yuno By xmco

PANORAMA DES MENACES CYBER 2025

par le CERT-XMCO

We deliver cybersecurity

Fort d'une trentaine d'experts, le CERT-XMCO analyse les menaces émergentes pour fournir des bulletins techniques et environnementaux à ses clients. Intégrée à Yuno, cette expertise vous aide à identifier les vulnérabilités critiques et les menaces en cours, tout en orientant vos priorités pour renforcer votre posture de sécurité et allouer efficacement vos ressources.

Cette production s'appuie sur la collecte et l'analyse de données issues de sources ouvertes et fermées, enrichies par le CERT-XMCO. La plateforme Yuno rend ces informations immédiatement exploitables : vous recevez des recommandations précises pour prioriser les correctifs et renforcer vos défenses face aux attaques. Avec Yuno, la veille devient un outil concret pour protéger durablement votre organisation.

Direction de la publication : XMCO
Conception : plusdebleu.com
Date de publication : Avril 2026
Crédit photo : AdobeStock

Avant-propos

Pour cette troisième édition du bilan annuel YUNO, le CERT-XMCO revient sur les événements marquants de l'année passée.

L'objectif de ce document est de fournir une vision globale du paysage et de l'évolution des cybermenaces, par un travail de synthèse et d'analyse des informations collectées au quotidien par nos analystes.

EN 2025, LE SERVICE YUNO A AINSI ENVOYÉ À CHACUN DE SES CLIENTS :

5950

Bulletins techniques, de type :
- **PATCH** - Publication d'un correctif
- **VULN** - Découverte d'une vulnérabilité sans correctif
- **EXPLOIT** - Publication d'un code d'exploitation

Dont :

187
Bulletins critiques

+65
Technologies supplémentaires ajoutées au suivi Yuno

617

Bulletins environnementaux de type **INFO**, relatifs à :
- Des attaques et campagnes d'attaques
- Des analyses de modes opératoires et de malware
- L'évolution des normes et du cadre réglementaire de la cybersécurité

Dont :

16
Bulletins critiques

+100
Attaques et campagnes d'attaques visant la France

316

Bulletins environnementaux de type **XMCO**, qui comprennent :
- **12** Observatoires des ransomware mensuels
- **52** Résumés de la semaine hebdomadaires
- **251** Revues de presse quotidiennes

Dont :

+25
Nouveaux groupes ransomware ajoutés à la surveillance

Panorama cyber 2025
Synthèse des évolutions majeures

L'année 2025 consacre une reconfiguration profonde du risque cyber, à l'intersection des dynamiques technologiques, économiques et géopolitiques.
L'intégration de l'intelligence artificielle dans les pratiques offensives, la progressive centralité du cloud dans les modes opératoires ainsi que la consolidation industrielle du cybercrime révèlent une mutation à l'œuvre, qui est amenée à se poursuivre en 2026.

Dans ce contexte, la diffusion de modèles criminels As-a-Service et la montée en puissance de techniques d'ingénierie sociale telles que ClickFix, mobilisées comme vecteurs d'accès initiaux dans un nombre croissant de campagnes, traduisent une recomposition des pratiques offensives autour de dispositifs standardisés et facilement réplicables. Face à cet environnement plus structuré et interdépendant, la conflictualité numérique se recompose autour d'acteurs de plus en plus instrumentalisés, justifiant une réponse souveraine qui s'incarne notamment dans le renforcement des dispositifs normatifs européens.

INTELLIGENCE ARTIFICIELLE

L'usage de l'intelligence artificielle par les attaquants, en particulier des LLM et de la GenAI, reconfigure en profondeur les opérations cyber offensives à chacune des étapes de la kill chain. Cette accessibilité nouvelle a permis l'industrialisation des activités de reconnaissance, renforce la crédibilité des campagnes de phishing et de deepfake, et facilite la génération comme l'obfuscation de code malveillant, bien qu'encore limitées par des contraintes techniques et la nécessité d'une supervision humaine. Ce contexte annonce l'émergence d'un environnement où attaquants et défenseurs s'appuient tous deux sur l'IA : les premiers en développant des agents de plus en plus autonomes et adaptatifs, les seconds en déployant des architectures Zero Trust, des capacités de détection prédictive et des mécanismes de réponse automatisée aux intrusions.

SERVICES LÉGITIMES ET CLOUD

La logique traditionnelle du « Living off the Land » bascule à l'échelle du cloud, les attaquants opérant désormais en « Living off the Cloud » en s'adossant massivement à des services de confiance tels que Microsoft 365, Google Workspace, AWS, Dropbox ou Cloudflare. Ils militarisent ces briques d'infrastructure pour en faire des points d'exfiltration discrets, des plateformes d'hébergement de payloads ou des canaux de commande et de contrôle furtifs. En se fondant dans le trafic HTTPS et les flux applicatifs d'écosystèmes réputés fiables, ces opérations brouillent la frontière entre activité légitime et malveillante, neutralisent une partie des défenses périmétriques classiques et imposent un basculement vers une détection centrée sur les comportements, les signaux faibles d'abus de services et la télémétrie fine au cœur même des environnements cloud d'entreprise.

CYBERCRIME

L'année 2025 fut témoin de la consolidation d'un cybercrime industrialisé, structuré autour de modèles As-a-Service où des acteurs spécialisés (développeurs, courtiers en accès, fournisseurs de plateformes) s'intègrent dans une chaîne de valeur fournissant outils, infrastructures et services clés en main à des profils peu techniques. Elle fut également marquée par une forme de « cartelisation » des écosystèmes de ransomware, fondée sur des alliances souples, le partage de ressources et la circulation d'affiliés entre labels, renforçant à la fois la résilience du système et le rapport de force vis-à-vis des victimes.

CLICKFIX

La technique d'ingénierie sociale ClickFix s'est imposée cette année comme une méthode d'attaque majeure exploitant la confiance de l'utilisateur, trompé pour exécuter lui-même des commandes malveillantes via de faux CAPTCHA ou de prétendues vérifications de sécurité. Diffusée par des campagnes

de phishing, de publicité malveillante ou à travers des sites compromis, elle permet d'infecter un poste sans contourner directement les défenses techniques. Employée aussi bien par des groupes cybercriminels tels que Lazarus et Interlock que par des acteurs étatiques comme TA427 et TA450, elle sert à déployer des vols de cryptomonnaies, des infostealers, des outils d'accès à distance et des ransomware. Son succès a conduit à la vente de kits prêts à l'emploi sur des forums clandestins.

GÉOPOLITIQUE

La conflictualité numérique s'affirme comme un prolongement direct des rivalités géopolitiques, où la distinction entre acteurs étatiques, structures criminelles et groupes idéologiques tend à s'estomper. Les exemples récents en Europe de l'Est ou au Proche-Orient soulignent que les opérations cyber ne se limitent plus à une logique de disruption technique : elles s'inscrivent pleinement dans la construction d'un rapport de force politique, mobilisant le cyberespace comme vecteur d'influence, de coercition et de légitimation. Dans ce contexte, des collectifs hacktivistes tels que NoName057(16) ont multiplié cette année les attaques contre des infrastructures ukrainiennes ou européennes, brouillant la frontière entre action militante, proxy étatique et cybercriminalité opportuniste. Leurs campagnes, souvent relayées sur des canaux de messagerie chiffrés et sur les réseaux sociaux, s'accompagnent d'une dimension psychologique et narrative, cherchant autant à affaiblir les capacités techniques adverses qu'à façonner la perception publique du conflit.

SOUVERAINETÉ EUROPÉENNE ET CADRE LÉGISLATIF

Face à l'intensification des menaces dans le cyberespace, l'Union européenne s'impose comme acteur normatif en encadrant la cybersécurité, l'intelligence artificielle et désormais la résilience numérique du secteur financier. Avec la directive NIS2 et la création en 2025 de l'EUVD par l'ENISA, elle renforce la résilience de ses infrastructures critiques et son autonomie stratégique. Parallèlement, l'AI Act positionne l'Europe comme pionnière de la régulation de l'intelligence artificielle, tandis que le règlement DORA (Digital Operational Resilience Act), entré en application en 2025, impose aux acteurs bancaires et financiers des exigences accrues en matière de gestion du risque numérique et de continuité opérationnelle. Ensemble, ces dispositifs traduisent la volonté de l'Europe de réduire sa dépendance aux infrastructures et régulations étrangères, et d'instrumentaliser le cyberespace comme levier de puissance, au service de sa souveraineté numérique et de sa sécurité collective.

Sommaire

yuno By xmco

1. INFORMATIONS DÉLIVRÉES PAR YUNO EN 2025

1.1 Panorama des vulnérabilités 2025

En 2025, le nombre de vulnérabilités a continué d'augmenter et davantage sont activement exploitées, les attaquants ciblant une large diversité de produits et de technologies à travers de multiples scénarios d'attaque. L'intégration de solutions tierces accroît les risques de compromission, car des vulnérabilités dans la chaîne d'approvisionnement permettent aux attaquants d'étendre leur impact à plusieurs organisations[1].

En parallèle, ces attaquants ciblent des composants critiques comme les passerelles réseau, les solutions d'accès à distance, ainsi que des outils de gestion IT (RMM) et des systèmes IAM, leur offrant ainsi un accès initial privilégié aux systèmes des victimes. Les compromissions sont principalement orchestrées par des groupes sophistiqués, tels que les clusters APT ou ransomware, qui exploitent des vulnérabilités 0-day et des failles non corrigées, pour mener des opérations à des fins financières ou d'espionnage.

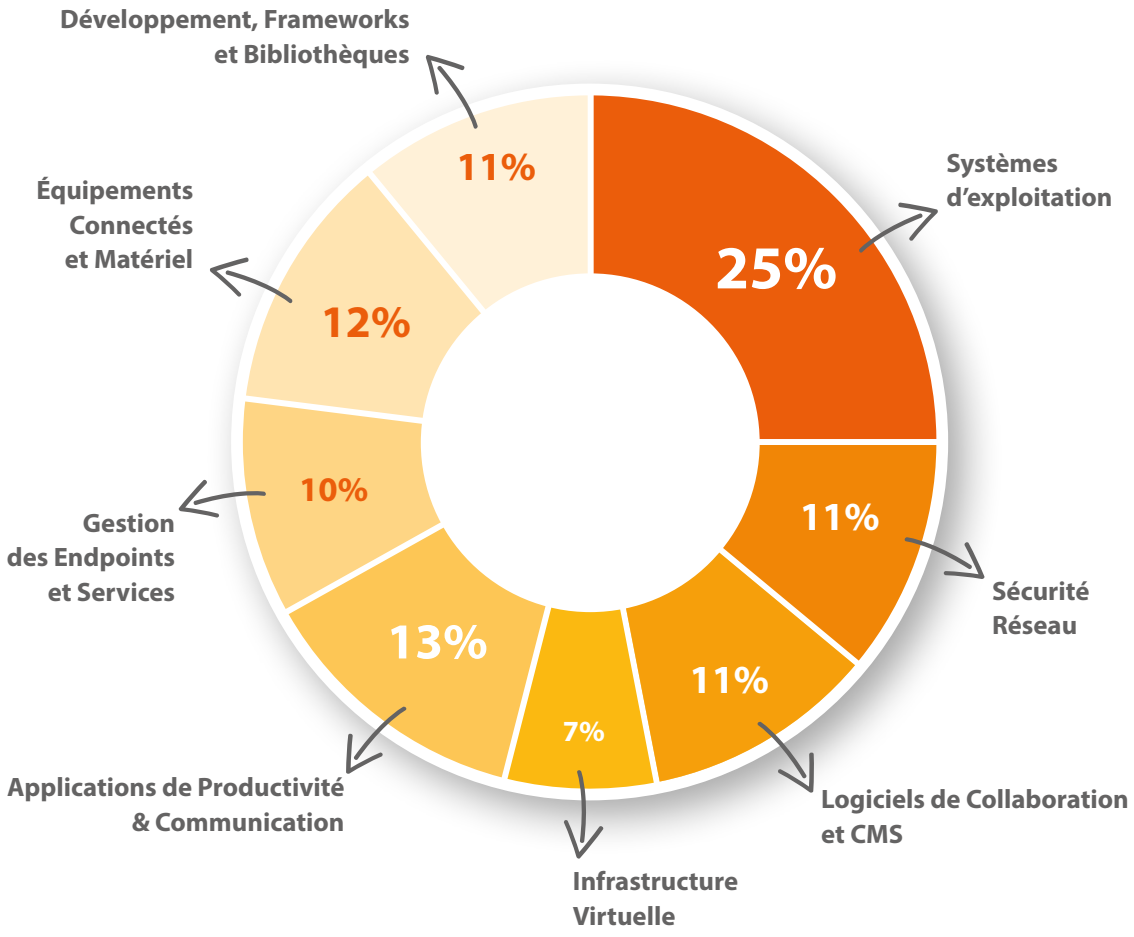
1.1.1
UN NOMBRE CROISSANT DE VULNÉRABILITÉS DÉCOUVERTES ET EXPLOITÉES

En 2025, le CERT-XMCO a recensé plus de 49 000 vulnérabilités ayant fait l'objet d'une attribution CVE soit une augmentation de 24% par rapport au plus de 40 000 publiées l'année précédente. Parmi elles, 245 vulnérabilités ont été ajoutées par l'agence américaine de cybersécurité (CISA) à son catalogue des failles activement exploitées (KEV - Known Exploited Vulnerabilities), contre 186 en 2024. Ce catalogue recense des vulnérabilités exploitées après la publication des correctifs (N-day) mais également des failles 0-day, qui ont représenté plus d'un tiers du total des vulnérabilités exploitées en 2025.

L'analyse de ces vulnérabilités montre que les produits les plus ciblés sont les systèmes d'exploitation (OS, noyaux, interfaces système) ainsi que les applications de productivité et communication (Outils de collaboration et de gestion de contenu) qui constituent des points d'entrée permettant d'accéder au cœur des systèmes, contrôler les communications et potentiellement escalader ses privilèges ou mener des attaques à distance.

Catégories de produits les plus ciblées parmi les 245 vulnérabilités ajoutées au KEV en 2025

Source : CISA

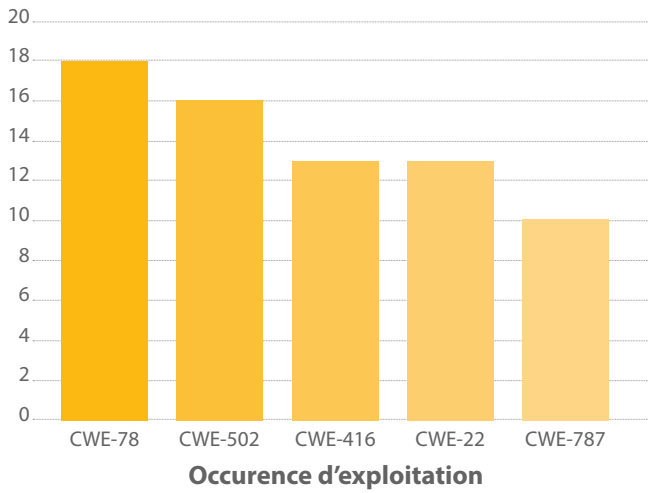


Cette année, les attaquants ont principalement exploité les failles d'injection de commandes (CWE-78) pour exécuter des commandes système arbitraires sur des serveurs ou machines cibles via des entrées utilisateur non validées. Cette vulnérabilité a été particulièrement privilégiée pour compromettre des instances en fin de support logiciel, comme la CVE-2021-20035 affectant les appliances SonicWall, afin de déployer la backdoor OVERSTEP[2].

Les failles de désérialisation de données non fiables (CWE-502) sont également largement exploitées. La CVE-2025-10035, une vulnérabilité de ce type affectant GoAnywhere MFT, a été utilisée par le groupe criminel Storm-1175 pour potentiellement déployer le ransomware Medusa[3].

Répartition des CWE les plus exploitées parmi les 245 vulnérabilités ajoutées au KEV en 2025

Source : CISA



Parmi ces vulnérabilités, une chaîne d'exploitation appelée ToolShell, composée de quatre failles, a marqué l'année 2025, que ce soit par son usage en tant que 0-day, par ses compromissions massives de victimes, ou par les impacts significatifs qu'elle a causés.

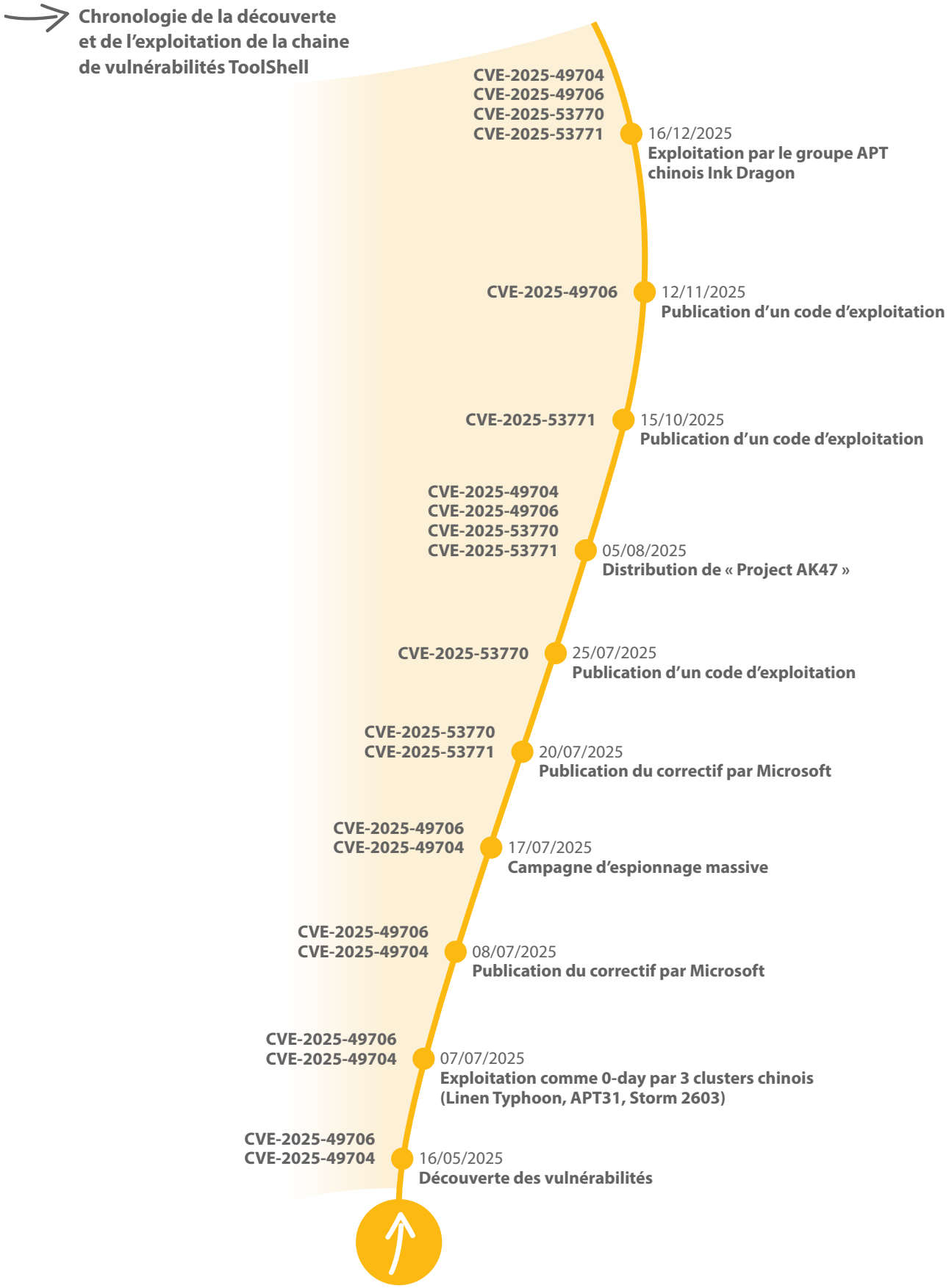
FOCUS VULNÉRABILITÉ

CVE-2025-49706, CVE-2025-49704, CVE-2025-53770 et CVE-2025-53771 (alias ToolShell) affectant Microsoft SharePoint

Le 16 mai 2025, lors de la compétition Pwn2Own Berlin, des chercheurs ont démontré l'exploitation en chaîne de vulnérabilités affectant Microsoft SharePoint, plus tard enregistrées sous les identifiants CVE-2025-49706 et CVE-2025-49704 et baptisées ToolShell[4]. Cette chaîne permettait à un attaquant distant non authentifié d'usurper l'identité d'un utilisateur de confiance, puis d'exécuter du code arbitraire sur le serveur SharePoint.

Microsoft a corrigé ces failles lors du Patch Tuesday du 8 juillet 2025. Toutefois, l'éditeur a indiqué par la suite que ces vulnérabilités avaient déjà été exploitées comme 0 day dès le 7 juillet 2025, par trois clusters distincts[5]. Les groupes Linen Typhoon et APT31, liés aux autorités chinoises, auraient mené des opérations d'espionnage, tandis qu'un troisième acteur, Storm 2603 (alias GOLD SALEM) affilié du groupe de ransomware Warlock serait associé à des attaquants sinophones aux motivations plurielles[6]. Ces failles ont également été exploitées après la publication du correctif entre le 17 et 19 juillet 2025 dans une vaste campagne mondiale d'espionnage, touchant de nombreux secteurs[7].

Peu après, il a été constaté que les correctifs initiaux pouvaient être contournés. Ces nouveaux vecteurs d'attaque, référencés CVE-2025-53770 et CVE-2025-53771 et corrigés le 19 juillet 2025, sont apparus comme conjointement exploitées avec les premières vulnérabilités par les mêmes acteurs notamment Storm 2603 pour distribuer le projet AK47 composé d'une backdoor, d'un ransomware et de loaders[8]. Ces dernières ont également été activement exploitées par le groupe APT chinois Ink Dragon pour cibler des organisations gouvernementales et des entreprises du secteur des télécommunications en Europe, en Afrique et en Asie du Sud Est[9].


Chronologie de la découverte et de l'exploitation de la chaine de vulnérabilités ToolShell
CVE-2025-49704
CVE-2025-49706
CVE-2025-53770
CVE-2025-53771
16/12/2025
Exploitation par le groupe APT chinois Ink Dragon
CVE-2025-49706
12/11/2025
Publication d'un code d'exploitation
CVE-2025-53771
15/10/2025
Publication d'un code d'exploitation
CVE-2025-49704
CVE-2025-49706
CVE-2025-53770
CVE-2025-53771
05/08/2025
Distribution de « Project AK47 »
CVE-2025-53770
25/07/2025
Publication d'un code d'exploitation
CVE-2025-53770
CVE-2025-53771
20/07/2025
Publication du correctif par Microsoft
CVE-2025-49706
CVE-2025-49704
17/07/2025
Campagne d'espionnage massive
CVE-2025-49706
CVE-2025-49704
08/07/2025
Publication du correctif par Microsoft
CVE-2025-49706
CVE-2025-49704
07/07/2025
Exploitation comme 0-day par 3 clusters chinois (Linen Typhoon, APT31, Storm 2603)
CVE-2025-49706
CVE-2025-49704
16/05/2025
Découverte des vulnérabilités

1.1.2 L'EXPLOITATION DE VULNÉRABILITÉS PARMI LES PRINCIPAUX VECTEURS DE COMPROMISSION

Dans la continuité de l'année 2024, l'exploitation des vulnérabilités informatiques reste un vecteur d'attaque majeur en 2025. Les acteurs exploitant ces failles sont diversifiés et ciblent un large éventail de produits, leur permettant de compromettre de nombreux environnements et d'étendre leur surface d'attaque.

1.1.2.1 DES ATTAQUES À GRANDE ÉCHELLE VIA LA CHAÎNE D'APPROVISIONNEMENT

L'intégration croissante de solutions tierces dans les systèmes d'information a élargi la surface d'attaque et accru les risques de compromission, y compris pour les organisations dotées de dispositifs de sécurité matures.

La compromission de la chaîne d'approvisionnement logicielle ou de services tiers (cloud, MSP) repose principalement sur l'exploitation de vulnérabilités présentes chez ces fournisseurs. Les acteurs de la menace tirent parti de ces failles pour étendre leur accès initial et propager leur compromission à grande échelle, affectant simultanément de multiples organisations clientes.

C'est par ce point de défaillance centralisé qu'en mars 2025, la vulnérabilité CVE-2025-30066 affectant la plateforme d'hébergement et de gestion de développement GitHub a permis à des acteurs malveillants d'exfiltrer des secrets CI/CD[10]. Son exploitation a été rendue possible après la compromission d'un jeton d'accès personnel GitHub (PAT) sur le dépôt du Github Action tj-actions/changed-files. Selon l'agence nationale de cybersécurité américaine (CISA), cette attaque a également été facilitée par une seconde vulnérabilité, CVE-2025-30154, touchant elle aussi GitHub[11].

FOCUS VULNÉRABILITÉ

Exploitation de la CVE-2025-61882 affectant Oracle E-Business Suite par le groupe de ransomware Cl0p[12]

Le 4 octobre 2025, Oracle a publié un correctif de sécurité pour une vulnérabilité affectant Oracle E-Business Suite, un ERP intégré qui centralise la gestion des achats, des stocks, de la production et de la logistique afin d'optimiser la chaine d'approvisionnement. Référencée CVE-2025-61882, cette faille permettait à un attaquant distant non authentifié de prendre le contrôle du système. Elle était exploitée en tant que 0-day depuis plusieurs mois par le groupe de ransomware Cl0p, dans le but de voler des données et de lancer des tentatives d'extorsion via l'envoi de courriels provenant de comptes tiers préalablement compromis par des infostealers.

Pour mener cette campagne, le groupe criminel aurait utilisé un code d'exploitation (PoC) diffusé sur le canal Telegram du collectif criminel SCATTERED LAPSUS$ HUNTERS. À ce jour, aucune information publique ne permet toutefois de déterminer avec précision la nature de la collaboration entre ces deux groupes.

1.1.2.2 L'EXPLOITATION DE SOLUTIONS D'ACCÈS DISTANT ET DE SÉCURITÉ RÉSEAU POUR OBTENIR UN ACCÈS INITIAL ET DÉPLOYER DES MALWARE

Les attaquants ne se contentent pas de cibler les composants principaux de la chaîne d'approvisionnement, ils s'attaquent aussi aux couches périphériques du système d'information, notamment les passerelles réseau et les solutions d'accès à distance. La compromission de ces équipements offre un accès direct au cœur du système d'information, ces solutions constituant des points d'entrée critiques au réseau interne et disposant généralement de droits importants. En exploitant les vulnérabilités propres à ces équipements, ils peuvent ensuite se déplacer latéralement dans l'environnement en vue d'accroître leurs privilèges et déployer des charges malveillantes.

Les types de malware utilisés sont variés, l'accès initial peut servir à installer des systèmes honeypot, déployer des backdoors ou encore déployer des ransomware[13][14]. Par exemple, la vulnérabilité CVE-2024-40766 affectant la solution VPN SonicWall SSL a conduit à la compromission de plusieurs organisations par le ransomware Akira[15]. Les solutions VPN de SonicWall figurent parmi les technologies les plus ciblées par les acteurs malveillants. En 2025, sur les 4 vulnérabilités exploitées et corrigées par l'éditeur, 3 concernaient des équipements VPN.

Vulnérabilités exploitées au sein des produits SonicWall en 2025

PRODUITS VULNÉRABLES	TECHNOLOGIE	RÉFÉRENCE CVE	CYCLE DE VIE	TRAITEMENT PAR YUNO
SMA1000	**VPN**	**CVE-2025-40602**	17/12/2025 Correctif & Exploitation	18/12/2025 – PATCH & INFO
SMA100	**VPN**	**CVE-2025-32819**	07/05/2025 Correctif 16/07/2025 Exploitation	12/05/2025 - PATCH 17/07/2025 - INFO
SMA1000	**VPN**	**CVE-2025-23006**	22/01/2025 Correctif 17/12/2025 Exploitation	23/01/2025 – PATCH 18/12/2025 - INFO
GEN6 GEN 7 TZ80	**PARE-FEU**	**CVE-2024-53704**	07/01/2025 Correctif 10/02/2025 Code d'exploitation 13/02/2025 Exploitation	08/01/2025 – PATCH 14/02/2025 – EXPLOIT 17/02/2025 - INFO

1.1.2.3

FLUX DE DONNÉES ET INFRASTRUCTURES DE GESTION : CIBLES STRATÉGIQUES DES CYBERATTAQUES

Les outils de gestion IT (RMM), qui pilotent à distance les systèmes, ainsi que les solutions de gestion des identités et des accès (IAM), qui centralisent les identités et les droits d'accès, sont également des cibles privilégiées. Leur compromission offre aux attaquants un point d'accès centralisé vers de nombreuses ressources critiques de l'entreprise.

L'exploitation de la vulnérabilité CVE-2025-61757 dans le produit Identity Manager de la suite Oracle Fusion Middleware a mis en évidence ce risque, en permettant aux attaquants de contourner les mécanismes de filtrage pour rendre accessibles des points de terminaison protégés et prendre ainsi le contrôle du système[16].

Par ailleurs, les solutions de transfert de fichiers sécurisé ou de messagerie, qui manipulent ou transportent des données sensibles, attirent particulièrement l'attention des cybercriminels. Dans le cadre de l'opération Roundpress, le groupe attribué à la Russie et référencé APT28 a par exemple exploité plusieurs vulnérabilités XSS au sein des logiciels de messagerie web (Roundcube, Horde, Zimbra et MDaemon), afin d'exfiltrer des informations confidentielles d'entités gouvernementales[17].

FOCUS VULNÉRABILITÉ

Exploitation de la CVE-2025-10035 affectant GoAnywhere MFT par Storm-1175[3]

Le 6 octobre 2025, les chercheurs de Microsoft ont publié un bulletin de sécurité à la suite de l'exploitation d'une faille affectant GoAnywhere MFT, une solution de transfert et de gestion de fichiers. Cette vulnérabilité, pour laquelle un PoC est disponible publiquement, a été exploitée comme 0-day par le groupe Storm-1175 pour déployer le ransomware Medusa.

Référencée CVE-2025-10035 et corrigée le 18 septembre 2025, cette vulnérabilité permettait à un attaquant distant et non authentifié de soumettre un objet malveillant via une réponse de licence à la signature forgée et ainsi de prendre le contrôle du système.

Actifs depuis au moins le 11 septembre 2025, les acteurs de la menace ont exploité cette faille de sécurité comme vecteur d'accès initial. Afin d'assurer leur persistance, ils ont déployé des outils de gestion à distance (RMM), puis mis en place une infrastructure de commande et de contrôle (C2), avant de procéder à l'exfiltration des données et au déploiement du ransomware Medusa sur les systèmes compromis.

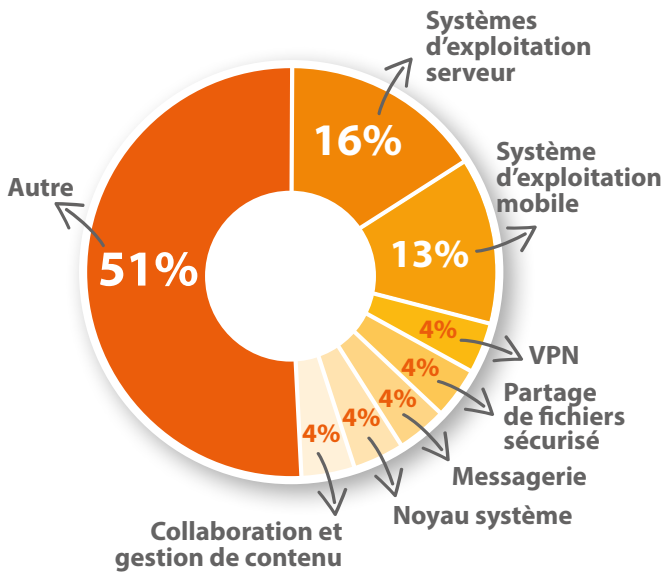
1.1.2.4

L'EXPLOITATION DES VULNÉRABILITÉS 0-DAY ET DU DÉLAI D'APPLICATION DES CORRECTIFS

Bien que les éditeurs des solutions ciblées maintiennent un cycle de correctifs régulier pour réduire la surface d'attaque, les groupes d'attaquants les plus sophistiqués contournent ces mesures en exploitant des vulnérabilités 0-day, souvent intégrées dans des chaînes d'exploitation et ciblant principalement les systèmes d'exploitation de serveurs et plus particulièrement Windows.

Type de technologie le plus ciblé pour exploiter des vulnérabilités 0-day en 2025

Source : XMCO



Les attaquants exploitent également des vulnérabilités de type N-day dans les environnements clients, en tirant parti des délais d'application des correctifs (Time to Patch) et des contraintes opérationnelles retardant la migration vers des produits encore supportés. Le groupe APT chinois Storm-1849 illustre cette méthode en ayant diffusé le malware LINE VIPER grâce à l'exploitation de deux vulnérabilités affectant des équipements Cisco arrivés en fin de support entre août 2022 et septembre 2025[18].

Ce phénomène est accentué lorsque des preuves de concept (PoC) ou des analyses de chercheurs sont publiées simultanément avec les correctifs, ce qui

peut faciliter l'exploitation des vulnérabilités par des acteurs malveillants avant que les correctifs n'aient pu être appliqués[19][20].

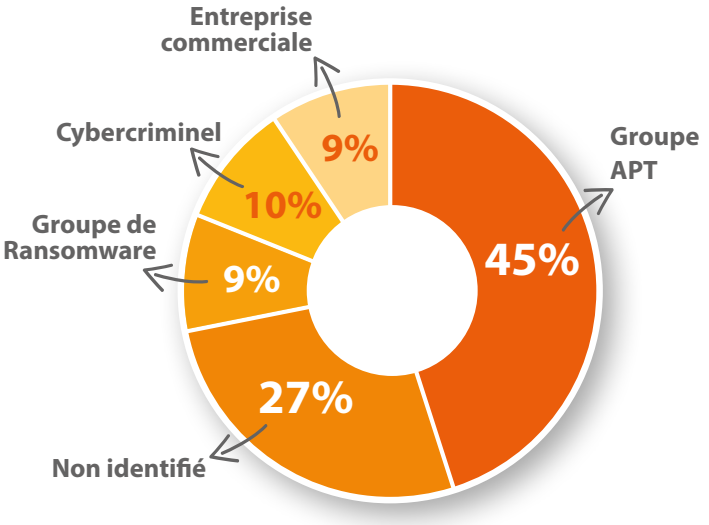
1.1.2.5

VULNÉRABILITÉS COMPLEXES EXPLOITÉES PAR DES ACTEURS SOPHISTIQUÉS

L'exploitation de vulnérabilités, en particulier des 0-day, reste une opération complexe. Seuls des acteurs sophistiqués parviennent à en tirer parti pour compromettre des systèmes critiques. En 2025, les groupes APT ont été parmi les acteurs les plus actifs dans l'exploitation de vulnérabilités 0-day. Leur objectif principal consiste principalement à déployer des malware et plus précisément des backdoors à des fins d'espionnage, comme le montrent les attaques ciblant Ivanti Connect Secure menées par des groupes APT chinois tels que UNC5337 et Silk Typhoon[20][21].

Type d'acteur ayant le plus exploité de vulnérabilités 0-day en 2025

Source : XMCO



Certains groupes ransomware ont également démontré leur capacité technique à exploiter ce type de vulnérabilités pour des motivations financières. Le 7 mai 2025, après avoir obtenu un accès initial via le détournement d'un pare-feu publiquement exposé, le groupe de ransomware Play a exploité comme 0-day la CVE-2025-29824 affectant le kernel driver Windows Common Log File System (CLFS) pour élever ses privilèges[22].

Outre les groupes APT et cybercriminels, certaines entreprises exploitent régulièrement des vulnérabilités 0-day dans une zone grise réglementaire, transformant la découverte de failles critiques en activité commerciale. Elles utilisent ces 0-day pour déployer des logiciels espions propriétaires, vendus à des clients gouvernementaux, médiatiques ou privés. Par exemple, la CVE-2025-43200 affectant iOS a permis de déployer le spyware Graphite de Paragon sur les smartphones de plusieurs personnalités médiatiques en Europe[23].

1.2 Panorama des ransomware 2025

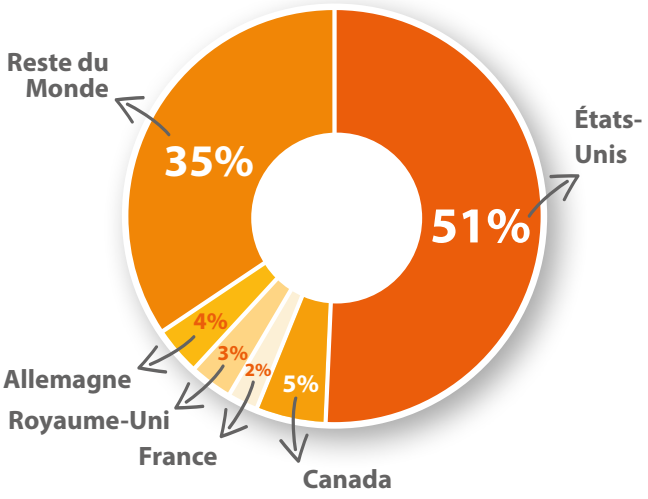
L'année 2025 a été marquée par une prolifération du phénomène criminel d'extorsion par vol et chiffrement de données. Malgré les opérations menées par les forces de l'ordre pour lutter contre le cybercrime, les collectifs de ransomware ont continué de prospérer cette année, gagnant en résilience grâce à des coopérations opportunistes et à l'usage détourné d'outils légitimes. Si la plupart des attaques restent motivées par l'appât du gain, 2025 a également vu certains collectifs instrumentalisés par des puissances étrangères étatiques.

1.2.1
2025 : UNE ANNÉE PROLIFIQUE POUR LES GROUPES DE RANSOMWARE

En 2025, les équipes du CERT-XMCO ont assuré un suivi quotidien des attaques revendiquées par les groupes ransomware. Les revendications observées cette année, en France comme à l'international, sont en hausse de respectivement 54% et 60% par rapport à 2024. La France représente par ailleurs un peu plus de 2% du total des attaques revendiquées au cours de cette période à l'échelle internationale contre 51% du total pour les États-Unis. Ces proportions demeurent stables par rapport à 2024.

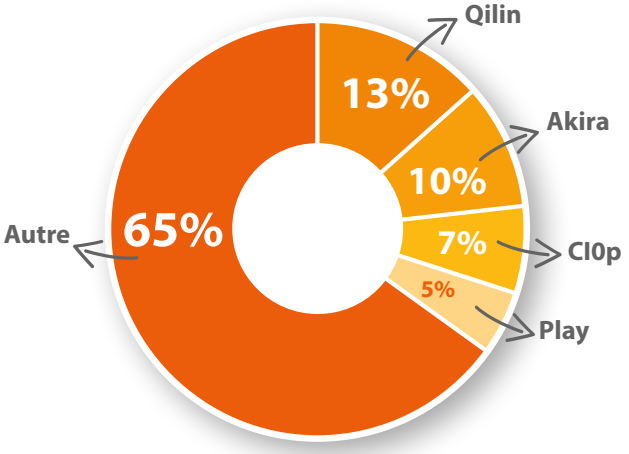
Pays les plus ciblés en 2025

Source : XMCO



Groupes ransomware les plus actifs en 2025

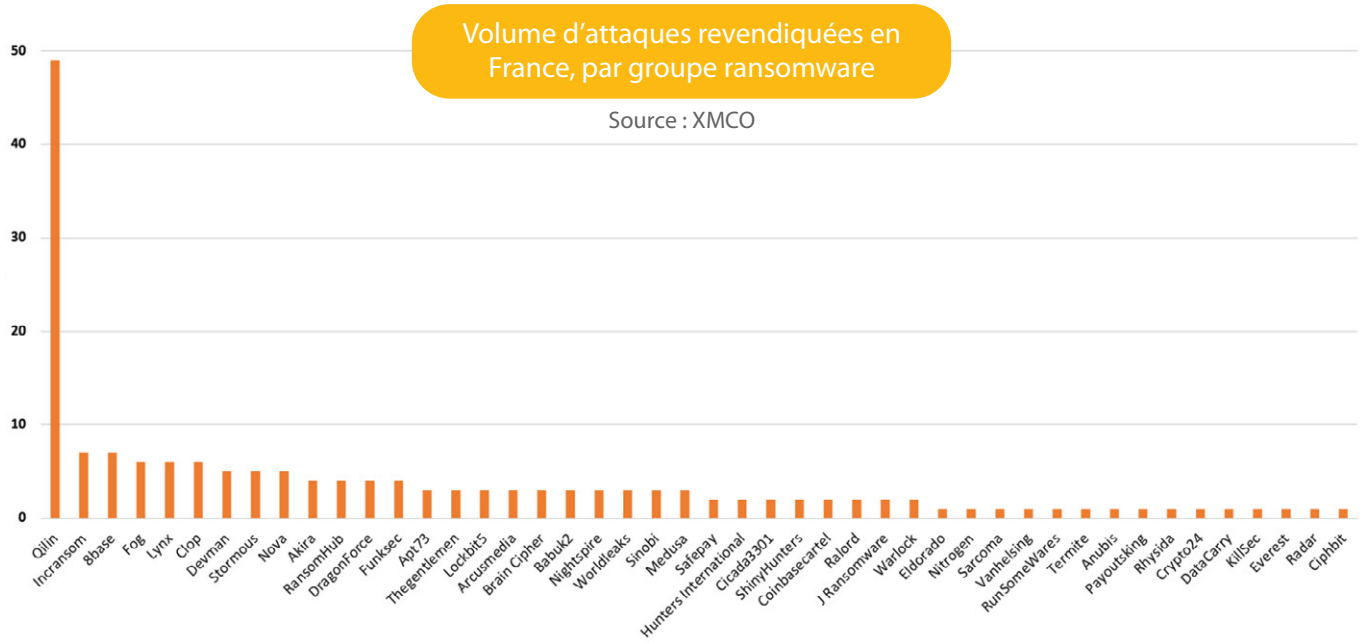
Source : XMCO



Ces statistiques fournissent un éclairage sur les collectifs cybercriminels et la nature de leur victimologie. Cette année, les groupes Qilin, Akira, Cl0p et Play se sont particulièrement distingués par leur proactivité, comptabilisant près de 35% du total des tentatives d'extorsion analysées par le CERT-XMCO.

À l'issue de l'année 2025, Qilin s'illustre comme le programme de Ransomware-as-a-Service (RaaS) ayant revendiqué le plus d'attaques sur son site vitrine. Le groupe cybercriminel aurait profité de la subite disparition du collectif RansomHub, hégémonique parmi les programmes de RaaS jusqu'en avril 2025, avant d'être victime d'une fuite massive de ses affiliés vers d'autres groupes plus attractifs, à l'instar de DragonForce, d'Akira ou encore de Qilin[24][25].

Dans ce contexte, Qilin s'illustre aussi comme le groupe criminel le plus actif en France, avec 49 attaques revendiquées sur son site vitrine contre des entités françaises, loin derrière les collectifs IncRansom, 8base et Clop. En tout, 47 groupes de ransomware distincts ont ciblé la France en 2025.



De multiples attaques par ransomware ont été médiatisées en raison des perturbations importantes qu'elles ont causées, à l'instar de la compromission de la région des Hauts-de-France par Qilin, bloquant l'accès au réseau de près de 80% des lycées publics de la région en octobre 2025[26]. Lors de l'année passée, plusieurs opérations policières ont démontré la rentabilité des collectifs de ransomware via la saisie de plusieurs millions de dollars sous forme de cryptomonnaies, comme en témoigne les actions menées contre les collectifs Zeppelin, BlackSuit ou encore Chaos[27][28][29].

Revendications d' attaques les plus marquantes sur des entreprises françaises en 2025 (Source : XMCO)

MOIS	GROUPE CRIMINEL	VICTIME FRANÇAISE
Janvier	Incransom	Mission Locale Montpellier
Février	Fog	Viseo
Mars	FunkSec	Sorbonne-Université
Avril	RunSomeWares	Harvest
Mai	Qilin	Bouygues Energies & Service
Juin	Anubis	Disneyland Paris
Juillet	Payoutsking	EvoluPharm
Août	Warlock	Orange
Septembre	Everest	Groupe Clarins
Octobre	ShinyHunters	Chanel
Novembre	Qilin	Christofle
Décembre	Devman	Fassic

1.2.2 ÉVOLUTION DU CYBERCRIME : DE L'ABUS D'OUTILS LÉGITIMES À L'INGÉRENCE ÉTATIQUE

1.2.2.1 RÉSILIENCE DES GROUPES DE RANSOMWARE ET DÉTOURNEMENT D'OUTILS LÉGITIMES

En dépit des actions menées par les forces de l'ordre, principalement occidentales, les groupes ransomware ont continué à prospérer en 2025. Le CERT-XMCO a comptabilisé 76 nouveaux sites vitrine opérés par des groupes de ransomware l'année passée. Cette tendance relève d'un processus de cartelisation des ransomware. La multiplication des collectifs cybercriminels s'explique par les logiques de coopération mises en place par différents groupes criminels de premier plan, à l'instar de Qilin, DragonForce et LockBit ayant annoncé leur triumvirat sur RAMP, obligeant le reste de l'écosystème cybercriminel à se réorganiser pour rester rentable[25].

Conjointement à ces logiques de coopérations, les groupes de ransomware ont amélioré leurs modes opératoires, s'appuyant sur un large éventail de vulnérabilités et sur le détournement d'outils légitimes d'administration à distance (RMM) tels qu'Atera, AnyDesk ou de sécurité, à l'instar de Velociraptor[30][31]. L'année 2025 a en outre été marquée par une recrudescence des accès initiaux obtenus par les opérateurs de ransomware via l'ingénierie sociale, comme en témoignent les vagues d'attaques opérées par le collectif criminel Scattered Lapsus$ Hunters.

FOCUS MENACE
Le groupe Scaterred Spider, ShinyHunters et Lapsus$

Le cluster Scattered Lapsus$ Hunters s'est imposé comme l'un des collectifs de ransomware les plus marquants de 2025. Sa montée en puissance s'explique par une collaboration historique de ses membres avec d'autres programmes de RaaS, à l'instar de RansomHub, DragonForce ou encore Qilin. À l'origine, les administrateurs de Lapsus$ sont connus pour exploiter des techniques sophistiquées d'ingénierie sociale afin d'obtenir l'accès initial, tandis que Scattered Spider serait davantage spécialisé dans le contournement des processus MFA et que ShinyHunters s'illustre par la vente de bases de données volées[32][33].

Cette convergence de savoir-faire a donné naissance à un groupe structuré, capable d'orchestrer des vagues d'extorsion à grande échelle en ciblant la chaine d'approvisionnement logicielle de centaines d'entreprises évoluant dans de multiples secteurs à l'international. Plusieurs incidents revendiqués par le groupe criminel ont impliqué la compromission d'environnements SaaS, conduisant au vol de données clients des solutions Salesforce, Gainsight et Zendesk[34][35].

Dans certains cas, ces opérations ont provoqué des interruptions d'activité significatives, en témoigne l'attaque contre le groupe Jaguar Land Rover survenue en septembre 2025 et qui aurait coûté 196 millions de livres sterling de pertes[36]. Les volumes de données volées par Scattered Hunters Lapsus$ ont renforcé la visibilité et la réputation du collectif cybercriminel, développant désormais un programme de Ransomware-as-a-Service pour attirer de nouveaux membres et étendre leurs opérations.

Le mode opératoire employé par Scattered Hunters Lapsus$ s'articule principalement sur des techniques d'ingénierie sociale, consistant à cibler les employés des structures ciblées.

Ces opérations de manipulation psychologique ont pris diverses formes en 2025, allant de l'usurpation d'un collaborateur bloqué auprès du support informatique, des opérations de MFA bombing, le recrutement d'insiders ou encore la distribution de leurres de phishing imitant des portails d'authentification légitimes de solutions populaires[37].

Ainsi, les opérateurs de Scattered Hunters Lapsus$ ont industrialisé leurs attaques par ingénierie sociale et démontré leur capacité à compromettre un vaste éventail d'organisations à l'international, leur extorquant par la suite des rançons sur la base des données sensibles.

En contraste avec les logiques de coopérations déjà évoquées, des conflits au sein de l'écosystème cybercriminel, sont susceptibles d'avoir exercé une influence sur l'organisation hiérarchique des programmes de Ransomware-as-a-Service (RaaS). Ce phénomène pourrait s'expliquer par la nécessité constante des administrateurs de RaaS d'attirer de nouveaux membres afin de rester techniquement supérieur face à la concurrence et de maximiser leurs profits.

Cette logique de concurrence au sein de l'écosystème cybercriminel a entrainé des opérations de dénigrement, visant à saper la réputation de programmes de RaaS adverses. Plusieurs exemples marquants ont été signalés en 2025, comme la divulgation des conversations internes du collectif Medusa par RebornVC, du doxing des opérateurs du même groupe par Silent ransomware, ou bien encore l'usurpation de l'identité d'Europol par Scattered Lapsus$ Hunters afin de faire pression sur Qilin[38][39][40].

1.2.2.2

UNE INSTRUMENTALISATION ÉTATIQUE DU CYBERCRIME ORGANISÉ

Bien que la majorité des attaques par ransomware soient motivées par des objectifs financiers, l'année 2025 a été marquée par l'instrumentalisation de collectifs de ransomware par des puissances étrangères, ajoutant davantage de confusion dans la compréhension de l'écosystème cybercriminel et de la victimologie de certains groupuscules. Plusieurs États sont ainsi soupçonnés d'avoir facilité, voire commandité, des attaques par ransomware pour répondre à leur agenda politique respectif. En s'appuyant sur des ressources cybercriminelles, les puissances étatiques sont en mesure de nier la responsabilité d'activités malveillantes, pouvant prendre la forme d'espionnage industriel, de déstabilisation informationnelle, voire de sabotage d'infrastructures physiques.

Cette situation est aussi bénéfique pour les groupes de ransomware qui profitent de la corruption de certaines structures étatiques, en particulier celles évoluant au sein la Communauté des États indépendants (CIS), pour étendre leurs activités. En matière de collecte illégale de données, le cluster RomCom a été un exemple marquant de 2025. Ce groupe d'attaquants, connu pour ses liens historiques avec les souches de ransomware Cuba, Industrial Spy et Team Underground, serait en réalité opéré par l'unité militaire russe n°29155, chargée des opérations offensives sur des réseaux informatiques pour le compte du renseignement militaire russe (GRU). Les motivations plurielles du groupe RomCom, à la fois financières et politiques, ont été soulignées par plusieurs sociétés de cybersécurité en 2025[41][42][43].

La convergence des intérêts économiques du cybercrime avec les enjeux politiques de puissances étrangères est une tendance qui semble également s'opérer en Chine et qui s'est illustrée en 2025 par l'exploitation coordonnée de failles de sécurité 0-day affectant Microsoft SharePoint par trois clusters, dont deux groupes APT chinois et un groupe de ransomware émergent, connu sous le nom de Warlock, poursuivant des objectifs transverses et susceptible de collaborer avec Pékin[44]. L'exploitation de cette chaîne de vulnérabilités nommée ToolShell est analysée plus en détail dans un focus dédié du panorama des vulnérabilités 2025.

De son côté, la Corée du Nord a continué d'avoir ponctuellement recours au détournement de souches de ransomware dans le cadre d'attaques destinées à financer son programme nucléaire et à maintenir le régime de Kim Jong-un au pouvoir. Suivant cette logique, le cluster Moonstone Sleet a déployé le ransomware Qilin lors d'attaques survenues en février 2025[45]. Les autorités iraniennes sont aussi soupçonnées d'avoir cherché à affaiblir leurs adversaires géopolitiques, au-devant desquels Israël et les États-Unis par l'intermédiaire de la distribution des ransomware Pay2Key, Handala, Darkbite, ou encore l'année dernière via une collaboration clandestine avec les collectifs NoEscape, Ransomhouse et ALPHV/BlackCat, dénoncée par les États-Unis[46][47].

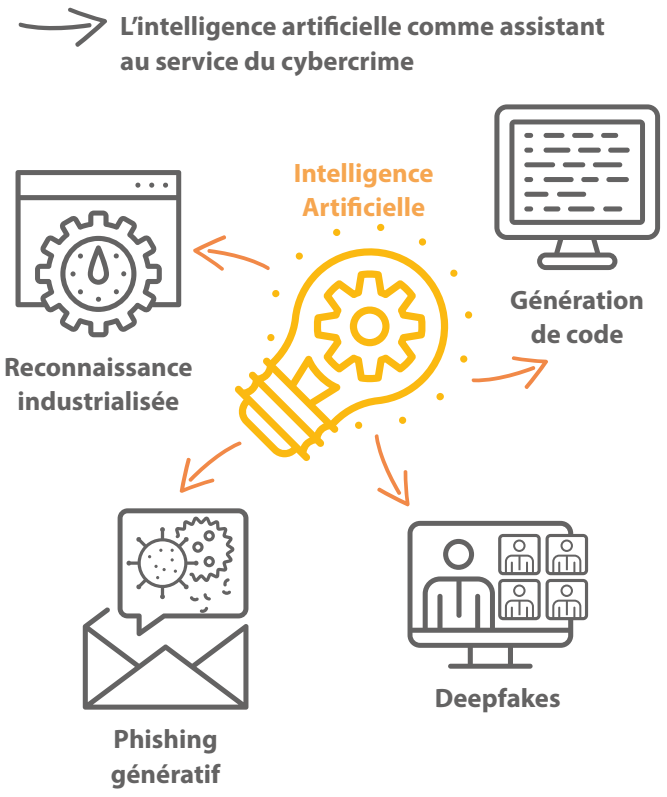
yuno By xmco

2. ANALYSE DES PRINCIPALES TENDANCES 2025

2.1

Accessibilité croissante des arsenaux cyber : l'intelligence artificielle

L'année 2025 s'impose comme un point d'inflexion dans l'usage offensif des technologies d'intelligence artificielle. La généralisation des grands modèles de langage et des systèmes génératifs agit comme un catalyseur, réduisant considérablement les prérequis techniques et ouvrant la voie à une industrialisation des campagnes malveillantes.



2.1.1 RECONNAISSANCE INDUSTRIALISÉE PAR L'IA

Les outils associant scraping et modèles de langage permettent désormais d'extraire, d'organiser et d'interpréter d'immenses volumes de données en un laps de temps réduit. Une étude universitaire menée par Stanford en 2024 démontre qu'il est possible de cartographier avec précision des écosystèmes professionnels complets, en reconstituant organigrammes et réseaux de sous-traitance à partir de données publiques grâce à des outils accessibles à tous[48].

Cette automatisation réduit l'écart de compétence entre novices et experts, en fournissant aux premiers une intelligence d'appui capable de compenser en partie leur manque de savoir-faire technique, ce qui leur permet de mener des opérations impactantes à grande échelle[49]. Des plateformes comme Apify proposent déjà des scrapers pilotés par modèles de langage, capables d'interpréter le code source HTML et de suivre des liens à partir d'instructions en langage naturel, permettant à des utilisateurs sans compétences techniques avancées de collecter automatiquement des données structurées sur des centaines de pages d'actualités ou de produits[50].

2.1.2 PHISHING GÉNÉRATIF : UNE SOPHISTICATION ET INDUSTRIALISATION DES LEURRES

D'après un rapport de KnowBe4 régulièrement cité, 82,6 % des emails de phishing observés entre septembre 2024 et février 2025 présentent des indices d'automatisation par intelligence artificielle, tandis que le volume global de campagnes malveillantes connaît une hausse de 17,3 % sur la même période[51]. Ces dernières s'appuient sur des modèles de langage capables de générer des messages exempts de fautes, parfaitement alignés sur le jargon métier et adaptés au contexte propre à l'organisation ciblée.

Cette sophistication linguistique s'accompagne d'une montée en puissance de tactiques polymorphes, l'IA produisant automatiquement de multiples variantes d'un même message afin de contourner les mécanismes de détection reposant sur des signatures fixes ou des modèles statiques. L'exigence de compétences rédactionnelles se trouve ainsi largement réduite : un acteur malveillant n'a plus besoin que de savoir décrire son scénario en langage naturel pour obtenir des contenus crédibles, déclinables à grande échelle.

2.1.3 DEEPFAKES : UN OUTIL DE FRAUDE ACCESSIBLE

Ces technologies permettent de créer des imitations quasi parfaites de voix et de visages, rendant les attaques d'ingénierie sociale considérablement plus convaincantes[52].

En février 2024, l'entreprise d'ingénierie britannique Arup a perdu plus de 25 millions de dollars suite à une fraude sophistiquée impliquant l'usage d'un deepfake au cours d'une vidéoconférence au sein de laquelle le directeur financier et d'autres collègues étaient générés par IA[53]. En l'état, la réalisation d'un deepfake live (en temps réel) demeure encore réservée aux acteurs sophistiqués disposant d'une puissance de calcul conséquente.

En 2025, les deepfakes passent néanmoins d'attaques ponctuelles à un outil courant de fraude, avec l'émergence de véritables offres de deepfake as a service sur les places de marché criminelles.

Des prestataires y vendent, pour quelques dizaines à quelques centaines de dollars la minute, des vidéos et voix synthétiques prêtes à l'emploi (explicitement proposées pour des escroqueries BEC, des fraudes à l'investissement ou le contournement de KYC) industrialisant la production de deepfakes pour des acteurs aux compétences techniques limitées et faisant exploser le volume de campagnes possibles[54] [55].

2.1.4 IA GÉNÉRATIVE : CATALYSEUR D'ATTAQUE SOUS CONTRÔLE HUMAIN

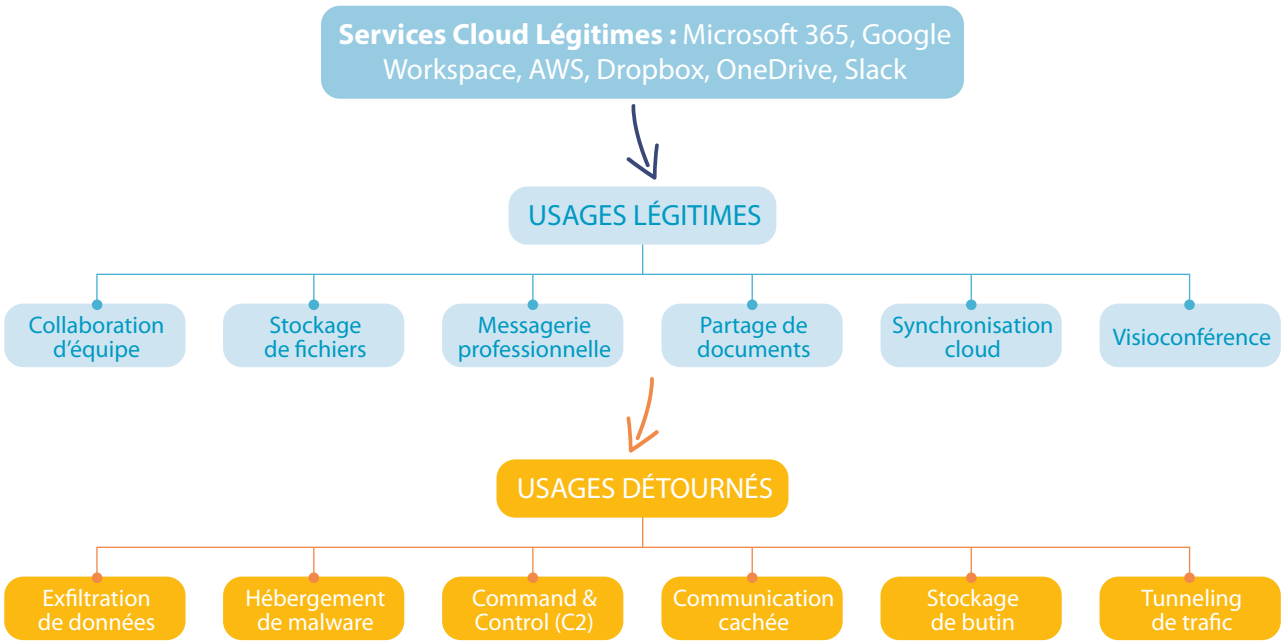
L'intelligence artificielle générative permet de générer des solutions ou des contenus inédits, pour autant l'accessibilité des modèles génératifs n'a pas produit d'explosion du nombre de nouveaux malware dans la nature. Les systèmes actuels de GenAI ne disposent pas des capacités spécifiques pour créer de manière indépendante des malware opérationnels, et requièrent de fait une intervention humaine afin de corriger et diriger le processus de création[56].

Les cybercriminels utilisent néanmoins les outils publics de GenAI pour créer des malware ou des scripts simples, améliorer les compétences des malware existants, ou en créer des variantes. À ce titre, le modèle Codex d'OpenAI annoncé en mai 2025 et conçu pour automatiser des tâches de programmation, pourrait être détourné par des acteurs malveillants malgré les garde-fous prévus, à l'image des précédents contournements de ChatGPT[57].

L'intelligence artificielle s'impose comme un véritable assistant d'attaque généraliste : accessible, performante et adaptable, elle renforce l'efficacité opérationnelle des acteurs tout en modifiant les dynamiques traditionnelles de la menace. Malgré cela, les modèles d'IA demeurent limités par un déficit d'autonomie, leur efficacité dépendant largement de la qualité des données d'entraînement et du guidage humain.

2.2
Le cloud comme vecteur d'attaques privilégié

Poursuivant la tendance amorcée à la fin de 2024, l'année 2025 confirme l'observation d'une mutation des techniques d'attaque abusant de services légitimes vers un modèle dit de « Living off the Cloud » (LOTC), prolongeant le concept de « Living off the Land » (LOTL)[58]. Cette adaptation stratégique voit les acteurs malveillants détourner des services cloud légitimes à des fins offensives, complexifiant significativement les capacités de détection des activités hostiles.



2.2.1 LE CLOUD DE CONFIANCE, NOUVEAU CHEVAL DE TROIE

Le principe repose sur la réutilisation de services tels que Microsoft 365, Google Workspace, Amazon Web Services, Dropbox ou OneDrive pour des fonctions d'exfiltration, d'hébergement de charges malveillantes ou de C2, sans recourir à une infrastructure dédiée visible. Au cours de tels scénarios, des fonctions serverless pourraient être exploitées comme points de terminaison C2 accessibles via des URL HTTPS, tandis que les services de stockage seraient mobilisés pour transférer des archives chiffrées ou héberger des charges malveillantes[59].

Ce basculement s'inscrit dans un environnement marqué par une intensification du volume d'alertes de sévérité élevées liées aux environnements cloud, dont le nombre moyen a augmenté de 235 % en 2024 selon les observations de Unit 42[60].

2.2.2 LES MULTIPLES USAGES DU CLOUD : ANALYSE DES GROUPES ATTAQUANTS

Ce constat est étayé par l'analyse de plusieurs attaques perpétrées en 2025 et orchestrées par des groupes dont les objectifs divergent, de même que leurs usages des solutions cloud.

UNK_SneakyStrike

Cette campagne avait pour objectif la compromission de comptes Microsoft Entra ID. Les acteurs malveillants ont eu recours à des serveurs Amazon AWS et à un compte Office 365 légitime afin d'effectuer une rotation géographique de l'origine de leurs tentatives de password spraying, complexifiant la détection et le blocage des connexions suspectes[61].

CL-STA-1020

Ce cluster d'espionnage se distingue par l'utilisation d'URL AWS Lambda comme canal de commande et de contrôle (C2) de sa backdoor HazyBeacon, permettant de dissimuler le trafic malveillant dans des communications HTTPS légitimes vers l'infrastructure AWS[62].

JavaGhost
Ce groupe a détourné des environnements Amazon Web Services (AWS) afin d'y déployer une infrastructure dédiée au phishing. En exploitant des clés d'accès exposées, il a abusé des services Amazon SES et WorkMail pour envoyer des emails malveillants depuis une infrastructure cloud préexistante, optimisant ses coûts et renforçant l'apparente légitimité de ses campagnes[63].

Lazarus
Dans le cadre de ses activités malveillantes à but financier, le groupe Lazarus a intégré le service de stockage Dropbox à son infrastructure de commande et de contrôle (C2), en l'utilisant comme relais pour l'exfiltration et le stockage des données dérobées, en complément d'autres services cloud dits bulletproof employés pour héberger et dissimuler son activité[64].

Tycoon 2FA
Ce kit de Phishing-as-a-Service a été conçu pour contourner les dispositifs d'authentification multifacteur. Il a d'abord abusé du service légitime Cloudflare Turnstile pour la gestion des CAPTCHA avant d'évoluer vers un mécanisme propriétaire, afin de limiter les risques de détection fondée sur la réputation de domaine[65].

2.2.3 L'ESSOR DES ATTAQUES EN RÉSEAU ALIMENTÉES PAR DES SERVICES LÉGITIMES

Au-delà de l'usage du cloud comme simple support d'infrastructure pour les attaquants, les cas étudiés en 2025 montrent un basculement vers l'exploitation malveillante directe des services cloud appartenant aux organisations ciblées. Les environnements SaaS, les identités associées et les intégrations applicatives deviennent autant de points d'entrée et de relais potentiels, au cœur même des chaînes de confiance numériques.

Pris dans leur ensemble, ces éléments traduisent une augmentation de la surface d'attaque exploitable par les adversaires, particulièrement visible dans les environnements cloud où l'interdépendance entre identités, services managés et intégrations tierces façonne de nouveaux vecteurs d'exposition[66].

Comme étayé dans les parties précédentes, cette dynamique met en évidence les tentatives croissantes de compromission de la chaîne d'approvisionnement logicielle par l'exploitation des vulnérabilités.

Dans ce cadre et dans une dynamique sécuritaire similaire à celle observée pour les infrastructures locales, de nombreuses organisations opèrent avec un volume important d'identités disposant de privilèges excessifs[67]. Cette dérive touche tout particulièrement les comptes techniques, dont les permissions dépassent souvent les stricts besoins opérationnels. La problématique s'aggrave avec l'exposition directe sur Internet d'API de gestion, de services de stockage et de messagerie, qui offrent aux attaquants des points d'entrée supplémentaires[68].

Dans ce contexte, la compromission d'un seul tenant cloud peut suffire à alimenter des campagnes de phishing ou d'exfiltration ciblant d'autres entités, comme le montrent les infrastructures frauduleuses bâties sur des services de messagerie. L'usage offensif de services de distribution (CDN) largement répandus, par exemple dans certains kits de phishing, renforce ce phénomène en offrant aux attaquants la possibilité de filtrer le trafic d'analyse et de bénéficier des mécanismes de réputation attachés à ces briques techniques[69].

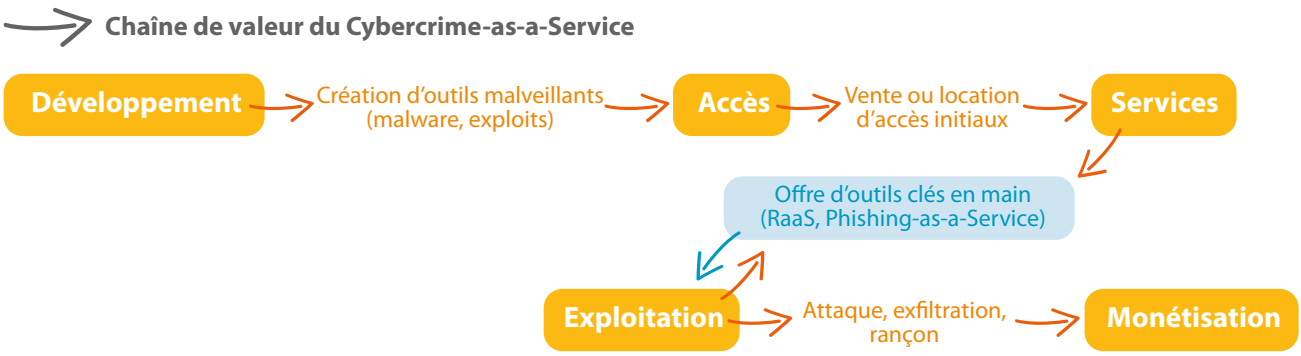
La surface d'attaque devient ainsi véritablement « en réseau », structurée par des chaînes de confiance et de délégation qui favorisent l'instrumentalisation des services cloud légitimes dans des opérations offensives de plus en plus difficiles à distinguer de l'activité métier ordinaire.

2.3

La professionnalisation des rôles au cœur de l'écosystème cybercriminel

Au cours de l'année 2025, le paysage cybercriminel a continué de se transformer, fonctionnant aujourd'hui en partie comme une économie de service, structurée et efficiente. L'émergence des modèles As-a-service traduit la mue d'un ensemble anarchique d'acteurs en un écosystème dans lequel chaque maillon s'est spécialisé, professionnalisé et intégré à une chaîne de valeur.

Ce modèle s'appuie désormais sur une organisation industrielle distribuée, chaque acteur représentant une fonction essentielle du système[70]. Ensemble, ils forment un réseau d'interdépendances : développeurs de malware, courtiers en accès initiaux et plateformes proposant des kits as-a-service assumant chacun une fonction spécifique au cours d'une compromission[71].



2.3.1 LE MODÈLE AS-A-SERVICE : LA TRANSFORMATION DU CYBERCRIME EN UNE INDUSTRIE RÉSILIENTE

Le modèle as-a-service s'appuie sur un ensemble d'acteurs spécialisés dans la fourniture d'infrastructures essentielles, parmi lesquels les plateformes cloud légitimes, de plus en plus exploitées pour héberger des serveurs de commande et de contrôle (C2), ainsi que les hébergeurs bulletproof, les fournisseurs de VPN résidentiels et les services de messagerie chiffrée[72].

À titre d'exemple, Aeza Group, entreprise russe basée à Saint-Pétersbourg constitue l'un de ces hébergeurs sanctionnés par les États-Unis en juillet 2025 pour avoir fourni des services d'hébergement opaques à des cybercriminels[73]. Ces derniers incluent le groupe BianLian spécialisé dans l'utilisation de ransomware, les opérateurs des infostealers RedLine Stealer et Lumma Stealer dédiés au vol d'identifiants, ainsi que des opérations de désinformation telles que Doppelgänger, attribuées à des acteurs russes. Cette configuration assure aux acteurs malveillants une résilience opérationnelle, les hébergeurs ignorant systématiquement les injonctions des autorités compétentes.

Au-delà de l'hébergement, les principes du modèle as-a-service se retrouvent également dans la conception et la commercialisation d'outils malveillants. Les plateformes de Malware-as-a-Service (MaaS) fonctionnent sur un modèle d'abonnement ou de commission : les développeurs de malware conçoivent et mettent à jour leurs produits tandis que les affiliés les déploient, les gains étant partagés a posteriori[74].

Le développement et la diffusion de malware, autrefois réservés à une minorité d'acteurs spécialisés, se sont profondément banalisés au sein de l'écosystème actuel. Il est désormais possible pour des cybercriminels aux capacités techniques limitées de sous-traiter la quasi-totalité de la chaîne opérationnelle. Cette délégation peut prendre plusieurs formes : l'achat d'un accès initial auprès de courtiers spécialisés, la location d'infrastructures automatisées facilitant la mise en œuvre d'attaques, ou encore le recours à des offres de ransomware « clef en main ».

Conçues sur le modèle des plateformes légitimes, ces offres fournissent une interface de gestion, des mises à jour régulières et une assistance technique complète[75]. Cette constellation d'acteurs forme un écosystème multinodal, où la redondance des rôles empêche l'effondrement du système. La suppression d'une place de marché illégale ne provoque qu'une perturbation temporaire dans l'écosystème criminel : très rapidement, une autre plateforme émerge pour capter l'ensemble de la clientèle et des vendeurs laissés sans interlocuteur.

2.3.2 CARTELISATION DES COLLECTIFS DE RANSOMWARE

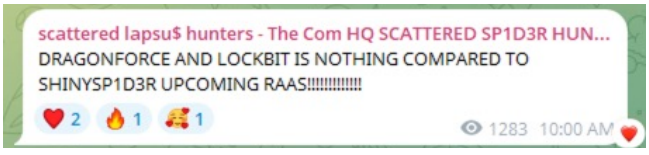
L'année 2025 voit se renforcer une dynamique de cartelisation des collectifs de ransomware, marquée par l'émergence continue de nouveaux programmes de Ransomware-as-a-Service (RaaS) structurés comme de véritables produits. C'est notamment le cas de ShinySp1d3r, dévoilé en novembre 2025 et développé en continu depuis par les groupes ShinyHunters, LAPSUS$ et Scattered Spider réunis sous la bannière Scattered LAPSUS$ Hunters[76].

Ce collectif émerge à l'été 2025 comme une alliance structurée, chaque membre apportant une expertise distincte : Scattered Spider est spécialisé dans l'obtention d'accès initiaux par ingénierie sociale, LAPSUS$ s'est fait connaître par son utilisation extrêmement efficace des techniques de Sim-Swapping et de contournement MFA, tandis que ShinyHunters alimente le collectif par sa capacité à exfiltrer et monétiser massivement les données sur les forums clandestins.

À partir d'août 2025, le canal Telegram shinysp1d3r / SLSH devient la vitrine de leur activité criminelle, d'abord comme hub d'extorsion tirant parti de chiffreurs tiers (ALPHV/BlackCat, Qilin, RansomHub, DragonForce), puis, à l'automne 2025, comme opérateur RaaS à part entière avec le lancement du rançongiciel ShinySp1d3r. Cette évolution illustre le passage d'une consommation opportuniste d'outils tiers à une logique d'intégration verticale, fondée sur le développement interne d'outils sophistiqués et la construction d'une marque RaaS disposant de son propre chiffreur, de capacités avancées de propagation et d'un cadre « éthique » revendiqué pour encadrer les affiliés.

Image issue du canal Telegram de Scattered Lapsus$ Hunter

Source : TELEGRAM



Cette industrialisation s'accompagne d'un mouvement de « cartelisation distribuée » des écosystèmes de ransomware, où des collectifs nouent des alliances souples, partagent ressources et affiliés et renforcent par là même leurs capacités d'attaques. Cette dynamique se manifeste à travers deux formes complémentaires de consolidation. La première, illustrée par DragonForce, LockBit ou Qilin, repose sur des alliances opportunistes entre écosystèmes RaaS déjà structurés, qui mutualisent notoriété, infrastructures et canaux de fuite pour accroître la pression sur les victimes et consolider leur position dominante[77].

La seconde, incarnée par des collectifs comme Scattered Spider, LAPSUS$, ShinyHunters, tous issus de la même communauté nommée The Com, traduit une approche plus fluide et adaptative, centrée sur des spécialistes de l'intrusion et de l'ingénierie sociale se greffant successivement à différents programmes RaaS selon les opportunités[33]. Ensemble, ces configurations brouillent les frontières entre les groupes, favorisent la circulation des affiliés d'un label à l'autre et déplacent le rapport de force dans un écosystème interconnecté, où une coordination informelle suffit à maintenir un niveau de menace élevé en dépit des opérations de lutte contre le cybercrime menée cette année. Ce fonctionnement est analysé dans le panorama ransomware 2025, qui illustre à la fois la résilience de l'écosystème ransomware et le jeu complexe entre coopération et rivalités internes.

2.4 ClickFix et l'exploitation du geste de confiance de l'utilisateur

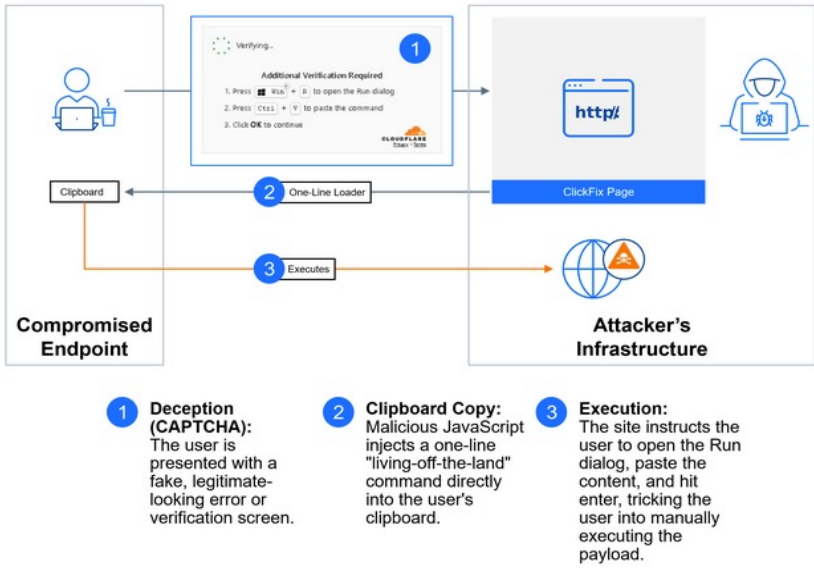
La technique ClickFix s'est imposée en 2025 comme une méthode d'attaque prépondérante, adoptée par un large spectre d'acteurs malveillants, allant des cybercriminels à motivation financière aux groupes étatiques, et ce pour plusieurs raisons : peu d'investissement technique, une forte réutilisabilité des kits et une automatisation poussée de la production de pages malveillantes maximisent le rendement par campagne[78].

En capitalisant sur des interfaces familières (CAPTCHA, écrans de mise à jour, pages de sécurité factices) et sur des actions réalisées par l'utilisateur lui-même, ClickFix contourne une partie des contrôles défensifs traditionnels et améliore le taux de conversion des attaques en accès effectifs au système, ce qui en fait un vecteur particulièrement attractif dans une logique de marché cybercriminel industrialisé.

2.4.1
INGÉNIERIE SOCIALE ET CLICKFIX : MANIPULATION ACTIVE DES UTILISATEURS

Cette méthode d'ingénierie sociale consiste à tromper l'utilisateur pour qu'il exécute lui-même des commandes malveillantes, en exploitant sa confiance ou sa volonté de résoudre un problème technique apparent, souvent par le biais de faux CAPTCHA ou de prétendues vérifications de sécurité. Le mode opératoire débute par une phase de leurre, disséminée via des campagnes de phishing, de la publicité malveillante (malvertising), ou des sites légitimes compromis. La victime est dirigée vers une page contrôlée par l'attaquant où, sous un faux prétexte, elle est incitée à copier-coller une commande dans un outil système comme PowerShell ou le terminal, notamment via Win+R[79].

Chaine d'attaque reposant sur la technique ClickFix
(Source : BitDefender, ClickFix: A KISS from Cybercriminals)



L'utilisateur, convaincu d'exécuter une action légitime, provoque en fait l'infection de sa machine. L'efficacité du procédé réside dans sa faculté à déjouer les défenses techniques traditionnelles en exploitant la confiance et la participation active de la victime, transformant ainsi l'humain en maillon d'exécution plutôt qu'en barrière de sécurité.

L'une des campagnes les plus marquantes observées en 2025, baptisée PHALT#BLYX et identifiée par les analystes de Securonix, met en lumière l'exploitation de la technique ClickFix au cœur d'une opération spécifiquement dirigée contre des organisations du secteur hôtelier[80].

Cette campagne exploitait des visuels trompeurs tels que de faux CAPTCHA et de fausses erreurs système (BSOD) pour inciter les victimes à exécuter manuellement une commande PowerShell. Le scénario d'attaque reposait sur de fausses notifications d'annulation de réservation hôtelière simulant un débit élevé, redirigeant les victimes vers un clone de site de réservation en ligne imitant fidèlement l'original.

L'infection aboutissait à l'installation d'un outil d'accès à distance (RAT), offrant aux attaquants un contrôle total sur le système compromis. Les attaquants ancrent fréquemment leurs campagnes dans des contextes temporels stratégiques, profitant de périodes de forte activité pour maximiser l'impact de leurs opérations. L'opération aurait débuté quelques mois avant les fêtes de fin d'année 2025, période particulièrement propice à ce type de fraude ciblant les acteurs du tourisme.

2.4.2
DE LA CYBERCRIMINALITÉ À LA GUERRE INFORMATIONNELLE : UN OUTIL COMMUN

Cette technique connaît aujourd'hui une diffusion particulièrement large, attestant de son efficacité et de sa polyvalence. Elle est mobilisée aussi bien par des acteurs cybercriminels cherchant à maximiser leurs gains financiers que par des groupes à parrainage étatique poursuivant des finalités stratégiques, qu'il s'agisse d'espionnage, de collecte d'informations sensibles ou de perturbation d'infrastructures ciblées.

- Le groupe nord-coréen Lazarus a utilisé cette technique dans sa campagne «ClickFake Interview» pour dérober des cryptomonnaies, ciblant des professionnels de la FinTech avec de fausses offres d'emploi. L'attaque visait à déployer la backdoor GolangGhost[81].

- Le groupe de ransomware Interlock a intégré ClickFix à son arsenal pour distribuer des infostealers comme LummaStealer et BerserkStealer en amont du déploiement de son ransomware, en utilisant des leurres de fausses mises à jour de navigateurs ou d'applications[82].

- Divers acteurs cybercriminels exploitent ClickFix pour distribuer un large éventail de malware, notamment les infostealers Lumma Stealer et Lampion, les RATs AsyncRAT et NetSupport RAT, ainsi que les loaders MintsLoader et Latrodectus. Le succès de la méthode a même conduit à la commercialisation de kits «ClickFix» sur des forums clandestins depuis la fin de l'année 2024[83].

- Des groupes à parrainage étatique tels que TA427 (Kimsuky) et TA450 (MuddyWater) sont également suspectés d'utiliser cette technique à des fins d'espionnage[84].

En matière de détection et d'analyse forensique, les attaques reposant sur ClickFix laissent malgré tout des traces techniques qui peuvent être exploitées. Lorsqu'un utilisateur lance une commande via la fenêtre « Exécuter » (Win+R), celle ci est enregistrée dans une zone spécifique du système, la clé de registre RunMRU, ce qui permet de retracer a posteriori les commandes saisies et de mettre en évidence un comportement suspect. Certains attaquants cherchent toutefois à limiter cette visibilité en passant par le menu d'accès rapide (Win+X) pour exécuter leur code, afin de ne pas apparaître dans cet historique.

Cette tentative d'évasion n'est cependant pas totalement efficace : une analyse attentive des journaux d'événements de Windows, ou l'usage de solutions de sécurité avancées de type EDR, permettent encore d'identifier la création de processus inhabituels ou suspects. Pris ensemble, ces éléments montrent que, malgré la sophistication de l'ingénierie sociale mobilisée par ClickFix, l'attaque continue de produire des artefacts exploitables, qui doivent être systématiquement intégrés aux pratiques d'investigation et de détection.

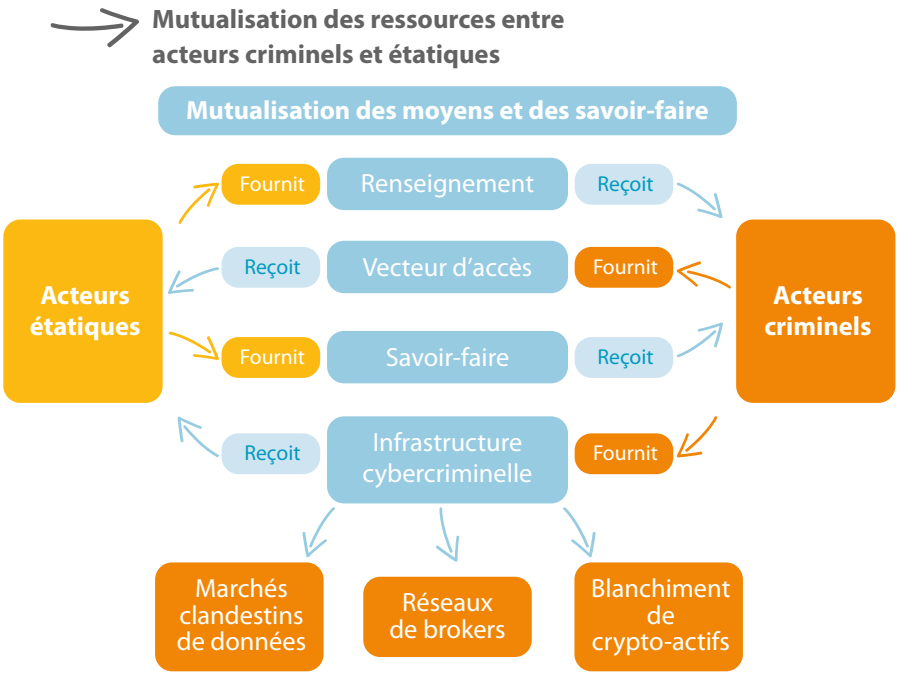
2.5
Le champ de bataille géopolitique

En 2025, la conflictualité numérique s'affirme comme un prolongement direct des rivalités géopolitiques, où la distinction entre acteurs étatiques, structures criminelles et groupes idéologiques tend à s'estomper[85]. À cette dynamique s'ajoutent les opérations continues de groupes APT sponsorisés par des États ciblant de manière sophistiquée des gouvernements, infrastructures critiques, entreprises privées et organisations de la société civile pour servir des objectifs de politique étrangère.

2.5.1
LE CYBERESPACE : INSTRUMENT DE COERCITION GÉOPOLITIQUE

Les campagnes orchestrées par ces groupes répondent directement à des objectifs géopolitiques, qu'elles prennent la forme d'opérations d'espionnage diplomatique, de sabotage énergétique en Europe, ou de financements clandestins via le vol massif de cryptomonnaies[86][87][88].

L'ENISA, dans son rapport Threat Landscape 2025, relève enfin une tendance structurelle à la mutualisation des ressources entre acteurs criminels et étatiques. Les premiers bénéficient de savoir-faire et de vecteurs d'accès issus de la sphère du renseignement, tandis que les seconds exploitent des infrastructures traditionnellement associées au cybercrime, telles que les réseaux de brokers, les services de blanchiment de crypto-actifs ou les marchés clandestins de données.



Les exemples récents en Europe de l'Est, au Proche Orient ou en Asie montrent que les opérations cyber dépassent désormais la simple disruption technique pour s'inscrire dans une logique de rapport de force politique, faisant du cyberespace un véritable instrument d'influence, de coercition et de légitimation. Au Proche Orient, la médiatisation en 2025 des opérations opposant des acteurs liés à l'Iran et à Israël, visant notamment des infrastructures financières et énergétiques, illustre cette utilisation du levier cyber pour peser sur la dynamique du conflit tout en maintenant un certain degré de déni stratégique[89].

Cette tendance est notamment incarnée par la cyberattaque revendiquée par le collectif pro israélien Predatory Sparrow contre la banque d'État iranienne Bank Sepah, qui a provoqué d'importantes interruptions de services pour les clients et perturbé le fonctionnement de cette infrastructure financière critique[90]. Dans ce contexte, les États s'appuient de plus en plus sur des proxies, qu'il s'agisse de groupes privés ou de structures cybercriminelles, afin de poursuivre leurs objectifs géopolitiques tout en brouillant l'attribution directe de leurs actions[91].

En Ukraine, les attaques soutenues contre le réseau énergétique, combinant frappes cinétiques et intrusions dans les systèmes industriels, illustrent cette volonté de faire pression sur les autorités et les populations pour peser sur les choix stratégiques de Kiev[92]. Les services de renseignement militaires russes (GRU) ont été régulièrement observés ciblant les infrastructures et acteurs assurant le soutien logistique occidental à l'effort de guerre ukrainien, tandis que les opérations de désinformation tournées vers l'Europe se sont complexifiées et structurées, à mesure que le conflit approchait de sa quatrième année[93][94].

2.5.2
HACKTIVISME ET GUERRES INFORMATIONNELLES

L'hacktivisme s'impose en 2025 comme un vecteur central de la conflictualité numérique, porté par des collectifs aux allégeances mouvantes qui articulent revendications idéologiques, logiques de mobilisation en ligne et soutien plus ou moins explicite à des agendas étatiques. Les opérations menées dans le

sillage du conflit entre l'Iran et Israël illustrent cette hybridation, ces dernières combinant campagnes de Déni de Service Distribué (DDoS), tentatives d'intrusion au sein d'infrastructures critiques et diffusion de narratifs politiques polarisants à grande échelle[95].

Des groupes comme NoName057(16) et DarkStorm participent ainsi à l'érosion des frontières entre activisme politique, prestation de services cyber au travers des opérations de DDoS et relais indirects et donc d'intérêts étatiques, DarkStorm se distinguant à ce titre par la centralité de ses narratifs pro palestiniens et anti OTAN[96].

FOCUS MENACE

Le groupe hacktiviste pro-russe NoName057(16) et son ciblage de l'Europe

Cette année, NoName057(16) a multiplié les attaques contre des infrastructures ukrainiennes et européennes, contribuant à brouiller la frontière entre action militante et instrumentalisations étatiques[97]. Selon l'analyse de Picus Security, 41,09 % des incidents documentés et menés par le groupe visaient des administrations publiques au sein de l'Union européenne. L'étude souligne une corrélation notable entre le rythme de ses opérations et les principales échéances politiques européennes.

Ce brouillage se renforce à mesure que ces acteurs mettent en œuvre des TTPs de plus en plus élaborées, incluant l'emploi de botnets comme DDoSia et le ciblage ciblé d'infrastructures liées à l'OTAN. D'après les observations réalisées par le CERT-XMCO, ces agissements laissent supposer des formes de soutien logistique ou de coordination indirecte avec des structures étatiques[98].

En France, NoName057(16) a mené en 2025 plusieurs vagues d'attaques contre des entités du secteur public, énergétique et des transports, justifiant ses actions par le soutien diplomatique et militaire apporté par Paris à l'Ukraine, dans la continuité des observations menées en 2024 par XMCO[99]. Ces opérations s'inscrivent dans une logique de rétorsion politique et de communication d'influence visant à fragiliser symboliquement les États membres les plus engagés en faveur de Kyiv.

Malgré l'opération Eastwood conduite par Europol, qui a entraîné le démantèlement de nombreux serveurs associés au groupe, son activité s'est rapidement reconstituée[100]. Elle se prolonge en outre aujourd'hui par des actions ciblant des événements à forte visibilité, à l'image des attaques DDoS récemment revendiquées contre des sites institutionnels et hôteliers liés aux Jeux olympiques d'hiver de Milan-Cortina 2026, explicitement justifiées par la posture pro-ukrainienne des autorités italiennes[101].

Les campagnes menées par des groupes hacktivistes, fréquemment relayées au sein de messageries chiffrées ainsi que sur les principaux réseaux sociaux, s'inscrivent dans une logique de confrontation informationnelle qui mobilise des ressorts psychologiques et narratifs sophistiqués[102]. Elles visent simultanément à dégrader les capacités de réaction de l'adversaire, en perturbant ses systèmes d'information et ses chaînes décisionnelles, et à orienter la perception publique du conflit par la diffusion de contenus émotionnels, polarisants ou présentés comme « exclusifs ».

Ce registre d'action s'inscrit dans un continuum entre opérations cyber, guerre de l'information et stratégies d'influence, en contribuant à l'entretien d'un brouillard informationnel qui complique l'attribution des attaques et rend plus difficile la distinction entre acteurs étatiques, paraétatiques et privés[103]. Ce faisant, il offre à certains États une marge de manœuvre pour instrumentaliser ces groupes, en testant des capacités, en élargissant le spectre des réponses possibles et en créant les conditions d'une légitimation d'actions clandestines menées en leur nom.

Face à cette hybridation croissante entre cybercrime, hacktivisme et opérations étatiques, les efforts de régulation du cyberespace, des normes de l'Union européenne en matière de cyber-résilience aux discussions de l'ONU concernant d'éventuelles normes non coercitives quant à l'utilisation des cyber-arsenaux, peinent à s'imposer dans un domaine par essence transfrontalier et anonyme[104].

2.6
Souveraineté : le sursaut européen

L'année 2025 marque la poursuite d'une inflexion nette dans la construction de la souveraineté cyber européenne, portée par une continuité de l'enrichissement de l'arsenal normatif qui vise à harmoniser les règles entre États membres, à renforcer la résilience des infrastructures critiques face à l'accroissement du volume d'attaques ainsi qu'à affirmer une autonomie stratégique face aux recompositions géopolitiques et à la dépendance aux technologies étrangères. Pour ce faire, l'Union européenne articule un ensemble de textes structurants (DSA, DMA, GDPR, NIS2, DORA, Cyber Resilience Act et AI Act) visant à encadrer les contenus, la concurrence, la protection des données et la résilience des infrastructures critiques[105].

2.6.1
EUROPE : LÉGISLATION ET DÉPENDANCE NUMÉRIQUE

Ce mouvement d'ensemble vise autant à structurer la législation européenne en produisant un cadre normatif qu'à réduire la dépendance technologique et réglementaire de l'Union vis-à-vis des puissances étrangères. Si ces chantiers avaient été engagés depuis plus d'une dizaine d'années, la réélection de Donald Trump et le durcissement de la doctrine américaine ont agi comme un électrochoc, donnant un coup d'accélérateur politique à l'agenda de souveraineté numérique européen et renforçant la légitimation des mesures adoptées en 2025.

Cette montée en puissance normative se déploie en effet dans un environnement géopolitique profondément reconfiguré par la remise en cause de l'alliance transatlantique depuis le début du second mandat du président des États-Unis, qui constituait jusqu'alors l'ossature de l'ordre occidental. Sur le plan numérique, les chiffres de 2025 rappellent l'ampleur de la dépendance : plus de 80% des dépenses européennes en logiciels et services cloud professionnels continuent de bénéficier à des acteurs américains, représentant une facture numérique de plusieurs centaines de milliards d'euros par an[106].

Cette situation alimente le diagnostic d'une « colonie numérique », où la croissance et l'emploi induits par les investissements numériques européens se matérialisent principalement hors du continent.

FOCUS INFORMATIONNEL
Création de la Base de données des vulnérabilités de l'Union Européenne (EUVD)

Le lancement en mai 2025 de l'EUVD par l'ENISA s'inscrit dans cette même logique d'affirmation d'une capacité propre européenne, en réponse à la crise de confiance provoquée par l'évolution de la gouvernance américaine des vulnérabilités[107].

Cette initiative intervient dans un contexte marqué par l'expiration du contrat de financement du MITRE par le gouvernement américain, que ce dernier n'a renouvelé qu'au dernier moment.

L'éventualité d'un arrêt du financement américain du programme CVE a souligné les failles structurelles de l'Europe en matière de gestion des vulnérabilités, encourageant le développement d'une base de données souveraine[108]. L'EUVD repose néanmoins principalement sur la base de données du programme CVE et ne remplit pas à ce stade son rôle dans l'enregistrement et l'enrichissement de nouvelles CVE.

À défaut de constituer une alternative au programme CVE, l'EUVD, via l'intégration future des vulnérabilités remontées dans le cadre des obligations imposées par le Cyber Resilience Act et du NIS2, devraient progressivement incarner une source de données européenne de référence[109].

Les initiatives franco-allemandes annoncées à Berlin en novembre 2025 illustrent la volonté des principaux États membres de traduire ce leadership normatif en capacités concrètes, via la mise en place d'un groupe de travail conjoint, la promotion d'une identité numérique européenne et l'appel à un moratoire sur certaines règles applicables aux IA à haut risque[110].

Les montants d'investissement affichés, de l'ordre de 12 milliards d'euros, demeurent toutefois très inférieurs aux besoins estimés, évalués à plusieurs centaines de milliards pour espérer bâtir un écosystème technologique et industriel capable de rivaliser avec les géants américains et chinois. Le décalage entre ambition politique et moyens financiers disponibles devient ainsi l'un des nœuds centraux de la souveraineté numérique européenne à l'horizon 2025–2026.

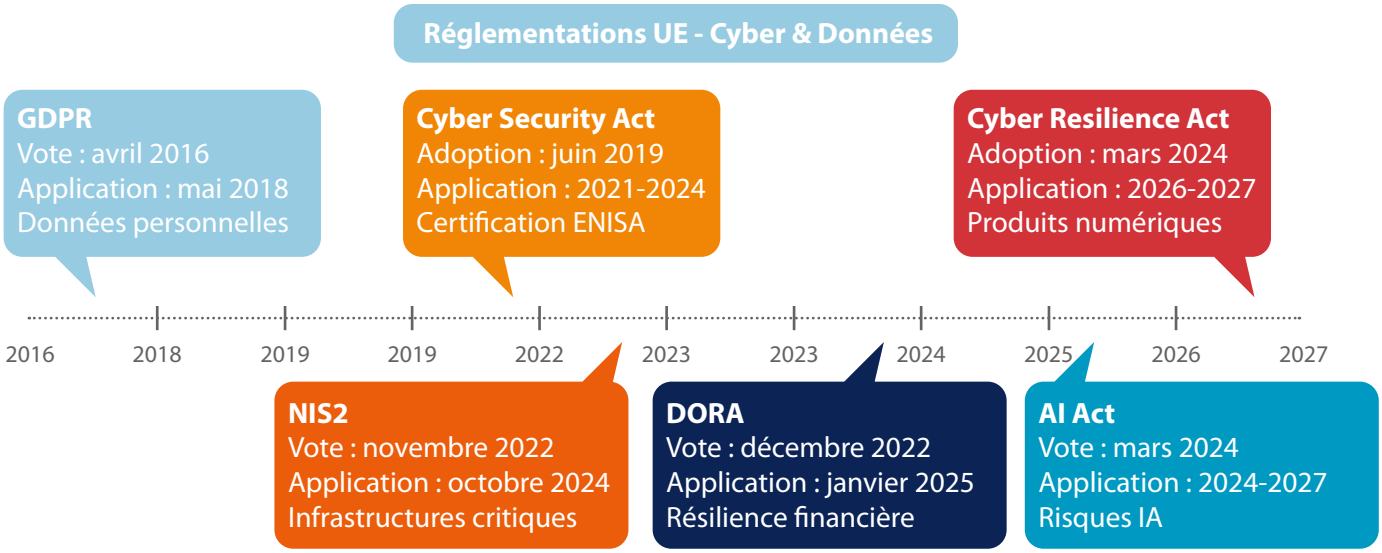
Au-delà des initiatives capacitaires (EUVD, coopérations bilatérales), c'est surtout par le droit que l'Union cherche à transformer cette prise de conscience en obligations concrètes et homogènes. Cette logique de standardisation fait de la réglementation le principal vecteur d'alignement des États membres. La directive NIS2 s'impose alors comme l'ossature de l'harmonisation européenne en matière de cybersécurité.

Le coeur de cette directive réside dans la responsabilisation explicite des organes de direction ainsi que dans la mise en place de mécanismes structurés de coordination, qui reflètent la volonté d'élever la cybersécurité au rang d'enjeu stratégique partagé plutôt que de simple question technique. Cette ambition se heurte toutefois à des inerties nationales, comme en témoigne la lenteur de la transposition en droit français de la directive NIS2[111].

C'est en 2027 que les effets du triptyque DORA, AI Act et Cyber Resilience Act se feront pleinement sentir, marquant une étape décisive dans la consolidation d'une résilience numérique européenne fondée sur une approche à la fois sectorielle et systémique[112] [113].

DORA harmonise la gestion des risques cyber dans le secteur financier pour renforcer la résistance du système face aux chocs numériques, tandis que l'AI Act consacre l'Union comme puissance normative en matière d'intelligence artificielle, conciliant innovation, droits fondamentaux et souveraineté technologique face aux standards extra-européens[114] [115].

Les différents textes réglementaires européens.



Le Cyber Resilience Act parachève cette dynamique en inscrivant, pour l'ensemble des produits numériques, une exigence de cybersécurité dès la conception, consolidant ainsi la souveraineté industrielle et la sécurité du marché intérieur[116].

2.6.2
L'EUROPE FACE AUX DÉFIS DE SA SOUVERAINETÉ CYBER

La conclusion qui se dessine en 2025 est celle d'une Europe à la croisée des chemins : soit elle parvient à convertir son avance réglementaire en une véritable puissance technologique, soit elle restera exposée aux décisions unilatérales de puissances tierces dans un contexte géopolitique instable. Les défis sont multiples : simplifier un millefeuille réglementaire qui risque d'encourager une conformité de façade, mobiliser des investissements massifs et coordonner les politiques industrielles pour éviter la dispersion des efforts.

Pourtant, les signaux récents indiquent que l'Union prend la mesure du défi, comme le montrent le renforcement continu de son cadre législatif et les décisions fortes annoncées pour préparer l'Europe à faire face aux cybermenaces. Ce basculement est d'autant plus net que les prises de position erratiques de Donald Trump - la suspension évoquée des actions contre la Russie en mars dernier, la mise en place d'un plan d'action contre la Chine faisant la part-belle à l'offensif au détriment de la mise en place d'infrastructures défensives solides et les réductions de capacité imposées à la CISA - alimentent l'idée que les États-Unis ne souhaitent plus du rôle de garant de la sécurité cyber occidentale, qu'ils s'étaient pourtant octroyés[117][118][119].

À ce titre, plusieurs tendances se dessinent au sein de l'Union. D'une part, cet objectif assumé de souveraineté numérique se traduit désormais en trajectoires d'investissement concrètes, bénéficiant d'une forte montée en puissance annoncée des dépenses dans les infrastructures de cloud souverain, appelées à plus que tripler entre 2025 et 2027 sous l'effet conjugué des tensions géopolitiques et des exigences réglementaires européennes[120].

Les gouvernements, les secteurs régulés et les opérateurs d'infrastructures critiques devraient en demeurer les moteurs principaux, faisant de la géopatriation des données et du recours à des fournisseurs européens ou de confiance un impératif stratégique plutôt qu'un simple argument de conformité.

La souveraineté cyber européenne tend ainsi à s'inscrire dans une approche plus extérieure : la nouvelle stratégie numérique internationale de l'UE insiste sur une autonomie qui ne doit pas être confondue avec l'autarcie, mais reposer sur la diversification des partenariats, la participation active aux forums de gouvernance numérique et la capacité à promouvoir ses standards au-delà de ses frontières[121].

Pour l'Europe, les prochaines années devraient donc être marquées moins par l'adoption de nouveaux textes que par l'industrialisation des ambitions de ceux existants déjà via la montée en charge progressive de NIS2, DORA, AI Act et Cyber Resilience Act, du déploiement d'infrastructures souveraines et du renforcement des capacités opérationnelles. Autant de conditions nécessaires pour transformer une avancée réglementaire en véritable puissance technologique devenant un levier d'influence.

Dans ce climat où l'allié historique revendique de manière croissante une logique de rapport de force, l'autonomie numérique et la capacité de l'Europe à se protéger seule ne relèvent plus du confort stratégique, mais bien d'une condition de survie politique. La souveraineté cyber n'apparaît plus comme une option stratégique parmi d'autres, mais comme une nécessité existentielle conditionnant la capacité du continent à maîtriser son destin.

yuno By xmco

GLOSSAIRE

Backdoor
Un accès caché à un système informatique permettant d'y entrer sans passer par les sécurités normales.

Bulletproof
Désigne un hébergeur qui accepte volontairement des activités illégales et ignore les plaintes ou demandes de retrait.

Business Email Compromise (BEC)
Une attaque par phishing ciblant les entreprises, où des cybercriminels usurpent l'identité d'un dirigeant ou partenaire pour tromper les employés et les inciter à transférer de l'argent ou des informations sensibles.

ClickFix
Une technique qui incite un utilisateur à exécuter lui-même une commande malveillante sous prétexte de "corriger" un faux problème technique affiché à l'écran.

Commande et de contrôle (C2)
Un serveur ou système utilisé par un attaquant pour contrôler à distance des machines compromises et leur donner des instructions.

CVE (Common Vulnerabilities and Exposures)
Un identifiant unique donné à une faille de sécurité. Il est attribué par MITRE et enrichit par la CISA-ADP qui fournit scores CVSS et détails techniques lorsqu'ils ne sont pas fournis par l'éditeur lui-même.

CWE (Common Weakness Enumeration)
Une liste de vulnérabilités courantes dans les logiciels, permettant de les identifier, les classer et les prévenir.

Deepfake
Une technologie qui permet de créer des vidéos, images ou audios truqués, imitant de manière réaliste des personnes en modifiant leurs expressions, voix ou actions.

Déni de Service Distribué (DDoS)
Une attaque informatique qui vise à rendre un site ou un service inaccessible par l'envoi d'un nombre très important de requêtes simultanées.

Ingénierie sociale
Désigne l'ensemble des techniques de manipulation psychologique utilisées pour amener une personne à divulguer des informations sensibles ou à réaliser une action qui compromet sa sécurité ou celle de son organisation.

GenAI
Désigne une IA qui crée du contenu toute seule (texte, images, code, sons) à partir d'une consigne.

Groupe APT
Un groupe d'attaquants sophistiqués, souvent lié à un État, qui mène des campagnes prolongées et ciblées pour voler des informations, espionner ou saboter des organisations.

Honeypot
Un faux système informatique conçu pour attirer les pirates afin d'observer leurs attaques et améliorer la sécurité.

Infostealer
Un malware conçu pour voler des informations de manière discrète.

Kill chain
Désigne le processus en plusieurs étapes qu'un attaquant suit pour réussir une cyberattaque.

Know Your Customer (KYC)
Un processus où les entreprises vérifient l'identité de leurs clients afin de prévenir la fraude, le blanchiment d'argent et le financement du terrorisme.

Living off the Cloud
Une technique où un attaquant abuse des services et fonctionnalités natives du cloud pour mener une attaque sans déployer de malware.

Living off the Land
Une technique où un attaquant utilise des outils déjà présents sur le système pour mener une attaque sans installer de malware.

LLM (Large Language Model)
Une IA entraînée sur énormément de textes pour comprendre et produire du langage humain.

MSP (Managed Service Provider)
Un prestataire qui gère et maintient l'infrastructure informatique d'une organisation à distance, via un contrat de services.

MFA bombing
Une technique d'attaque qui consiste à bombarder une victime de demandes d'authentification multi-facteurs (MFA) jusqu'à ce qu'elle finisse par en accepter une par erreur ou par fatigue.

Outils RMM (Remote Monitoring and Management)
Ils permettent de surveiller, administrer et maintenir à distance des systèmes informatiques (postes, serveurs, réseaux).

Password spraying
Technique consistant à tester des mots de passe courants sur de nombreux comptes pour éviter les protections contre les tentatives répétées.

PowerShell
Un outil en ligne de commande et un langage de script de Microsoft qui permet d'administrer et d'automatiser des tâches sur Windows et d'autres systèmes.

Preuve de concept (PoC)
Une démonstration montrant qu'une faille, un logiciel ou une idée peut fonctionner dans la pratique.

RunMRU
Une entrée du registre Windows enregistrant l'historique des commandes exécutées via la fenêtre « Exécuter ».

Service de distribution, ou CDN (Content Delivery Network)
Un réseau de serveurs qui stocke et livre des contenus depuis le serveur le plus proche de l'utilisateur pour que leur accès soit plus rapide et fiable.

Scraping
Désigne l'extraction automatisée de données à partir de sites web, au moyen de scripts ou de bots qui collectent et structurent l'information pour un usage ultérieur.

Secrets CI/CD
Des informations sensibles stockées de manière sécurisée et utilisées automatiquement par les pipelines d'intégration et de déploiement continus (GitHub Actions), sans jamais être exposées dans le code ou les journaux.

Serverless
Des programmes dans le cloud qui s'exécutent automatiquement sans avoir à gérer de serveur.

Systèmes IAM (Identity and Access Management)
Servent à gérer les identités et les accès dans une organisation : création de comptes, contrôle des droits, authentification et suivi des accès.

Sim-Swapping
Une arnaque où un pirate fait transférer ton numéro de téléphone sur sa propre carte SIM.

Software-as-a-Service (SaaS)
Un modèle de fourniture de logiciels dans lequel l'application est hébergée par un prestataire cloud et accessible à distance via Internet.

RaaS
Un modèle criminel où des cybercriminels louent un ransomware clé en main à d'autres attaquants, en échange d'une part des rançons.

TTPs
Désignent les tactiques, techniques et procédures utilisées par les attaquants pour mener des cyberattaques.

URL HTTPS
Une adresse web qui utilise le protocole sécurisé HTTPS, ce qui permet de transmettre des données de façon chiffrée entre le navigateur et le site.

Win+R
Un raccourci clavier sous Windows qui ouvre la fenêtre Exécuter, permettant de lancer rapidement des programmes, fichiers ou commandes.

Zero Trust
Un modèle de sécurité consistant à réduire la confiance implicite accordée par défaut, même à l'intérieur du réseau.

0-day
Une vulnérabilité « n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif au moment de son exploitation ».

yuno By xmco

BIBLIOGRAPHIE

[1] First, «Vulnerability Forecast 2026,» 2 Janvier 2026. [En ligne].
Available: https://www.first.org/blog/20260211-vulnerability-forecast-2026

[2] Google Cloud, «Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign using the OVERSTEP Backdoor,» Juillet 2025. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor?hl=en

[3] Microsoft, «Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability,» Octobre 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/

[4] TrendAI Zero Day Initiative, «Confirmed!! Dinh Ho Anh Khoa (@_l0gg) of Viettel Cyber Security,» Mai 2025. [En ligne].
Available: https://x.com/thezdi/status/1923317597673533552

[5] Microsoft, «Disrupting active exploitation of on-premises SharePoint vulnerabilities,» Juillet 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[6] CheckPoint, «Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations,» Juillet 2025. [En ligne].
Available: https://research.checkpoint.com/2025/before-toolshell-exploring-storm-2603s-previous-ransomware-operations/

[7] E. Research, «SharePoint Under Siege: ToolShell Exploit (CVE-2025-49706 & CVE-2025-49704),» Juillet 2025. [En ligne].
Available: https://research.eye.security/sharepoint-under-siege/

[8] Palo Alto, «Project AK47: Uncovering a Link to the SharePoint Vulnerability Attacks,» Aout 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/ak47-activity-linked-to-sharepoint-vulnerabilities/

[9] Check Point, «Inside Ink Dragon: Revealing the Relay Network and Inner Workings of a Stealthy Offensive Operation,» Décembre 2025. [En ligne].
Available: https://research.checkpoint.com/2025/ink-dragons-relay-network-and-offensive-operation/

[10] StepSecurity, «Harden-Runner detection: tj-actions/changed-files action is compromised,» Mars 2025. [En ligne].
Available: https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised

[11] C. & I. S. Agency, «Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-30066) and reviewdog/action-setup@v1 (CVE-2025-30154),» Mars 2025. [En ligne].
Available: https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-tj-actionschanged-files-cve-2025-30066-and-reviewdogaction

[12] G. Cloud, «Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign,» Octobre 2025. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation?hl=en

[13] Sekoia, «ViciousTrap – Infiltrate, Control, Lure: Turning edge devices into honeypots en masse.,» Mai 2025. [En ligne].
Available: https://blog.sekoia.io/viciousTrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/

[14] Sekoia, «PolarEdge: Unveiling an uncovered ORB network,» Février 2025. [En ligne].
hAvailable: ttps://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/

[15] Huntress, «Huntress Threat Advisory: Active Exploitation of SonicWall VPNs,» Aout 2025. [En ligne].
Available: https://www.huntress.com/blog/exploitation-of-sonicwall-vpn

[16] S. T. Institute, «Oracle Identity Manager Exploit Observation from September (CVE-2025-61757),» Novembre 2025. [En ligne].
Available: https://isc.sans.edu/diary/Oracle+Identity+Manager+Exploit+Observation+from+September+CVE202561757/32506/

[17] ESET, «Operation RoundPress,» Mai 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/operation-roundpress/

[18] Cisco, «Cisco Event Response: Continued Attacks Against Cisco Firewalls,» Septembre 2025. [En ligne].
Available: https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

[19] Wiz, «Wiz Research Identifies Exploitation in the Wild of Aviatrix Controller RCE (CVE-2024-50603),» Janvier 2025. [En ligne].
Available: https://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603

[20] G. Cloud, «Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation,» Janvier 2025. [En ligne].
Available: https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en

[21] Microsoft, «Silk Typhoon targeting IT supply chain,» Mars 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

[22] Symantec, «Ransomware Attackers Leveraged Privilege Escalation Zero-day,» Mai 2025. [En ligne].
Available: https://www.security.com/threat-intelligence/play-ransomware-zero-day

[23] C. Lab, «Graphite Caught - First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted,» Juin 2025. [En ligne].
Available: https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

[24] Group-IB, «Ransomware debris: an analysis of the RansomHub operation,» Avril 2025. [En ligne].
Available: https://www.group-ib.com/blog/ransomware-debris/

[25] Yarix, «In depth analysis of the alleged Qilin, DragonForce and LockBit alliance,» Décembre 2025. [En ligne].
Available: https://labs.yarix.com/2025/12/in-depth-analysis-of-the-alleged-qilin-dragonforce-and-lockbit-alliance/

[26] R. Hauts-de-France, «Incident de cybersécurité dans plusieurs lycées de la région Hauts-de-France,» Octobre 2025. [En ligne].
Available: https://www.hautsdefrance.fr/incident-de-cybersecurite-dans-plusieurs-lycees-de-la-region-hauts-de-france/

[27] O. o. P. A. -. U. D. o. Justice, «Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets,» Aout 2025. [En ligne].
Available: https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets

[28] O. o. P. A. -. U. D. o. Justice, «Justice Department Announces Coordinated Disruption Actions Against BlackSuit (Royal) Ransomware Operations,» Aout 2025. [En ligne].
Available: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

[29] U. S. A. Office, «United States files a civil complaint in the Northern District of Texas seeking the forfeiture of over $1.7 million worth of cryptocurrency seized by Dallas FBI,» Aout 2025. [En ligne].
Available: https://www.justice.gov/usao-ndtx/pr/united-states-files-civil-complaint-northern-district-texas-seeking-forfeiture-over-17

[30] CISA, «#StopRansomware: Medusa Ransomware,» Mars 2025. [En ligne].
Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

[31] Sophos, «Velociraptor incident response tool abused for remote access,» Aout 2025. [En ligne].
Available: https://www.sophos.com/en-us/blog/velociraptor-incident-response-tool-abused-for-remote-access

[32] LevelBlue, «Scattered LAPSUS$ Hunters: Anatomy of a Federated Cybercriminal Brand,» Novembre 2025,» Novembre 2025. [En ligne].
Available: https://www.levelblue.com/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand

[33] ReSecurity, «Trinity of Chaos: The LAPSUS$, ShinyHunters, and Scattered Spider Alliance Embarks on Global Cybercrime Spree,» Septembre 2025. [En ligne].
Available: https://www.resecurity.com/blog/article/trinity-of-chaos-the-lapsus-shinyhunters-and-scattered-spider-alliance-embarks-on-global-cybercrime-spree

[34] Reliaquest, «Is Zendesk Scattered Lapsus$ Hunters' Latest Campaign Target?,» Novembre 2025. [En ligne].
Available: https://reliaquest.com/blog/zendesk-scattered-lapsus-hunters-latest-target/
[35] SaleForce, «Security Advisory: Unusual Activity Related to Gainsight Applications,» Décembre 2025. [En ligne].
Available: https://status.salesforce.com/generalmessages/20000233
[36] «Statement on Cyber Incident,» Septembre 2025. [En ligne].
Available: https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident
[37] Bleeping Computer, «CrowdStrike catches insider feeding information to hackers,» Novembre 2025. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/crowdstrike-catches-insider-feeding-information-to-hackers/#shinyhunters
[38] B. Computer, «Europol confirms $50,000 Qilin ransomware reward is fake,» Aout 2025. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/europol-confirms-that-qilin-ransomware-reward-is-fake/
[39] X - Twitter , «Ransom-DB - Silent ransomware,» Novembre 2025. [En ligne].
Available: https://x.com/Ransom_DB/status/1991000214241476999
[40] Ransomware.Live, «Medusa - Uncovered by RansomedVC,» Juillet 2025.
Available: Available: https://www.ransomware.live/id/TWVkdXNhQHJlYm9ybnZj
[41] ESET, «Update WinRAR tools now: RomCom and others exploiting zero-day vulnerability,» Aout 2025. [En ligne].
Available: https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/
[42] Prodaft, «Inside the Latest Espionage Campaign of Nebulous Mantis,» Avril 2025. [En ligne].
Available: https://catalyst.prodaft.com/public/report/inside-the-latest-espionage-campaign-of-nebulous-mantis/overview#heading-1000|0
[43] A. Wolf, «Russian RomCom Utilizing SocGholish to Deliver Mythic Agent to U.S. Companies Supporting Ukraine,» Novembre 2025. [En ligne].
Available: https://arcticwolf.com/resources/blog/romcom-utilizing-socgholish-to-deliver-mythic-agent-to-usa-companies-supporting-ukraine/
[44] Sophos, «GOLD SALEM tradecraft for deploying Warlock ransomware,» Décembre 2025. [En ligne].
Available: https://www.sophos.com/en-us/blog/gold-salem-tradecraft-for-deploying-warlock-ransomware
[45] Microsoft, «Microsoft has observed Moonstone Sleet, a North Korean state actor, deploying Qilin ransomware,» Mars 2025. [En ligne].
Available: https://x.com/MsftSecIntel/status/1897738961348374621
[46] Morphisec, «Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West,» Juillet 2025. [En ligne].
Available: https://www.morphisec.com/blog/pay2key-resurgence-iranian-cyber-warfare/
[47] G. o. Canada, «Iran-linked hacker group doxes journalists and amplifies leaked information through AI chatbots,» Septembre 2025. [En ligne].
Available: https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/iran-hack-piratage-iranien.aspx?lang=eng
[48] ANSSI, «L'IA GÉNÉRATIVE FACE AUX ATTAQUES INFORMATIQUES SYNTHÈSE DE LA MENACE EN 2025,» Février 2025. [En ligne].
Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-001.pdf
[49] N. D. G. W. Arth Bhardwaj, «Beyond BeautifulSoup: Benchmarking LLM-Powered Web Scraping for Everyday Users,» Janvier 2025. [En ligne].
Available: https://arxiv.org/abs/2601.06301
[50] Apify, «LLM web scraping: Using plain English to get web data,» Juin 2025. [En ligne].
Available: https://blog.apify.com/llm-web-scraping/
[51] KnowBe4, «Phishing Threat Trends Report,» Mars 2025. [En ligne].
Available: https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf
[52] T. Micro, «AI-Powered Deepfake Tools Becoming More Accessible Than Ever,» Juillet 2024. [En ligne].
Available: https://www.trendmicro.com/en_us/research/24/g/ai-deepfake-cybercrime.html
[53] CNN, « Finance worker pays out $25 million after video call with deepfake 'chief financial officer',» Février 2024. [En ligne].
Available: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
[54] Keepnet, «Deepfake Statistics & Trends 2025: Growth, Risks, and Future Insights,» Novembre 2025. [En ligne].
Available: https://keepnetlabs.com/blog/deepfake-statistics-and-trends
[55] N. A. Suleiman, « Deepfake-as-a-Service: The Next Challenge for Enterprise Cybersecurity,» Janvier 2025. [En ligne].
Available: https://ideas.repec.org/a/bhx/ojtjts/v7y2025i3p47-59id2752.html
[56] R. Future, « AI Malware: Hype vs. Reality,» Décembre 2025. [En ligne].
Available: https://www.recordedfuture.com/blog/ai-malware-hype-vs-reality
[57] coolja86, «Chat GPT «DAN»,» 2025. [En ligne].
Available: https://gist.github.com/coolaj86/6f4f7b30129b0251f61fa7baaa881516
[58] G. Technology, «'Living Off the Cloud': Hackers Modernize an Old-School Tactic,» Juillet 2022. [En ligne].
Available: https://www.govtech.com/security/living-off-the-cloud-hackers-modernize-an-old-school-tactic
[59] P. A. (. 42), «Behind the Clouds: Attackers Targeting Governments in Southeast Asia Implement Novel Covert C2 Communication,» Juillet 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/windows-backdoor-for-novel-c2-communication/
[60] P. A. (. 42), «Cloud Threats on the Rise: Alert Trends Show Intensified Attacker Focus on IAM, Exfiltration,» Mars 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/2025-cloud-security-alert-trends/
[61] ProofPoint, «Attackers Unleash TeamFiltration: Account Takeover Campaign (UNK_SneakyStrike) Leverages Popular Pentesting Tool,» Juin 2025. [En ligne].
Available: https://www.proofpoint.com/us/blog/threat-insight/attackers-unleash-teamfiltration-account-takeover-campaign
[62] R. Offseq, «Behind the Clouds: Attackers Targeting Governments in Southeast Asia Implement Novel Covert C2 Communication,» Juillet 2025. [En ligne].
Available: https://radar.offseq.com/threat/behind-the-clouds-attackers-targeting-governments--e7eb126e
[63] P. A. (. 42), «JavaGhost's Persistent Phishing Attacks From the Cloud,» Février 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/javaghost-cloud-phishing/
[64] G. Hackers, «Lazarus Group Exploits Trusted Apps for Data Theft via Dropbox,» Février 2025. [En ligne].
Available: https://gbhackers.com/lazarus-group-exploits-trusted-apps/
[65] CTS, « Tycoon 2FA Phishing Attack Explained & 9 Ways to Protect Your Business,» Août 2025. [En ligne].
Available: https://cts-tex.com/2025/08/13/tycoon-2fa-the-phishing-threat-explained/
[66] C. Angel, «External Threat Intelligence Report,» Février 2025. [En ligne].
Available: https://cybelangel.com/blog/resource/2025-external-threat-intelligence-report/

[67] Reliaquest, «Too Much Trust: The Danger of Over-Privileged Cloud Identities,» Novembre 2025. [En ligne].
Available: https://reliaquest.com/blog/threat-spotlight-danger-of-over-privileged-cloud-identities/
[68] FortifyData, «Understanding the Cloud Attack Surface: Key Risks and Mitigations,» Août 2025. [En ligne].
Available: https://fortifydata.com/blog/understanding-cloud-attack-surface-risks-mitigations/
[69] HPE, «Abused CDNs: From Speedy Content to Stealthy Malware,» Septembre 2023. [En ligne].
Available: https://blogs.juniper.net/en-us/threat-research/abused-cdns-from-speedy-content-to-stealthy-malware
[70] Future CISO, «The industrialisation of cybercrime in 2026,» Décembre 2025. [En ligne].
Available: https://futureciso.tech/the-industrialisation-of-cybercrime-in-2026/
[71] CheckPoint, «Threats to the Homeland: Cyber Operations Targeting US Government and Critical Infrastructure,» Décembre 2025. [En ligne].
Available: https://2034462.fs1.hubspotusercontent-na1.net/hubfs/2034462/Cyber%20Operations%20Targeting%20US%20Government%20(1).pdf
[72] SentinelOne, «Qu'est-ce que l'hébergement bulletproof ?,» Juillet 2025. [En ligne].
Available: https://www.sentinelone.com/fr/cybersecurity-101/threat-intelligence/bulletproof-hosting/
[73] L. Monde, «Les Etats-Unis sanctionnent Aeza Group, un fournisseur de services russe utilisé par les cybercriminels,» Juillet 2025. [En ligne].
Available: https://www.lemonde.fr/pixels/article/2025/07/02/les-etats-unis-sanctionnent-aeza-group-un-fournisseur-de-services-russe-utilise-par-les-cybercriminels_6617365_4408996.html
[74] G. Information Management Systems Institute of Athena Research Centre, «The Malware as a Service ecosystem,» Mai 2024. [En ligne].
Available: https://arxiv.org/html/2405.04109v1
[75] Varonis, «Cybercrime Goes SaaS: Renting Tools, Access, and Infrastructure,» Décembre 2025. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/cybercrime-goes-saas-renting-tools-access-and-infrastructure/
[76] B. Computer, «Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters,» Novembre 2025. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/
[77] N. Security, «The Dragonforce Cartel: LockBit–Qilin–DragonForce Alliance,» Novembre 2025. [En ligne].
Available: https://www.nuharborsecurity.com/blog/the-ransomware-cartel-inside-the-lockbit-qilin-dragonforce-alliance
[78] Microsoft, «Think before you clickfix analyzing the clickfix social engineering technique,» Août 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/
[79] Palo Alto, «Fix the Click: Preventing the ClickFix Attack Vector,» Juillet 2025. [En ligne].
Available: https://unit42.paloaltonetworks.com/preventing-clickfix-attack-vector/
[80] Securonix, «Analyzing PHALT#BLYX: How Fake BSODs and Trusted Build Tools Are Used to Construct a Malware Infection,» Janvier 2025. [En ligne].
Available: https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/
[81] Sekoia, «From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic,» Mars 2025. [En ligne].
Available: https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
[82] Sekoia, «Interlock ransomware evolving under the radar,» Avril 2025. [En ligne].
Available: https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/
[83] Microsoft, «Think before you Click(Fix): Analyzing the ClickFix social engineering technique,» Août 2025. [En ligne].
Available: https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/
[84] ProofPoint, «Around the World in 90 Days: State-Sponsored Actors Try ClickFix,» Avril 2025. [En ligne].
Available: https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix
[85] Brandefense, «Introduction: The Expanding Role of Nation-State Cyber Threat Actors,» Août 2025. [En ligne].
Available: https://brandefense.io/blog/how-nation-state-cyber-threats-are-evolving-in-2025-part-i/
[86] WeLiveSecurity, «Rapport d'activité APT d'ESET T2 2025 - T3 2025,» Novembre 2025. [En ligne].
Available: https://www.welivesecurity.com/fr/dernieres-recherches/rapport-dactivite-apt-deset-t2-2025-t3-2025/
[87] ENISA, «ENISA THREAT LANDSCAPE 2025,» Octobre 2025. [En ligne].
Available: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf
[88] Chainalysis, «North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion,» Décembre 2025. [En ligne].
Available: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/
[89] A. Council, «What the Israel-Iran conflict revealed about wartime cyber operations,» Juillet 2025. [En ligne].
Available: https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/
[90] Picus, «Predatory Sparrow: Inside the Cyber Warfare Targeting Iran's Critical Infrastructure,» Novembre 2025. [En ligne].
Available: https://www.picussecurity.com/resource/blog/predatory-sparrow-inside-the-cyber-warfare-targeting-irans-critical-infrastructure
[91] Oragne, «Security Navigator 2026 : Le cybercrime s'industrialise et devient un des épicentres des équilibres géopolitiques. Un front commun doit se structurer,» Décembre 2025. [En ligne].
Available: https://newsroom.orange.com/securitynavigator2026/
[92] ACAPS, «Energy infrastructure attacks: updated outlook and impact during the 2024–2025 cold season,» Février 2025. [En ligne].
Available: https://www.acaps.org/fileadmin/Data_Product/Main_media/20250219_ACAPS_Ukraine_-_Energy_infrastructure_attacks-_Updated_outlook_and_impact_during_the_2024-2025_cold_season_.pdf
[93] C. &. I. S. A. (CISA), « Russian GRU Targeting Western Logistics Entities and Technology Companies,» Mai 2025. [En ligne].
Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a
[94] Viginum, «Guerre en Ukraine Trois années d'opérations informationnelles russes,» Février 2025. [En ligne].
Available: https://www.sgdsn.gouv.fr/files/files/Publications/20250224_TLP-CLEAR_NP_SGDSN_VIGINUM_Guerre%20en%20Ukraine_Trois%20ann%C3%A9es%20d%27op%C3%A9rations%20informationnelles%20russes_1.0_VF.pdf
[95] Outpost24, «How hacktivist cyber operations surged amid Israeli-Iranian conflict,» Novembre 2025. [En ligne].
Available: https://outpost24.com/blog/hacktivist-cyber-operations-iran-israel/
[96] SafeSecurity, « Dark Storm Is Coming – Are You Safe Enough to Handle It?,» Avril 2025. [En ligne].
Available: https://safe.security/resources/blog/dark-storm-is-coming-are-you-safe-enough-to-handle-it/
[97] Cyble, «Threat Actor Profile: NoName057(16),» Novembre 2025. [En ligne].
Available: https://cyble.com/threat-actor-profiles/noname05716/

[98] P. Security, «How NoName057(16) Uses DDoSia to Attack NATO Targets,» Janvier 2026. [En ligne].
Available: https://www.picussecurity.com/resource/blog/how-noname05716-uses-ddosia-to-attack-nato-targets
[99] XMCO, «LA FRANCE : CIBLE DE L'HACKTIVISME GÉOPOLITIQUE,» Août 2024. [En ligne].
Available: https://www.xmco.fr/wp-content/uploads/2024/08/WEB_2024-08_hacktivisme.pdf
[100] Europol, «Global operation targets NoName057(16) pro-Russian cybercrime network,» Juillet 2025. [En ligne].
Available: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
[101] ANSA, «Russian-led cyberattacks on embassies and hotels in Cortina foiled says Tajani (3),» Février 2025. [En ligne].
Available: https://www.ansa.it/amp/english/newswire/english_service/2026/02/04/russian-led-cyberattacks-on-embassies-and-hotels-in-cortina-foiled-says-tajani_dcd64cdd-4cee-4e7b-8715-6c0f9ffa0dd6.html
[102] Thalès, «Discord et Telegram : la démocratisation de la cybercriminalité,» Juillet 2025. [En ligne].
Available: https://cds.thalesgroup.com/fr/hot-topics/discord-et-telegram-la-democratisation-de-la-cybercriminalite
[103] IRSEM, «RÉFLEXIONS SUR LE CYBER : QUELS ENJEUX ?,» Juillet 2015. [En ligne].
Available: https://www.irsem.fr/storage/file_manager_files/2025/03/plaf-32.pdf
[104] O. d. N. Unies, « Secretary-General Welcomes Adoption of Final Report of Open-ended Working Group on Security, Use of Information and Communications Technologies,» Juillet 2025. [En ligne].
Available: https://press.un.org/en/2025/sgsm22726.doc.htm
[105] TaylorWessing, «The new EU digital laws,» Septembre 2025. [En ligne].
Available: https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2025/09/session_eu-digital-laws_english.pdf
[106] E. Parliament, «European Software and Cyber Dependencies,» Décembre 2025. [En ligne].
Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf
[107] ENISA, «European Union Vulnerability Database,» Mai 2025. [En ligne].
Available: https://euvd.enisa.europa.eu/
[108] Synetis, « Coupes budgétaires sous Trump : quels sont les impacts pour les CVEs,» Mai 2025. [En ligne].
Available: https://www.synetis.com/coupes-budgetaires-sous-trump-quels-sont-les-impacts-pour-les-cves/
[109] ENISA, «FAQ,» [En ligne].
Available: https://euvd.enisa.europa.eu/faq
[110] Élysée, «Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe.,» Novembre 2025. [En ligne].
Available: https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe
[111] Clubic, «La loi cybersécurité dort dans les tiroirs de l'Assemblée nationale depuis des mois, un député lance l'alerte,» Janvier 2026. [En ligne].
Available: https://www.clubic.com/actualite-595063-la-loi-cybersecurite-dort-dans-les-tiroirs-de-l-assemblee-nationale-depuis-des-mois-un-depute-crie-a-l-urgence.html
[112] U. Européenne, «Implementation Timeline,» Juillet 2024. [En ligne].
Available: https://artificialintelligenceact.eu/implementation-timeline/
[113] U. Européenne, «Cyber Resilience Act,» Décembre 2024. [En ligne].
Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[114] E. I. O. P. Authority, «Digital Operational Resilience Act (DORA),» Janvier 2025. [En ligne].
Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[115] E. A. I. Act, « La loi européenne sur l'intelligence artificielle Développements et analyses actualisés de la loi européenne sur l'IA,» 2025. [En ligne].
Available: https://artificialintelligenceact.eu/fr/
[116] E. Commission, «Cyber Resilience Act,» 2025. [En ligne].
Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[117] BBC, «Hegseth orders pause in US cyber-offensive against Russia,» Mars 2025. [En ligne].
Available: https://www.bbc.com/news/articles/c2er34w0jgdo
[118] C. o. F. Relations, «The Trump Administration's Cyber Strategy Fundamentally Misunderstands China's Threat,» Janvier 2026. [En ligne].
Available: https://www.cfr.org/articles/the-trump-administrations-cyber-strategy-fundamentally-misunderstands-chinas-threat
[119] Cyberscoop, « Lawmakers probe CISA leader over staffing decisions,» Janvier 2026. [En ligne].
Available: https://cyberscoop.com/cisa-madhu-gottumukkala-house-homeland-hearing-workforce-staffing-levels/
[120] L. M. Informatique, «D'ici 2027, l'Europe triplera ses dépenses dans le cloud souverain,» Février 2026. [En ligne].
Available: https://www.lemondeinformatique.fr/actualites/lire-d-ici-2027-l-europe-triplera-ses-depenses-dans-le-cloud-souverain-99308.html
[121] E. U. I. f. S. Studies, « Autonomy is not autarky: But is the EU's new Digital International Strategy's focus on partnerships enough?,» Juin 2025. [En ligne].
Available: https://www.iss.europa.eu/publications/commentary/autonomy-not-autarky-eus-new-digital-international-strategys-focus

xmco

We deliver cybersecurity expertise

Nos consultants pensent comme les attaquants pour mieux les contrer, puis vérifient manuellement chaque vulnérabilité potentielle afin de livrer une vision claire et exploitable des risques Cyber. Audits, pentests, réponse à incident, conformité PCI DSS, veille CERT et CTI : nous couvrons tout le cycle de vie de la cybersécurité.

Cette exigence transforme la sécurité en levier de performance mesurable. Certifiés PASSI et PCI QSA, nous demeurons indépendants et engagés pour la réussite numérique de nos clients.

Date de création :	2002
Effectif salariés :	plus de 100
Qualifications :	PASSI, QSA et CERT officiel
Clients actifs :	plus de 450
dont clients CERT :	plus de 100
Secteurs :	Banque, Assurance, Industrie, Institutions, Transports, Médias, Luxe, etc.

UGAP C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière cert by xmco ANSSI qsa

Renseignement :

info@xmco.fr

01 79 35 29 30

www.xmco.fr