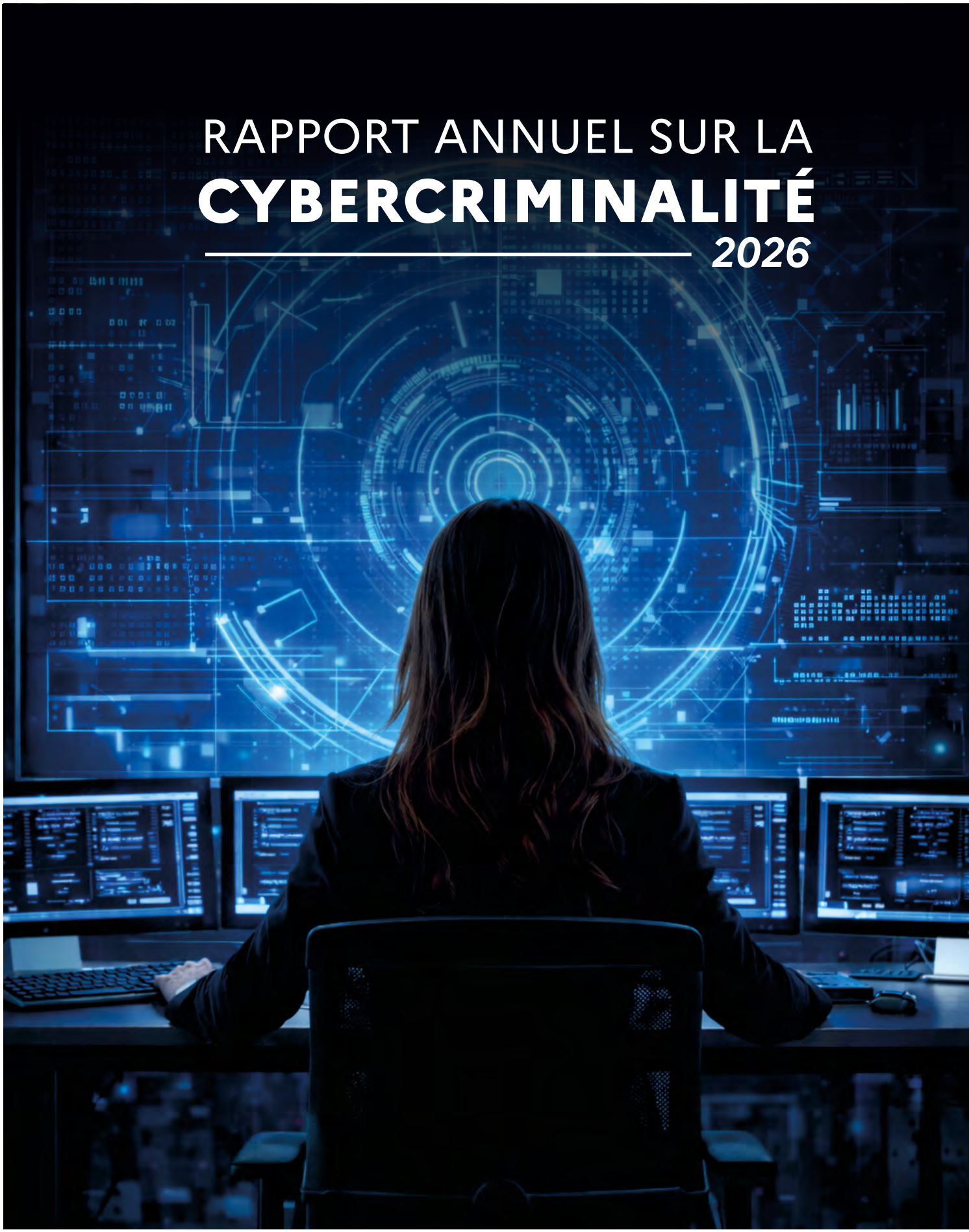
MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2026



COMCYBER-MI

« Nos forces, pour votre cyber-protection »

RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2026

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Commandement du ministère
de l'Intérieur dans le cyberespace

SOMMAIRE

Le temps où la sécurité de nos concitoyens se limitait à l'espace public semble désormais révolu. Aujourd'hui, violences physiques, trafics internationaux et cybercriminalité ne sont plus des phénomènes distincts : ils se conjuguent et imposent une réponse ajustée de l'État.

La criminalité organisée en général, le narcotrafic en particulier, demeure l'un des moteurs principaux de cette violence. Ses réseaux, plus structurés mais aussi plus numérisés, ont désormais volontiers recours à des plateformes chiffrées, des cryptoactifs et des circuits internationaux de blanchiment. Élevée au rang des priorités absolues du Gouvernement, notre action contre le narcotrafic et la criminalité organisée est plus que jamais déterminée, y compris dans le champ cyber : démantèlement des filières, renforcement des coopérations internationales et mobilisation accrue de la police, de la gendarmerie (en lien étroit avec les autres services de l'État) grâce notamment au renforcement des capacités de renseignement et d'investigation des enquêteurs par la loi du 13 juin 2025. Nous ne laisserons aucune zone d'ombre aux trafiquants.

Parallèlement, de nouveaux publics sont aujourd'hui ciblés : professionnels de la crypto-finance, dirigeants de plateformes technologiques, influenceurs et créateurs de contenus. Ils sont exposés à des cambriolages ciblés, à des tentatives d'enlèvement ou d'extorsion, signe de la capacité des groupes criminels à exploiter les opportunités offertes par l'économie numérique. Sur ce volet, nous avons renforcé significativement les dispositifs de protection et de signalement, ainsi que l'action de nos services spécialisés pour prévenir ces violences.

En 2025, le volume d'attaques informatiques poursuit sa progression, confirmant une pression cyber durable et structurelle. L'industrialisation du cybercrime, l'usage massif de l'intelligence artificielle, la recherche de failles dans les chaînes d'approvisionnement numériques ou encore la capacité à mêler ciblage numérique et menaces physiques constituent des défis majeurs pour notre sécurité collective. Le ministère consolide ses capacités d'anticipation, de détection, de réaction et intensifie ses coopérations avec ses partenaires publics et privés, notamment grâce au COMCYBER-MI.

Face à ces menaces hybrides, notre réponse doit rester globale : un cadre juridique modernisé, une action judiciaire déterminée, une coopération internationale renforcée et un soutien constant aux forces qui protègent les Français au quotidien.

Je veux saluer leur engagement. Grâce à leur détermination et à leur expertise, dont la valeur ajoutée est singulièrement forte lorsqu'il est question de cybercriminalité, nous pouvons continuer à protéger nos concitoyens jusque dans l'espace numérique et préserver nos intérêts fondamentaux.

Aussi loin que la surface d'attaque s'étendra, aussi loin la mobilisation du ministère de l'Intérieur répondra.

Laurent Nuñez
Ministre de l'Intérieur

*CHIFFRES CLÉS 2025**

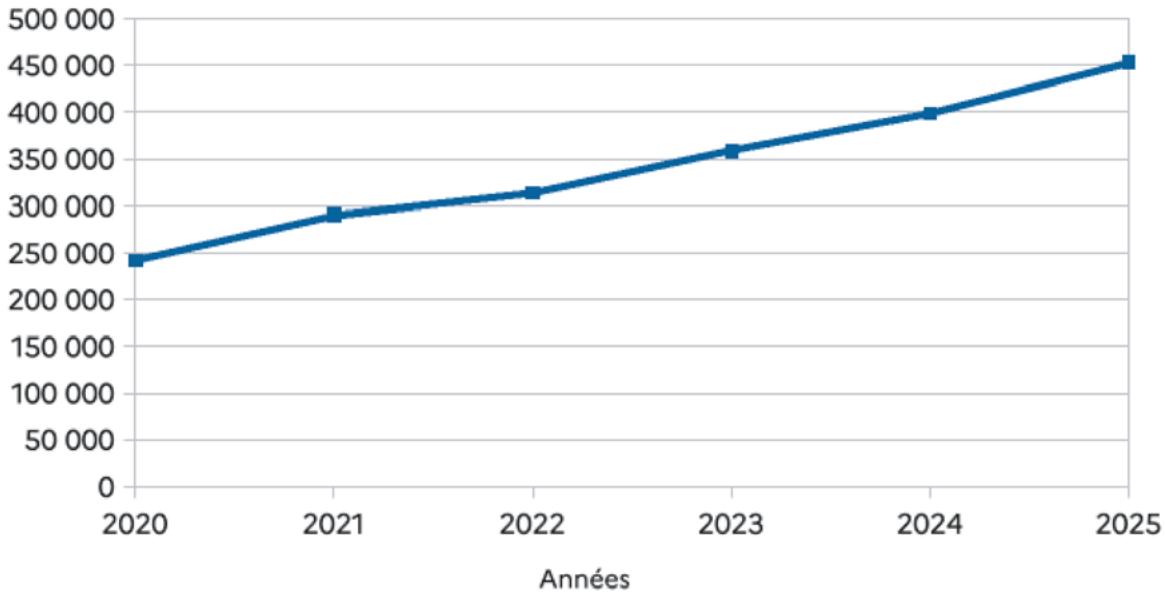
453 200

atteintes numériques enregistrées en 2025

+87%

d'atteintes numériques sur les cinq dernières années

Nombre d'infractions constatées annuellement depuis 2020



THESEE

116 695

plaintes ou signalements relatifs aux escroqueries sur internet enregistrés sur la plateforme Thésée

PHAROS

231 853

signalements de contenus illicites reçus par la plateforme Pharos

PERCEV@L

206 902

signalements d'usages frauduleux de cartes bancaires enregistrés par la plateforme Perceval

** NB : les chiffres présentés proviennent de données établies par le service statistique ministériel de la sécurité intérieure, complétées par d'autres sources institutionnelles : section J3 du Parquet de Paris, Office anti-cybercriminalité de la Police nationale, Unité Nationale Cyber de la Gendarmerie nationale.*

61,9%
d'atteintes numériques aux biens

33%
d'atteintes numériques aux personnes

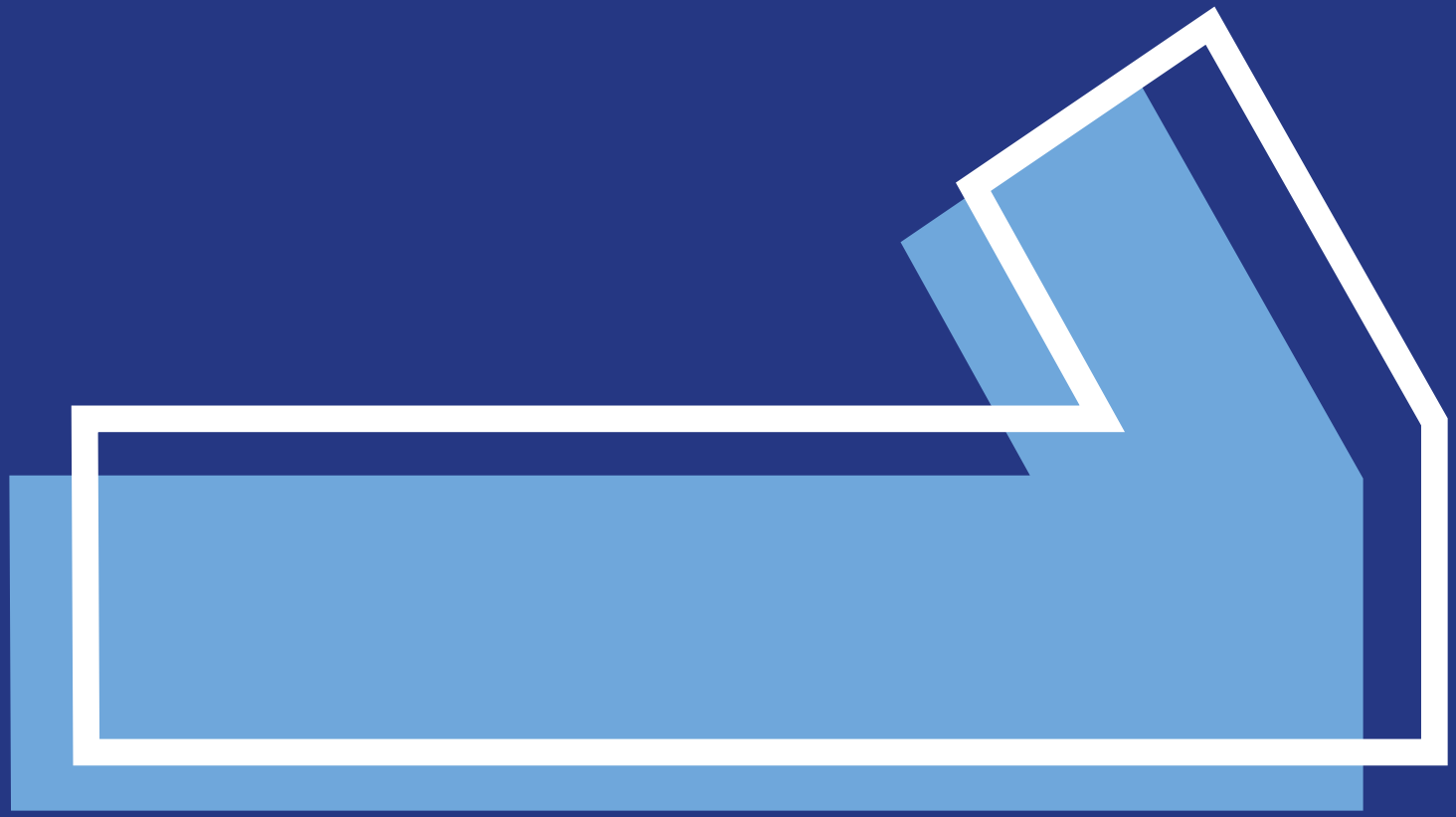
17 600
atteintes aux systèmes d'information en 2025

On observe une diminution de 19% des saisines d'attaque par rançongiciel par rapport à l'année 2024 (365 faits en 2025 contre 449 en 2024), venant confirmer la baisse amorcée et un changement dans la manière d'opérer des attaquants (chiffrement des données après exfiltration non systématique).

4,7%
d'atteintes numériques aux institutions et à l'ordre public

0,4%
infractions aux législations et réglementations spécifiques au numérique

100 700
personnes physiques mises en cause pour des atteintes numériques



TENDANCES MAJEURES ET ÉVOLUTION DE LA CYBERCRIMINALITÉ

1 TENDANCES MAJEURES ET ÉVOLUTION DE LA CYBERCRIMINALITÉ

L'écosystème de la cybercriminalité connaît depuis plusieurs années une évolution rapide. Les acteurs se professionnalisent, les méthodes s'industrialisent et les motivations se diversifient. Dans un contexte où le numérique irrigue désormais l'ensemble des activités économiques, sociales et institutionnelles, les attaques informatiques constituent un risque majeur dont les conséquences dépassent largement le seul champ technique.

Les cybermenaces s'inscrivent aujourd'hui dans un *continuum* : elles vont de la délinquance opportuniste, fondée sur des actions de masse, à des opérations structurées menées par des groupes organisés, parfois appuyés ou guidés par des intérêts étatiques. Elles exploitent à la fois les vulnérabilités technologiques et les fragilités humaines, en combinant de plus en plus souvent espace cyber, champ informationnel et, parfois, milieu physique.

Cette première partie propose une analyse des tendances majeures observées au cours de l'année 2025. Elle met en perspective les évolutions marquantes : professionnalisation des écosystèmes criminels, transformation des modèles économiques illicites, appropriation de technologies émergentes et montée des logiques de confrontation idéologique et géopolitique. L'objectif est d'offrir une lecture structurée de ces dynamiques afin d'éclairer les décideurs, les acteurs opérationnels et, plus largement, l'ensemble des parties prenantes sur les risques actuels et les trajectoires possibles de la menace.

1 | Panorama des attaques et tendances générales

Parmi ses missions, le Centre d'analyse des cybermenaces (CECyber) du commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) est chargé d'observer et d'analyser l'évolution des modes d'action employés par les acteurs cybercriminels spécialisés dans les atteintes aux systèmes de traitement automatisé de données (ASTAD)[1]. Cette analyse repose notamment sur une veille continue des espaces numériques investis par les acteurs malveillants : forums spécialisés, messageries publiques ou chiffrées, blogs et plateformes de revendication.

Les observations menées tout au long de l'année 2025 permettent de dégager plusieurs tendances structurantes et d'identifier des évolutions notables du paysage de la menace cyber visant le territoire national.

Tendances générales observées en 2025

Entre le 1er janvier et le 31 décembre 2025, le COMCYBER-MI a recensé 1 347 revendications ou annonces de cyberattaques visant la France[2], contre 1 062 sur la même période en 2024. Cette hausse significative de 27% revêt une signification particulière. En 2024, le volume élevé d'attaques s'expliquait en partie par des évènements à forte portée médiatique, tels que les Jeux olympiques et paralympiques de Paris ou encore l'interpellation du fondateur de Telegram, Pavel Durov. En 2025, et ce malgré l'absence d'évènement de cette ampleur, le niveau d'activité observé est supérieur à 2024. Ceci traduit une pression cyber durable et structurelle.

Trois tendances majeures sont observées : s'inscrivent en première place les attaques par déni de service distribué *(DDoS)*, principalement revendiquées par des groupes se réclamant de l'hacktivisme. Les vols et reventes de données compromises et les attaques par rançongiciel se positionnent respectivement en deuxième et troisième place.

Plus rares mais particulièrement préoccupantes, les intrusions visant des systèmes industriels de type *SCADA*[3] connaissent une augmentation notable. Ces attaques consistent à accéder à des interfaces de supervision de systèmes indus-

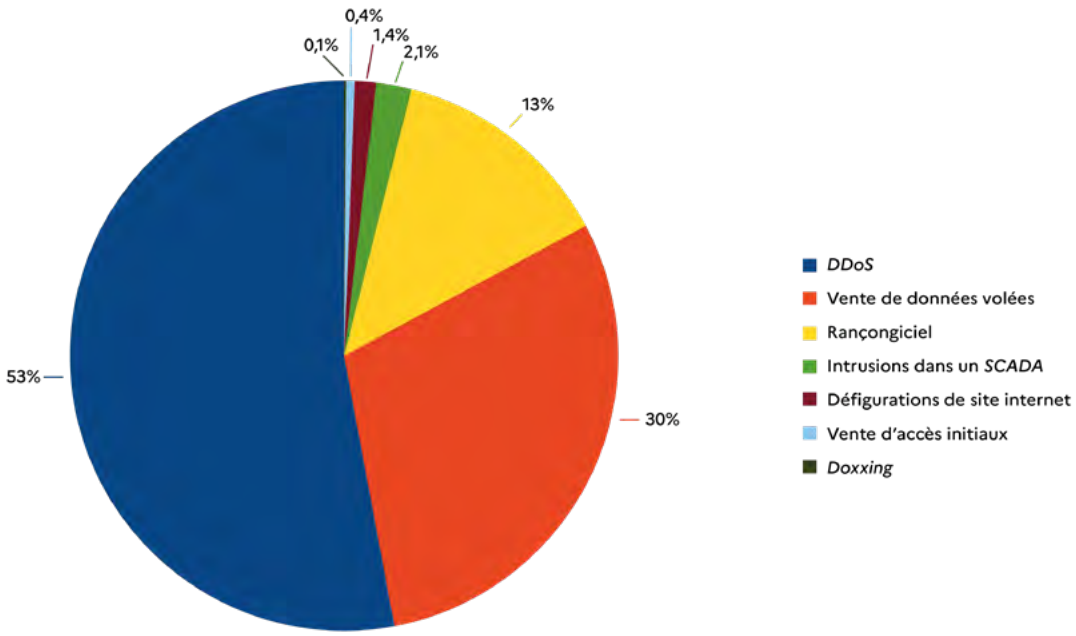
1. Pour ce volet de l'activité du COMCYBER-MI, la cybercriminalité liée aux escroqueries (hameçonnages, pourriels, faux virements…) ou aux *Advanced Persistent Threat* n'est pas prise en compte.
2. Rançongiciels, hacktivisme et ventes de données volées principalement.
3. *Supervisory Control and Data Acquisition* ou Système de contrôle et d'acquisition de données, à savoir des systèmes de gestion à distance d'outils de production.

triels (barrages hydroélectriques, installations énergétiques, infrastructures de traitement de l'eau, etc.) afin d'en modifier les paramètres de fonctionnement. Jusqu'à présent, les dispositifs de sécurité en place ont permis d'éviter des dommages significatifs, mais ces incidents illustrent une montée en gamme préoccupante des modes d'action observés.

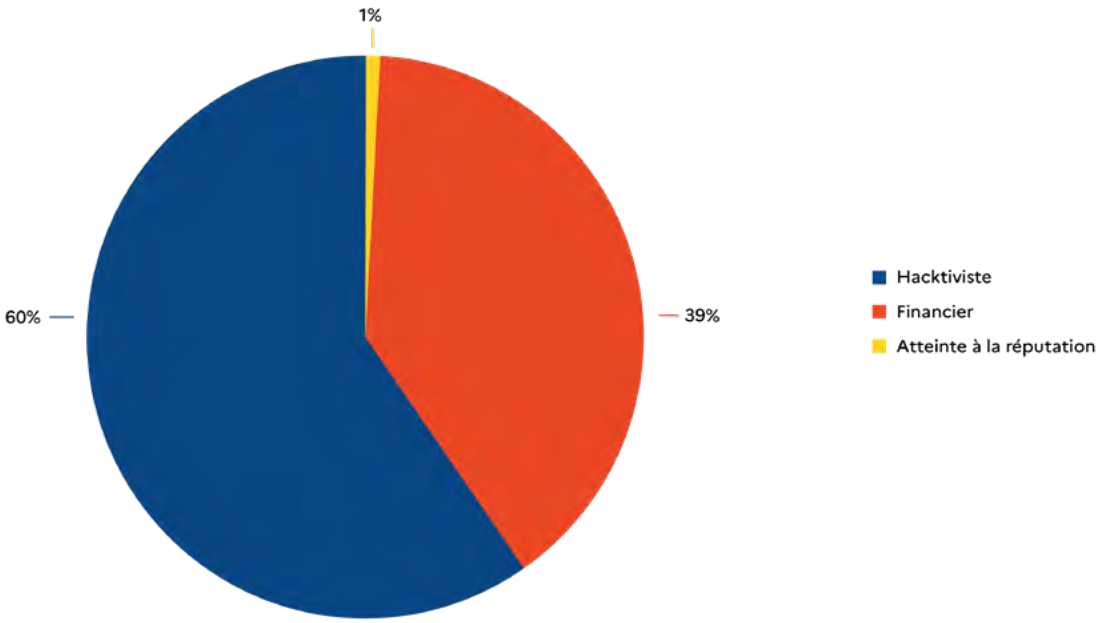
À l'inverse, les défigurations de sites internet, très répandues en 2024, sont en net recul : 152 cas recensés en 2024 contre seulement 19 en 2025.

Les attaquants privilégient désormais des modes opératoires à plus fort impact, notamment les attaques *DDoS*, parfois proposées sous forme de *DDoS-as-a-Service*. Cette évolution pourrait toutefois rester conjoncturelle et ne préjuge pas d'un abandon définitif de ce mode d'action.

Enfin, l'analyse des revendications met en évidence une forte dimension idéologique : près des deux tiers des attaques recensées en 2025 sont attribuées à des acteurs se revendiquant de causes politiques ou religieuses.



Répartition des principales catégories de cyberattaques détectées par le CECyber sur l'année 2025



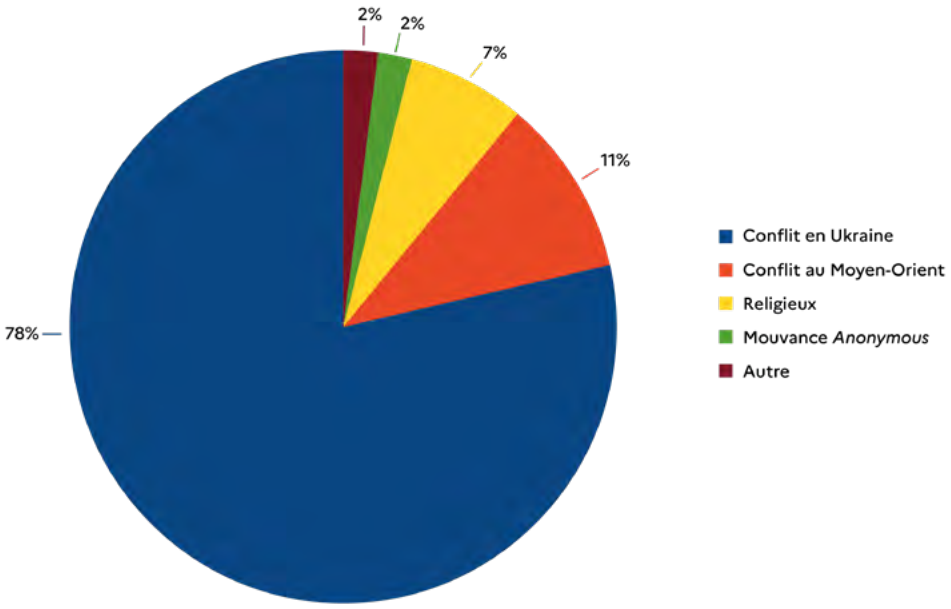
Répartition des principales motivations des cyberattaques détectées par le CECyber sur l'année 2025

Hacktivisme : prédominance des attaques par déni de service distribué

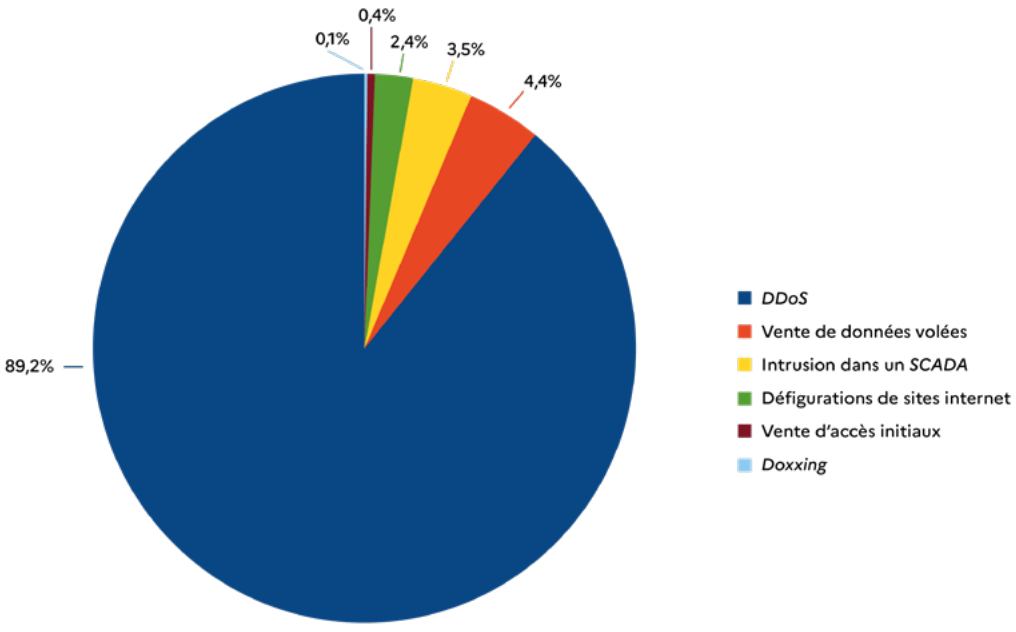
Sur fond de conflits internationaux persistants, l'hacktivisme confirme en 2025 sa place durable dans le paysage cyber. Les modes d'action évoluent rapidement : alors que les attaques *DDoS* représentaient 64%[4] des revendications en 2024, cette proportion atteint 89,2% en 2025, reléguant les autres techniques à un rôle marginal.

En effet, les vols et diffusions de données compromises, qui représentaient 12% des revendications en 2024, ne constituent plus en 2025 que 4,4%. Dans le même ordre d'idées, les intrusions dans des systèmes industriels demeurent quantitativement limitées, mais leur portée symbolique et les risques associés en font un sujet de vigilance particulier.

L'analyse des revendications des hacktivistes montre une forte corrélation avec l'actualité géopolitique : 78% des attaques font référence au conflit en Ukraine, 11% au conflit au Moyen-Orient, tandis que les autres revendications se rattachent à des causes diverses, notamment la mouvance *Anonymous*.



Répartition des motivations hacktivistes revendiquées lors des attaques DDoS détectées par le CECyber sur l'année 2025



Répartition des modes d'action hacktivistes détectés par le CECyber sur l'année 2025

4. Le reste étant constitué de défigurations (22%), vols ou diffusions de données volées (12%) et de mises à disposition d'accès initiaux (2%).

Démocratisation des ventes de données volées

La vente de données compromises s'impose désormais comme un levier de monétisation privilégié pour de nombreux acteurs cybercriminels. Ce marché attire des profils variés, allant de cybercriminels expérimentés bénéficiant d'une réputation établie à une multitude d'acteurs opportunistes.

Les premiers proposent généralement des bases de données crédibles et valorisées par la communauté cybercriminelle. Les seconds, souvent éphémères, apparaissent sur les forums pour de courtes périodes avant de disparaître, changer d'identité numérique ou être exclus[5].

Attirés par des gains rapides, ces acteurs proposent fréquemment des données déjà diffusées[6], issues de sources publiques, voire totalement fabriquées à l'aide d'outils d'intelligence artificielle. Ces individus sont parfois très jeunes.

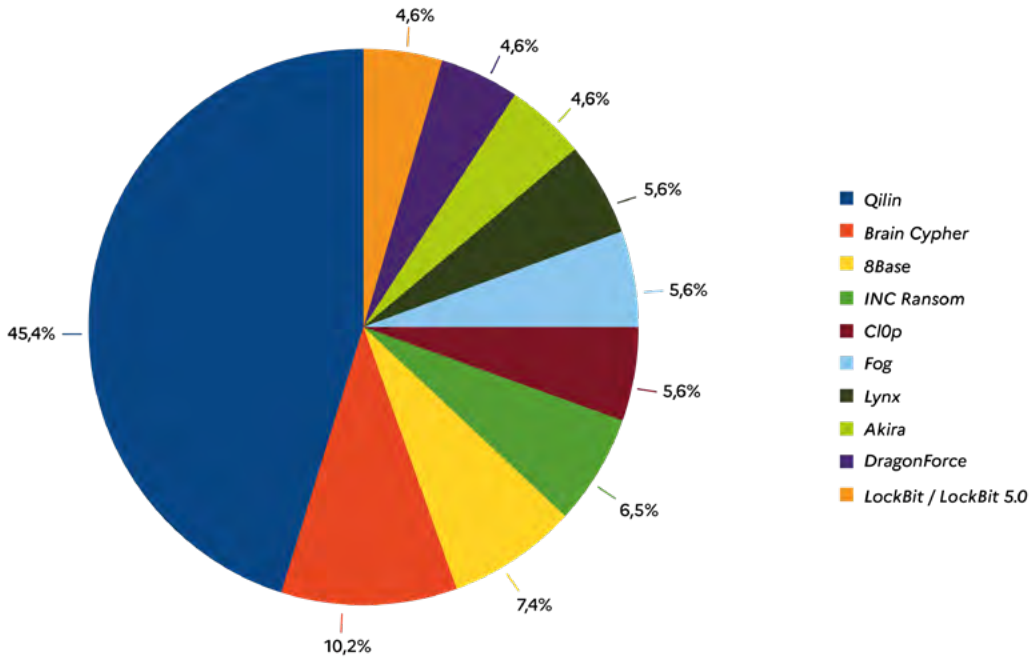
Alors qu'en 2024 les revendications de vols de données constituaient un levier privilégié des campagnes hacktivistes visant à affaiblir la confiance dans les institutions et les entreprises françaises, ces pratiques sont en net recul en 2025. Les vols de données revendiqués par des hacktivistes ne représentent plus que 4,4% des cas, la majorité des attaques étant désormais motivée par des considérations financières.

Rançongiciels : recomposition des groupes et évolution des stratégies

La menace liée aux rançongiciels demeure élevée en 2025, avec une augmentation de 36% des revendications d'attaques ciblant la France par rapport à l'année précédente[7].

Toutefois, l'année 2025 se caractérise par une recomposition marquée de la hiérarchie des groupes cybercriminels. Alors que *LockBit* et *RansomHub* dominaient en 2024, les groupes *Qilin* et *Brain Cypher* se sont imposés en 2025 comme les principaux acteurs, concentrant à eux seuls 55,6% des revendications. D'autres groupes, peu actifs, tels qu'*Akira* ou *DragonForce*, connaissent une montée en puissance significative.

Parallèlement, les modes opératoires évoluent. Les cybercriminels tendent à délaisser le chiffrement systématique des systèmes d'information au profit de la simple exfiltration des données. Cette stratégie permet d'accroître la rapidité et la fréquence des attaques, tout en exerçant une pression constante sur les victimes par la menace de divulgation publique d'informations sensibles.



Nombre de revendications de cyberattaques par groupe de rançongiciel détectées par le CECyber sur l'année 2025

5. Les forums de cybercriminels disposent de mécanismes de réputation jouant un rôle d'autorégulation, conduisant régulièrement à l'exclusion des acteurs jugés peu fiables.
6. Certaines bases de données d'entreprises françaises ont été recyclées parfois plusieurs dizaines de fois sur les forums cybercriminels spécialisés dans la vente de données volées.
7. 177 revendications d'attaques par rançongiciels ont été recensées par le COMCYBER-MI en 2025.

2 | Attaques ciblant les infrastructures critiques

Les cyberattaques constituent une menace permanente qui impose une vigilance numérique constante et partagée. Même en appliquant des mesures de sécurité adaptées, tout individu ou toute organisation demeure susceptible d'être confronté à une tentative d'hameçonnage sophistiquée ou à une compromission de données.

Lorsque ces attaques ciblent des administrations ou des entreprises relevant de secteurs critiques, leurs conséquences peuvent toutefois dépasser largement le cadre numérique. Les atteintes portées aux secteurs de la santé, des transports, de l'énergie ou des télécommunications sont susceptibles d'affecter la continuité des services essentiels, la sécurité des populations, voire la sûreté de l'État.

Principaux vecteurs d'intrusion observés

Quel que soit le secteur ciblé, plusieurs techniques d'intrusion sont récurrentes :

Réutilisation d'identifiants compromis :

Les attaquants exploitent des listes d'identifiants (couples identifiant/mot de passe) issues de fuites de données pour tenter des connexions à des services exposés sur internet.

Accès à distance non sécurisés *(RDP[8], VPN* et environnements Citrix[9]*)* :

L'obtention d'un accès distant à un poste de travail ou à un réseau permet aux attaquants de compromettre tout ou partie du système d'information.

Achat d'accès initiaux auprès de courtiers spécialisés *(Initial Access Brokers)* :

Ces accès, vendus à prix élevé, sont réputés fiables et permettent des attaques ciblées à forte valeur ajoutée.

Hameçonnage ciblé :

Des courriels usurpant le nom de domaine et la charte graphique de l'organisation ciblée sont adressés aux employés, généralement pour solliciter une mise à jour urgente de leurs identifiants. Les attaquants misent sur la crédulité des destinataires afin d'obtenir ces informations sensibles.

Usurpation de comptes sur les réseaux sociaux :

Cette technique, particulièrement répandue dans le secteur des transports (compagnies aériennes, ferroviaires, métros, tramways), vise à tromper les usagers ou les employés pour collecter des informations sensibles.

Attaques *via* la chaîne d'approvisionnement :

Les attaquants ciblent des fournisseurs ou prestataires moins sécurisés afin d'accéder indirectement aux systèmes de la cible finale.

8. *Remote Desktop Protocol* : protocole développé par Microsoft qui permet à un utilisateur de se connecter à distance à son poste de travail.
9. Citrix est une solution de virtualisation d'espace de travail accessible depuis n'importe quel poste à distance.

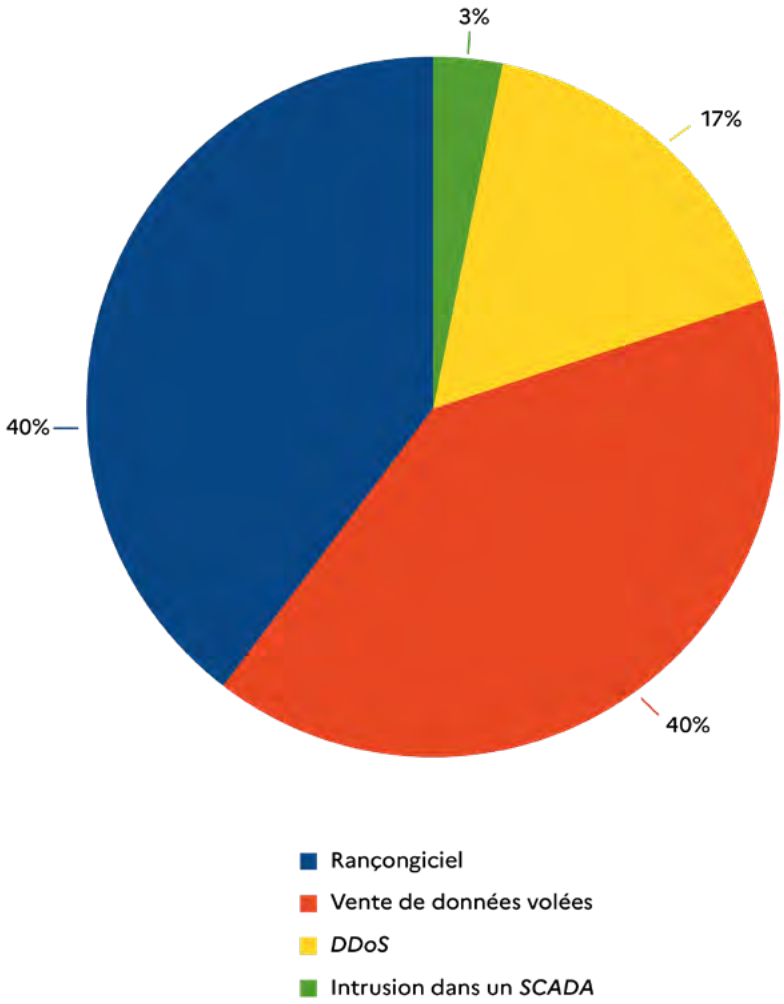
Secteur de la santé

Parmi les secteurs critiques[10], le secteur de la santé demeure, en 2025, le plus fréquemment ciblé à la fois par des attaques par rançongiciel mais surtout par la revente de données médicales volées. Les précédentes attaques très médiatisées contre des établissements hospitaliers ont durablement marqué les esprits, en raison de leurs conséquences opérationnelles directes.

Les hôpitaux, cliniques, mais également les praticiens, pharmaciens et laboratoires figurent parmi les cibles privilégiées. L'attrait de ce secteur pour les cybercriminels repose sur plusieurs facteurs : l'impératif de continuité des soins, la sensibilité des données traitées et la coexistence de systèmes informatiques parfois obsolètes avec des équipements connectés récents.

Les données dérobées (dossiers médicaux, informations administratives, données du personnel, documents de recherche) présentent une valeur élevée et peuvent être exploitées à des fins d'extorsion, de revente ou d'espionnage.

En 2025, un incident revendiqué par un groupe hacktiviste illustre ces risques : une intrusion dans un système de régulation d'oxygène d'un établissement de santé a été rendue publique, accompagnée d'images de la console d'administration. Si aucun paramétrage critique n'a été modifié, cet événement met en évidence les conséquences potentiellement dramatiques de l'exposition à distance de systèmes sensibles.



Répartition des types d'attaque pour le secteur de la santé détectés par le CECyber sur l'année 2025

10. Détection et analyse par le centre d'analyse des cybermenaces (CECyber).

Secteur des transports

Le secteur des transports est régulièrement la cible de campagnes hacktivistes visant à déstabiliser des entreprises majeures ou des institutions publiques. Ces attaques se traduisent principalement par des opérations de *DDoS* ciblant les sites vitrines des victimes, tandis que les défigurations sont plus rares. En 2025, 88% des cyberattaques recensées contre le secteur des transports relèvent de ce mode d'action[11].

Pour autant, la menace la plus impactante demeure celle des rançongiciels, en particulier dans le secteur aérien. Si aucune attaque majeure n'a affecté la France en 2025, plusieurs pays européens ont été confrontés à des situations critiques à la suite d'attaques ciblant des prestataires de services[12].

Les entreprises du secteur sont également exposées au vol de données, notamment de données clients, souvent issues de campagnes d'*infostealers* et diffusées sous forme de *combolists*[13]. Des informations sensibles telles que des contrats, des plans d'infrastructures ou des communications internes peuvent également être ciblées.

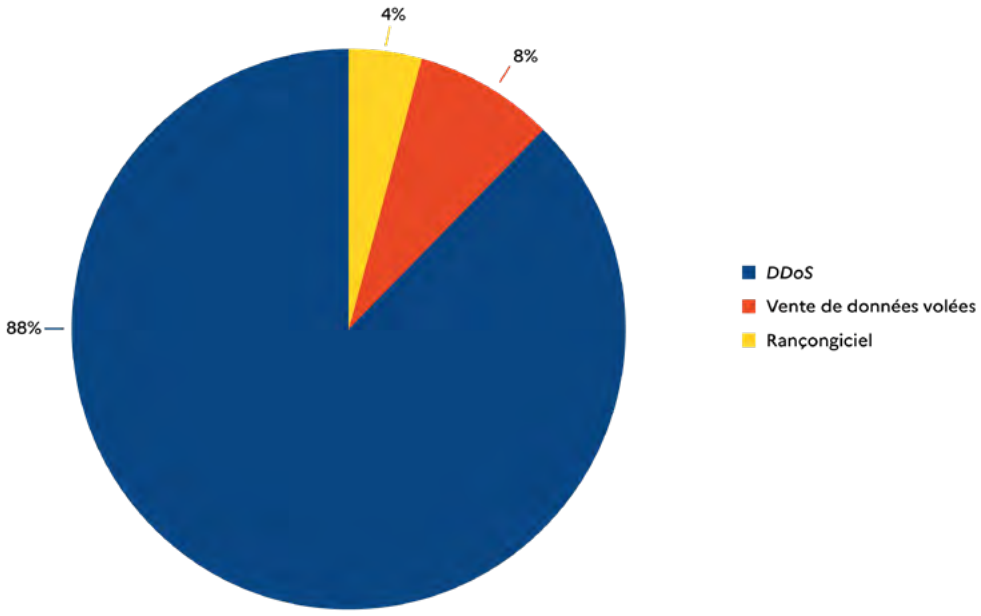
Les impacts potentiels d'une cyberattaque d'envergure sur ce secteur sont multiples :

- risque d'accidents en cas de compromission de systèmes critiques ;

- perturbation ou interruption des services ;

- diffusion de fausses informations susceptibles de provoquer des mouvements de foule ;

- prise de contrôle ou altération de systèmes de régulation du trafic.



Répartition des types d'attaques pour le secteur des transports détectés par le CECyber sur l'année 2025

11. Ce recensement ne prend pas en compte les escroqueries en ligne (hameçonnage par exemple).
12. En septembre 2025, une attaque par rançongiciel a visé un fournisseur de solutions de gestion des passagers et des bagages, entraînant par effet domino l'interruption de plusieurs services dans les aéroports de Dublin, Londres, Bruxelles et Berlin (source : https://www.lefigaro.fr/conjoncture/londres-berlin-dublin-la-situation-s-ameliore-dans-les-aeroports-europeens-apres-la-cyberattaque-20250921).
13. Fichiers contenant des associations « email : mot de passe » issus de vols de données.

Secteur de l'énergie

Le secteur de l'énergie demeure une cible stratégique, tant pour les cybercriminels motivés par l'appât du gain que pour les hacktivistes engagés dans des logiques idéologiques ou géopolitiques.

En 2025, le COMCYBER-MI a recensé 94 revendications de cyberattaques visant des entreprises du secteur énergétique, dont 78% sont attribuées à des hacktivistes. Les attaques par *DDoS* sont les plus fréquentes, sans qu'elles aient, à ce stade, provoqué de perturbations majeures.

Plus préoccupante pour ce secteur critique est la recrudescence des intrusions dans les systèmes industriels *(SCADA)*. Ces actions, principalement revendiquées dans le contexte du conflit en Ukraine, consistent à modifier à distance des paramètres critiques. Si les impacts constatés demeurent limités, le risque de sabotage ou de perturbation durable reste élevé.

Par ailleurs, le secteur énergétique constitue une cible privilégiée pour des opérations d'espionnage, en particulier dans les domaines liés au nucléaire, compte tenu du savoir-faire stratégique français.

Les principales menaces pesant sur les entreprises du secteur de l'énergie sont :

L'hacktivisme

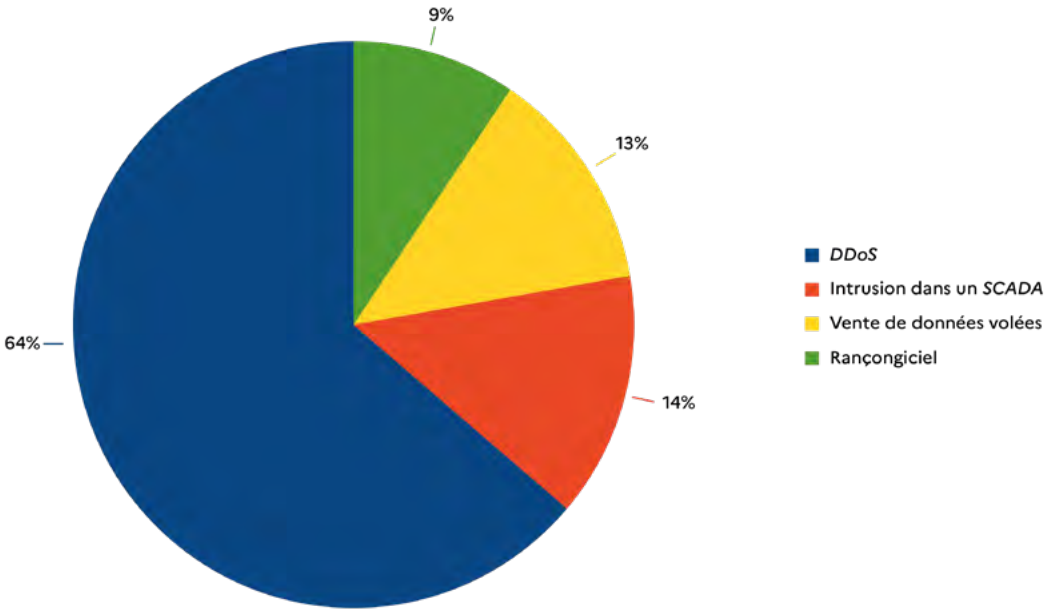
Les attaques par rançongiciels

Les campagnes d'hameçonnage ciblé

Les compromissions de postes de travail *via* des *infostealers*

Les actes de sabotage visant à déstabiliser les entreprises

L'espionnage notamment le vol de brevets et de plans stratégiques



Répartition des types d'attaques pour le secteur de l'énergie détectés par le CECyber sur l'année 2025

Secteur des télécommunications

Véritable colonne vertébrale d'une société connectée, le secteur des télécommunications est exposé à des menaces multiples, allant des cyberattaques sophistiquées aux actes de sabotage physique.

Les vols massifs de données affectant des opérateurs télécoms favorisent une cascade d'actes de cyberdélinquance : escroqueries, campagnes d'hameçonnage, usurpations d'identité.

Les attaques hacktivistes, principalement sous forme de *DDoS*[14], restent fréquentes.

Elles soulèvent deux enjeux majeurs :

- le recours à des opérations sous faux drapeau, visant à masquer des actions étatiques ;
- l'utilisation de ces attaques comme outils de propagande.

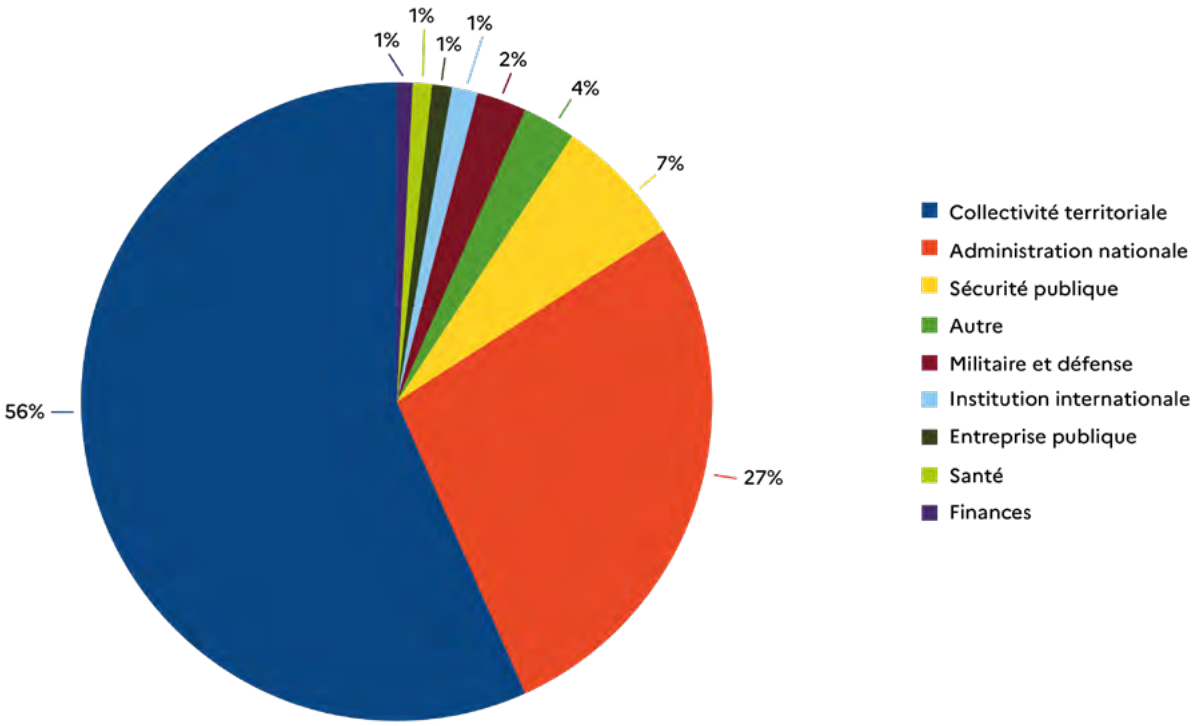
Enfin, le secteur est particulièrement exposé aux opérations d'espionnage étatique et de sabotage, ciblant aussi bien les infrastructures que les câbles sous-marins, essentiels au transit mondial des communications[15].

Autres secteurs sensibles

Collectivités territoriales

Les collectivités territoriales sont régulièrement ciblées par des campagnes *DDoS*, qui représentent 93% des attaques revendiquées en 2025 contre ce secteur. Si les impacts opérationnels demeurent limités, ces attaques visent avant tout la visibilité médiatique.

Par ailleurs, plusieurs intrusions signalées en 2025[16] mettent en évidence les risques liés aux plateformes numériques mutualisées, notamment chez des prestataires gérant des services essentiels pour plusieurs collectivités.

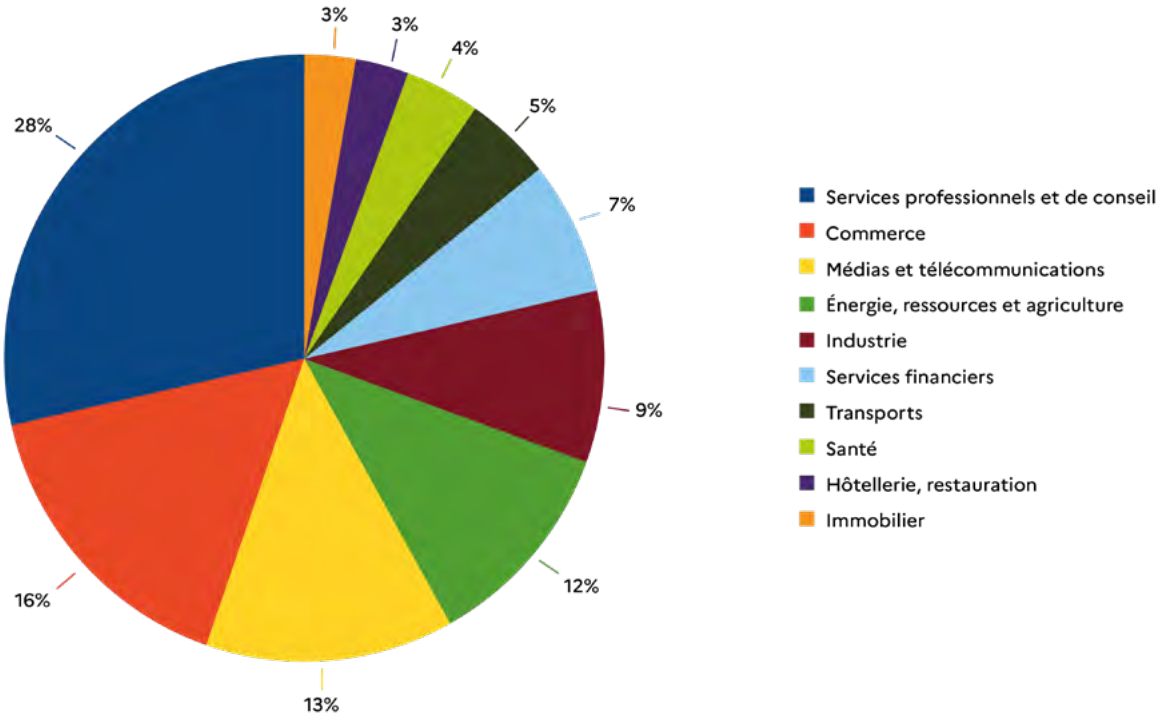


Sous-catégories les plus visées par les cybercriminels dans le secteur institutionnel en 2025

14. 59% de l'ensemble des revendications d'attaques recensées par le COMCYBER-MI en 2025.
15. https://www.01net.com/actualites/trois-cables-sous-marins-ete-sabotes-un-apres-autre-europe.html
16. En novembre 2025, plusieurs communes de Bretagne et d'Île-de-France ont signalé des intrusions ainsi que de possibles vols de données personnelles. Les auteurs auraient exploité une vulnérabilité au sein de la plateforme informatique d'un prestataire chargé de la prise de rendez-vous pour l'établissement des cartes nationales d'identité et des passeports. https://www.leparisien.fr/high-tech/demarches-en-mairie-la-rochelle-clichy-brest-une-fuite-de-donnees-reperee-dans-1300-communes-24-11-2025-QRSBCFWF55GVLHNMEL6NYWAFAQ.php

Entreprises publiques et privées

Les entreprises françaises, tous secteurs confondus, sont exposées à l'ensemble des menaces observées : rançongiciels, vente d'accès et fuites de données, sabotage et espionnage. Depuis 2024, certains secteurs apparaissent plus fréquemment ciblés, notamment les services professionnels et le conseil, qui concentrent 28% des attaques, suivis du secteur du commerce avec 16% des attaques, puis celui de médias et télécommunications avec 13%[17].



Les principaux secteurs des entreprises attaquées depuis le 1er janvier 2024

FOCUS

Les risques pesant sur la chaîne d'approvisionnement

Les attaques visant la chaîne d'approvisionnement constituent aujourd'hui l'une des menaces les plus complexes à détecter et à maîtriser. Plutôt que de viser directement une organisation bien protégée, les attaquants s'intéressent aux éléments les moins sécurisés de son écosystème : prestataires, éditeurs de logiciels, fournisseurs de services *cloud*, sous-traitants techniques ou encore développeurs de composants tiers. En s'introduisant chez ces acteurs tiers, ils cherchent à obtenir un accès indirect aux systèmes ou aux données de la cible finale.

L'attaque ayant visé la solution de transfert de fichiers *MOVEit* en 2023 illustre l'ampleur potentielle de ces scénarios : une vulnérabilité unique a conduit à la compromission de centaines d'organisations à travers le monde[18]. Ce type d'incident rappelle qu'un logiciel unique, largement employé pour des échanges de données sensibles, peut devenir, dès qu'il présente une vulnérabilité, une porte d'entrée conduisant à de nombreuses victimes.

17. Chiffres CECyber du 1er janvier 2024 au 31 décembre 2025.
18. https://www.lemonde.fr/pixels/article/2023/10/30/moveit-des-milliers-d-organisations-piratees-a-la-suite-d-une-faille-logicielle-exploitee-par-le-groupe-cybercriminel-clop_6197353_4408996.html

3 | Hacktivisme : idéologie, géopolitique et convergence des luttes

En 2025, l'hacktivisme s'affirme comme un reflet direct des tensions géopolitiques internationales. Cette dynamique, déjà observable en 2024, s'est renforcée avec la multiplication d'alliances entre groupes auparavant indépendants et l'émergence continue de nouveaux acteurs dans la sphère clandestine.

Les collectifs hacktivistes partagent désormais outils, capacités techniques et canaux de communication. Les cibles privilégiées demeurent majoritairement symboliques (portails institutionnels, médias, entreprises emblématiques), mais certaines attaques visent également des infrastructures critiques, notamment des systèmes industriels *(SCADA)*, traduisant une volonté de tester les limites des dispositifs de protection.

Les plateformes de messagerie, comme Telegram, jouent un rôle central dans la structuration de cet écosystème. Elles servent à la fois de vecteurs de coordination opérationnelle, de diffusion idéologique et de mise en scène médiatique des attaques. Cette hybridation des usages contribue à la convergence de causes parfois distinctes, alignées ponctuellement contre des cibles occidentales communes.

L'hacktivisme pro-russe : une menace géopolitique persistante

Le conflit en Ukraine continue de constituer un moteur central de l'activité hacktiviste pro-russe. Les campagnes observées en 2025 ont été déclenchées par des événements variés : annonces de sanctions, aides militaires ou financières, décisions judiciaires, rencontres diplomatiques ou prises de position politiques.

Ces opérations revêtent plusieurs dimensions :

- perturbation de services par des attaques *DDoS* ;
- collecte d'informations ;
- diffusion de contenus de désinformation ou de propagande.

Si les attaques demeurent, pour la plupart, techniquement peu sophistiquées, leur impact médiatique est réel. L'opération *Eastwood*, menée en juillet 2025 sous l'égide d'Europol, a illustré cette dynamique[19]. Bien que l'infrastructure du groupe *NoName057(16)* ait été temporairement neutralisée, les acteurs ont rapidement repris leurs activités, accompagnées de campagnes de communication revendicatives, ciblant notamment les pays impliqués dans l'opération, dont la France.

L'hacktivisme pro-palestinien : alliances stratégiques et opportunisme

Les tensions au Moyen-Orient alimentent également une activité hacktiviste soutenue. Plusieurs collectifs pro-palestiniens revendiquent régulièrement des attaques symboliques visant des institutions publiques ou des entreprises occidentales.

Le groupe *Keymous+*, apparu en 2022, s'est illustré par son soutien explicite à la cause palestinienne, tout en nouant des alliances opportunistes avec des collectifs pro-russes tels que *NoName057(16)*. La structure de *Keymous+* comprend une équipe dédiée aux fuites de données et une autre spécialisée dans les attaques par *DDoS*. Le groupe revendique une posture anti-oppression, mais ses motivations semblent également commerciales, proposant notamment un service payant de *DDoS*. Ses cibles englobent des entités israéliennes ou perçues comme pro-israéliennes, ainsi que des pays africains ou européens, selon des logiques opportunistes. En 2025, la France figure parmi ses cibles régulières.

Cette porosité entre motivations idéologiques, recherche de visibilité et intérêts financiers caractérise une partie croissante du paysage hacktiviste.

19. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

Cyberattaques et actualité internationale : une réactivité accrue

L'activité hacktiviste observée en 2025 se distingue par une réactivité quasi immédiate à l'actualité internationale. Les campagnes se succèdent rapidement, en lien avec des événements survenus en Europe de l'Est, au Moyen-Orient, en Afrique du Nord ou en Asie.

Des coalitions transnationales se forment en fonction des contextes. Certains groupes recrutent des partenaires éloignés géographiquement, notamment en Asie, afin d'accroître leur capacité d'action. À l'inverse, des alliances ponctuelles peuvent émerger entre groupes traditionnellement opposés, unis temporairement contre des cibles occidentales.

L'opération *#Hack_For_Humanity*, lancée en février 2025, illustre cette convergence[20]. Initiée par *Keymous+* et rapidement rejointe par de nombreux collectifs aux profils hétérogènes, cette campagne démontre comment un mot-dièse devient à la fois un outil de revendication, un marqueur identitaire et un vecteur de mobilisation transversale.

Actions isolées et persistance des ressentiments

Outre les campagnes coordonnées, des actions isolées sont régulièrement observées en France. Certains événements, parfois anciens, continuent de susciter des réactions hostiles. Des décisions judiciaires, des arrestations médiatisées ou des manifestations culturelles et sportives peuvent encore servir de prétexte à des attaques, plusieurs mois voire plusieurs années après les faits[21].

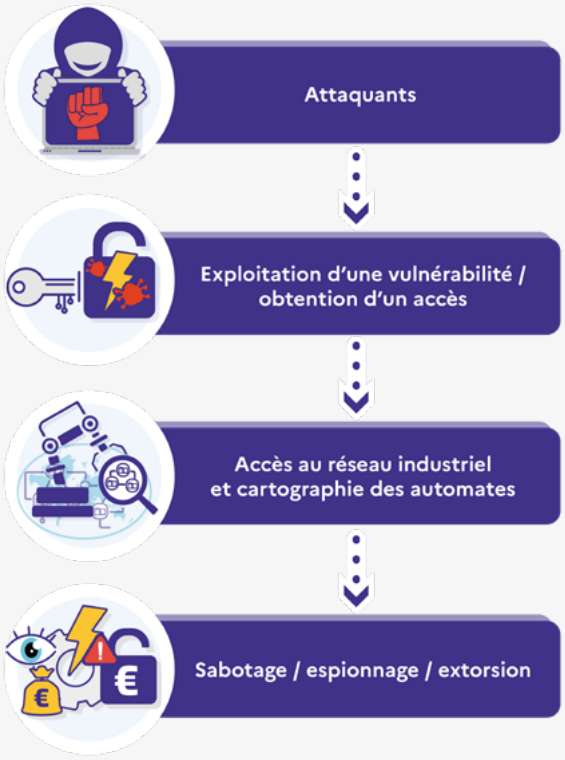
Ces actions, bien que limitées en portée, contribuent à maintenir une pression constante sur les institutions et les entreprises françaises. Leur volume et la diversité des acteurs confirment qu'en 2025, l'hacktivisme constitue une source majeure de menace cyber en France.

FOCUS

SCADA : infrastructures industrielles sous pression

Les systèmes *SCADA* assurent la supervision et le contrôle à distance d'infrastructures industrielles critiques telles que les réseaux électriques, les installations de production d'énergie, les systèmes de traitement de l'eau, les transports ou certains équipements hospitaliers. Ils reposent sur un ensemble de capteurs, d'automates programmables et de logiciels de pilotage, indispensables à la continuité et à la sûreté des installations.

Leur niveau d'exposition au risque cyber est aggravé par plusieurs facteurs structurels : obsolescence de certains équipements, interconnexion croissante avec les systèmes informatiques traditionnels et complexité des opérations de mise à jour ou de correction, susceptibles d'interrompre les processus industriels.



20. https://cybelangel.com/blog/keymous-ddos-warfare
21. Les caricatures de Mahomet publiées par Charlie Hebdo (en 2006 et à nouveau en 2025), l'arrestation de Pavel Durov ou encore la cérémonie d'ouverture des Jeux olympiques de Paris en 2024.

Ciblage des systèmes industriels : enjeux et risques

Les attaques visant les infrastructures industrielles connaissent une augmentation notable en Europe et particulièrement en France. Ces actions malveillantes soulèvent des enjeux majeurs : perturbation de la production et de la distribution d'énergie, risques de sabotage, manipulation de données de contrôle, mais aussi atteinte à l'image et à la crédibilité des opérateurs et des États concernés.

En France, ces attaques sont majoritairement revendiquées par des groupes hacktivistes affiliés à des mouvances pro-russes, qui ciblent des secteurs tels que l'énergie, l'eau ou le traitement des déchets. Les impacts observés demeurent, à ce stade, limités dans le temps et dans leur portée. Ces actions visent avant tout un effet médiatique et symbolique, davantage qu'un sabotage d'ampleur. Elles témoignent néanmoins d'une montée en gamme préoccupante des modes opératoires.

Hybridation des attaques numériques et physiques

Les attaques ciblant les systèmes *SCADA* illustrent une hybridation croissante entre le cyberespace et le monde physique. Une action numérique, telle que la modification d'un paramètre *via* une interface de supervision, peut entraîner des effets concrets : ouverture ou fermeture d'une vanne, arrêt d'une pompe, dérèglement d'un aiguillage ferroviaire ou perturbation d'un système de distribution.

Certains groupes exploitent cette capacité pour renforcer l'impact médiatique de leurs revendications. L'existence de logiciels malveillants capables d'interagir directement avec des équipements industriels confirme que la frontière entre attaque informatique et incident physique tend à s'estomper.

Cette évolution ne se traduit pas nécessairement par une multiplication d'incidents spectaculaires, mais elle révèle une mutation stratégique de la menace, orientée vers la production d'effets tangibles, même limités, sur les infrastructures réelles.

Exemples sectoriels et acteurs impliqués

En 2025, le groupe hacktiviste *Z-ALLIANCE*, anciennement connu sous le nom de *Z-PENTEST ALLIANCE*, revendique régulièrement des intrusions dans des systèmes *SCADA* d'entités françaises. Rattaché à la mouvance pro-russe et se présentant comme originaire de Serbie, ce collectif agit dans le cadre de campagnes coordonnées, notamment celles orchestrées par *NoName057(16)*.

D'autres groupes tels que *RipperSec*, *Sector16*, *Diplomat* et *StillNet* mènent des actions similaires, partageant une posture hacktiviste affirmée et un soutien explicite à la Russie.

Ces attaques ciblent plusieurs secteurs critiques et comportent des risques potentiellement graves, parmi lesquels :

Secteur	Type d'attaque	Conséquences possibles
Énergie	Rançongiciel sur un barrage hydroélectrique	Coupure d'électricité
Transport	Piratage des feux de signalisation	Accidents, embouteillage, blocage du trafic
Eau	Manipulation des capteurs de chloration	Eau impropre à la consommation
Santé	Attaque sur les systèmes de distribution d'oxygène, fluides médicaux, gestion du froid, groupes électrogènes, etc.	Mise en danger directe des patients

À ce stade, les incidents recensés en France concernent majoritairement des installations de petite taille (parcs éoliens, micro-centrales, centres de traitement de l'eau), souvent moins sécurisées ou directement exposées à internet, ce qui en fait des cibles privilégiées.

Renforcement de la coordination nationale et européenne

Face à la multiplication des attaques visant les infrastructures industrielles, la coordination nationale et européenne s'est considérablement renforcée. Les États membres partagent de manière accrue informations et analyses afin d'identifier les menaces émergentes et les groupes ciblant des infrastructures sensibles.

Ce renforcement s'accompagne d'une consolidation du cadre juridique, notamment à travers :

- la directive NIS 2, entrée en vigueur en 2024, qui impose aux États membres de renforcer la protection des infrastructures critiques et de systématiser le signalement des incidents[22] ;
- des règlements sectoriels spécifiques, définissant des exigences adaptées aux secteurs de l'énergie, des transports ou des télécommunications.

22. Pour aller plus loin : https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2

ÉCOSYSTÈME ET MODES OPÉRATOIRES DES CYBERCRIMINELS

2 ÉCOSYSTÈME ET MODES OPÉRATOIRES DES CYBERCRIMINELS

Au-delà des tendances générales de la menace, la compréhension fine de l'écosystème cybercriminel et de ses modes opératoires est essentielle pour anticiper les attaques et adapter les réponses.

La cybercriminalité s'organise désormais selon une logique industrielle, fondée sur la spécialisation des acteurs, la segmentation des tâches et le développement de chaînes de valeur illicites. Services clés en main, modèles d'affiliation et places de marché clandestines permettent à des profils très hétérogènes d'accéder à des capacités d'attaque autrefois réservées à des acteurs experts.

Cette partie présente les principales dynamiques observées en 2025 : structuration du *cybercrime-as-a-service*, recomposition des écosystèmes clandestins, essor de nouveaux modèles économiques liés aux cryptoactifs et rôle central des forums et marchés noirs. Elle vise à éclairer les mécanismes à l'œuvre afin de mieux appréhender les risques et les évolutions de la menace.

1 | Cybercrime-as-a-Service : chaîne de valeur, rôles et services

Le modèle du *Cybercrime-as-a-Service (CaaS)* se démocratise progressivement. Il devient accessible à des profils moins expérimentés, en abaissant le niveau de compétences techniques nécessaires au passage à l'acte.

Cette évolution repose sur une spécialisation des rôles au sein de l'écosystème cybercriminel, organisée autour d'acteurs complémentaires.

On observe notamment :

- les développeurs d'*infostealers* : utilisant des logiciels malveillants dédiés au vol de données (*cookies*, identifiants, informations de session, etc.), qui alimentent massivement des bases d'accès compromis ;

- les courtiers en accès initial *(Initial Access Brokers - IAB)* : chargés de trier, enrichir et valoriser ces accès en identifiant des points d'entrée exploitables pour cibler des organisations.

Ces accès sont ensuite mobilisés par les opérateurs de rançongiciel pour conduire des attaques ciblées, maximisant la rentabilité des opérations.

Cette segmentation confère une efficacité accrue : chaque acteur occupant une place précise au sein d'une chaîne de production criminelle rationalisée. Les outils proposés dans le cadre du *CaaS* sont désormais largement accessibles et simples d'utilisation : *bots* automatisés, abonnements mensuels, documentation et, parfois, support technique.

L'essor de l'intelligence artificielle renforce cette dynamique en facilitant la production de contenus malveillants, la génération de scripts et l'optimisation des campagnes d'intrusion.

Les volumes massifs de données exfiltrées par les *infostealers* constituent une ressource abondante et constamment actualisée pour les *IAB*. Cette disponibilité permet d'identifier des cibles plus pertinentes, d'ajuster les stratégies d'extorsion (y compris le niveau des rançons) et d'accélérer la mise en œuvre des attaques. Il en résulte des opérations plus rapides, plus précises et plus impactantes, attirant de nouveaux entrants et accentuant la concurrence au sein de l'écosystème.

Cybercrime-as-a-service

Exploitation de l'IA par les cybercriminels : AI-as-a-Service

Les forums clandestins et les canaux de communication chiffrés diffusent désormais des outils et services malveillants s'appuyant sur l'intelligence artificielle, regroupés sous l'appellation *AI-as-a-Service (AIaaS)*. Ces services, polyvalents, contribuent à abaisser la barrière technique et à structurer des campagnes d'attaque plus élaborées.

L'*AIaaS* permet notamment :

- de mener des opérations d'hameçonnage à grande échelle ou très personnalisées ;
- de concevoir et d'adapter des logiciels malveillants ;
- d'exploiter des vulnérabilités ;
- de produire des contenus manipulés, tels que des *deepfakes*.

Certaines familles de maliciels recourent à des modèles de langage pour générer automatiquement du code et mettre en œuvre des techniques d'obfuscation[23] avancées afin d'échapper à la détection.

On observe également l'émergence de logiciels malveillants plus autonomes, capables d'adapter leur comportement aux dispositifs de sécurité rencontrés, rendant possible le lancement d'attaques par des profils peu expérimentés, avec un haut degré d'automatisation.

À l'image du *Cybercrime-as-a-Service (CaaS)*, les opérateurs d'*AIaaS* proposent ces outils sous forme de location, avec un accompagnement technique et des mises à jour.

La réputation des fournisseurs demeure un critère déterminant dans un environnement clandestin où la confiance conditionne la rentabilité.

Parmi les offres observées figurent notamment :

- *DarkGPT*, utilisé pour générer du code malveillant, des contenus d'hameçonnage et de désinformation ;
- *SpamGPT*, conçu pour adapter la tonalité émotionnelle des messages et accroître leur efficacité ;
- *Nytheon AI*, présenté avec une interface simplifiée, visant un public néophyte ;
- *EvilAI*, mis en avant pour ses capacités d'adaptation *via* un entraînement continu.

Alliances entre Qilin, LockBit et DragonForce

En septembre 2025, l'acteur malveillant *DragonForce*, opérateur du rançongiciel *DragonForce RaaS*, a annoncé la formation d'une coalition stratégique avec les familles de rançongiciels *LockBit* et *Qilin*. Cette alliance vise à accroître les profits, favoriser un développement collaboratif et renforcer l'influence de ces groupes au sein de l'écosystème cybercriminel.

Longtemps considéré comme l'un des plus prolifiques, *LockBit* avait été fortement perturbé à la suite d'opérations judiciaires, ayant notamment conduit à la saisie de plus de 7 000 clés de déchiffrement. Son retour, annoncé en septembre 2025 avec le lancement du programme d'affiliation *LockBit 5.0*, traduit une volonté de regagner une position centrale dans l'écosystème cybercriminel.

La constitution de cette coalition laisse présager une intensification de l'activité des groupes de rançongiciel, ainsi qu'une montée en sophistication des techniques employées.

23. Technique qui consiste à rendre un code, des données ou une information volontairement difficiles à comprendre afin d'en masquer le fonctionnement ou l'intention sans en modifier le comportement.

Ransomware-as-a-Service : une dynamique économique structurante

Le *Ransomware-as-a-Service (RaaS)* désigne un modèle dans lequel des opérateurs mettent à disposition des affiliés des outils et services clés en main permettant de conduire des attaques à des fins lucratives. Cette économie parallèle s'organise autour de marchés clandestins où s'échangent logiciels, kits d'exploitation et services associés : support technique, analyse des données volées, négociation avec les victimes ou blanchiment des fonds.

Les plateformes *RaaS* reproduisent des logiques commerciales proches de celles de services légitimes : abonnements, commissions sur les gains générés, programmes de fidélisation, etc.

En 2025, une tendance notable réside dans la convergence des modèles *RaaS* avec d'autres maliciels, rendant les attaques plus polyvalentes et plus difficiles à contrer, notamment :

RaaS + wiper :

Ajout de modules destructeurs de données (*wiper*) rendant les sauvegardes inexploitables (par exemple : *Anubis*[24]), renforçant la pression exercée sur les victimes.

Infostealers + RaaS :

Déploiement en amont d'infostealers (par exemple : *RedLine, Raccoon*) afin d'exfiltrer des données et renforcer l'extorsion.

FOCUS

ShinyHunters et les attaques contre Air France, Cartier et Chanel

Le collectif *SCATTERED SP1D3R HUNTERS* est une alliance cybercriminelle émergente en 2025, administrée par un acteur connu sous le pseudonyme *ShinyHunters*. Ses membres proviennent notamment de l'écosystème *The-Com*, regroupant de jeunes pirates informatiques anglophones.

En juin 2025, une application de l'entreprise Salesforce a été piratée par le collectif ouvrant l'accès à des informations sensibles relatives aux clients. À la suite de cette intrusion, le collectif a lancé une campagne d'extorsion visant plusieurs entreprises françaises dont Air France, Cartier, Allianz Life, LVMH et Chanel.

Les revendications se sont accompagnées de menaces de diffusion publique des données en l'absence de paiement. Pour crédibiliser leurs demandes, des échantillons ont été publiés sur des canaux Telegram dédiés. Une fois rendus publics, ces extraits ont été récupérés et réutilisés par des acteurs opportunistes.

Les données ont ensuite circulé sur les marchés clandestins, où elles ont été revendues ou partagées, alimentant une multiplication de revendications secondaires (parfois infondées ou exagérées) contre les entités concernées.

24. https://www.trendmicro.com/fr_fr/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

2 | Du cybercrime opportuniste à un écosystème professionnel structuré

Parallèlement à la démocratisation du *Cybercrime-as-a-Service (CaaS)*, l'écosystème cybercriminel connaît en 2025 une dégradation qualitative marquée des compétences et des modes opératoires. Les marchés clandestins apparaissent plus instables, plus fragmentés et traversés par des pratiques frauduleuses croissantes, ce qui fragilise la confiance entre acteurs. Cette instabilité résulte notamment de la concurrence accrue, de la multiplication d'acteurs peu qualifiés et des perturbations engendrées par les opérations judiciaires ciblant les principales plateformes.

Cette évolution ne traduit toutefois pas un affaiblissement global du cybercrime. Au contraire, elle s'accompagne d'un renforcement sélectif de certains piliers structurants, qui gagnent en maturité, en efficacité et en fiabilité.

Parmi eux figurent notamment :

- les développeurs de *malwares*, qui conçoivent des *infostealers* toujours plus performants ;

- les courtiers en accès initial (*Initial Access Brokers – IAB*), qui structurent et filtrent leurs catalogues d'accès compromis ;

- les *pentesters* criminels, capables d'exploiter rapidement ces accès avec un haut niveau d'expertise.

Cette spécialisation accrue des rôles favorise une coopération plus étroite entre les différents segments de la chaîne criminelle. Les attaques reposant sur un accès initial fiable et rapidement exploitable gagnent ainsi en efficacité, malgré l'instabilité globale du marché.

Revendications fallacieuses et réutilisation de données anciennes

Tout au long de l'année 2025, une multiplication des revendications de vols ou de diffusions de données a été observée. Une part importante de ces annonces repose toutefois sur la réutilisation de fuites anciennes déjà connues ou largement diffusées par le passé. Ces pratiques sont principalement le fait d'acteurs peu qualifiés techniquement, animés par des motivations crapuleuses.

Plusieurs comportements récurrents ont été identifiés :

- la republication d'anciennes annonces afin de maintenir une visibilité ou une réputation ;
- la réutilisation de bases de données déjà diffusées sur d'autres plateformes ;
- la présentation de preuves de compromission fictives ou générées à l'aide d'outils d'intelligence artificielle ;
- la recomposition artificielle de bases de données à partir de *combo-lists*, d'*infostealers* et de données publiques, revendiquées comme des intrusions récentes.

Dans ce contexte, l'évaluation de la crédibilité des acteurs et de l'authenticité des données devient particulièrement complexe. Les annonces trompeuses reposent souvent sur des échantillons réduits, mal structurés, erronés voire entièrement générés par l'IA. Cette dynamique contribue à brouiller la lecture de la menace.

Si ces revendications sont parfois infondées, la réutilisation répétée de données personnelles n'en demeure pas moins préjudiciable. Elle expose durablement les personnes concernées à des risques accrus d'usurpation d'identité et d'escroquerie, d'autant plus que certains utilisateurs ne procèdent pas à la modification de leurs mots de passe malgré les alertes.

Instabilités récurrentes de BreachForums et recomposition du darkweb

L'année 2025 a également été marquée par la fermeture successive de plusieurs forums cybercriminels majeurs tels que *BreachForums*, *XSS.is, Dark French Anti System, Cracked* et *Nulled*, entraînant des perturbations significatives de l'écosystème clandestin. Ces démantèlements ont provoqué des mouvements rapides de migration vers d'autres plateformes, souvent moins stables ou plus éphémères.

Les membres des forums fermés se sont principalement redéployés vers des espaces alternatifs, tout en conservant, pour certains, leurs pseudonymes afin de préserver leur capital réputationnel. Les anciennes annonces y sont fréquemment repostées, multipliant artificiellement les revendications. Des acteurs opportunistes profitent également de ces phases de transition pour s'attribuer, sans fondement, la responsabilité d'intrusions existantes.

Les administrateurs parviennent souvent à relancer leurs activités sous de nouveaux noms de domaine ou *via* d'autres infrastructures. Cette capacité de résilience illustre une nouvelle fois l'adaptabilité de l'écosystème cybercriminel, malgré la pression judiciaire constante.

FOCUS

BreachForums : trajectoire d'une plateforme structurante du cybercrime

BreachForums (également connu sous le nom de *Breached*) s'est imposé depuis 2022 comme l'une des plateformes centrales de la diffusion et de la commercialisation de données volées. Hébergé à la fois sur le *clearweb* et le *darkweb* selon ses itérations, ce forum a joué un rôle structurant dans l'écosystème cybercriminel, en particulier pour les activités liées aux fuites de données et à l'extorsion.

Genèse et montée en puissance

BreachForums apparaît en mars 2022, à la suite de la fermeture de *RaidForums* par les autorités américaines. Il se positionne rapidement comme une plateforme de remplacement, attirant une large communauté d'acteurs malveillants spécialisés dans la vente, l'échange et la diffusion de bases de données compromises.

Son succès repose sur plusieurs facteurs :

- une facilité d'accès, favorisant l'afflux d'acteurs aux profils variés ;
- une forte visibilité médiatique liée aux données mises en vente ;
- un rôle de vitrine pour les campagnes d'extorsion par la publication d'échantillons.

Une succession de perturbations judiciaires

Dès sa création, *BreachForums* fait l'objet d'une attention soutenue de la part des autorités judiciaires.

Plusieurs événements marquants jalonnent son histoire :

Novembre 2022
Compromission interne du forum, entraînant la fuite des données de ses membres.

Mars 2023
Arrestation par les autorités américaines de son fondateur et administrateur principal, connu sous le pseudonyme *Pompompurin*.

Mai 2024
Saisie du forum, de son site sur le *darkweb* et de son canal Telegram associé.

Juillet 2024
Diffusion publique de l'intégralité de la base de données d'une version antérieure du forum.

Malgré ces actions, *BreachForums* connaît plusieurs tentatives de relance sous différentes formes, illustrant la résilience de ce type de plateforme.

Recomposition et dérives vers l'extorsion

En 2025, les membres de *BreachForums* migrent vers d'autres espaces, notamment *DarkForums*, tout en maintenant des pratiques similaires. Certaines itérations du forum évoluent progressivement vers des modèles d'extorsion, fondés sur la publication graduée de données afin de faire pression sur les organisations victimes.

Cette dynamique culmine en octobre 2025, lorsqu'une nouvelle version du site, devenue essentiellement un site de fuite de données, est démantelée lors d'une opération conjointe menée par le *Department of Justice*, la Brigade de lutte contre la cybercriminalité de la préfecture de Paris (BL2C) et le Parquet de Paris (J3).

Si cette action met fin à une énième itération du forum, elle n'entraîne pas pour autant la dissolution de la communauté qui s'y était structurée. Depuis la réouverture du forum, intervenue le 13 décembre 2025, une recrudescence significative de revendications ciblant des organisations nationales est observée, s'inscrivant dans une logique manifeste de représailles à l'encontre des autorités françaises. Cette phase est en outre caractérisée par la publication massive de bases de données recyclées, issues de compromissions anciennes, réexploitées à des fins de visibilité et de revendication plutôt que de monétisation effective.

Un forum emblématique des dynamiques cybercriminelles

Sur l'ensemble de son existence, *BreachForums* a connu :

- une activité très soutenue, avec plus d'un million de messages publiés ;
- une communauté étendue, comptant plusieurs centaines de milliers de membres ;
- plusieurs opérations judiciaires majeures, menées entre 2023 et 2025.

L'histoire de *BreachForums* illustre les dynamiques caractéristiques de l'écosystème cybercriminel : capacité de résilience, recomposition rapide après les démantèlements, mais aussi fragilisation progressive de la confiance et dispersion des communautés. Elle met en lumière les limites structurelles des forums à forte visibilité, particulièrement exposés aux actions judiciaires coordonnées, tout en soulignant leur rôle central dans la diffusion massive de données compromises.

3 | Crypto-criminalité : évolutions récentes et nouveaux modèles économiques

L'essor des cryptoactifs a profondément transformé certaines formes de cybercriminalité. En 2025, la crypto-criminalité ne se limite plus à des escroqueries isolées : elle repose désormais sur des modèles économiques structurés, combinant outils techniques, ingénierie sociale et circuits financiers spécialisés.

L'essor des draineurs : une industrialisation du vol de cryptoactifs

Les draineurs se sont imposés comme un maillon central de la criminalité liée aux cryptoactifs. Proposés majoritairement sous forme de *Drainer-as-a-service (DaaS)*, ces outils permettent de vider automatiquement les portefeuilles des victimes *via* des *smart contracts* frauduleux, des transactions de signature trompeuses ou des interfaces web falsifiées.

Ce modèle repose sur une organisation fortement structurée :

- des développeurs conçoivent et maintiennent les outils techniques ;
- des affiliés sont chargés de diffuser les campagnes frauduleuses et d'attirer les victimes ;
- les revenus sont répartis automatiquement entre les différents acteurs.

Ce fonctionnement multitâche facilite l'entrée d'acteurs peu qualifiés techniquement et contribue à la massification des vols de cryptoactifs.

Vecteurs de diffusion et ingénierie sociale

Les campagnes de draineurs reposent essentiellement sur des techniques d'ingénierie sociale. Les affiliés déploient des interfaces web frauduleuses, imitant des plateformes légitimes ou des projets populaires, afin d'inciter les victimes à connecter leur portefeuille.

Pour générer du trafic, plusieurs leviers sont utilisés :

- compromission de comptes certifiés sur les réseaux sociaux ;
- campagnes publicitaires malveillantes ;
- faux événements promotionnels (*airdrops*, ventes privées).

La tactique repose sur la création d'un sentiment d'urgence ou d'opportunité pour diminuer la vigilance des cibles.

Les victimes sont incitées à signer des transactions présentées comme anodines. En réalité, ces signatures accordent aux attaquants des droits étendus leur permettant de siphonner les actifs, parfois de manière différée, rendant la fraude difficilement détectable.

Des flux financiers automatisés et difficiles à tracer

Une fois la transaction validée, le vol s'exécute de manière quasi instantanée. Les fonds sont répartis automatiquement selon des règles prédéfinies, avant d'être rapidement déplacés afin de compliquer leur traçabilité.

Cette automatisation réduit les interactions humaines, accélère les opérations et limite l'exposition des opérateurs aux risques judiciaires.

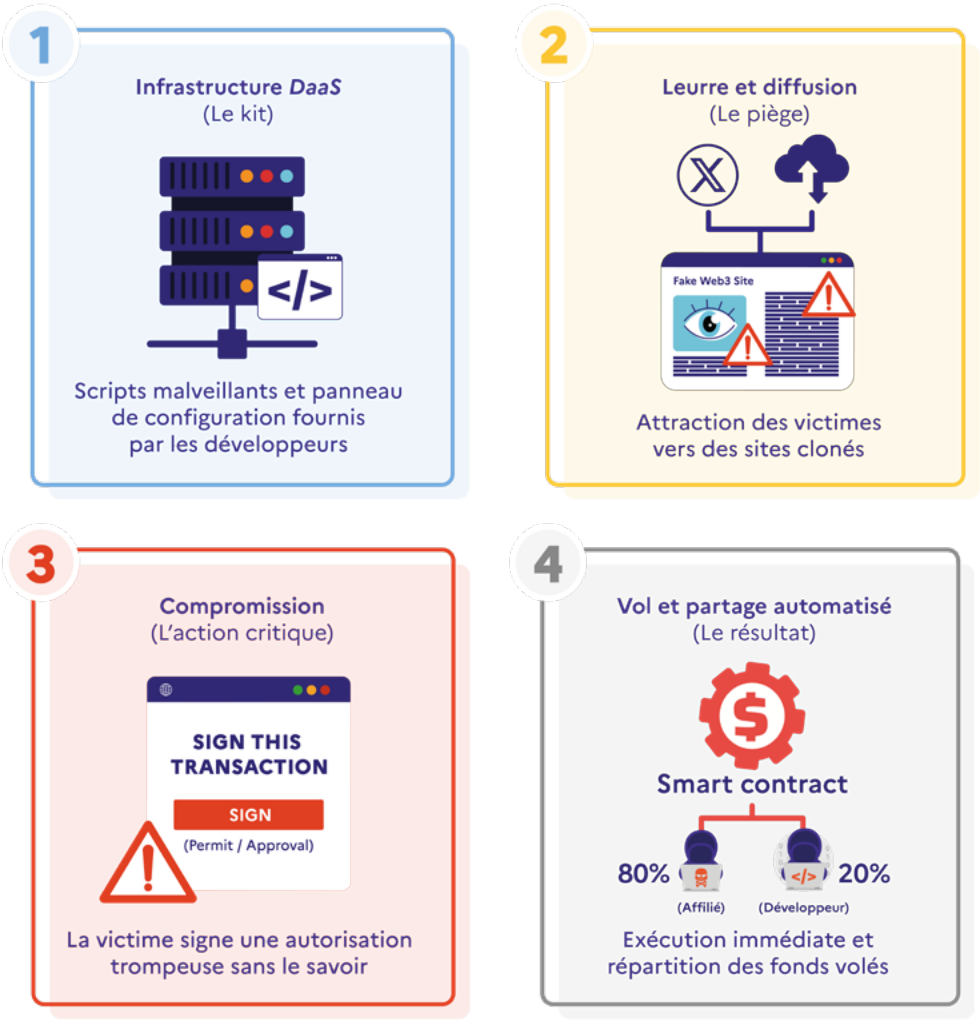


Schéma représentant le mécanisme d'un draineur de portefeuille de cryptoactifs

FOCUS

Plateformes d'échange sous pression : l'exemple de Bybit

Le 21 février 2025, la plateforme d'échange Bybit a été victime d'un vol estimé à 1,5 milliard de dollars (USD) en cryptoactifs, constituant à ce jour le plus important vol de ce type.

L'incident illustre plusieurs tendances majeures :

- le ciblage prioritaire des plateformes centralisées ;
- la rapidité accrue des opérations de blanchiment ;
- l'abandon progressif de certaines techniques d'anonymisation jugées trop lentes face aux volumes en jeu.

Les escroqueries à la fausse romance : une criminalité à forte dimension humaine

Les escroqueries à la fausse romance combinent manipulation émotionnelle et fraude financière.

Elles reposent sur un processus en plusieurs étapes :

- prise de contact *via* les réseaux sociaux ou applications de rencontre ;
- construction d'une relation de confiance sur plusieurs semaines ;
- orientation vers de fausses opportunités d'investissement, souvent liées aux cryptoactifs ;
- siphonnage progressif des fonds, puis disparition des escrocs.

Ces fraudes s'inscrivent dans une logique industrielle, reposant sur des centres organisés, principalement situés en Asie du Sud-Est, où des milliers de personnes seraient contraintes de participer à ces activités dans des conditions proches de l'esclavage.

Les fonds volés font ensuite l'objet de circuits de blanchiment complexes, combinant cryptoactifs, plateformes d'échange et réseaux de comptes intermédiaires.

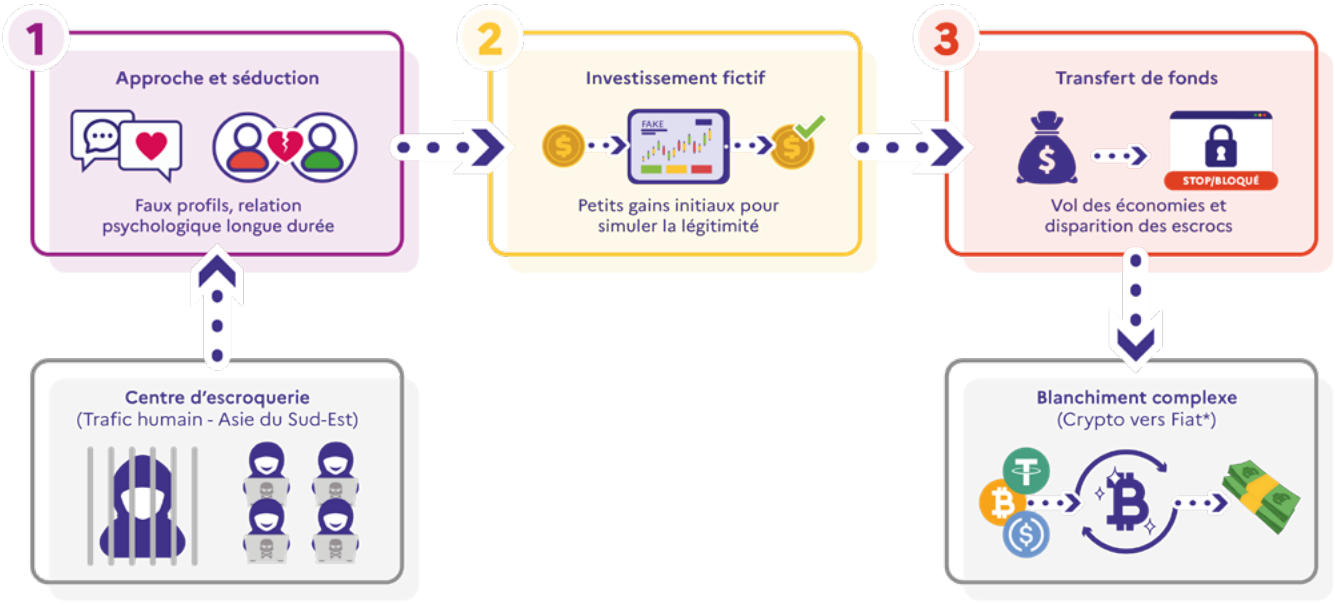


Schéma du mécanisme global de l'escroquerie à la fausse romance

* Monnaie ayant cours légal

Usurpation d'identité et infiltration professionnelle

Un phénomène particulièrement préoccupant concerne l'infiltration d'entreprises par des travailleurs informatiques nord-coréens opérant sous de fausses identités. Selon des estimations relayées par Microsoft[25], plusieurs milliers de profils seraient actifs à l'échelle mondiale.

Ces individus utilisent des identités numériques falsifiées pour intégrer des entreprises, notamment dans les secteurs technologiques et financiers.

Les objectifs sont doubles :

- financement du régime nord-coréen ;
- espionnage ou sabotage, une fois l'accès aux systèmes obtenu.

Ce mode opératoire illustre l'hybridation croissante entre cybercriminalité, criminalité financière et stratégies étatiques.

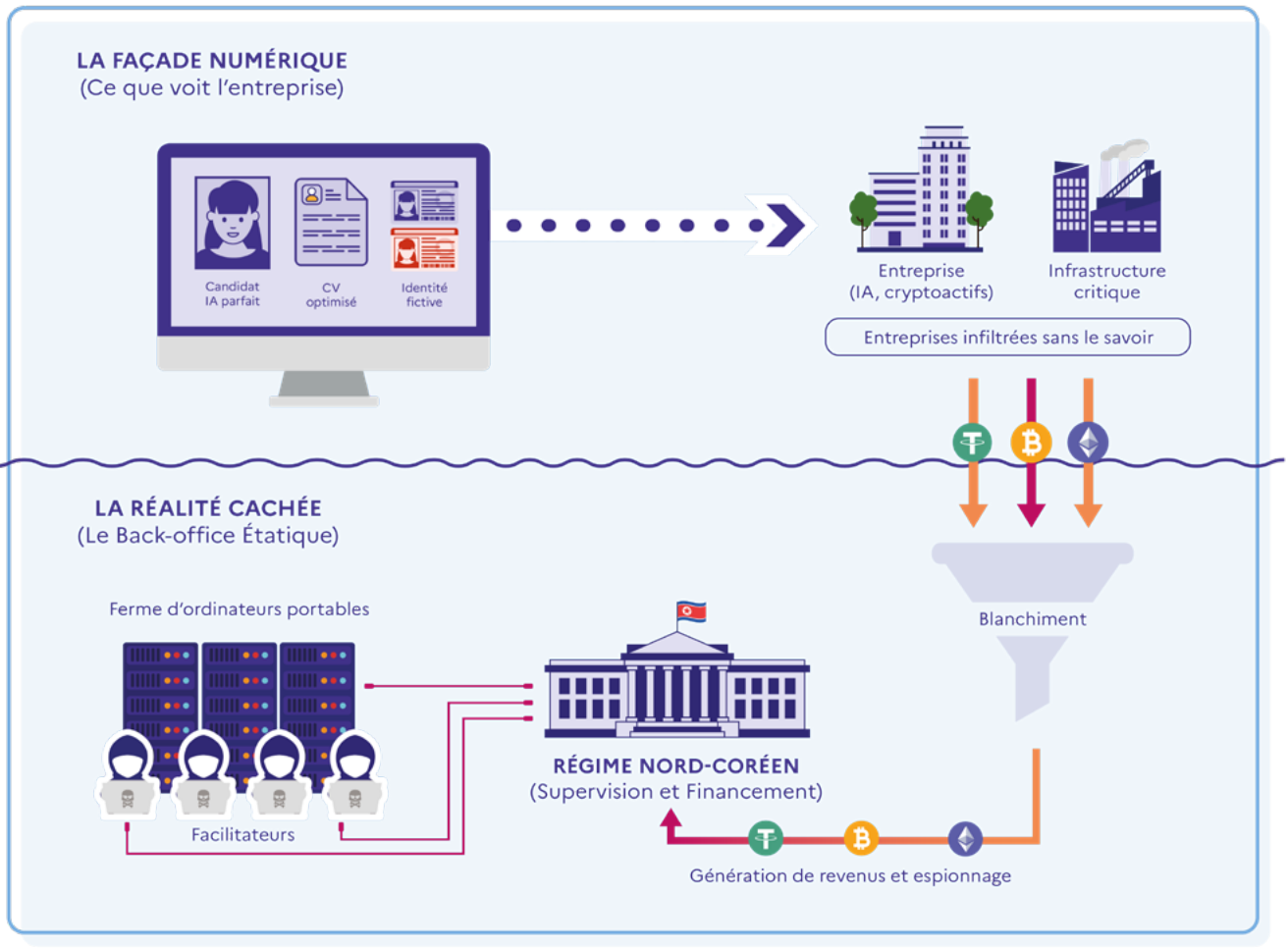


Schéma de l'employé infiltré dans une entreprise innovante

Cryptoactifs et risques physiques : une menace hybride

Enfin, l'année 2025 a été marquée par une recrudescence d'enlèvements ciblant des professionnels du secteur des cryptoactifs, pour obtenir une rançon. Cette évolution traduit un basculement vers une criminalité hybride, mêlant violences physiques et exploitation des mécanismes numériques notamment les fuites de données.

Face à cette menace, le commandement du ministère de l'Intérieur dans le cyberespace a coordonné un dispositif national associant prévention, sécurisation des acteurs exposés et actions de sensibilisation, en lien avec l'ADAN[26].

25. https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/
26. https://www.adan.eu/publication/newsletter-de-ladan-juin-2025/

CRYPTOACTIFS : LES BONS RÉFLEXES POUR SE PROTÉGER

PRÉVENTION ET SÉCURITÉ AU QUOTIDIEN

1 RÉDUIRE SON EXPOSITION

- Ne pas afficher ses avoirs ou gains en ligne
- Éviter les captures d'écran de portefeuilles
- Rester discret sur ses activités crypto

2 SÉCURISER SES ACCÈS

- Mots de passe et identifiants uniques et dédiés
- Authentification forte
- Délai déterminé pour le déblocage de montants importants

3 DÉJOUER LES ESCROQUERIES

- Se méfier des offres trop attractives
- Ne pas cliquer sur des liens non vérifiés
- Ne jamais partager ses clés privées

4 RESTER VIGILANT

- Éviter d'évoquer ses avoirs en public
- Attention aux informations partagées hors ligne
- La discrétion est une protection

EN CAS D'URGENCE, composez le **17** (24/7)

POUR SIGNALER EN LIGNE des faits rendez-vous sur **Ma Sécurité** Application Grand Public (24/7)

MOINS D'EXPOSITION, PLUS DE PROTECTION

4 | Forums et marchés noirs en mutation

Les forums cybercriminels constituent l'un des piliers structurants de l'économie souterraine numérique. Ils jouent un rôle central dans la rencontre, l'échange et la coordination des acteurs malveillants. On y retrouve l'ensemble des profils clés du cybercrime : vendeurs d'accès initiaux, opérateurs de rançongiciels, développeurs de logiciels malveillants, revendeurs de données dérobées, administrateurs de *botnets* ou encore groupes spécialisés dans l'extorsion.

Au-delà de leur fonction commerciale, ces plateformes remplissent également un rôle social et formatif. Elles permettent à des acteurs moins expérimentés d'acquérir des compétences, de se familiariser avec des outils offensifs et d'intégrer progressivement des réseaux criminels plus structurés.

Une pression judiciaire accrue et des démantèlements répétés

Depuis plus d'une décennie, la coopération judiciaire internationale s'est considérablement renforcée. Plusieurs opérations coordonnées ont conduit aux démantèlements de forums emblématiques tels que *RaidForums*, *BreachForums, Genesis Market*, puis en 2025 *Cracked* et *Nulled* dans le cadre de l'opération TALENT, menée sous l'égide d'Europol avec le soutien de partenaires internationaux, dont le FBI et les autorités françaises.

Ces actions ont profondément perturbé les équilibres de l'écosystème cybercriminel, sans toutefois entraîner sa disparition. Elles ont, en revanche, accéléré sa transformation.

Instabilité, fragmentation et recomposition permanente

L'année 2025 met en évidence trois dynamiques majeures :

- une instabilité croissante des forums cybercriminels. Chaque opération judiciaire entraîne la fermeture ou la saisie d'une plateforme, rapidement suivie par l'apparition de nouveaux forums, souvent éphémères ;
- une érosion progressive de la confiance. La multiplication des démantèlements, des infiltrations et des escroqueries internes fragilise la crédibilité de ces espaces. Certains acteurs s'en détournent, estimant les risques trop élevés ;
- une fragmentation accrue de l'écosystème. Les grandes plateformes à forte audience cèdent progressivement la place à une constellation de forums plus restreints, de canaux privés ou de groupes hébergés sur des messageries chiffrées.

Typologie des forums et spécialisation des usages

Les forums cybercriminels se distinguent par leur positionnement et leur niveau d'exigence.

Les forums techniques russophones (tels que *RAMP, Exploit.in* ou *XSS.is*) occupent une place prédominante dans les activités les plus sophistiquées. Leur accès est restreint et conditionné à des critères stricts (cooptation, réputation, capacités techniques, paiement). Ils concentrent des acteurs expérimentés et des échanges de haut niveau, notamment autour du développement de *malwares*, de l'exploitation de vulnérabilités et des modèles économiques du *Cybercrime-as-a-service*.

À l'inverse, les forums généralistes (comme *Cracked, Nulled ou BreachForums*) jouent un rôle de porte d'entrée. Ils attirent un public hétérogène, mêlant cyberdélinquants opportunistes et acteurs plus aguerris. Le volume d'annonces y est important, mais la qualité et la fiabilité des contenus sont très variables.

D'autres espaces comme *Dread Forum* occupent une position intermédiaire. Hébergés sur le réseau Tor, ils servent à la fois de lieu de repli, de relais d'information et de point de convergence pour différentes communautés, dont des groupes francophones.

Organisation interne et mécanismes de confiance

Malgré leur diversité, ces forums présentent une architecture interne similaire. Ils s'articulent autour de sections dédiées à la vente de services, aux fuites de données, aux échanges techniques et aux discussions communautaires.

Dans un environnement fondé sur l'anonymat, la réputation constitue un élément central. Elle repose sur l'historique des transactions, la qualité des contributions et le respect des engagements.

Pour encadrer ces relations, les forums mettent en place des mécanismes de gouvernance informelle : modération, arbitrage des litiges et exclusion des profils jugés peu fiables.

Le recours à des services de séquestre *(escrow)* est fréquent. Ces tiers de confiance temporaires sécurisent les transactions, en particulier lors de ventes sensibles telles que les accès initiaux ou les bases de données volées.

Circuits financiers et monétisation

Les transactions s'effectuent quasi exclusivement *via* des cryptoactifs. Si le Bitcoin (BTC) demeure largement utilisé, de nombreux forums privilégient désormais des monnaies plus difficiles à tracer, comme le Monero (XMR). Ces flux financiers s'inscrivent dans des circuits complexes, impliquant plateformes d'échange, services de conversion et réseaux de mules.

Les opérations judiciaires démontrent que la saisie des avoirs numériques constitue un levier particulièrement efficace pour fragiliser durablement ces écosystèmes.

Effets des opérations judiciaires sur l'écosystème

Les démantèlements successifs produisent des effets ambivalents. À court terme, ils perturbent fortement les activités et provoquent des migrations massives. À moyen terme, ils renforcent paradoxalement la valeur des espaces perçus comme plus sûrs, au bénéfice des forums fermés et des canaux privés.

Cette dynamique alimente un mouvement constant entre centralisation et dispersion, caractéristique d'un écosystème à la fois résilient et vulnérable.

Vers une économie de la donnée recyclée

L'une des évolutions les plus marquantes observées en 2025 est l'essor d'une économie de la donnée recyclée. Les mêmes bases de données circulent sur plusieurs plateformes, parfois présentées comme des fuites récentes alors qu'elles résultent d'agrégations d'anciennes compromissions.

La valeur ne réside plus uniquement dans la nouveauté de la donnée, mais dans sa mise en forme, sa contextualisation et son potentiel d'exploitation. Cette pratique alimente les revendications opportunistes et complique l'analyse de la menace.

Place des communautés francophones

Les communautés francophones s'insèrent dans cet écosystème. Présentes sur des forums internationaux et des espaces dédiés, elles constituent à la fois des lieux d'échange, des points d'entrée pour des acteurs moins expérimentés et des relais pour des modèles criminels importés.

L'observation de ces espaces permet d'anticiper certaines évolutions, d'identifier des acteurs émergents et de documenter les chaînes complètes d'attaque, de la compromission initiale à la monétisation.

CADRE JURIDIQUE, COOPÉRATION INTERNATIONALE ET ACTIONS DE LUTTE

3 CADRE JURIDIQUE, COOPÉRATION INTERNATIONALE ET ACTIONS DE LUTTE

La cybercriminalité s'inscrit dans des dynamiques transnationales, où les acteurs malveillants exploitent la rapidité des échanges numériques, la déterritorialisation des infrastructures et les écarts de réglementation pour conduire leurs activités. Ce contexte impose une adaptation constante des réponses publiques, tant sur le plan juridique qu'opérationnel.

Cette troisième partie présente les évolutions du cadre normatif, les mécanismes de coopération internationale et les principales actions de lutte conduites en 2025. Elle met en lumière la manière dont les autorités françaises, en lien étroit avec leurs partenaires européens et internationaux, renforcent leurs capacités d'intervention afin de faire face à une menace cyber en mutation permanente.

1 | Un cadre juridique en constante évolution

L'année 2025 est marquée par une dynamique de renforcement et d'adaptation du cadre juridique applicable à la lutte contre la cybercriminalité. Cette évolution répond à un double impératif : d'une part, doter les autorités compétentes de moyens d'enquête adaptés à des menaces numériques toujours plus complexes et transnationales ; d'autre part, garantir un encadrement juridique respectueux des libertés fondamentales et de la protection des données personnelles.

Un cadre international en consolidation

Sur le plan international, la signature par la France de la Convention des Nations Unies contre la cybercriminalité, les 25 et 26 octobre 2025 à Hanoï, marque une étape structurante.

Ce texte constitue le premier instrument onusien visant à harmoniser les législations nationales et à renforcer la coopération judiciaire internationale en matière de cybercriminalité. Inspiré de la Convention de Budapest de 2001, il en reprend les principes essentiels tout en intégrant des dispositions adaptées à l'ampleur actuelle des menaces et aux enjeux contemporains de coopération entre États.

Cette convention traduit un équilibre recherché entre l'efficacité de la lutte contre la cybercriminalité, la fluidité des échanges d'informations entre autorités judiciaires et la préservation des droits fondamentaux. Son entrée en vigueur interviendra après ratification par quarante États signataires.

Renforcement des moyens procéduraux des enquêteurs

Au niveau national, la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic marque un tournant dans la stratégie de lutte contre la criminalité organisée. Elle renforce significativement les capacités d'investigation des enquêteurs, y compris dans le champ cyber.

Elle élargit notamment le recours aux techniques spéciales d'enquête, en autorisant, sous contrôle judiciaire strict, la captation d'images et de sons par activation à distance d'équipements électroniques fixes ou mobiles[27], ainsi que l'usage d'*IMSI-catchers* dans des lieux privés[28]. Ces dispositifs, compte tenu de leur caractère intrusif, ont fait l'objet d'un encadrement précis par le Conseil constitutionnel, qui a rappelé la nécessité de les réserver aux infractions les plus graves, commises en bande organisée et passibles de peines élevées.

La loi renforce également le cadre de l'enquête sous pseudonyme, en autorisant l'utilisation de technologies permettant de modifier la voix ou l'apparence physique des enquêteurs afin de préserver leur anonymat[29]. Cette évolution marque l'introduction explicite de technologies d'hypertrucage dans la procédure pénale française, exclusivement à des fins de protection et d'efficacité des investigations[30].

27. Les infractions visées aux 1° à 6° et 11° à 12° de l'article 706-73 du Code de procédure pénale, ainsi que pour leur blanchiment et l'association de malfaiteurs en vue de leur préparation.
28. Art. 706-95-20, III du Code de procédure pénale.
29. Art. 230-46 du Code de procédure pénale.
30. Art. 3 du règlement européen sur l'intelligence artificielle (RIA).

Encadrement de l'intelligence artificielle

Le règlement européen sur l'intelligence artificielle (RIA), entré en vigueur le 2 août 2024, prévoit une mise en application échelonnée de ses dispositions. L'année 2025 marque ainsi plusieurs étapes de sa mise en œuvre effective. Depuis le 2 février 2025, sont prohibés les systèmes d'IA à risque inacceptable, c'est-à-dire ceux dont les usages portent atteinte aux droits fondamentaux (comme le *social scoring*). À ce titre, de nouvelles obligations s'imposent aux employeurs afin de garantir un niveau minimal de compétences en IA de leur personnel.

Depuis le 2 août 2025, sont applicables les dispositions relatives aux modèles d'IA à usage général, imposant aux fournisseurs des exigences accrues de transparence et de responsabilité.

Le 22 juillet 2025, la CNIL a publié ses recommandations sur le développement des systèmes d'IA. Ces recommandations ont été élaborées en cohérence avec le règlement européen, puisque le RIA et le RGPD s'appliquent conjointement lorsque des données personnelles sont utilisées pour concevoir ou entraîner des systèmes d'IA.

Encadrement des cryptoactifs

Le cadre juridique applicable aux cryptoactifs s'est également renforcé. Entré en vigueur le 30 décembre 2024, le règlement européen *MiCA (Markets in Crypto-Assets)* vise à réguler le marché des cryptoactifs et à protéger les investisseurs. Pour en assurer la mise en œuvre effective en droit français, le décret n° 2025-169 du 21 février 2025 a modifié la partie réglementaire du Code monétaire et financier, harmonisant ainsi le régime national avec le droit européen.

Il fixe notamment le montant des contributions dues à l'Autorité des marchés financiers (AMF) par les prestataires de services sur cryptoactifs (PSCA) et prévoit une période transitoire, courant jusqu'au 30 juin 2026, concernant la procédure d'enregistrement des prestataires de services sur actifs numériques.

Apports jurisprudentiels récents

Chambre criminelle, 17 juin 2025, n° 24-87.110

Une décision importante rendue par la Chambre criminelle de la Cour de cassation (17 juin 2025, n° 24-87.110) est venue préciser la portée territoriale de la captation de données informatiques prévue à l'article 706-102-1 du Code de procédure pénale.

Dans cette affaire, un dispositif de captation implanté dans le téléphone d'un suspect permettait aux enquêteurs d'accéder en temps réel aux données de l'appareil, y compris lorsque celui-ci se trouvait hors du territoire national. Le mis en examen soutenait que cette opération, réalisée sans autorisation de l'État concerné, violait le principe de souveraineté.

La Cour de cassation a rejeté cet argument : le simple transit des données par un réseau étranger ne constitue pas une atteinte à la souveraineté de cet État et la captation reste régulière dès lors qu'elle ne requiert aucune assistance technique d'un État tiers. Toutefois, lorsque la captation vise un support localisé dans un État membre de l'Union européenne, s'impose le respect des obligations de notification prévues à l'article 31 § 1, de la directive 2014/41/UE relative à la décision d'enquête européenne. En effet, selon une interprétation de la Cour de justice de l'Union européenne, la captation informatique s'assimile à une interception de télécommunications (CJUE, 30 avril 2024, M. N., C-670/22), et est donc soumise, à l'instar de cette dernière, à l'obligation de notification.

Cette décision clarifie le cadre juridique des captations informatiques transfrontalières. En écartant l'exigence d'une autorisation préalable de l'État étranger, elle facilite la mise en œuvre des captations de données à l'étranger et renforce concrètement les capacités d'enquête des autorités nationales.

2 | Coopération internationale et priorités européennes (EMPACT 2026-2029)

Face à une cybercriminalité largement déterritorialisée, la coopération internationale constitue un levier indispensable de l'action publique. Elle permet d'articuler les capacités nationales avec des mécanismes de coordination européens et internationaux, afin de cibler des menaces qui dépassent, par nature, les frontières étatiques.

L'inscription de la France dans les priorités européennes EMPACT

L'action du ministère de l'Intérieur s'inscrit pleinement dans le cadre de la plateforme européenne *EMPACT (European Multidisciplinary Platform Against Criminal Threats)*, pilotée par Europol. *EMPACT* constitue le dispositif central de coordination de la lutte contre la criminalité grave et organisée au sein de l'Union européenne.

Ce mécanisme repose sur des cycles pluriannuels définis à partir de l'évaluation de la menace produite par Europol, le rapport *SOCTA (Serious and Organised Crime Threat Assessment)*, publié tous les quatre ans. Ce rapport permet aux États membres d'identifier collectivement les formes de criminalité les plus préoccupantes et de définir des priorités opérationnelles communes, déclinées ensuite en plans d'action opérationnels *(OAP)* assortis de financements dédiés. Les *OAP* sont ensuite déclinés en actions opérationnelles *(OA)*.

Le rapport *SOCTA* publié en mars 2025 souligne le caractère désormais transversal et structurant du cyberespace dans l'ensemble des formes de criminalité organisée. Il met en évidence le rôle central des infrastructures numériques, qui facilitent la mise à l'échelle rapide des activités criminelles, ainsi que l'effet accélérateur de technologies telles que l'intelligence artificielle.

Des priorités cyber renforcées pour le cycle 2026-2029

Parmi les menaces identifiées comme connaissant la croissance la plus rapide au niveau européen, trois relèvent directement de la cybercriminalité :

Les cyberattaques

Les escroqueries en ligne

L'exploitation sexuelle des mineurs en ligne

Depuis le 1er janvier 2026, ces trois priorités font l'objet de plans d'action opérationnels spécifiques, tous pilotés par des services du ministère de l'Intérieur français (respectivement l'OFAC[31], l'UNCyber[32] et l'OFMIN[33]). Cette configuration inédite traduit la reconnaissance, à l'échelle européenne, de l'expertise française dans la lutte contre la cybercriminalité, tant sur le plan opérationnel que stratégique.

Dans ce cadre, la France assurera également la conduite de plusieurs *OA* ciblées portant notamment sur :

- l'utilisation de l'intelligence artificielle à des fins criminelles ;

- les infrastructures cybercriminelles ;

- le blanchiment par cryptoactifs ;

- les escroqueries en ligne liées à certaines zones géographiques ;

- les échanges de contenus pédocriminels *via* des réseaux *peer-to-peer*.

Coopération internationale et renforcement capacitaire

Au-delà des actions opérationnelles, la coopération internationale en matière de cybercriminalité poursuit également un objectif de renforcement des capacités des États partenaires. Cette approche vise à améliorer durablement la sécurité intérieure, en favorisant l'élévation du niveau de compétence des services d'enquête étrangers confrontés aux mêmes menaces.

Dans cette logique, la France contribue activement au développement de structures de formation spécialisées, notamment à travers la mise en place d'Écoles nationales à vocation régionale dédiées au cyber (ENVR)[34]. Ces dispositifs, soutenus par la coopération de sécurité et de défense, accueillent des formateurs issus des forces de sécurité intérieure françaises et favorisent le partage de savoir-faire opérationnel.

Le Centre national de formation à la lutte contre la cybercriminalité du ministère de l'Intérieur (CNFCYBER-MI), composante du COMCYBER-MI, joue un rôle central dans ce dispositif. Il intervient à la fois dans la professionnalisation des formateurs, le développement de compétences rares et la conduite de sessions de formation européennes, notamment dans le cadre d'EMPACT ou sous labellisation de CEPOL[35]. Le CNFCYBER-MI participe également aux travaux du groupe d'experts *ECTEG (European Cybercrime Training and Education Group)*, chargé de développer des contenus de formation communs au niveau européen.

31. Office anti-cybercriminalité (direction nationale de la police judiciaire – Police nationale).
32. Unité nationale cyber de la Gendarmerie nationale.
33. Office des mineurs (direction nationale de la police judiciaire – Police nationale).
34. La première fut celle de Dakar au Sénégal, créée dès 2018. Une seconde mise en place à Podgorica au Monténégro, appelée « Centre des capacités cyber des Balkans occidentaux » (C3BO), fut inaugurée en décembre 2024.
35. Agence européenne pour la formation des services répressifs.

3 | Retours d'enquêtes majeures (OFAC, UNCyber, et BL2C)

L'année 2025 a été marquée par une intensification des actions judiciaires et opérationnelles contre les infrastructures et les acteurs structurants de la cybercriminalité. Ces enquêtes illustrent la capacité des services français à agir de manière coordonnée, en mobilisant à la fois les leviers nationaux et les mécanismes de coopération internationale.

OPÉRATION XSS.IS

Nom : *XSS.is*

Apparition : *XSS.is*, dont le nom de domaine a été enregistré en septembre 2018, est le successeur du forum *DaMaGeLaB* (fondé en 2005) après l'arrestation de son administrateur

Communauté : russophone

Technicité : élevée

Sécurité opérationnelle : élevée

Activités : échanges et ventes de *malwares*, de vulnérabilités, d'accès initiaux, ventes de données sensibles, *bulletproof hosting*, *botnets*, kits d'hameçonnage, etc.

Nombre de membres : environ 50 000 membres

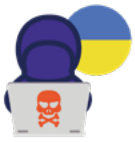
Les faits :

L'année 2025 a constitué un tournant dans la lutte contre les forums cybercriminels russophones les plus techniques. Le forum *XSS.is*, actif depuis près de vingt ans et regroupant plusieurs dizaines de milliers de membres, constituait une place centrale pour l'échange de *malwares*, de vulnérabilités, d'accès initiaux et de services facilitant les attaques à grande échelle.

Grâce à un important travail d'investigation, d'analyse technique et de coopération judiciaire internationale, les enquêteurs ont identifié l'un des administrateurs centraux du forum, acteur clé de la coordination interne de cette place de marché criminelle.

L'opération conduite en Ukraine, avec l'appui des autorités locales et la mobilisation des enquêteurs français de la Brigade de lutte contre la cybercriminalité (BL2C), a permis l'interpellation de cet individu et de perturber significativement l'écosystème criminel lié à *XSS.is*, en coupant un nœud de confiance essentiel au fonctionnement des réseaux russophones structurés autour de ce type de plateformes.

LES RÉSULTATS DE L'OPÉRATION



1 administrateur interpellé en Ukraine

1 domaine saisi rendant le site temporairement indisponible

EFFECTIFS ENGAGÉS

L'enquête ouverte dès 2021 a été pilotée par la section J3 du Parquet de Paris et confiée à la BL2C. Les enquêteurs français ont réalisé des investigations techniques dès 2021, notamment sur un serveur de communication du forum. L'opération a mobilisé les autorités ukrainiennes, notamment le *Sluzhba Bezpeky Ukrayiny (SBU)*, avec le soutien opérationnel d'Europol.

LES PRINCIPAUX ACTEURS DE LA COOPÉRATION INTERNATIONALE

BL2C

SBU

Europol

OPÉRATION VOLS DE VÉHICULES ET REPROGRAMMATION DE CLÉS

L'année 2025 a mis en lumière la professionnalisation des réseaux de vol de véhicules, qui délaissent les méthodes d'effraction classiques au profit d'intrusions informatiques ciblées. L'alerte a été donnée à la suite de la détection d'activités suspectes sur les systèmes d'information d'un constructeur automobile majeur : des consultations ciblées de données techniques précises intervenaient systématiquement peu de temps avant le vol des véhicules concernés.

Ce mode opératoire repose sur l'exploitation préalable d'informations constructeurs sensibles. En accédant frauduleusement à ces bases de données, les auteurs extraient les codes nécessaires à la reprogrammation de clés, revendus ensuite *via* des messageries chiffrées à des équipes de terrain. Pour accéder au véhicule, celles-ci recourent à une effraction mécanique (bris de custode, portière forcée) ou électronique (brouilleur, attaque relais), avant de générer un double de clé sans laisser de trace d'effraction apparente. Les véhicules ainsi dérobés alimentaient également des réseaux de criminalité organisée : règlements de comptes, vols à main armée, trafic vers l'étranger.

L'enquête :

L'enquête a permis de démontrer que les auteurs agissaient comme facilitateurs pour d'autres réseaux criminels, en leur fournissant des codes de reprogrammation extraits frauduleusement. La revente s'organisait sur des canaux Telegram, dont les flux financiers ont été minutieusement analysés. L'analyse des transactions, mêlant numéraire et actifs numériques, a permis d'identifier une dizaine d'individus opérant depuis le territoire national. Les interpellations simultanées ont été rendues possibles grâce au maillage territorial de la gendarmerie en région, en lien étroit avec les services de sécurité du constructeur impacté.

LES RÉSULTATS DE L'OPÉRATION

10 interpellations en France

2 placements en détention provisoire

3 mis en cause placés sous contrôle judiciaire

1 véhicule saisi

8 000 euros de cryptoactifs et **13 000** euros en numéraire saisis

EFFECTIFS ENGAGÉS

L'enquête, initiée en 2024, a été conduite par les services spécialisés en cybercriminalité sous la direction de la juridiction compétente (section J3 du Parquet de Paris). Les investigations techniques ont été réalisées en collaboration avec les services de sécurité du constructeur impacté, permettant de sécuriser les serveurs de communication et d'identifier les accès illégitimes.

LES PRINCIPAUX ACTEURS DE LA COOPÉRATION INTERNATIONALE

UNCyber

Magistrats spécialisés

ESCROQUERIES NUMÉRIQUES ET CRIMINALITÉ FINANCIÈRE ORGANISÉE : FAUX INVESTISSEMENTS CRYPTOACTIFS

Les faits :

Fin octobre 2025, l'UNCyber a démantelé un vaste réseau criminel international impliqué dans des escroqueries aux faux investissements en cryptomonnaies sous la direction de la JUNALCO. Les victimes, attirées par de fausses plateformes promettant des rendements élevés, effectuaient des virements sans pouvoir récupérer leurs fonds. Près de 700 millions d'euros ont été blanchis par ce réseau.

L'enquête :

L'enquête, ouverte en 2023, était conduite sous la direction de la JUNALCO. Celle-ci était menée par l'UNCyber en coopération avec les autorités belges et chypriotes, avec le soutien d'Eurojust. Des interpellations ont eu lieu dans plusieurs pays d'Europe, mettant fin à l'activité criminelle.

Les résultats :

- 9 interpellations à Chypre, en Espagne et en Allemagne ;
- Saisie de 800 000 euros sur des comptes bancaires, 415 000 euros en cryptoactifs, 300 000 euros en numéraire, ainsi que de montres de luxe.

PRISON BREAK

Les faits :

En mai 2025, dans le cadre de l'opération Prison Break, 66 lieux de détention sur le territoire national ont été perquisitionnés afin de détecter et saisir les téléphones miniatures introduits clandestinement en détention.

L'enquête :

Cette enquête, ouverte en 2024, a été menée conjointement par la BL2C et l'UNCyber, avec le soutien de l'administration pénitentiaire. Les téléphones miniatures ciblés par l'opération judiciaire étaient vendus comme indétectables aux portiques d'entrée des lieux de détention. Ils servaient à commettre des délits et crimes depuis les cellules des détenus.

Les résultats :

- 164 saisies de téléphones dont 88 miniatures ;
- 200 personnes entendues dont 17 sous le régime de la garde à vue ;
- 367 cellules perquisitionnées ;
- 500 téléphones destinés à la vente et 70 000 euros en espèces saisis.

VOLS DE VÉHICULES PAR LE BIAIS DE DISPOSITIFS TECHNIQUES

Les faits :

En novembre 2025, un réseau international de fabrication et de vente de dispositifs techniques facilitant le vol de nombreux modèles de véhicules a été démantelé. Celui-ci exportait ce type d'appareils partout en Europe et dans le monde.

L'enquête :

L'enquête, ouverte en 2023, a été confiée à l'UNCyber. Celle-ci révèle que le réseau de malfaiteurs vendait des dispositifs de déverrouillage et de démarrage de véhicules par le biais de messageries chiffrées. L'opération judiciaire a été conduite en France et en Italie par l'intermédiaire d'Eurojust.

Les résultats :

- 5 interpellations en France ;
- 1 million d'euros d'équipements saisis ;
- 38 000 euros en espèces et 76 000 euros sur comptes saisis ;
- 6 véhicules saisis.

DÉMANTÈLEMENT DE BREACHFORUMS

Les faits :

En juin 2025, quatre pirates informatiques français ont été interpellés pour leur implication dans l'administration du forum *BreachForums*, spécialisé dans la vente de données dérobées. Ces interpellations interviennent quelques semaines après le démantèlement du site par les autorités américaines en avril 2025.

L'enquête :

L'enquête, menée par la BL2C en coopération étroite avec le FBI, fait suite aux multiples démantèlements de *BreachForums*. Les quatre suspects interpellés en France étaient impliqués dans l'administration technique du forum. Ils contribuaient à maintenir *BreachForums* opérationnel malgré les précédents démantèlements.

Les résultats :

- 4 interpellations réalisées en France ;
- Mise hors ligne du forum.

DROGUES DE SYNTHÈSE VENDUES SUR LE DARKNET

Les faits :

En février 2025, l'UNCyber a démantelé un réseau de trafic de drogues de synthèse sur le *darknet*. Opéré depuis 2022, ce réseau proposait à la vente des produits stupéfiants tels que de la MDMA, 3-MMC, 2-CB, LSD, ecstasy, méthamphétamine et cocaïne. La plateforme aurait réalisé plus de 3 700 ventes depuis juillet 2024.

L'enquête :

L'enquête a débuté avec une cyberpatrouille en juillet 2022 qui a identifié un profil suspect fortement actif sur le *darknet*. Les investigations de l'UNCyber ont permis de localiser et d'interpeller plusieurs suspects dans l'agglomération grenobloise et d'analyser les flux financiers liés aux cryptomonnaies.

Les résultats :

- 5 individus interpellés ;
- 20,7 kg de drogues de synthèse saisis pour une valeur estimée à 400 000 euros ;
- Saisie de matériel de conditionnement, 4 200 timbres postaux et 6 373 enveloppes destinées à l'expédition ;
- À l'issue des gardes à vue : 4 personnes mises en examen, 2 en détention provisoire et 2 sous contrôle judiciaire.

ENDGAME (PHASE 2025)

Les faits :

L'opération internationale ENDGAME s'est intensifiée en 2025 avec deux vagues majeures (mai et novembre) visant à démanteler les infrastructures de diffusion de *malwares* (*droppers*[36] et *infostealers*). Ces réseaux servaient de porte d'entrée (accès initiaux) pour des cyberattaques complexes, notamment des déploiements de rançongiciels. Les souches neutralisées incluent *BumbleBee, Qakbot, Rhadamanthys* et *VenomRAT*.

L'enquête :

Coordonnée par Europol et Eurojust, l'enquête a mobilisé une coalition internationale. En France, l'opération a été pilotée par l'OFAC dans le cadre d'une co-saisine avec la BL2C et l'UNCyber, sous la direction de la section J3 du Parquet de Paris. Les investigations ont permis de cartographier des milliers de serveurs de commande et de contrôle *(C2)* à travers le monde.

Les résultats :

- Phase de mai 2025 : 300 serveurs mis hors service, 650 domaines neutralisés, 20 mandats d'arrêt internationaux et 3,5 millions d'euros saisis en cryptoactifs ;
- Phase de novembre 2025 : 1 025 serveurs neutralisés, 20 domaines criminels saisis et 1 interpellation majeure en Grèce ;
- Impact technique : désarticulation des chaînes d'attaque pour les *malwares Bumblebee, Latrodectus, Qakbot, HijackLoader, DanaBot, TrickBot, WarmCookie, Rhadamanthys, VenomRAT* et *Elysium*.

AFFILIÉ LOCKBIT INTERPELLÉ

Les faits :

En juillet 2025, un affilié au groupe de rançongiciel *LockBit* de nationalité ukrainienne a été interpellé par l'UNCyber. Celui-ci serait à l'origine de plusieurs dizaines d'attaques en France et à l'étranger.

L'enquête :

Début 2024, une vaste opération internationale d'interpellations avait largement perturbé le fonctionnement du groupe *LockBit*. À la suite de cette opération, le Parquet de Paris avait ouvert une nouvelle enquête confiée à l'UNCyber permettant d'identifier cet affilié basé en Ukraine.

Les résultats :

- 1 interpellation en Ukraine ;
- Perturbation de l'activité du groupe *LockBit*.

36. Un programme informatique conçu pour installer un logiciel malveillant sur un système cible.

PROSPECTIVE ET POINTS D'ATTENTION

4 PROSPECTIVE ET POINTS D'ATTENTION

L'évolution rapide des technologies numériques, conjuguée à l'adaptation constante des usages malveillants, transforme en profondeur l'environnement de la menace cyber. Certaines dynamiques, encore émergentes, laissent entrevoir des ruptures susceptibles d'affecter durablement les équilibres de sécurité, tant pour les institutions que pour les acteurs économiques et la société dans son ensemble. La porosité croissante entre cyberespace et monde physique, l'appropriation d'outils numériques à des fins de coercition ou de surveillance, ainsi que l'impact direct de certaines pratiques sur l'intégrité et la sécurité des personnes, participent à cette recomposition du paysage de la menace.

L'analyse prospective des points d'attention identifiés met en perspective les transformations technologiques, l'évolution des modes opératoires adverses et les nouveaux espaces de vulnérabilité, y compris dans des sphères longtemps perçues comme relevant de la vie privée.

1 | L'ère post-quantique

Comprendre l'enjeu de la cryptographie quantique

La cryptographie constitue un pilier fondamental de la sécurité numérique. Elle permet de protéger les données et les échanges en garantissant que seules les personnes ou entités autorisées puissent y accéder grâce à l'utilisation de clés cryptographiques. Aujourd'hui, la majorité des usages numériques (signature électronique, paiements, communications sécurisées) repose sur des algorithmes dits « classiques », tels que le RSA[37] ou les courbes elliptiques.

Ces algorithmes reposent sur des calculs mathématiques extrêmement complexes, dont la résolution nécessiterait, avec les capacités informatiques actuelles, des milliers d'années.

L'émergence de l'informatique quantique modifie cependant profondément ce contexte. Grâce aux propriétés du qubit[38], capable de traiter simultanément plusieurs états, les ordinateurs quantiques pourraient à terme, réduire drastiquement le temps nécessaire pour casser ces algorithmes.

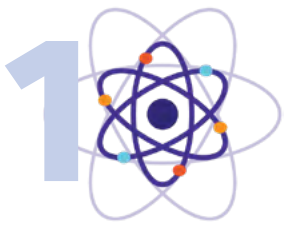
L'informatique quantique ouvre ainsi des perspectives majeures dans de nombreux domaines (cryptographie, optimisation financière ou *machine learning*), mais elle fait également peser un risque inédit sur la sécurité des systèmes d'information.

Des risques majeurs pour les systèmes numériques et financiers

La menace dite « quantique » réside dans la capacité future des ordinateurs quantiques à compromettre une part significative des mécanismes de chiffrement actuellement déployés.

Ce risque concerne en priorité les secteurs les plus dépendants de la confiance numérique, au premier rang desquels le secteur financier, les infrastructures critiques et les technologies *blockchains*.

Trois scénarios de risques principaux sont identifiés :



- le « jour quantique » *(Q-day)*, moment à partir duquel les algorithmes de chiffrement actuels deviendraient vulnérables ;

37. Créé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman, l'algorithme RSA est très utilisé dans le commerce électronique.
38. Unité élémentaire de l'informatique quantique, qui, contrairement au bit, peut prendre à la fois les valeurs binaires 0 et 1.

- la stratégie dite « collecter aujourd'hui pour déchiffrer demain » *(« store now, decrypt later »)*, consistant à exfiltrer dès à présent des données chiffrées afin de les exploiter ultérieurement ;

- la concentration des capacités quantiques dans certains États ou acteurs privés, susceptible de créer des déséquilibres stratégiques en matière de cybersécurité et d'intelligence économique (espionnage industriel ou fuite de documents classifiés).

Ces risques sont d'autant plus sensibles que certaines données, notamment financières, industrielles ou institutionnelles, conservent une valeur stratégique sur le long terme.

Enjeu : anticiper la transition vers la cryptographie post-quantique

À ce stade, aucun consensus scientifique ne permet de fixer avec certitude la date à laquelle les capacités quantiques atteindront un seuil critique. Les estimations varient généralement entre 2030 et 2035. Face à cette incertitude, les autorités publiques ont fait le choix d'anticiper.

En France, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) a annoncé qu'à compter de 2027, elle ne qualifiera plus de nouveaux produits reposant exclusivement sur des algorithmes cryptographiques classiques[39]. Cette échéance marque un jalon structurant : la transition vers des solutions dites « post-quantiques » devient un impératif stratégique.

Ces nouveaux algorithmes sont développés et évalués à l'échelle internationale, dans un cadre à la fois collaboratif et concurrentiel, notamment sous l'égide du National Institute of Standards and Technology (NIST). Plusieurs expérimentations sont déjà en cours, en particulier dans le secteur financier, afin de tester la robustesse et l'intégration de ces solutions dans des environnements opérationnels complexes[40].

Accompagner les organisations dans la transition

La principale difficulté ne réside plus dans la disponibilité des algorithmes post-quantiques, mais dans leur déploiement progressif au sein des systèmes d'information existants. Cette transition doit s'inscrire dans une démarche structurée et anticipée.

Les autorités recommandent notamment :

- d'identifier les données et usages les plus sensibles ;
- de planifier le renouvellement des équipements et logiciels concernés ;
- d'intégrer progressivement des solutions hybrides combinant algorithmes classiques et post-quantiques ;
- de renforcer la capacité d'adaptation des systèmes, afin de pouvoir évoluer rapidement en fonction des avancées technologiques.

La cryptographie post-quantique ne constitue pas une réponse immédiate à une menace actuelle, mais un investissement stratégique indispensable pour préserver, à moyen et long terme, la confiance dans les systèmes numériques.

39. https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/
40. Depuis 2022, la Banque de France mène plusieurs expérimentations post-quantiques, notamment des échanges sécurisés avec la Bundesbank, la Banque des Règlements Internationaux (BRI), la banque centrale de Singapour, ainsi que des retours d'expérience d'acteurs financiers comme Allianz.

2 | Le développement de l'intelligence artificielle agentique : vers des attaques autonomes

D'une intelligence assistée à une intelligence capable d'agir

L'intelligence artificielle (IA) est en pleine révolution, dépassant rapidement les simples capacités génératives pour devenir opérationnelle et auto-adaptative. Cette évolution ouvre la voie à une nouvelle génération de cyberattaques, menées par des agents autonomes capables de planifier, exécuter et ajuster leurs actions sans intervention humaine directe. Ce phénomène, encore émergent mais déjà observable, soulève des enjeux cruciaux pour la cybersécurité, tant sur le plan technique que stratégique.

De l'IA générative à l'IA opérationnelle et auto-adaptative

Les modèles dits « génératifs », largement diffusés depuis 2023, ont ouvert la voie à une nouvelle étape : celle d'IA capables non seulement de produire du texte, des images ou du code, mais également d'agir de manière autonome dans des environnements numériques complexes.

Cette évolution marque le passage progressif d'une IA réactive, répondant à des requêtes humaines, vers une IA opérationnelle, intégrée à des systèmes capables de planifier des actions, d'interagir avec d'autres outils, d'évaluer leurs résultats et d'adapter leur comportement en continu. On parle alors d'IA agentique, c'est-à-dire d'agents autonomes dotés d'objectifs, de capacités décisionnelles et d'une forme d'apprentissage dynamique.

Dans le domaine de la cybersécurité, cette mutation technologique constitue un changement de paradigme majeur.

Des agents autonomes au service de la cybercriminalité

Appliquée à des fins malveillantes, l'IA agentique permet d'automatiser l'ensemble de la chaîne d'attaque.

Un agent autonome peut ainsi :

Analyser une cible et cartographier son environnement numérique

Identifier des vulnérabilités exploitables

Sélectionner et tester différentes techniques d'intrusion

Ajuster sa stratégie en fonction des mécanismes de défense rencontrés

Poursuivre ses actions sans supervision humaine directe

Ces agents peuvent également fonctionner de manière coordonnée, dans des architectures dites multi-agents, échangeant des informations et répartissant les tâches afin d'augmenter leur efficacité. Les attaques deviennent alors plus rapides, plus persistantes et plus difficiles à anticiper, car elles évoluent en temps réel au contact des défenses mises en place.

L'un des premiers effets observables de cette dynamique est la montée en puissance de *malwares* adaptatifs, capables de modifier automatiquement leur comportement ou leur signature pour échapper aux outils de détection traditionnels. De la même manière, les campagnes d'hameçonnage automatisées peuvent désormais ajuster leurs messages en fonction du profil de la victime, augmentant significativement leur taux de succès.

Premiers signaux faibles et cas documentés

Si ces usages restent encore émergents, plusieurs signaux confirment leur matérialisation progressive.

En septembre 2025, Anthropic a révélé avoir détecté et neutralisé une campagne d'attaques cyber d'ampleur, reposant sur l'utilisation détournée d'un agent d'IA configuré en mode autonome[41].

Selon ces éléments, un groupe présumé lié à des intérêts étatiques aurait utilisé une version altérée de l'outil Claude Code pour mener des intrusions contre plusieurs dizaines de cibles, incluant des entreprises technologiques, des institutions financières et des entités gouvernementales. L'IA aurait exécuté de manière autonome la majorité des phases de l'attaque (reconnaissance, exploitation, collecte d'identifiants et exfiltration de données), l'intervention humaine se limitant essentiellement à la supervision générale.

Cet épisode illustre un basculement : l'IA n'est plus seulement un outil d'assistance, mais devient un acteur opérationnel de la menace.

Des défis majeurs pour la détection et la défense

L'essor de ces agents autonomes remet en question les approches classiques de cybersécurité, largement fondées sur des règles statiques et des signatures connues. Face à des menaces capables d'apprendre, de se transformer et de contourner les protections, les dispositifs défensifs doivent eux aussi évoluer.

La détection repose de plus en plus sur l'analyse comportementale, l'identification d'anomalies et l'usage d'IA défensives capables de s'adapter en continu. Des outils comme les leurres dynamiques (*honeypots* évolutifs) permettent notamment d'attirer ces agents, d'observer leurs modes opératoires et d'enrichir les capacités de détection.

Cette course technologique accentue toutefois l'asymétrie entre attaquants et défenseurs, en particulier pour les organisations les moins dotées en ressources humaines et techniques.

Enjeux stratégiques, éthiques et réglementaires

Au-delà des enjeux techniques, l'IA agentique soulève des questions fondamentales en matière de responsabilité, de maîtrise des usages et de stabilité du cyberespace. La perspective d'attaques menées par des systèmes capables d'agir de manière autonome accroît le risque d'escalade incontrôlée, de dommages collatéraux et de brouillage des chaînes de responsabilité.

Ces évolutions appellent une anticipation renforcée, tant sur le plan réglementaire que stratégique. L'encadrement du développement et de l'utilisation des systèmes d'IA autonomes, en particulier lorsqu'ils sont susceptibles d'être détournés à des fins malveillantes, constitue un enjeu majeur pour les années à venir.

Dans ce contexte, la capacité des États à conjuguer innovation technologique, régulation adaptée et coopération internationale sera déterminante pour contenir les effets les plus déstabilisateurs de cette nouvelle génération de menaces.

41. https://crisehelp.fr/ia-claude-agent-attaque-cyber-gtg-1002

3 | Menaces hybrides : du clic à l'action

Une continuité entre cyberespace et monde physique

Les menaces dites « hybrides » traduisent une évolution profonde des modes opératoires malveillants.

Elles reposent sur une articulation étroite entre actions numériques et actions physiques, où le cyberespace constitue désormais le point d'entrée privilégié de nombreuses attaques. Le passage à l'acte ne débute plus sur le terrain, mais bien en ligne, par un travail préparatoire de ciblage, de collecte d'informations et de fragilisation des défenses.

Avant toute action concrète (intrusion, sabotage, intimidation, enlèvement ou opération d'influence), les acteurs malveillants exploitent systématiquement les outils numériques pour identifier leurs cibles, analyser leurs vulnérabilités et affiner leurs scénarios d'attaque. Cette logique du « clic avant l'action » complexifie considérablement la prévention et la détection des menaces.

Ainsi, la menace hybride n'est plus une simple addition de cyberattaques et d'actions physiques, mais un continuum d'opérations coordonnées où le numérique joue un rôle central dans la préparation et l'exécution des actes hostiles.

Le cyber comme outil de préparation opérationnelle

Le ciblage numérique s'appuie sur une combinaison de techniques désormais largement répandues : exploitation de données en sources ouvertes, surveillance des réseaux sociaux, compromission d'identifiants, infiltration de systèmes d'information ou observation des habitudes professionnelles et personnelles. Ces méthodes permettent de reconstituer des profils précis, d'identifier des personnes clés, des routines, des failles organisationnelles ou humaines.

Cette phase préparatoire offre aux attaquants un avantage stratégique déterminant. Elle leur permet d'adapter leurs actions au contexte spécifique de la cible et d'augmenter significativement les chances de succès de l'opération finale, qu'elle soit numérique, physique ou informationnelle.

La menace interne, un facteur aggravant

Dans ce continuum entre cyber et monde réel, les menaces internes occupent une place particulière. Elles concernent les individus disposant d'un accès légitime aux systèmes ou aux informations sensibles : employés, anciens collaborateurs, prestataires ou sous-traitants. Ces profils présentent un risque spécifique en raison de leur connaissance fine des environnements, des procédures et des points de fragilité.

Selon les analyses du Google Threat Intelligence Group[42], les incidents liés aux menaces internes demeurent relativement peu fréquents, mais leurs conséquences peuvent être particulièrement graves, notamment lorsqu'ils touchent des infrastructures critiques ou des données stratégiques. Les motivations sont diverses : appât du gain, ressentiment, pression extérieure, espionnage étatique ou simple négligence.

La détection de ces comportements reste complexe. Les actions malveillantes s'inscrivent souvent dans des usages *a priori* légitimes et peuvent passer inaperçues pendant de longues périodes. Cette réalité renforce la nécessité de combiner sécurité technique, gouvernance des accès et sensibilisation des personnels.

42. Rapport Mandiant du 23/06/2025.

Influence, désinformation et exposition des publics

Les menaces hybrides ne se limitent pas aux atteintes physiques ou aux intrusions techniques. Elles englobent également des opérations d'influence visant à manipuler l'opinion, déstabiliser des institutions ou exploiter des communautés spécifiques au sein desquelles les créateurs de contenus et les acteurs du jeu vidéo occupent une position centrale.

Leur forte visibilité et la jeunesse de leurs audiences en font des cibles privilégiées pour des campagnes de désinformation ou de manipulation. Les plateformes sociales constituent aujourd'hui une source d'information majeure pour les publics les plus jeunes, souvent peu outillés pour identifier les contenus trompeurs ou les stratégies d'instrumentalisation[43].

Les dynamiques algorithmiques amplifient ce phénomène en favorisant les contenus clivants, émotionnels ou sensationnels, indépendamment de leur fiabilité. Certains créateurs, parfois involontairement, deviennent ainsi des relais de rumeurs, de fausses informations ou de narratifs hostiles, contribuant à une surcharge informationnelle et à une perte de repères pour les publics. Ces publications polémiques ou hostiles bénéficient d'une exposition accrue.

Le biais algorithmique des plateformes sociales contribue :

- à la normalisation de discours violents ou mensongers ;
- à la multiplication des campagnes de harcèlement en ligne ;
- à une plus grande viralité des opérations de manipulation informationnelle.

Des opérations d'influence ciblant directement les créateurs

Entre 2022 et 2024, plus de 2 000 influenceurs européens ont été contactés pour relayer des messages pro-russes[44]. Une vingtaine d'entre eux, dont plusieurs en France, auraient accepté ces sollicitations. Les campagnes ciblaient principalement TikTok et Instagram et reprenaient les éléments narratifs de la propagande russe, notamment autour du conflit en Ukraine.

Cette stratégie témoigne d'une évolution significative : reliant désormais des figures visibles plutôt que des comptes anonymes, les opérations d'ingérence informationnelle élargissent considérablement leur portée potentielle.

Une amplification des rumeurs et faux signalements : l'exemple « Dupont de Ligonnès »

En 2025, un influenceur très suivi a affirmé disposer d'une photographie prouvant qu'il avait retrouvé Xavier Dupont de Ligonnès[45]. Cette annonce a suscité une mobilisation massive, générant de nombreuses fausses pistes. La justice a rapidement démenti l'information, soulignant le caractère chronophage de l'épisode et son impact perturbateur sur l'enquête. Cet exemple illustre la capacité d'un créateur à amplifier une rumeur infondée, entraînant une désorientation du public et une surcharge opérationnelle pour les autorités.

Vers une approche globale de la sécurité

La montée en puissance des menaces hybrides impose une approche intégrée de la sécurité, dépassant les cloisonnements traditionnels entre cybersécurité, sécurité physique, renseignement et communication stratégique. Anticiper ces menaces suppose de détecter les signaux faibles en amont, d'articuler les capacités techniques et humaines, ainsi que de renforcer la coordination entre acteurs publics et privés.

Dans ce contexte, la résilience ne repose plus uniquement sur la protection des systèmes, mais également sur la capacité des organisations et des citoyens à comprendre les mécanismes de manipulation, à limiter leur exposition numérique et à réagir de manière coordonnée face à des menaces de plus en plus transversales.

43. 81,3% des 15-24 ans déclarent s'informer quotidiennement *via* Instagram, TikTok ou Snapchat. Parallèlement, 62% des influenceurs reconnaissent ne pas vérifier systématiquement leurs sources, contribuant à un contexte informationnel où la diffusion rapide de contenus trompeurs devient particulièrement facilitée. https://www.mediametrie.fr/fr/les-15-24-ans-des-pratiques-medias-intensives-individuelles-et-connectees https://www.unesco.org/fr/articles/2/3-des-influenceurs-ne-verifient-pas-leurs-sources-mais-veulent-apprendre-le-faire-enquete-unesco
44. https://www.lemonde.fr/pixels/article/2024/12/18/guerre-en-ukraine-des-milliers-d-influenceurs-dont-des-francais-approches-pour-diffuser-de-la-propagande-prorusse_6455494_4408996.html
45. https://www.ladepeche.fr/2025/04/28/xavier-dupont-de-ligonnes-linfluenceur-aqababe-pretend-lavoir-retrouve-pourquoi-les-enqueteurs-sagacent-12663433.php

4 | Cyberviolences et technologies intrusives : les stalkerwares

Les *stalkerwares* constituent une catégorie spécifique de logiciels espions grand public, principalement utilisés dans le cadre de violences sexistes et sexuelles (VSS). Installés sur les téléphones mobiles des victimes, ces outils permettent une surveillance intrusive et continue des activités numériques. La définition du *stalkerware* a été formalisée en 2019 par le Citizen Lab, qui en souligne l'usage abusif dans des contextes de contrôle coercitif et de violence conjugale[46].

Les travaux de recherche et les études institutionnelles confirment l'ampleur du phénomène. Selon une étude menée en 2018 par le Centre Hubertine Auclert sur les cyberviolences conjugales[47], 90% des femmes interrogées, victimes de violences conjugales, déclaraient avoir également subi des cyberviolences. Parmi elles, 21% indiquaient avoir été surveillées au moyen de logiciels espions installés par leur partenaire, tandis que 69% estimaient que ce dernier avait accédé à leurs informations personnelles sans leur consentement.

L'augmentation du recours à ces outils est corroborée par des incidents de sécurité récents, notamment la fuite massive de données du fournisseur mSpy[48], qui a mis en évidence l'existence de près de deux millions d'utilisateurs uniques.

Depuis la publication du rapport fondateur du Citizen Lab, qui recensait une vingtaine d'applications, l'écosystème des *stalkerwares* s'est considérablement étoffé.

Les jeux de données publics permettent aujourd'hui d'identifier au moins 91 familles distinctes de *stalkerwares*, traduisant une industrialisation progressive de cette offre logicielle.

Fonctionnement technique et modalités d'installation

À la différence de logiciels espions commerciaux sophistiqués tels que Pegasus ou Predator, l'installation d'un *stalkerware* ne requiert pas l'exploitation préalable d'une vulnérabilité technique ni l'obtention de privilèges avancés sur le terminal ciblé. Dans la majorité des cas, l'auteur des faits exploite sa proximité avec la victime pour installer directement l'application sur le téléphone.

Trois stratégies principales sont observées :

- l'installation directe du logiciel par l'auteur lors d'un accès physique au terminal ;
- la présentation du *stalkerware* comme un outil de protection ou de bien-être ;
- le camouflage de l'application sous l'apparence d'un service légitime.

Cette dernière méthode repose sur la technique dite de *masquerading*, décrite dans la matrice MITRE ATT&CK Mobile, consistant à attribuer à l'application un nom ou une icône évoquant un service courant du système Android (par exemple *« Wifi »*, *« Google Service »* ou *« Backup »*)[49].

Processus de contrôle et exploitation des données

L'auteur s'inscrit préalablement sur le site de l'éditeur du *stalkerware*, télécharge l'application après souscription d'un abonnement payant, puis procède à son installation manuelle sur le terminal de la victime. Depuis 2020, ces applications ont été bannies des magasins officiels, contraignant les éditeurs à recourir à des canaux de distribution alternatifs.

L'installation nécessite l'activation d'un ensemble étendu d'autorisations : accès aux messages, au calendrier, aux fichiers multimédias, aux notifications d'autres applications et aux services d'accessibilité. Une fois le logiciel activé, l'ensemble des données collectées est transmis et stocké sur l'infrastructure du fournisseur, puis consultable par l'auteur *via* un portail web dédié.

46. Parsons, C., Molnar, A., Dalek, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). The Predator in Your Pocket. https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry
47. Centre Hubertine Auclert. Accueil | Centre Hubertine Auclert. https://www.centre-hubertine-auclert.fr
48. Whittaker, Z. (2024). Data breach exposes millions of mSpy spyware customers. TechCrunch. https://techcrunch.com/2024/07/11/mspy-spyware-millions-customers-data-breach
49. https://attack.mitre.org/matrices/mobile

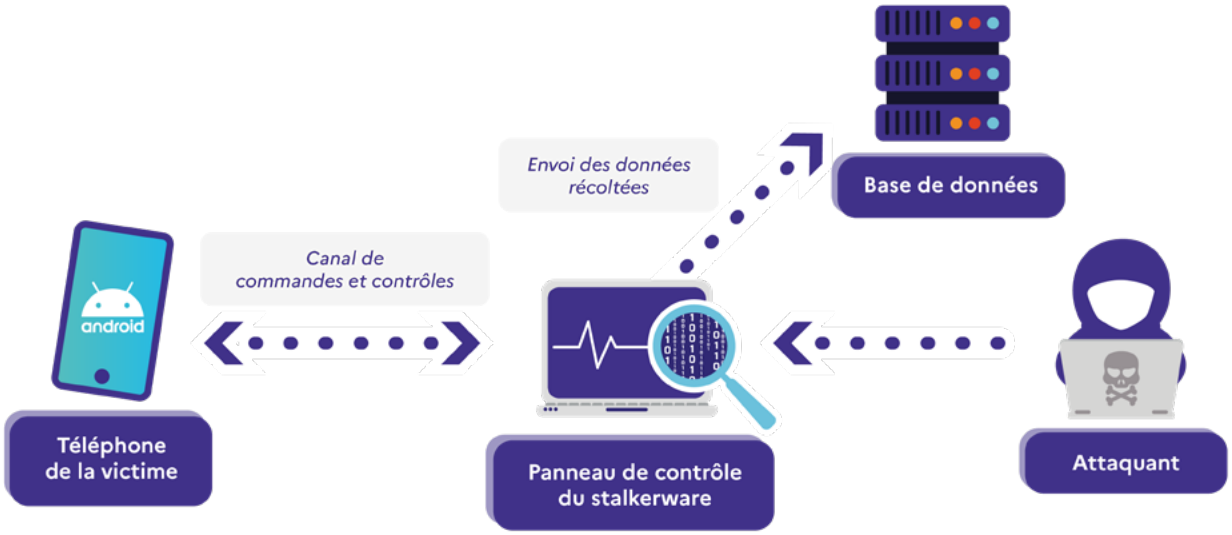


Schéma stalkerware

Organisation commerciale et stratégies de contournement juridique

Les éditeurs de *stalkerwares* ont structuré des modèles économiques reposant sur des abonnements, parfois précédés de périodes d'essai gratuites. Afin de se prémunir juridiquement, ces acteurs présentent systématiquement leurs produits comme des solutions de contrôle parental ou de surveillance légitime, assorties de conditions d'utilisation visant à exclure toute responsabilité en cas d'usage abusif à l'encontre d'adultes.

Enjeux juridiques et pistes de réponse

L'usage de *stalkerwares* est susceptible de caractériser plusieurs infractions pénales, notamment l'atteinte à la vie privée, l'accès et le maintien frauduleux dans un système de traitement automatisé de données, l'interception illégale de correspondances, ainsi que la collecte ou la conservation illicite de données personnelles.

Face à ces enjeux, des travaux de recherche sont en cours afin de proposer une réponse systémique à cette menace. Une thèse de doctorat co-dirigée avec le laboratoire LORIA de l'université de Lorraine vise notamment à analyser l'écosystème des *stalkerwares*, leurs modèles de monétisation, à améliorer leur détection sur les terminaux mobiles et à renforcer l'accompagnement des victimes, notamment à travers le développement de structures de type « cliniques cyber », en appui aux associations et aux forces de l'ordre[50].

50. Thèse de doctorat menée par Sébastien Larinier, co-dirigée avec le laboratoire LORIA de l'université de Lorraine.

RESSOURCES ESSENTIELLES POUR SIGNALER ET SE PROTÉGER

Se renseigner

CYBERMALVEILLANCE.GOUV.FR

Participe à la sécurisation des systèmes d'information des organisations.

Prévenir et sensibiliser les internautes sur la cybercriminalité.

SecNum académie ANSSI

Être sensibilisé à la sécurité numérique (MOOC).

CSIRT RÉGIONAUX

Des centres régionaux pour vous aider à trouver des prestataires proches de chez vous.

MesServicesCyber Innovation ANSSI

Découvrez les guides, services et outils gratuits proposés par l'Agence nationale de la sécurité des systèmes d'information et ses partenaires.

L'ATELIER RGPD

Le MOOC Atelier RGPD est un parcours d'auto-formation gratuit et accessible à tous, quel que soit son niveau, pour s'initier à la protection des données ou approfondir ses connaissances en la matière.

CONTINUITÉ D'ACTIVITÉ

Guide, élaboré par le SGDSN et accessible gratuitement. Il a pour ambition d'accompagner tous types d'organismes dans la mise en place d'une démarche de continuité d'activité et notamment la réalisation d'un plan de continuité d'activité.

Construire sa sécurité cyber

Connaître et déployer les bonnes pratiques. Signaler des vulnérabilités.

ANSSI

Des guides pour renforcer son système d'information et se préparer à une crise cyber.

MonAideCyber INNOVATION ANSSI

Un service gratuit de diagnostic cyber rapide, réalisé par des tiers de confiance, pour développer la maturité cyber des organisations.

Se renseigner sur les données personnelles, l'exercice de ses droits ou faire un MOOC sur le RGPD.

CNIL.

Comprendre ses obligations légales. Des outils à disposition pour aider à protéger les données à caractère personnel.

E-sensibilisation de cybermalveillance, découvrez les mécanismes des principales menaces sur internet et apprenez à mieux vous en protéger.

SENSCYBER E-sensibilisation à la cybersécurité pour tous

MOOC d'initiation à la gestion de crise cyber pour les petites et moyennes structures, comprenant des outils et conseils simples à mettre en œuvre.

SenCyCrise Initiation à la gestion de crise cyber

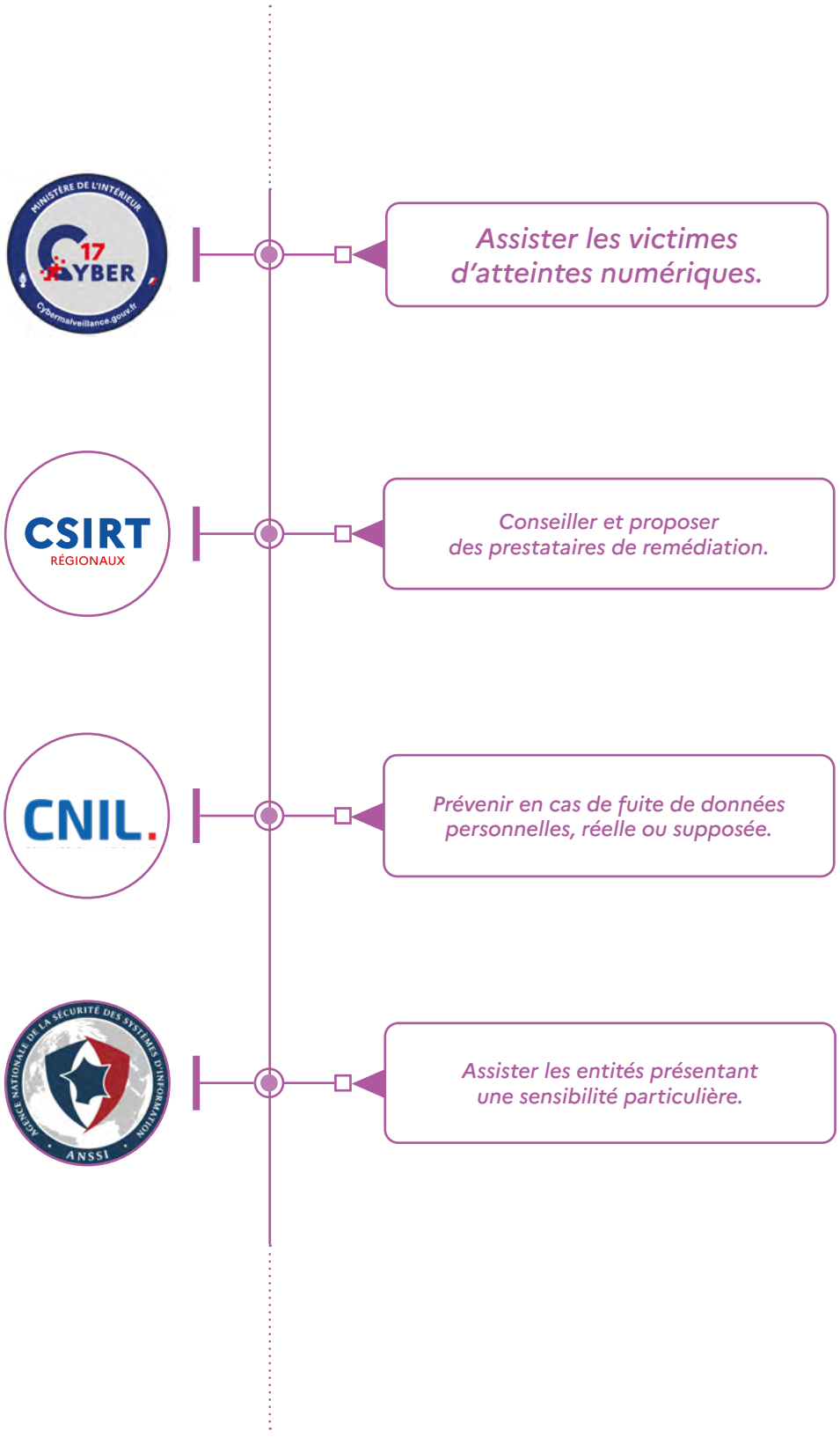
VOUS AVEZ UN DOUTE SUR UN E-MAIL OU UN SMS ?

Signalez-le comme spam sur les plateformes
SIGNAL SPAM (mail) / 33 700 (sms) :

signal spam

33700 La plateforme de lutte contre les spams vocaux et sms

Réagir face à des atteintes numériques



SENSCYBER

Comprendre les menaces et adopter les bonnes attitudes sur le site :

cybermalveillance.gouv.fr

SECNUMACADÉMIE

Pour s'initier à la cybersécurité sur le site :

secnumacademie.gouv.fr

L'ATELIER RGPD

Mieux comprendre les enjeux du Règlement Général sur la Protection des Données (RGPD) sur le site :

atelier-rgpd.cnil.fr

CONTINUITÉ ACTIVITÉ

Guide pour la mise en place d'un plan de continuité d'activité sur le site :

continuiteactivite.sgdsn.gouv.fr

SENCY-CRISE

Initiation à la préparation à la gestion de crise d'origine cyber sur le site :

cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

MES SERVICES CYBER

Pour bénéficier d'un diagnostic cyber en tant qu'organisation sur le site :

messervices.cyber.gouv.fr

L'ANSSI

L'ANSSI assiste les entités essentielles et les entités importantes, fournit des guides et met à disposition un MOOC cyber pour tous :

cyber.gouv.fr

CSIRT RÉGIONAUX

Les CSIRT régionaux répondent aux demandes d'assistance et mettent en relation avec des partenaires de proximité :

cert.ssi.gouv.fr/csirt/csirt-regionaux

17CYBER

Le 17Cyber pour obtenir une aide et des conseils personnalisés en direct ou via un tchat de la part d'un gendarme ou d'un policier :

17cyber.gouv.fr

CNIL

La CNIL est le régulateur des données personnelles. Elle accompagne les professionnels et aide les particuliers :

cnil.fr

CYBERMALVEILLANCE.GOUV.FR

Cybermalveillance permet de s'informer sur les menaces et trouver de l'assistance en tant que victime :

cybermalveillance.gouv.fr

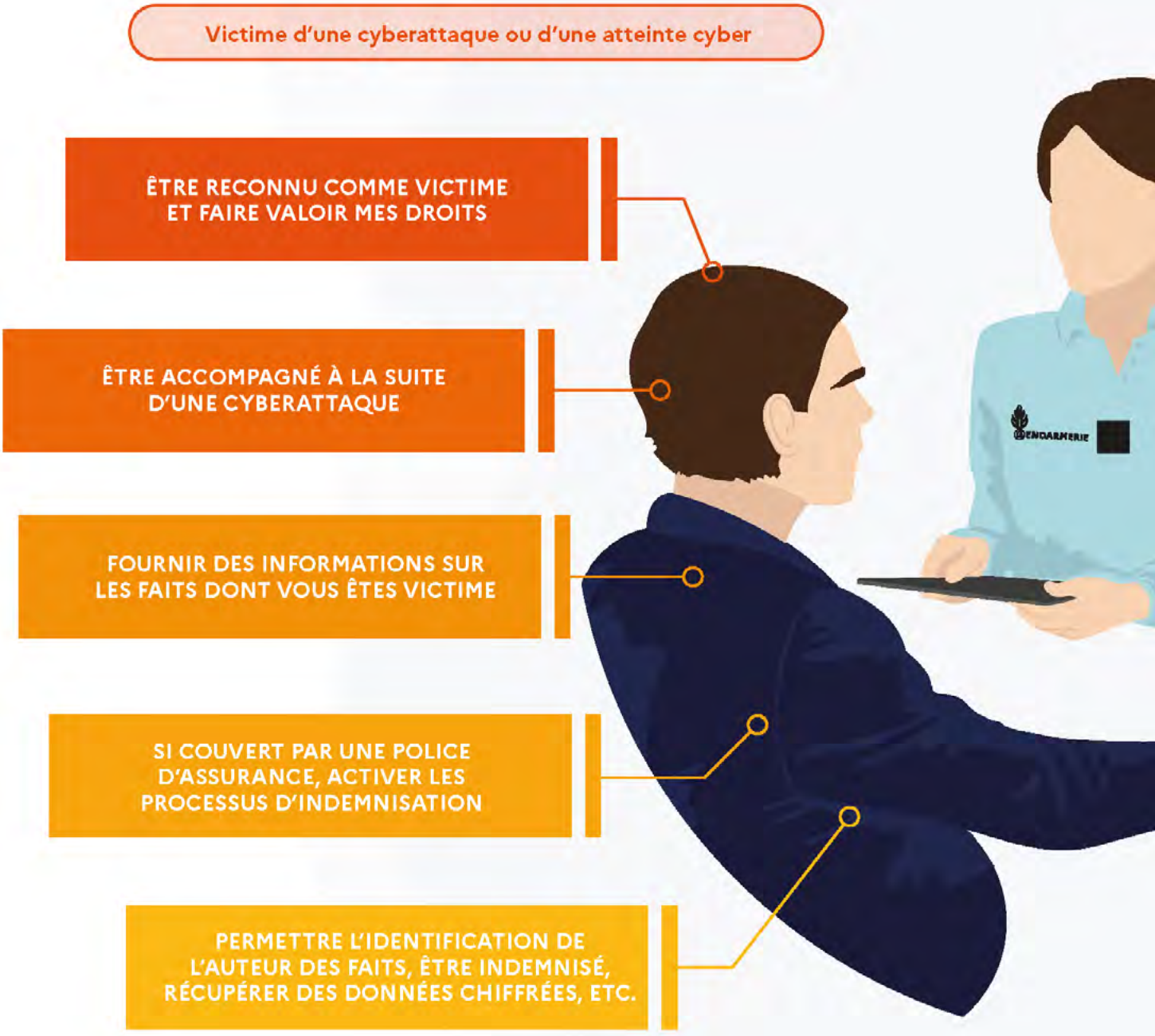
MA SÉCURITÉ

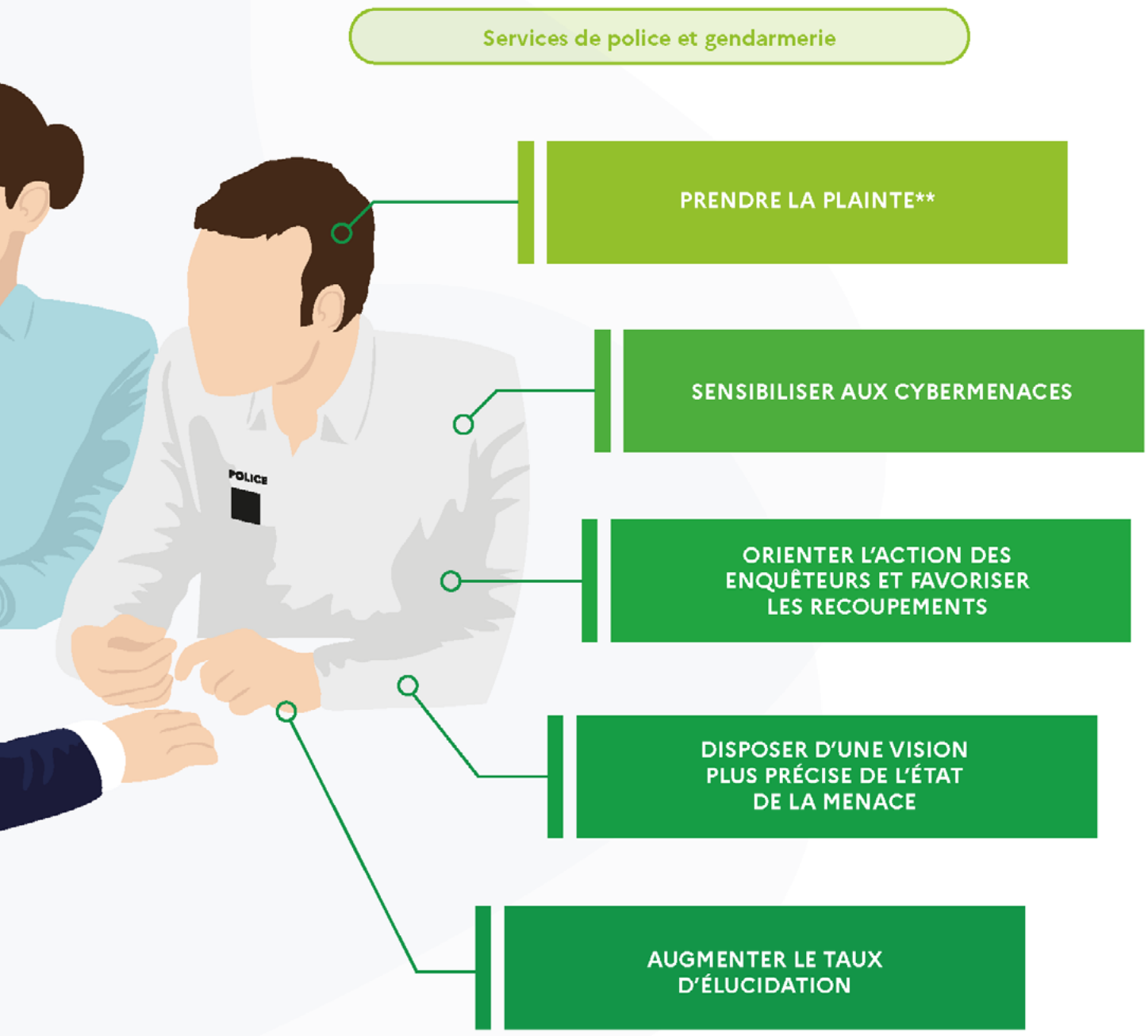
Le 17 pour contacter les forces de l'ordre par téléphone ou sur le site :

masecurite.interieur.gouv.fr

AGISSEZ CONTRE LA CYBERCRIMINALITÉ

DÉPOSER PLAINTE





** La loi d'orientation et de programme du ministère de l'Intérieur de 2023 impose aux personnes morales et aux personnes physiques victimes d'attaques informatiques malveillantes dans le cadre de leur activité professionnelle de porter plainte pour préserver leur droit à indemnisation au titre de leur contrat d'assurance. Le dépôt de plainte doit intervenir dans les 72 heures après la connaissance de l'atteinte par la victime.

Affiliés *(affiliates)* :
Cybercriminels qui louent des outils malveillants clé en main (notamment des rançongiciels) auprès de développeurs spécialisés, conduisent les attaques et reversent une commission sur les gains obtenus. Ce modèle d'affiliation constitue le fondement économique du *Cybercrime-as-a-Service*.

AI-as-a-service (AIaaS) :
Mise à disposition d'outils d'intelligence artificielle monnayant une certaine somme, permettant aux utilisateurs (légitimes ou criminels) d'exploiter ces IA.

ANSSI :
Agence nationale de la sécurité des systèmes d'information.

ASTAD (Atteintes aux Systèmes de Traitement Automatisé de Données) :
Infractions informatiques prévues par le Code pénal, visant le piratage, l'altération ou l'entrave au fonctionnement de systèmes informatiques (vol de données, sabotage, intrusion).

Attaques par la chaîne d'approvisionnement *(Supply Chain Attacks)* :
Compromission d'un fournisseur ou prestataire légitime pour infiltrer une cible finale, *via* les dépendances qu'elles ont entre elles.

Attaques sous « faux drapeau » :
Attaques trompeuses faisant croire qu'elles proviennent d'un autre acteur (pays ou groupe) pour brouiller les pistes et détourner l'attribution de la cyberattaque.

BL2C :
Brigade de lutte contre la cybercriminalité de la préfecture de Paris.

***Blockchain* (chaîne de blocs) :**
Registre distribué fonctionnant en réseau avec une grande diversité de nœuds (des ordinateurs en réseau) qui décident par consensus (et non autour d'une entité centrale) de la validité et de l'ordre des transactions. Elles sont ensuite inscrites sur un registre comptable public, exhaustif et mondial, qui est répliqué sur chacun des ordinateurs du réseau.

***Botnet* :**
Réseau de machines compromises, administré à distance par un ou plusieurs acteurs malveillants *via* des serveurs de commande et contrôle *(C2)*. Les machines intégrées au *botnet* (dites « zombies ») agissent généralement à l'insu de leurs propriétaires. Utilisés pour mener des attaques *DDoS*, envoyer du spam, diffuser des logiciels malveillants ou miner des cryptoactifs.

***Bulletproof hosting* :**
Services d'hébergement tolérant des contenus illégaux *(phishing, malwares)*, opérant depuis des juridictions laxistes, rendant leur fermeture difficile.

Citrix :
Solution de virtualisation d'espace de travail accessible depuis n'importe quel poste à distance.

CJUE (Cour de justice de l'Union européenne) :
Plus haute juridiction de l'UE, interprète le droit européen et veille à son application uniforme dans les États membres.

***Cloud* :**
Modèle de fourniture de ressources informatiques (puissance de calcul, stockage, applications) à la demande sans gestion directe d'infrastructure physique par l'utilisateur. Son usage massif par les cybercriminels pour héberger des infrastructures malveillantes en complique l'attribution et le démantèlement.

CNIL :
Commission nationale de l'informatique et des libertés.

***Combo-lists* :**
Fichiers contenant des associations « email : mot de passe » issus de vols de données. Les pirates les utilisent pour tenter de se connecter à divers services en ligne.

***Cookies* :**
Fichiers stockés par les sites web sur le navigateur pour conserver des informations utilisateur.

Cryptoactif :
Actif numérique utilisant notamment la cryptographie et la technologie *blockchain* pour sécuriser et vérifier les transactions.

Crypto-criminalité :
Ensemble des activités illégales impliquant des cryptoactifs (cryptomonnaies, *tokens*, *NFT*, *stablecoins*), qu'il s'agisse de leur utilisation comme moyen de paiement illicite, d'instrument de blanchiment, ou de cible d'attaques (vols, draineurs, escroqueries).

Cybercriminalité en tant que service *(Cybercrime-as-a-Service, CaaS)* :
Mise à disposition en ligne de services ou de conseils cybercriminels. Plusieurs déclinaisons existent selon le type de phénomène, tels que le *RaaS* (rançongiciel), le *BaaS (botnet)*, le *MaaS (malware)*, etc.

Cyberespace :
Espace de communication immatériel et sans frontière constitué par l'interconnexion d'équipements de traitement automatisé de données.

Cyberharcèlement (harcèlement en ligne) :
Acte ou propos intentionnel d'un individu ou d'un groupe d'individus au moyen de formes de communications électroniques, de façon répétée à l'encontre d'une victime, occasionnant une dégradation des conditions de vie de celle-ci.

***Darknet* :**
Réseaux tels que Tor ou Freenet qui permettent d'accéder à des ressources cachées du web traditionnel. La somme des informations accessibles sur les *darknets* forme le *darkweb*.

***Darkweb* :**
Partie cachée du web accessible avec des logiciels spécifiques. De nombreuses activités illicites y sont disponibles, notamment la mise en vente de logiciels malveillants ou l'échange de contenus illégaux.

***Data leaks* (fuites de données) :**
Divulgation accidentelle ou malveillante de données sensibles (emails, mots de passe, infos personnelles), souvent *via* piratage ou erreurs humaines.

***DDoS-as-a-Service (DaaS)* :**
Plateformes clandestines proposant à la location des capacités d'attaque par déni de service distribué, permettant à tout acheteur de commander une attaque contre une cible donnée sans compétence technique. Également appelé *« booter »* ou *« stresser »*.

***Deepfake* :**
Technique de falsification de contenus audiovisuels par intelligence artificielle, permettant de substituer le visage ou la voix d'une personne dans une vidéo ou un enregistrement sonore. Utilisée à des fins d'escroquerie (usurpation d'identité, fraude au président), de désinformation, de chantage ou de production de contenus intimes non consentis.

Défiguration de sites internet :
Résultat d'une cyberattaque qui a modifié l'apparence ou le contenu d'un site internet, et a donc violé l'intégrité des pages en les altérant.

Déni de service *(DoS)* :
Vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à saturation ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Déni de service distribué *(DDoS)* :
Version distribuée du *DoS* avec les mêmes objectifs, qui utilise plusieurs machines, en général un *botnet*.

DGSI :
Direction Générale de la Sécurité Intérieure.

Directive NIS2
***(Network and Information Security 2)* :**
Directive européenne de 2022 renforçant les obligations de cybersécurité pour les opérateurs de services essentiels et les entreprises critiques.

Données à caractère personnel :
Éléments d'identification se rapportant à une personne physique identifiée ou identifiable (nom, prénom, date de naissance, numéro de sécurité sociale, etc.).

***Drainer-as-a-Service (DaaS)* :**
Kits malveillants loués aux cybercriminels, conçus pour vider automatiquement les portefeuilles de cryptoactifs des victimes, généralement *via* de faux sites de mint ou des transactions malveillantes approuvées à l'insu de l'utilisateur.

Draineur (cryptoactifs) :
Logiciel malveillant utilisé pour inciter un utilisateur à signer une transaction permettant de siphonner ses cryptoactifs.

Fausse romance :
Arnaque sentimentale où un escroc crée un lien affectif avec la victime pour lui soutirer de l'argent ou des données personnelles.

Forum :
Espace public d'échanges virtuel entre internautes. Moyen de communication prisé par les cybercriminels, accessible sur le *clearweb* comme sur le *darkweb*.

Hacktivisme :
Activisme numérique utilisant le piratage pour promouvoir des causes idéologiques, politiques ou sociales, souvent en attaquant des sites web ou en divulguant des données.

Hameçonnage *(phishing)* :
Technique de tromperie visant à soutirer des informations sensibles (identifiants, mots de passe, coordonnées bancaires) ou à inciter la victime à exécuter une action malveillante. Les vecteurs incluent le courriel *(phishing)*, le SMS (hameçonnage par SMS ou *smishing*), l'appel téléphonique (hameçonnage vocal ou *vishing*) et les faux sites internet. Le harponnage *(spearphishing)* en est une forme ciblée.

***IMSI-Catcher* :**
Dispositif de surveillance imitant une antenne-relais mobile afin d'intercepter les communications des téléphones environnants. Il capture notamment l'*IMSI (International Mobile Subscriber Identity)*, identifiant unique de la carte SIM, permettant de localiser une personne ou d'écouter ses échanges. Son usage est strictement encadré par la loi.

***Infostealers* :**
Malwares conçus pour voler automatiquement des informations sensibles (mots de passe, cartes bancaires, *cookies*, historiques de navigation) depuis l'ordinateur infecté.

Ingénierie sociale :
Ensemble des techniques de manipulation psychologique visant à amener une personne à divulguer des informations confidentielles ou à exécuter une action compromettant la sécurité d'un système, en exploitant des biais cognitifs tels que la confiance, l'urgence, l'autorité ou la peur. L'ingénierie sociale constitue souvent le vecteur initial d'une cyberattaque, en contournant les protections techniques par la manipulation humaine.

***Initial access broker* :**
Cybercriminels vendant des accès illégitimes à des systèmes d'information à d'autres cybercriminels qui vont les exploiter dans le cadre d'une attaque de plus grande envergure.

JUNALCO :
Juridiction nationale de lutte contre la criminalité organisée.

Maliciel *(malware)* :
Logiciel malveillant, ou tout programme développé dans le but de nuire à un système d'information ou à un réseau.

***Malware-as-a-Service (MaaS)* :**
Location ou vente de *malwares* prêts à l'emploi, souvent avec support technique.

OFAC :
Office anti-cybercriminalité (direction nationale de la police judiciaire – Police nationale).

***Pentester* criminel :**
Individu qui utilise les techniques de test d'intrusion (recherche de failles) illégalement pour pirater des systèmes.

Rançongiciel *(ransomware)* :
Logiciel malveillant générant une demande de rançon après le chiffrement et/ou l'exfiltration de données.

Rançongiciel en tant que service *(RaaS, Ransomware-as-a-Service)* :
Modèle économique d'affiliation dans lequel des développeurs mettent à disposition de cybercriminels (affiliés) un rançongiciel clé en main. L'offre comprend un panneau de gestion, un support technique et un appui à la négociation avec les victimes. En échange, les développeurs perçoivent une commission sur les rançons obtenues, généralement comprise entre 20 et 30%. Ce modèle a industrialisé la menace rançongiciel en la rendant accessible sans compétence technique avancée.

***RDP (Remote Desktop Protocol)* :**
Protocole de connexion à distance développé par Microsoft, permettant de prendre le contrôle d'un ordinateur *via* le réseau.

Règlement MiCA *(Markets in Crypto-Assets)* :
Règlement européen encadrant les cryptoactifs, visant à protéger les investisseurs et prévenir les abus sur les marchés numériques.

RGPD :
Règlement général sur la protection des données.

RSA (Rivest Shamir Adleman) :
Algorithme de cryptographie asymétrique, l'un des plus répandus. Il repose sur un couple de clés (publique/privée) et est principalement utilisé pour l'échange sécurisé de clés de chiffrement et la signature numérique.

SBU :
Sluzhba Bezpeky Ukrayiny, principal service de renseignement intérieur et de contre-espionnage ukrainien.

SCADA (Supervisory Control and Data Acquisition) :
Systèmes industriels supervisant et contrôlant des infrastructures critiques (électricité, eau, gaz). Ils permettent le pilotage à distance d'équipements *via* des capteurs et automates.

Serveurs de *Command and Control (C2)* :
Serveurs utilisés par les cybercriminels pour piloter des machines compromises à distance.

***Smart contract* :**
Programme informatique autonome déployé sur une *blockchain*, s'exécutant automatiquement lorsque des conditions prédéfinies sont remplies, sans intervention de tiers. Leur caractère immuable une fois déployés les rend vulnérables aux failles de code.

***Spearphishing* (hameçonnage ciblé) :**
Hameçonnage ciblé visant une personne précise avec un message personnalisé.

***Stalkerwares* :**
Logiciels espions installés discrètement sur l'appareil d'une victime (smartphone ou ordinateur) afin d'en surveiller à distance la localisation, les communications, les applications et l'activité à l'insu de son propriétaire. Principalement utilisés dans des contextes de violence conjugale et de contrôle coercitif. Leur usage est constitutif de plusieurs infractions pénales.

Système de traitement automatisé de données (STAD) :
Ensemble d'éléments physiques et applicatifs utilisés pour le traitement de données (réseaux, supports informatiques, etc.).

Système d'information :
Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

UNCyber :
Unité nationale cyber de la Gendarmerie nationale.

UNPJ :
Unité nationale de police judiciaire de la Gendarmerie nationale.

VPN (Virtual Private Network) :
Réseau privé virtuel créant un tunnel chiffré entre l'utilisateur et un serveur distant, masquant son adresse IP réelle et protégeant ses communications.

Wallet :
Logiciel ou dispositif physique permettant d'accéder et de gérer des cryptoactifs liés à une adresse publique.

Wiper :
Logiciel malveillant dont l'objectif est de détruire irréversiblement les données ou les systèmes de la victime, sans demande de rançon. Instrument de sabotage numérique, ils sont fréquemment associés à des opérations étatiques ou hacktivistes visant des infrastructures critiques.

NOTES

Directeur de publication :
Général de division Patrick TOUAK

Équipe éditoriale et contributeurs :
Le présent rapport a été établi grâce aux contributions :

- du cabinet du ministère de l'Intérieur ;
- du service statistique ministériel de la sécurité intérieure ;
- de la préfecture de Police de Paris ;
- des directions générales du ministère de l'Intérieur : police nationale, gendarmerie nationale, sécurité intérieure ;
- et du ministère de la Justice (section J3 du Parquet de Paris).

Sa rédaction a été réalisée par le Centre d'analyse des cybermenaces du commandement du ministère de l'Intérieur dans le cyberespace.

Conception graphique et réalisation :
Commandement du ministère de l'Intérieur dans le cyberespace
Section communication rayonnement et multimédia

Crédits photographiques et illustrations :
Image générée avec Freepik IA et utilisée conformément à la licence Freepik. (www.freepik.com)
Photographie © Ministère de l'Intérieur

Contact :
Commandement du ministère de l'Intérieur dans le cyberespace

rapport-ccmi@gendarmerie.interieur.gouv.fr

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Commandement du ministère
de l'Intérieur dans le cyberespace