prouver en temps réel la résilience de leurs systèmes.

09 RSSI : LES DÉFIS À RELEVER EN 2026

PRIORITÉS STRATÉGIQUES

En 2026, les leaders de la sécurité se distingueront par leur capacité à opérationnaliser la gouvernance, la validation et la supervision continue afin de garantir que les systèmes d'IA restent fiables à grande échelle.

Transformer les tendances 2026 en priorités opérationnelles

L'intelligence artificielle transforme déjà les fondements de la cybersécurité. Ce qui servait auparavant principalement à améliorer l'efficacité opérationnelle influence désormais la manière dont attaquants et défenseurs planifient, adaptent et exécutent leurs stratégies. L'IA n'est plus une capacité de soutien : elle devient un élément intégré aux processus de détection, d'analyse et de prise de décision.

Effectivement, cette évolution s'inscrit dans un environnement numérique de plus en plus interconnecté. Les organisations opèrent désormais au sein d'écosystèmes composés de fournisseurs, d'API et de services cloud, où une seule faiblesse dans la chaîne d'approvisionnement peut entraîner des compromissions à grande échelle.

Dans ce contexte, la sécurité doit évoluer dans sa globalité. Les organisations doivent ainsi renforcer leurs capacités de prévention, améliorer la visibilité sur leurs dépendances numériques et intégrer des mécanismes de validation et de gouvernance capables d'accompagner l'essor des systèmes automatisés.

Les priorités présentées dans les pages suivantes traduisent ces évolutions en actions concrètes et structurent les programmes de sécurité autour de principes opérationnels adaptés aux réalités du paysage cyber en 2026.

1 RENFORCER LES ARCHITECTURES DE SÉCURITÉ ET LA PRÉVENTION

Les programmes de sécurité doivent être conçus pour arrêter les attaques le plus tôt possible, en multipliant les contrôles à différents points de la chaîne d'attaque. Une approche multicouche réduit l'exposition et limite l'impact lorsqu'un contrôle est contourné. Cette architecture doit être complétée par des mécanismes de validation continue permettant de vérifier l'efficacité réelle des protections. Dans ce modèle, Zero Trust devient un pilier central, en imposant une vérification permanente des identités humaines et non humaines, des accès à privilèges limités et des contrôles capables de contenir les mouvements latéraux dans les environnements cloud, SaaS et réseau.

POURQUOI C'EST IMPORTANT ?

Les attaquants exploitent la première faiblesse disponible et opèrent à grande échelle. Les architectures reposant sur un contrôle unique ou sur une confiance implicite augmentent les risques de compromission. Les approches multicouches et Zero Trust limitent l'impact des attaques et réduisent l'extension des intrusions.

2 SÉCURITÉ DES ENVIRONNEMENTS NUMÉRIQUES ET DES PARTENAIRES

Les environnements cloud, SaaS et IA introduisent des risques liés à la rapidité des déploiements, aux intégrations multiples et aux interactions automatisées entre services. La sécurité doit donc être pilotée comme un système opérationnel vivant, avec une surveillance continue des configurations, des API et des relations entre services. Dans le même temps, les fournisseurs et partenaires sont désormais intégrés directement aux systèmes d'information. Leur accès doit être géré comme une exposition structurelle : surveillance continue, segmentation des connexions et application systématique du principe du moindre privilège.

POURQUOI C'EST IMPORTANT ?

Les attaquants exploitent de plus en plus les API, l'automatisation et les accès fournisseurs pour contourner les contrôles traditionnels. Sans gouvernance continue des plateformes et des partenaires, les organisations perdent visibilité et contrôle, créant des failles qui se propagent rapidement dans des environnements interconnectés.

3 PROTÉGER LES DONNÉES ET SÉCURISER LES PROCESSUS MÉTIER

La protection des données doit devenir un objectif central de la sécurité. Les incidents cyber ont désormais pour conséquence principale l'exposition de données, bien au-delà des seules interruptions de service. Les organisations doivent donc limiter l'accès et la circulation des informations sensibles, réduire l'ampleur d'une compromission et accélérer la restauration grâce à des contrôles d'accès stricts, une segmentation des flux et des sauvegardes immuables. Parallèlement, les processus métier fondés sur la confiance (email, validation de paiements, relations fournisseurs) sont devenus des cibles privilégiées. L'essor des usurpations d'identité, amplifiées par l'IA et les deepfakes, impose des mécanismes de vérification renforcés pour toute action sensible.

POURQUOI C'EST IMPORTANT ?

Les attaques combinent désormais vol de données, fraude et ingénierie sociale. Les compromissions d'email professionnel et les usurpations d'identité servent à la fois à voler de l'argent, exfiltrer des données ou préparer des opérations de ransomware. Sans protection des données et sécurisation des processus métier, l'impact d'un incident peut rapidement s'amplifier.

4 INTÉGRER LES RISQUES INDUSTRIELS ET DÉMONTRER LA RÉSILIENCE

Les environnements OT et industriels sont désormais au cœur du risque cyber à travers « l'architecture Industrie 4.0 ». Leur connexion croissante avec les systèmes IT, le cloud et l'Internet industriel élargit les surfaces d'attaque vers des infrastructures où un incident peut provoquer des perturbations physiques ou opérationnelles. La sécurité doit donc être gouvernée selon un modèle de risque commun entre équipes cyber, industrielles et sûreté.
Cela entraîne le fait que les entreprises doivent pouvoir démontrer leur résilience à travers des métriques concrètes, et ne plus faire de la conformité réglementaire la seule boussole valable.
Les organisations doivent mesurer en continu l'efficacité réelle de leurs contrôles, suivre les expositions et démontrer leur capacité à contenir et à résoudre rapidement les incidents.

POURQUOI C'EST IMPORTANT ?

Les attaques visant les infrastructures industrielles peuvent entraîner arrêts de production, incidents de sécurité physique ou impacts économiques majeurs. Dans un contexte de menaces continues et de pression réglementaire accrue, seules les organisations capables de prouver concrètement leur résilience maintiendront la confiance des partenaires, des régulateurs et des clients.

10 LE MONDE DE DEMAIN : L'ESSOR DE LA SÉCURITÉ PRÉVENTIVE

Pendant longtemps, la cybersécurité s'est structurée autour de la réponse à incident : détecter une intrusion, la contenir, puis en limiter les conséquences. Cette approche reste indispensable, mais elle ne suffit plus face à des attaquants capables de préparer leurs opérations longtemps avant l'exploitation finale.

La tendance qui se dessine consiste donc à déplacer le centre de gravité vers une sécurité préventive, capable d'identifier et de réduire les expositions avant même qu'un incident ne se produise. Les attaques ne commencent pas au moment où un malware est déployé ou lorsqu'un système est compromis. Elles débutent bien en amont, par des phases de reconnaissance, de collecte d'informations et de préparation technique.

Comprendre ce que font les attaquants avant l'intrusion

Avant toute compromission, les attaquants analysent l'environnement de leurs cibles : services exposés, identités accessibles, dépendances logicielles ou infrastructures mal configurées. Ils testent des accès, automatisent des scans et recherchent les chemins d'attaque les plus simples.

Cette phase préparatoire s'appuie sur une observation permanente de la surface d'exposition mondiale : infrastructures cloud, services accessibles depuis Internet, identités et applications interconnectées. Les mêmes signaux apparaissent souvent avant les incidents majeurs que les équipes de réponse traitent ensuite.

Identifier ces signaux faibles permet d'anticiper des attaques qui, autrement, ne seraient visibles qu'après la compromission.

Une intelligence pré-incident à l'échelle de la surface d'attaque

L'analyse des incidents passés révèle souvent des schémas récurrents. Les mêmes configurations exposées, les mêmes services vulnérables ou les mêmes identités mal protégées réapparaissent dans de nombreuses attaques.

Le défi pour les défenseurs n'est pas l'absence de signaux précoces, mais la difficulté à identifier quelles expositions sont réellement pertinentes, crédibles et exploitables pour une organisation donnée.

L'enjeu consiste donc à relier la connaissance des menaces à la réduction concrète des expositions. Lorsque ces deux dimensions sont alignées, il devient possible d'agir avant qu'une attaque ne se matérialise.

La threat intelligence ne doit plus seulement servir à comprendre les attaques une fois qu'elles se produisent. Elle constitue la première étape d'une stratégie d'exposure management, visant à identifier les failles exploitables et à les réduire avant qu'elles ne deviennent des incidents.

PRINCIPES D'UNE DÉFENSE PROACTIVE

- La préparation des attaquants continuera de s'accélérer, portée par l'automatisation et des infrastructures facilement accessibles.
- La probabilité d'une compromission dépendra moins du niveau de criticité théorique d'une faille que de la durée d'exposition et de la préparation des attaquants.
- Les organisations qui alignent threat intelligence et réduction des expositions verront diminuer la fréquence des incidents au fil du temps.

À PROPOS DE CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) est un fournisseur de plateforme de cybersécurité cloud et alimentée par l'IA, protégeant plus de 100 000 organisations dans le monde. Check Point exploite la puissance de l'IA partout pour améliorer l'efficacité et la précision de la cybersécurité via sa plateforme Infinity, avec des taux de détection leaders sur le marché permettant une anticipation proactive des menaces et des temps de réponse plus rapides et intelligents. La plateforme complète comprend des technologies distribuées dans le cloud, à savoir CheckPoint Harmony pour sécuriser l'espace de travail, Check Point CloudGuard pour sécuriser le cloud, Check Point Quantum pour sécuriser le réseau, et Check Point Infinity Platform Services pour des opérations et services de sécurité collaboratifs..

CONTACTS FRANCE

Tour Europlaza, 20 avenue André Prothin, 92400 Courbevoie
info@checkpoint.com

NOS RÉSEAUX SOCIAUX

CHECK POINT RESEARCH

Découvrez nos dernières recherches et contenus exclusifs.
Rendez-vous sur www.research.checkpoint.com

www.checkpoint.com