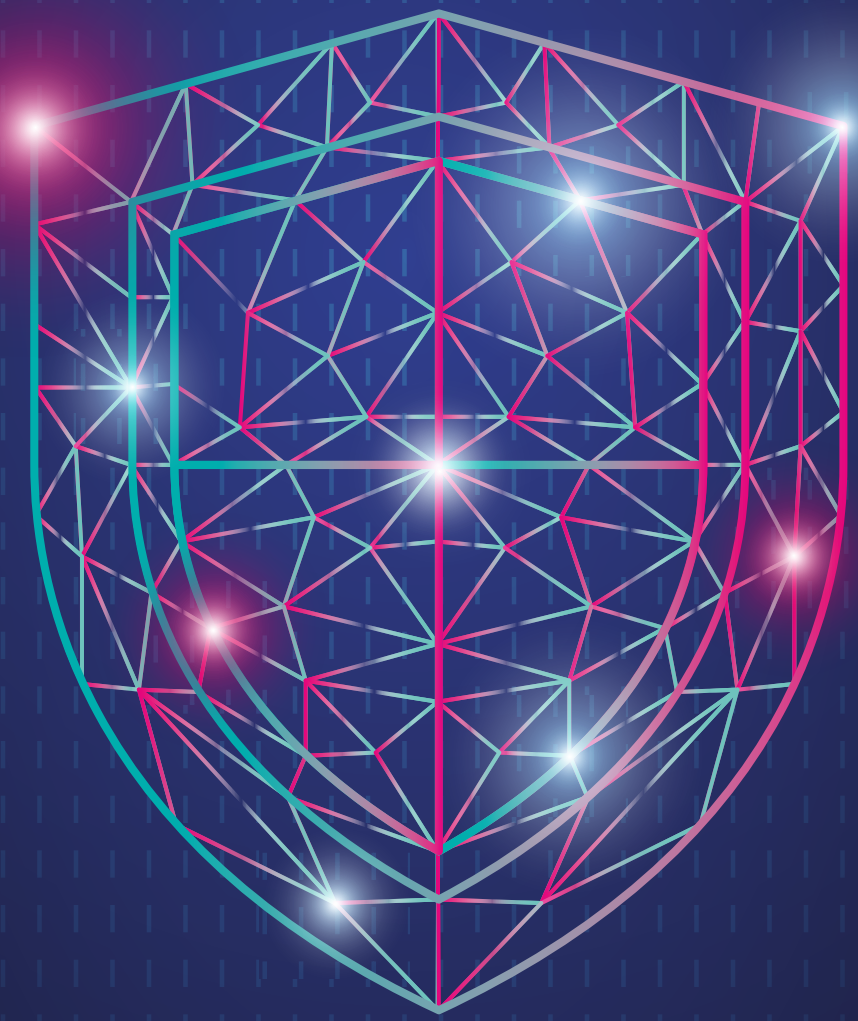
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2024



COMCYBER-MI

« Nos forces, pour votre cyber-protection »

SOMMAIRE

Face à l'essor de la cybercriminalité qui menace nos institutions, notre économie et la sécurité de chaque citoyen, notre réponse doit être collective et résiliente.

En ces temps où la frontière entre le cyberespace et notre réalité quotidienne devient de plus en plus floue, la vigilance et l'innovation sont nos meilleurs boucliers.

Ce premier rapport du commandement du ministère de l'Intérieur dans le cyberespace dresse un état des lieux sans concession des défis cyber auxquels la France a été confrontée en 2023.

La première étape dans la lutte contre la cybercriminalité est l'identification et la compréhension approfondie de ces menaces.

Notre analyse de l'écosystème cybercriminel et de ses modes opératoires est cruciale pour élaborer des contre-mesures efficaces.

Ces efforts nous permettent d'identifier et d'arrêter les auteurs d'infractions dans le cadre d'enquêtes judiciaires, souvent menées en étroite coopération internationale.

Le rapport souligne la capacité d'adaptation, la modernisation et la résilience des cybercriminels.

En anticipant leurs actions, nous affinons notre vision stratégique et orientons plus efficacement les opérations de nos unités et nos services sur le terrain.

Ce bilan de 2023, réalisé en complémentarité avec les analyses annuelles de l'ANSSI, bénéficie des travaux du CEntre d'analyse et de regroupement des Cybermenaces (CECyber) du COMCYBER-MI.

Visant à être à la fois pragmatique et accessible, il repose aussi sur les données du Service statistique ministériel de la sécurité intérieure (SSMSI) complétées par d'autres sources institutionnelles.

En conclusion, ce rapport met en avant l'approche concertée du ministère de l'Intérieur dans la lutte contre la cybercriminalité, illustrée par des retours d'enquêtes significatifs.

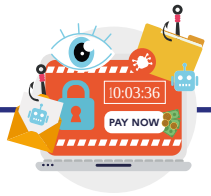
Notre détermination à sécuriser l'espace numérique français est plus forte que jamais et nous continuerons à innover et à coopérer, tant au niveau national qu'international, pour relever ces défis.

Général de division Christophe Husson
Chef du commandement du ministère de l'Intérieur dans le cyberespace

CHIFFRES CLÉS 2023

278 770
atteintes numériques enregistrées en 2023

+40% d'atteintes numériques en 5 ans



59%
d'atteintes aux biens

34,5%
d'atteintes aux personnes

6%
d'atteintes aux institutions et à l'ordre public

0,5%
d'atteintes aux législations et règlementations spécifiques numériques

17 700
atteintes aux systèmes d'information en 2023

+28% de saisines pour des attaques par rançongiciel

THESEE

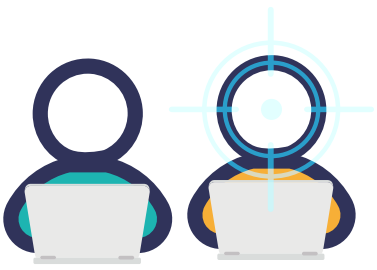
104 439 plaintes ou signalements relatifs aux escroqueries sur internet enregistrés sur la plateforme Thésée

PHAROS

211 543 signalements de contenus illicites reçus par la plateforme Pharos

PERCEV@L

259 094 signalements d'usages frauduleux de cartes bancaires répertoriés par la plateforme Perceval



50% des victimes d'une atteinte numérique à la personne sont des femmes âgées de 18 à 44 ans

47 000 mis en cause pour des atteintes numériques

NB : Les chiffres présentés ici proviennent de données établies par le Service statistique ministériel de la sécurité intérieure, complétées par d'autres sources institutionnelles : Office Anti-Cybercriminalité de la police nationale, Unité Nationale Cyber de la gendarmerie nationale, section J3 du parquet

La **cybercriminalité** recouvre l'ensemble des crimes et des délits commis à l'encontre ou par le biais des systèmes d'information. Ces infractions renvoient à une large diversité de phénomènes criminels qui vont des escroqueries au harcèlement, en passant par les rançongiciels, la compromission d'identifiants, ou encore l'usurpation d'identité.

La **persistance des cybermenaces** représente une tendance de fond, avec une augmentation constante du nombre d'infractions liées au numérique enregistrées ces dernières années en France. La répartition observée en 2023 entre les principaux types d'atteintes s'inscrit dans la continuité des années précédentes.

Le **contexte national et international agité en 2023** s'est révélé propice aux attaques envers des organisations françaises, entreprises comme institutions. Elles ont essentiellement pris la forme d'attaques par déni de service distribué ou de défigurations. Un des objectifs était une recherche de médiatisation afin de faire passer un message revendicatif.

Les **cyberdélinquants** sont la plupart du temps guidés par des motivations financières. Ils attaquent en masse, se montrent créatifs et à l'affût de toute nouvelle opportunité possible. Il s'agit d'un écosystème mouvant, protéiforme, international qui se compose d'une diversité d'acteurs, allant de l'amateur à la structure organisée.

Le champ de la criminalité numérique n'a cessé de croître ces dix dernières années, avec une **professionnalisation** significative en matière d'appropriation des outils techniques et une **industrialisation des processus cybercriminels.**

L'année 2023 a été d'autre part marquée par l'avènement des usages grand public de l'Intelligence Artificielle (IA). L'IA peut cependant être exploitée à des fins criminelles comme pour générer des *deepfakes*, ou bien faciliter la production et la diffusion d'escroqueries au travers de courriels frauduleux.

Plusieurs **opérations judiciaires** significatives, menées par les services de police et de gendarmerie, ont eu lieu en 2023. Elles ont par exemple visé des groupes spécialisés dans les rançongiciels ou les escroqueries cyber, mais aussi abouti au démantèlement d'infrastructures criminelles. La France connaît des tendances communes au reste de l'Union européenne en matière de cybercriminalité, justifiant une coopération internationale toujours accrue.

Différents axes seront à suivre avec **vigilance en 2024**, parmi lesquels les reconfigurations probables des groupes criminels touchés par des opérations policières en 2023, l'extension possible des usages de l'IA à des fins malveillantes, ou bien encore le fait que certains services cybercriminels puissent devenir plus facilement accessibles.

Victime d'une cyberattaque ou d'une atteinte cyber

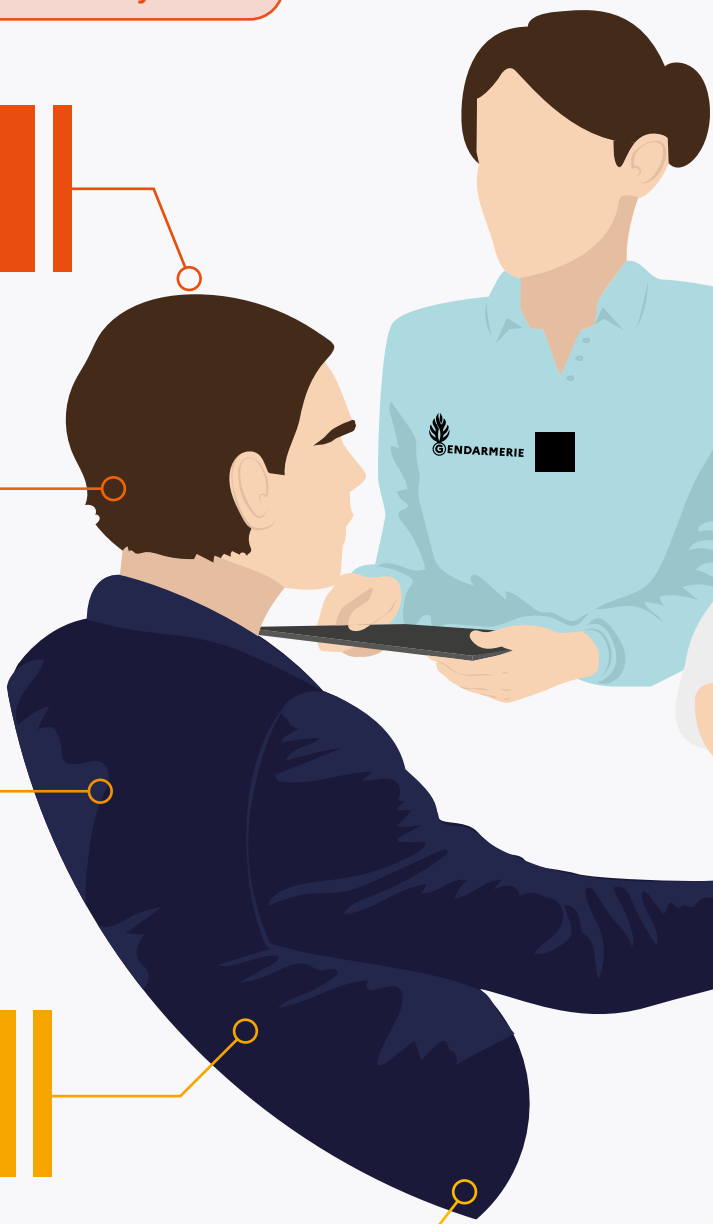
ÊTRE RECONNU COMME VICTIME ET FAIRE VALOIR SES DROITS

ÊTRE ACCOMPAGNÉ À LA SUITE D'UNE CYBERATTAQUE

FOURNIR DES INFORMATIONS SUR LES FAITS DONT VOUS ÊTES VICTIME

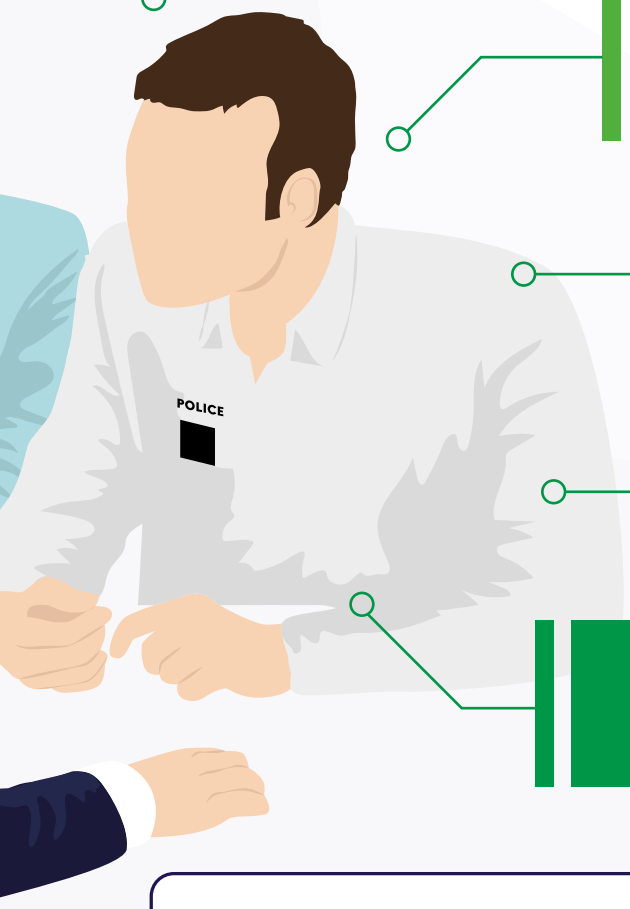
SI COUVERT PAR UNE POLICE D'ASSURANCE, ACTIVER LES PROCESSUS D'INDEMNISATION

PERMETTRE L'IDENTIFICATION DE L'AUTEUR DES FAITS, ÊTRE INDEMNISÉ, RÉCUPÉRER DES DONNÉES CHIFFRÉES,...



* Pour les modalités de dépôt de plainte, voir page 48 « Informations utiles et contacts ».
** La loi d'orientation et de programmation 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.

Services de police et de gendarmerie



PRENDRE LA PLAINTE**

SENSIBILISER AUX CYBERMENACES

ORIENTER L'ACTION DES ENQUÊTEURS ET FAVORISER LES RECOUPEMENTS

DISPOSER D'UNE VISION PLUS PRÉCISE DE L'ÉTAT DE LA MENACE

AUGMENTER LE TAUX D'ÉLUCIDATION

Après le dépôt de plainte

Après le dépôt de plainte s'ouvre un temps nouveau : **le temps judiciaire**. Les services d'enquête dédiés prennent alors le relais.

À l'issue du dépôt de plainte, l'enquêteur informe le procureur de la République territorialement compétent. Sous son autorité, **une enquête est alors réalisée**.

À l'issue des investigations, la procédure lui est transmise pour décider de l'**opportunité des poursuites**.

Dans le cadre des enquêtes complexes, une **ouverture d'information** peut être demandée par le procureur de la République.

Dans ce cas, il saisira un juge d'instruction qui sera en charge de la direction des investigations et décidera de l'orientation de la procédure.

Dans le cas d'une ouverture d'information, **la victime peut se constituer partie civile et se voit reconnaître certains droits** : obtenir l'assistance d'un avocat choisi ou commis d'office pour l'accompagner durant la procédure, avoir accès au dossier, demander à être auditionnée par le juge et solliciter de ce dernier qu'il accomplisse certains actes d'enquête complémentaires (nouvelles auditions et confrontations).

Toutefois, pour les dossiers de cyberattaques de grande ou de très grande complexité, notamment pour toutes les infractions d'atteintes aux systèmes de traitement automatisé de données et de cybersabotage de tels systèmes, **la section J3** (spécialisée en matière de cybercriminalité) **du parquet de Paris** peut exercer sa compétence nationale et se saisir de la procédure quel que soit le lieu de commission des faits sur le territoire national.

01 Des phénomènes cybercriminels impactants en 2023

DES PHÉNOMÈNES CYBERCRIMINELS IMPACTANTS EN 2023

01

1 DE QUOI PARLE-T-ON ?

Cybercriminalité et phénomènes cybercriminels

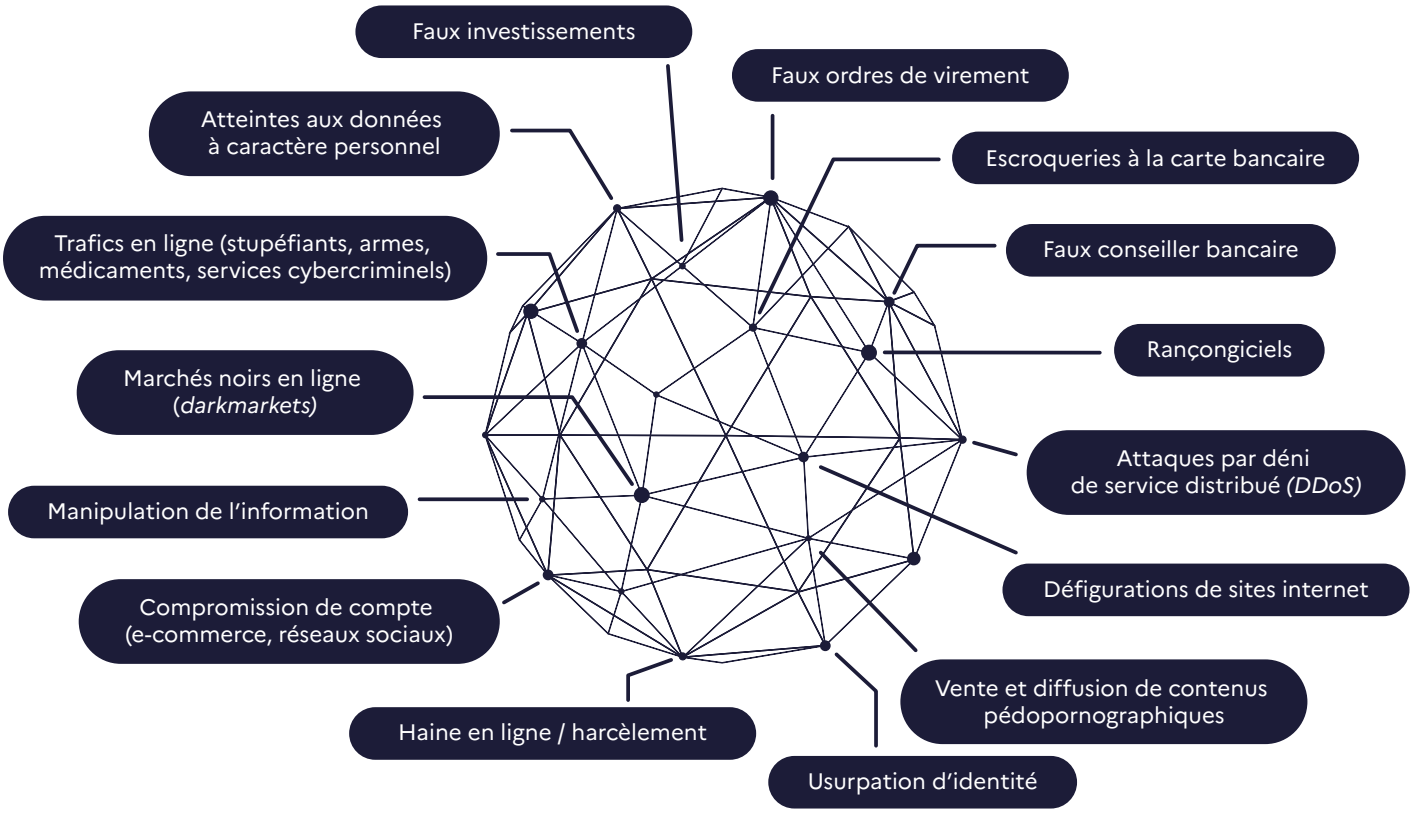
La cybercriminalité recouvre l'ensemble des délits et crimes commis à l'encontre ou par le biais des systèmes d'information.

Chaque année, des milliers de dépôts de plainte sont enregistrés par les unités de la gendarmerie nationale et les services de la police nationale.

Les nouvelles technologies permettent aux cybercriminels d'être **plus efficients**, de **se structurer** en bandes organisées, de contourner les systèmes répressifs traditionnels, voire de **créer et de sophistiquer** leurs modes opératoires.

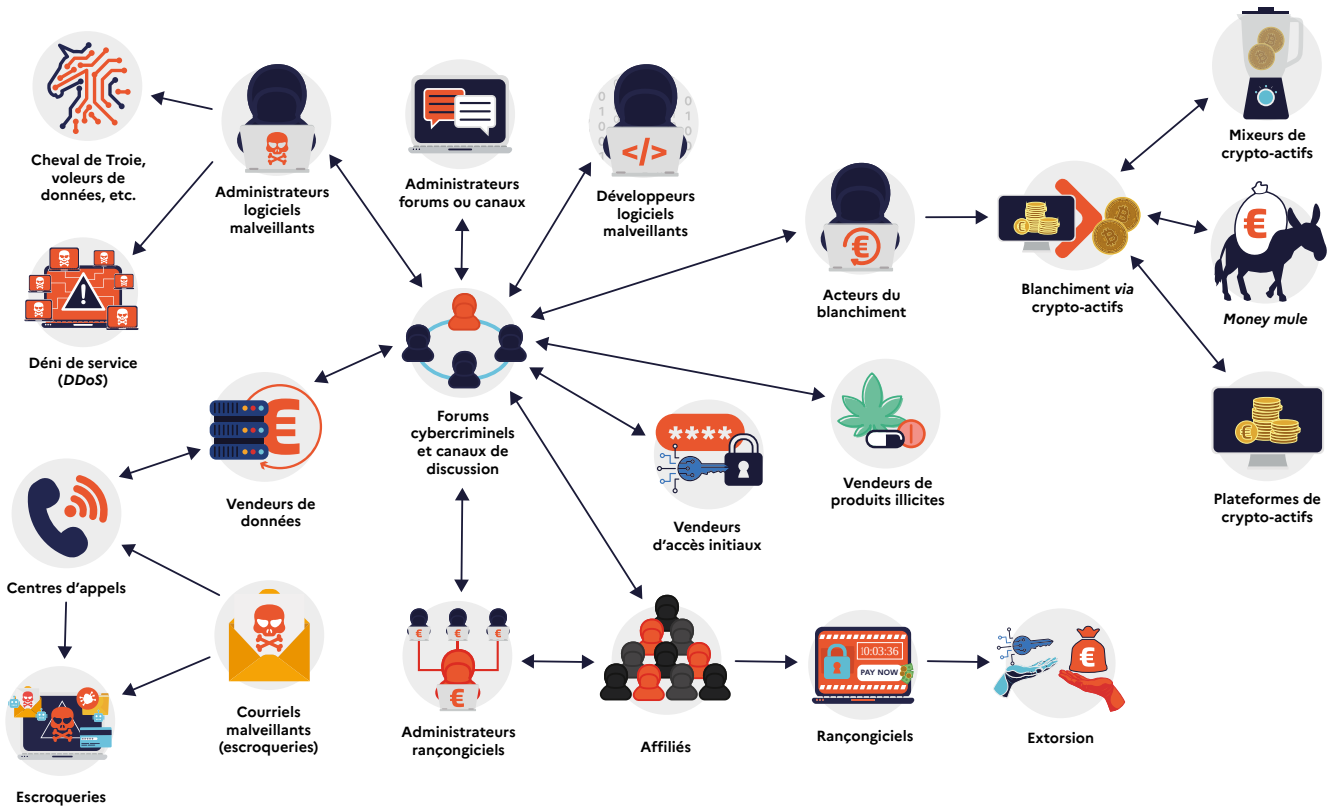
> « Ainsi, la multiplication des activités cybercriminelles, au-delà de constituer un ensemble d'infractions de droit commun, peut devenir par ses impacts un facteur de déstabilisation de notre société. »

De nombreux phénomènes cybercriminels sont recensés. Ils peuvent prendre la forme d'atteintes aux personnes, d'escroqueries, d'atteintes aux systèmes d'information, de services illicites ou bien encore d'atteintes aux institutions, etc.



Exemples de phénomènes cybercriminels

L'écosystème cybercriminel



Exemple de modélisation d'un écosystème cybercriminel

Le champ de la criminalité numérique n'a cessé de croître depuis ces dix dernières années, avec une professionnalisation significative en matière d'**appropriation des outils techniques** et d'**industrialisation des processus** cybercriminels.

Pour mettre en œuvre leurs activités illicites, les acteurs malveillants s'appuient sur de **nombreux vecteurs** (serveurs, logiciels malveillants, etc.) et **canaux de communication** (forums, messageries chiffrées, réseaux sociaux, etc.) leur permettant d'interagir et d'optimiser leurs actions.

> « À titre d'exemple, les forums cybercriminels permettent d'acheter et vendre des services, logiciels malveillants ou données pour mener des cyberattaques ou des escroqueries en ligne. »

Les cyberdélinquants sont également en lien étroit avec les **acteurs du blanchiment**, notamment certaines plateformes de crypto-actifs peu regardantes sur l'origine des fonds, parfois criminels, qui sont transférés par le biais de leurs services.

Cybercriminalité : tous concernés

L'analyse de la donnée judiciaire montre que **tous les acteurs** de la société sont ciblés par les cybercriminels, qu'il s'agisse de particuliers, d'entreprises, de collectivités, d'administrations ou d'associations. L'année 2023 a confirmé cette tendance.

Les **principales menaces** qui pèsent sur les victimes potentielles sont les rançongiciels, les escroqueries en ligne, les compromissions d'identifiants personnels ou professionnels, les atteintes aux personnes (vente et diffusion de contenus pédopornographiques, cyberharcèlement, haine en ligne, etc.), les vols de données personnelles ou économiques, ou encore l'usurpation d'identité…

2 LES CHIFFRES DE LA CYBERCRIMINALITÉ

Les chiffres présentés ici proviennent de données établies par le Service statistique ministériel de la sécurité intérieure[1], complétées par d'autres sources institutionnelles.

Atteintes numériques

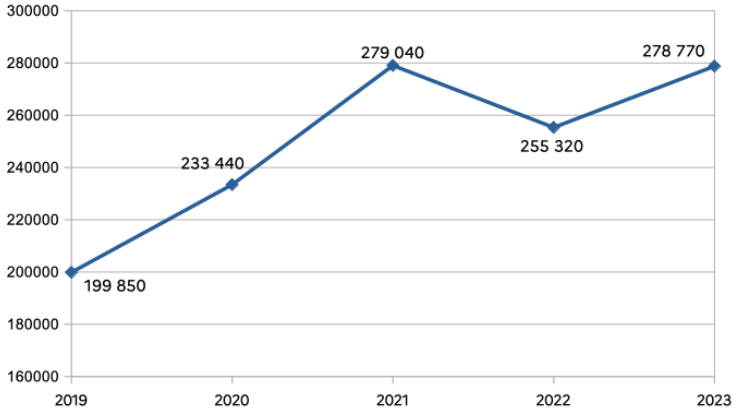
En dehors des faits détectés par le biais des plateformes en ligne du ministère de l'Intérieur, **278 770 atteintes numériques** ont été enregistrées en 2023 par les services de police et de gendarmerie. 255 320 atteintes numériques avaient été identifiées en 2022.

Au total, au cours des 5 dernières années, de 2019 à 2023, une augmentation de 40% des infractions numériques a été constatée, soit une moyenne annuelle de 8%.

Plusieurs hypothèses peuvent expliquer la hausse observée au cours des dernières années : un développement des usages numériques et un accroissement de la surface d'attaque possible, mais aussi une amélioration du signalement des infractions. **La persistance de la menace demeure ainsi une tendance de fond.**

Néanmoins, un certain nombre d'infractions numériques ne fait pas pour autant encore l'objet d'un dépôt de plainte ou d'un signalement. Il existe une partie significative de la cybercriminalité qui n'est pas enregistrée dans les données judiciaires.

+ 40%
d'atteintes numériques en 5 ans



Infractions liées au cyber

Plateformes en ligne du ministère de l'Intérieur

Les données issues des trois plateformes en ligne du ministère de l'Intérieur permettent de compléter l'état de la menace.

PERCEV@L

La plateforme Perceval, qui permet de signaler les usages frauduleux des cartes bancaires, a enregistré 259 094 **signalements**[2] en 2023.

PHAROS

La plateforme Pharos, qui permet de signaler les contenus illicites en ligne, a reçu 211 543 **signalements**[3] en 2023.

THESEE

La plateforme Thésée, qui permet aux victimes ou témoins d'escroqueries sur internet de déposer plainte ou de signaler l'infraction en ligne, a enregistré 104 439 **déclarations**[3] en 2023.

1. Service statistique de la sécurité intérieure – Les infractions liées au numérique enregistrées par la police et la gendarmerie de 2016 à 2023 : Panorama d'une criminalité hétérogène. (https://www.interieur.gouv.fr/Media/SSMSI/Files/Interstats-Analyse-67-Les-infractions-liees-au-numerique-enregistrees-par-la-police-et-la-gendarmerie-de-2016-a-2023-Panorama-d-une-criminalite-heterogene/?nomobredirect=true)
2. Chiffres fournis par l'Unité Nationale Cyber de la gendarmerie nationale.
3. Chiffres fournis par l'Office Anti-Cybercriminalité de la police nationale.

Répartition des infractions

La répartition observée en 2023 en France entre les principales catégories d'infractions numériques s'inscrit dans la **continuité des années précédentes.**

Les atteintes aux biens représentent la majorité des infractions enregistrées. 130 000 escroqueries ont été répertoriées en 2023, représentant 79% des atteintes numériques aux biens.

Atteintes aux biens

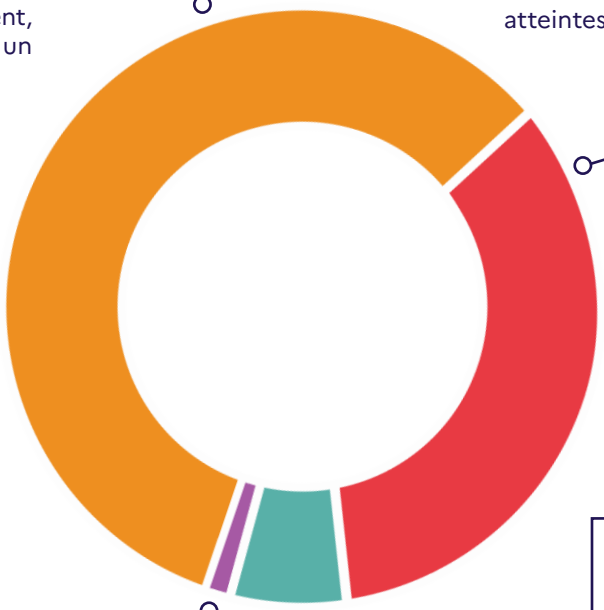
59%

Ex : escroqueries, détournement de moyens de paiement, infractions occasionnant un préjudice financier...

Atteintes aux personnes

34,5%

Ex : harcèlement, injures, menaces, discriminations, atteintes aux mineurs...



Atteintes aux législations et règlementations spécifiques numériques

0,5%

Ex : infractions au droit d'auteur, infractions au RGPD...

Atteintes aux institutions et à l'ordre public

6%

Ex : troubles à l'ordre public, atteintes à la sûreté de l'État et aux institutions, trafics, contrefaçon, recel...

Atteintes aux systèmes d'information

Les atteintes aux systèmes d'information dites atteintes aux systèmes de traitement automatisé des données (ASTAD) constituent une **catégorie spécifique au cyber**.

Elles peuvent aller de la simple intrusion, par exemple dans des boîtes courriel ou des comptes de réseaux sociaux, jusqu'à la mise hors service de l'outil numérique atteint, comme dans le cas d'une attaque par rançongiciel. On y retrouve également les attaques par déni de service ou les défigurations de sites internet.

En 2023, ce sont **17 700 atteintes aux systèmes d'information** qui ont été enregistrées par les services de police et de gendarmerie sur le territoire français. Ces infractions représentent au total 6,30% des infractions numériques de l'année.

Les atteintes aux systèmes d'information ont la particularité d'être **transverses aux atteintes aux personnes et aux atteintes aux biens.** 98% de ces infractions relevaient en 2023 des atteintes aux biens.

17 700

Atteintes aux systèmes d'information en 2023

FOCUS

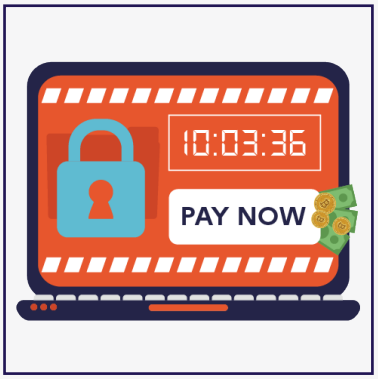
Rançongiciels

L'année écoulée, **542 saisines** suite à des attaques par rançongiciel ont été enregistrées par la **section J3 du Parquet de Paris**, spécialisée dans les atteintes aux systèmes de traitement automatisé de données. 425 saisines avaient été effectuées en 2022.

Ce chiffre représente une augmentation de 28% entre 2022 et 2023.

L'augmentation du volume des attaques s'explique par une industrialisation des processus, dans un marché criminel lucratif qui attire chaque jour de nouveaux cybercriminels. Le rançongiciel en tant que service permet aussi une démocratisation de ce type d'attaque.

Enfin, le volume des **fuites de données a également progressé en 2023**. Ces données concernent notamment des accès initiaux qui constituent autant de portes d'entrée supplémentaires sur des systèmes d'information.



+28%

en 2023 de saisines du parquet de Paris concernant des attaques par rançongiciel

Préjudices, victimes et mis en cause

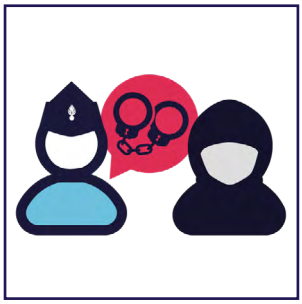
Le préjudice de l'ensemble de la cybercriminalité en France reste difficile à évaluer, mais il peut être estimé à plusieurs centaines de millions d'euros en préjudices directs, et plusieurs milliards d'euros en préjudices directs et indirects par an.

50%

Les femmes âgées de 18 à 44 ans ont représenté 50% des victimes d'une atteinte numérique à la personne en 2023, alors que cette catégorie ne constituait que 16% de la population française au 1er janvier 2024[1].

+45%

Même si elles n'ont représenté que 9 710 infractions, une hausse significative des atteintes numériques à l'encontre des mineurs est à noter en 2023. Au cours des 5 dernières années, ces atteintes ont augmenté de 45%, soit une augmentation annuelle moyenne de 13%.



47 000

Le nombre de mis en cause pour des atteintes numériques s'est élevé à 47 000 personnes en 2023.

En ce qui concerne les atteintes aux biens, il s'agit d'hommes majeurs de moins de 45 ans dans 62% des cas.

1. INSEE – Bilan démographique 2023

3 ZOOM SUR LES ESCROQUERIES EN LIGNE

Les escroqueries ont représenté les infractions numériques les plus fréquemment enregistrées au cours de l'année 2023. Les cyberattaquants, toujours créatifs, ajustent leurs stratégies pour exploiter les avancées technologiques et les tendances sociétales.

Le ***smishing***, contraction de ***SMS*** et de ***phishing***, est une technique d'attaque par laquelle les acteurs malveillants tentent d'obtenir des **données sensibles (numéros de cartes bancaires, identifiants de connexion, etc.)** et de dérober l'argent des victimes par le biais de **messages textes frauduleux**.

Dans ces messages, les attaquants se font passer pour des entités légitimes qui invitent par exemple à récupérer un **colis**, un **titre de transport** ou encore à renouveler sa **carte vitale**.

Les **fausses transactions s'opèrent souvent** *via* des sites internet utilisant l'apparence de sites légitimes. Ces reproductions ont pour objectif de **tromper la vigilance de l'utilisateur** et de l'inciter à divulguer des informations sensibles telles que des **identifiants de connexion** ou des **données bancaires**.

Il s'agit généralement de **faux sites marchands** ou de **fausses annonces** (achat, vente, location). La victime pense faire une bonne affaire, mais ne reçoit pas sa commande ou verse de l'argent pour une location d'un bien en réalité inexistant.

Concernant l'escroquerie aux **faux investissements**, l'escroc contacte la victime *via* les réseaux sociaux, par téléphone ou par courriel pour l'amener à investir dans un faux produit financier. Il peut s'agir de **faux trading**, de **forex**, de **crypto-actifs**, de **biens immobiliers** ou de tout autre support d'investissement.

Ces escrocs s'appuient sur trois types de services : des **fournisseurs de moyens** chargés de constituer les fichiers clients, des **démarcheurs** organisés depuis des centres d'appels et des **blanchisseurs d'argent sale**.

Les **faux ordres de virements** (FOVI) sont des escroqueries sur fond d'ingénierie sociale qui visent à détourner un virement bancaire vers le compte d'un malfaiteur se faisant passer pour quelqu'un de légitime. Il s'agit de la **fraude au président** et de la **fraude au changement de RIB**.

La fraude au président consiste à manipuler un collaborateur habilité à effectuer les paiements de l'entreprise, en usurpant par exemple l'identité d'un dirigeant de la société.

Dans le cas de fraudes au changement de RIB, l'escroc usurpe l'identité d'un fournisseur ou d'un salarié pour faire opérer un changement de RIB. Dans certains cas, cette fraude fait suite au piratage de la messagerie de la personne ou de l'entité usurpée.

Cas concret : fraude au faux conseiller bancaire

L'attaquant se présente comme un conseiller bancaire ou le service anti-fraude de la banque intervenant dans l'urgence pour corriger de supposées opérations frauduleuses sur le compte de la victime. En réalité, il lui fait réaliser des achats en ligne ou des virements bancaires.

Selon le cas d'espèce, plusieurs **infractions** sont susceptibles d'être retenues : collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite ; escroquerie commise en bande organisée ; accès frauduleux à un système de traitement automatisé de données.

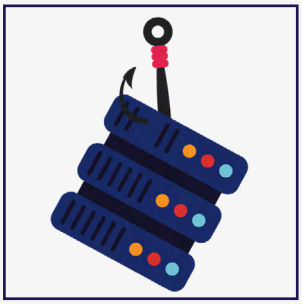
Ces infractions sont prévues et réprimées par le Code Pénal. Les peines peuvent aller jusqu'à **10 ans d'emprisonnement et un million d'euros d'amende.**

Source : Canva Creative Studio - Panneaux bande dessinée

En juin 2023, Mme Martin reçoit l'appel d'une personne qui se présente comme étant son conseiller bancaire. Ledit conseiller lui fait réaliser plusieurs manipulations bancaires dont un virement pour mettre ses fonds en sécurité sur le compte d'un responsable de la banque. Au final, en 2h20 d'échange téléphonique, Mme Martin a perdu 20 400 euros.

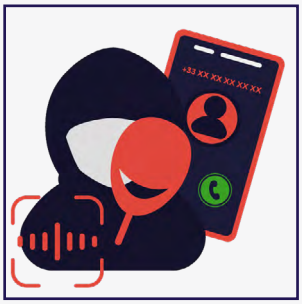
Témoignage issu d'une procédure judiciaire en cours, anonymisé avec l'accord de la victime

Mode opératoire



Les escrocs récupèrent des **données personnelles de leurs victimes** notamment sur le ***darkweb***, gratuitement ou contre faible paiement pour mener à bien leurs attaques et gagner en crédibilité lors de l'échange avec la victime.

Ils créent alors un **effet de surprise** et exercent une **pression psychologique** insistant principalement sur **l'urgence à agir**, pour induire les victimes en erreur.



Ils peuvent s'appuyer sur des **technologies modernes** pour modifier leur voix, usurper un numéro de téléphone ***(spoofing)*** et se rendre **quasi anonymes**.

02 Des cybercriminels à l'affût

DES CYBERCRIMINELS À L'AFFÛT

02

1 DE QUI PARLE-T-ON ?

Les caractéristiques des cyberdélinquants

Les possibilités d'anonymisation permises par internet et divers outils ainsi qu'une **prise de risques physiques limitée** offrent un sentiment d'impunité aux cybercriminels. La cyberdélinquance s'affranchit en outre des frontières.

> « Les cybercriminels attaquent en masse, se montrent créatifs et à l'affût de toute nouvelle opportunité possible. Ils sont susceptibles d'affecter un large éventail de la population française. »

Il s'agit d'un écosystème mouvant, international et protéiforme qui se compose d'**une diversité d'acteurs**, allant de l'amateur à la structure organisée. Des cybercriminels indépendants et experts spécialisés dans leurs domaines gravitent également autour de certains groupes.

Une **professionnalisation des cybercriminels** est par ailleurs à noter, de même qu'une tendance à l'**industrialisation des cyberattaques**, avec des niveaux de technicité variables. La multiplication des attaques est facilitée par l'ampleur des services criminels proposés clé en main (cybercriminalité en tant que service, *Cybercrime-as-a-Service*). L'année 2023 s'est inscrite dans la continuité de cette tendance.

À cela s'ajoute le **développement croissant de l'écosystème de la cybercriminalité**, au sens économique du terme.

Les motivations des cybercriminels sont majoritairement financières, mais elles peuvent également être liées à des considérations idéologiques (politiques ou religieuses), de prédation sexuelle, de haine en ligne, ou encore à la recherche de notoriété.

Les principaux acteurs cybercriminels peuvent être classés en plusieurs catégories :

	Individu seul	Bande organisée	Groupe bénéficiant des moyens d'un Etat
Atteintes aux biens, atteintes aux systèmes d'information	Pirates informatiques		
	Cybermilitants ou hacktivistes		
	Spécialistes des escroqueries		
	Trafiquants, commerces illicites		
	Intermédiaires, mules		
	Amateurs		
Atteintes aux personnes	Harceleurs / violences morales		
	Proxénètes		
	Pédocriminels		

Exemples d'acteurs cybercriminels

FOCUS

Exemples de 3 typologies de cybercriminels

LES AMATEURS : des acteurs imprévisibles et autodidactes

Composition : principalement des individus seuls

Motivations : financières, idéologiques, ego, atteintes aux personnes

Niveau technique : variable (faible à intermédiaire) et souvent autodidacte

Visibilité : en recherche de reconnaissance de leurs pairs

Activité : acteur isolé, activité secondaire

Exemple : tenter une intrusion dans le système d'information d'un établissement scolaire pour modifier des résultats d'examen

LES HACKTIVISTES : des acteurs nombreux et engagés

Composition : majoritairement des groupes organisés et quelques acteurs isolés

Motivations : désinformation, influence, haine en ligne

Niveau technique : très variable, s'allient entre eux pour augmenter leur cercle d'influence, leur force de frappe ainsi que leurs connaissances techniques

Visibilité : degré de discrétion suffisant pour se protéger

Activité : communication massive sur les réseaux sociaux ou les messageries chiffrées, alliance entre groupes pour un effet de masse

Exemple : saturer des sites de transports pour bloquer les services de réservation de billets en ligne pendant plusieurs heures et faire passer un message idéologique

LES PIRATES INFORMATIQUES : des professionnels motivés par le gain financier

Composition : groupes organisés, indépendants et experts spécialisés

Motivations : gain financier

Niveau technique : intermédiaire à élevé

Visibilité : restreinte concernant leurs activités sur les forums ou les canaux cybercriminels. Communiquent cependant sur leurs victimes pour les contraindre à payer une rançon

Activité : professionnalisation, développement d'outils pour une mise en location ou en vente. Organisation décentralisée avec des rôles définis pour chaque acteur

Exemple : mener des attaques par rançongiciel pour paralyser le système d'information de la victime, dérober des données, et exiger une rançon

La criminalité organisée dans le cyberespace : ce que dit la loi

> « La cybercriminalité constitue l'une des menaces les plus critiques en matière de criminalité organisée. »

Cette dernière notion est définie dans la législation française principalement par **deux articles du Code Pénal**.

Le premier est la circonstance aggravante de la **commission d'un crime ou d'un délit en bande organisée** (article 132-71 du Code Pénal).

Le législateur sanctionne plus sévèrement au travers de cette circonstance aggravante les activités illicites des groupes criminels, c'est à dire des individus qui s'unissent spécifiquement pour préméditer et commettre des infractions.

Le second est l'**association de malfaiteurs** (article 450-1 du Code Pénal). Contrairement à la bande organisée qui est une circonstance aggravante, l'association de malfaiteurs est une infraction à part entière.

2 LES CYBERDÉLINQUANTS SPÉCIALISÉS DANS LES RANÇONGICIELS

L'étude de la typologie des familles de **rançongiciels ayant affecté la France en 2023 révèle 4 profils principaux de cybercriminels** illustrés ci-dessous.

MENEURS

Principaux groupes cybercriminels ou familles de rançongiciel actifs en France, innovants, ayant des impacts significatifs sur les organisations.

COMPÉTITEURS

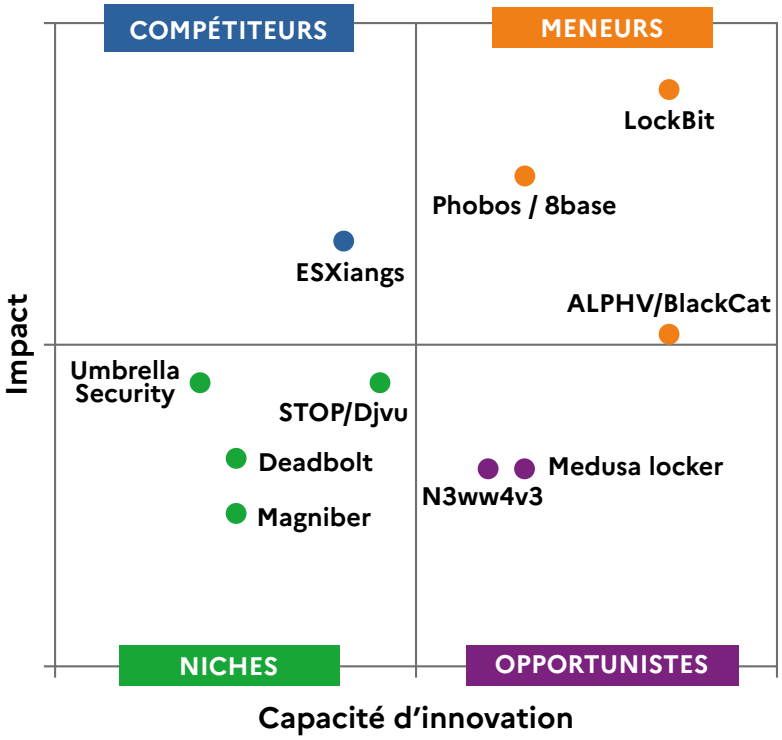
Familles pouvant impacter de nombreux secteurs mais ayant des capacités limitées pour mettre en œuvre de nouvelles techniques d'attaques.

OPPORTUNISTES

Familles ayant la capacité d'anticiper et d'identifier de nouvelles techniques malveillantes ciblées, sans adresser un spectre large.

NICHES

Familles se concentrant avec succès sur des secteurs spécifiques à faible protection tels que les particuliers et les petites entreprises.



Évaluation des 10 principales familles de rançongiciel ayant touché la France en 2023 d'après les données de la section J3 du parquet de Paris

Les noms attribués aux rançongiciels font référence au **maliciel** utilisé pour perpétrer l'attaque et souvent au **groupe de cybercriminels** qui la met en œuvre (*LockBit, Phobos, ALPHV/BlackCat*, etc.).

> « En marge des acteurs principaux et médiatisés du rançongiciel figurent d'autres groupes, moins dotés en moyens stratégiques ou techniques ou encore moins visibles, mais tout aussi néfastes. »

Des acteurs de niche ou opportunistes vont par exemple exploiter des vulnérabilités sur une courte période, ou bien cibler des TPE (très petites entreprises) ou des particuliers.

L'univers des rançongiciels est constitué d'une nébuleuse d'acteurs malveillants utilisant parfois plusieurs souches pour parvenir à leurs fins, et se renouvelant constamment.

Le cyberespace étant sans frontières, les attaquants opèrent depuis les différents continents. Les groupes les plus médiatisés sont majoritairement russophones.

Une attaque par rançongiciel implique en général : **une équipe de management, des développeurs** (qui produisent ou modifient des solutions déjà existantes), **des pentesteurs** (chargés de trouver des portes d'entrées sur les systèmes des organisations ciblées), des ***initial access brokers*** (revendeurs spécialisés d'accès initiaux) et **des affiliés** (qui organisent les attaques grâce à ces outils).

Enfin, viennent s'ajouter **des blanchisseurs**, dont l'une des tâches est de transformer en monnaie fiduciaire les crypto-actifs perçus lors du versement des rançons.

3 LES CYBERCRIMINELS SPÉCIALISÉS DANS LES ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ

La finalité d'une attaque par déni de service est de **rendre indisponible** un site *web*, une application ou un réseau, afin de perturber l'activité ou de nuire à l'image de l'entité ciblée.

De fait, n'importe quelle infrastructure connectée à internet peut être la cible de ce type d'attaque.

Les préjudices générés par les attaques *DDoS* varient. Dans le cas d'une entreprise, rendre un site *web* indisponible peut aller jusqu'à engendrer des **pertes financières conséquentes**.

Les cybercriminels spécialisés dans les attaques *DDoS* sont souvent liés à **des groupes hacktivistes,** particulièrement actifs en 2023.

Leurs motivations peuvent être d'ordre financier, idéologique (religieux et politique), concurrentiel, voire relever du défi ou de la vengeance. Les plus actifs en 2023 ont mis leurs compétences et outils à disposition d'autres attaquants pour promouvoir leur idéologie à des fins de déstabilisation.

De la désinformation, des vols ou des divulgations de données peuvent parfois être associés aux attaques *DDoS* ou menés en complément des défigurations de sites internet.

L'objectif est de **nuire à la réputation** de l'entité et/ou du pays ciblé, et de **diffuser des messages de propagande**.

> « Les groupes hacktivistes constituent une menace régulière car ils ciblent tous les secteurs. »

Ces attaques coïncident le plus souvent avec l'**actualité géopolitique**, **sociale et de grands évènements**, des décisions de politique étrangère et des visites diplomatiques associées aux pays ciblés.

Outre le secteur public, les secteurs des transports, de l'énergie, de la finance ou des médias ont été visés de manière récurrente.

Les acteurs malveillants spécialisés dans les attaques *DDoS* évoluent constamment et demeurent **imprévisibles**.

Faisant preuve de curiosité et de détermination, ils se **professionnalisent** et développent leurs **propres outils d'attaque** qu'ils commercialisent.

D'autres groupes profitent de leur cercle d'influence, démultiplient leur pouvoir de nuisance par des alliances à plus ou moins long terme, ponctuelles ou régulières.

	Anonymous Sudan	**NoName057(16) *DDoSia Project***
Apparition	Janvier 2023	Mars 2022
Motivations	Hacktivisme	Hacktivisme
Types d'attaques	• Attaque *DDoS* • Défiguration de sites *web* • Désinformation	• Attaque *DDoS* • Exfiltration de données • Désinformation
Secteurs ciblés	Tous les secteurs	Tous les secteurs
Pays ciblés	Tous horizons : pays de l'UE, Moyen Orient, Afrique, État-Unis, Israël	• Pays membres de l'OTAN • Pays alliés à l'Ukraine
Particularités du groupe	• Professionnalisation et commercialisation des outils (*DDoS*) • Potentielles opérations sous faux drapeaux, à des fins de déstabilisation et de propagande	• Mise à disposition d'outils prêts à l'emploi • Les utilisateurs nommés «clients» sont rémunérés *au prorata* de leur participation aux attaques

Exemples de groupes ayant opéré des attaques DDoS en 2023

Vers une cybercriminalité plus accessible ?

Mener des attaques complexes n'est plus seulement l'apanage de pirates chevronnés. La cybercriminalité en tant que service et l'assistance apportée par l'intelligence artificielle permettent à des délinquants aux compétences informatiques limitées de se lancer dans des activités cybercriminelles.

Les amateurs sont cependant loin d'avoir supplanté les spécialistes. Certains outils et techniques innovants restent réservés aux cybercriminels ayant de solides bases techniques.

Outils et services cybercriminels clé en main

Des attaquants peu qualifiés sont désormais en mesure de mener des opérations grâce à des solutions clé en main fournies par des cybercriminels. Ces derniers mettent à disposition notamment des *botnets*, des kits d'hameçonnage, des maliciels, des rançongiciels, etc.

Les outils et abonnements sont proposés sur des forums cybercriminels ou sur des applications telles que Telegram (par exemple des services d'attaques par déni de service distribué, pour un tarif pouvant osciller entre quelques dizaines et plusieurs centaines d'euros par attaque).

Réseaux sociaux et trafics illicites

Outre le *darkweb*, les réseaux sociaux communément utilisés constituent également une porte d'entrée vers des sites frauduleux grâce à leur large diffusion et leur facilité d'utilisation.

Il peuvent être utilisés par les trafiquants pour rabattre des « clients » ou des victimes et les amener à échanger ensuite sur des messageries chiffrées. Toutes les catégories de trafics sont concernées : armes, stupéfiants, médicaments, fausse monnaie, animaux protégés ou données personnelles.

L'ingénierie sociale ou l'exploitation de la psychologie humaine et des biais cognitifs

Le facteur humain reste l'une des principales vulnérabilités exploitées par les cyberdélinquants malgré la diffusion de nombreuses campagnes de prévention.

Les escrocs peuvent s'appuyer sur des scénarios pré-définis. Ils multiplient les leviers psychologiques pour parvenir à leurs fins : une situation alarmante nécessitant une action urgente, une promesse de gains financiers rapides, une usurpation d'identité, la promesse d'une relation amoureuse, etc.

Quelle que soit la technique de manipulation mise en œuvre, l'objectif est toujours de dérober des fonds à la victime.

Autres techniques notables en 2023

OTP bots : le recours accru à des authentifications à plusieurs facteurs[1] a amené les pirates à développer de nouvelles techniques pour les contourner.

Les *OTP bots* sont des dispositifs s'insérant entre les utilisateurs et les services auxquels ils se connectent. Le code d'authentification est récupéré puis utilisé immédiatement par le cyberdélinquant qui accède alors aux données ou aux fonds de la victime.

Malvertising et *SEO poisoning* : ces techniques visent à faire remonter artificiellement des résultats trompeurs sur les moteurs de recherche.

L'objectif est notamment d'amener les internautes à télécharger un maliciel sous l'apparence d'un logiciel légitime.

FOCUS

Les usages criminels de l'Intelligence Artificielle en 2023

Les progrès de l'Intelligence Artificielle (IA) et son usage par les cyberdélinquants représentent aujourd'hui, comme pour les années à venir, un défi majeur pour les forces de sécurité intérieure.

Depuis l'avènement des larges modèles de langage sur lesquels s'appuie l'IA générative, nombreuses sont les opportunités d'imposture que ce soit **dans le domaine de l'image, de l'audio ou du texte.**

Et l'espace cyber ne manque pas à l'appel puisqu'il y est possible de générer, modifier ou optimiser des **maliciels** ou encore de réaliser des **campagnes d'hameçonnage**.

L'IA offre ainsi la possibilité d'améliorer les campagnes de *phishing* non seulement en générant de nouvelles techniques mais aussi en démultipliant les cibles potentielles notamment par du multilinguisme.

Ces techniques, réservées à une criminalité organisée il y a quelques années, sont aujourd'hui à la portée du délinquant **d'opportunité sans compétence ni budget importants.**

L'IA, c'est encore la possibilité de gérer des réseaux de **machines zombies** (*botnets*) et d'augmenter l'efficience des attaques de type *DDoS* par exemple en adaptant les schémas d'attaques aux mesures de sécurité mises en place sur les systèmes d'information visés.

Parmi les enjeux à fort impact, le phénomène des ***deepfakes,*** au regard de la célérité et de la diversité des développements, est à prendre en compte dès à présent par les forces de sécurité intérieure.

Toujours plus réalistes, ces impostures accroissent considérablement l'efficacité des faux ordres de virement, la vraisemblance des théories complotistes ou encore des atteintes à l'identité numérique.

1. L'authentification à plusieurs facteurs consiste à exiger au moins deux éléments d'identification pour accéder à un service. Il peut s'agir d'un mot de passe, d'un code fourni par SMS, courriel, application externe installée sur le smartphone de l'utilisateur, voire d'une empreinte digitale.

03 Lutter contre toute forme de délinquance en ligne

LUTTER CONTRE TOUTE FORME DE DÉLINQUANCE EN LIGNE

03

1 ECOSYSTÈME ÉTATIQUE DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Services du Premier ministre

Ministère de la Justice

Ministère de l'Intérieur

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Construit et organise la protection de la nation face aux cyberattaques en contribuant à renforcer le niveau de cybersécurité global et la stabilité du cyberespace.

Assure la défense des systèmes numériques d'intérêt pour la nation.

Juridiction nationale chargée de la lutte contre la criminalité organisée

La section J3 Cybercriminalité du parquet de Paris, spécialisée dans la lutte contre la cybercriminalité, exerce une compétence concurrente nationale pour les dossiers de cyberattaques de grande ou de très grande complexité, notamment pour toutes les infractions d'atteintes aux systèmes de traitement automatisé de données et de cybersabotage de tels systèmes.

COMCYBER-MI

Compétences rares projetables

- *INVESTIGATIONS SPÉCIALISÉES*
- *EXPERTISES NUMÉRIQUES*
- *SCIENCES DE LA DONNÉE*

Centre national de formation cyber

- *INGÉNIERIE DE FORMATION*
- *PARTENARIATS ACADÉMIQUES*

Stratégie et anticipation

- *ÉTAT DE LA MENACE*
- *GESTION DE CRISE*
- *STRATÉGIE MINISTÉRIELLE*
- *COOPÉRATION INTERNATIONALE*

OFAC : Office Anti-Cybercriminalité

L'OFAC contribue à la répression des formes spécialisées, organisées ou transnationales de la cybercriminalité et aux actions de prévention. Il est notamment chargé d'animer et de coordonner au plan opérationnel la lutte contre la cybercriminalité et constitue le point de contact central dans les échanges opérationnels internationaux.

UNCyber : Unité Nationale Cyber

L'UNCyber coordonne le dispositif des 10 000 cybergendarmes répartis sur le territoire, déclinant les fonctions contact, prévention et investigation dans le cyberespace, et conduit les enquêtes visant la cybercriminalité organisée ou transnationale pour la gendarmerie.

BL2C : Brigade de Lutte Contre la Cybercriminalité

La BL2C a une mission d'investigation judiciaire concernant les infractions liées aux atteintes aux systèmes de traitement automatisé de données et appuie techniquement les autres services de la Préfecture de Police de Paris.

DGSI : Direction Générale de la Sécurité Intérieure

La DGSI est compétente sur les menaces cyber portant sur les intérêts fondamentaux de la nation. Elle héberge en outre les capacités techniques mutualisées de captation, de déverrouillage et de déchiffrement, accessibles à l'ensemble des acteurs de l'écosystème judiciaire et couvertes par le secret de la défense nationale.

2 EVOLUTIONS JURIDIQUES

L'année 2023 a vu l'adoption de la **loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI)** - destinée en partie à répondre aux nouveaux enjeux de lutte contre la cybercriminalité - et de la **loi d'orientation et de programmation du ministère de la Justice (LOPMJ)**.

L'apparition de nouvelles infractions dans le droit français

L'enjeu principal de la LOPMI a été la lutte contre les écosystèmes criminels présents sur internet et notamment les plateformes constituées en places de marché *(marketplaces)* de produits ou de services illicites.

La loi a créé d'une part le **délit d'administration d'une plateforme en ligne proposant des produits illicites**, et d'autre part le **délit d'intermédiation ou de séquestre pour les plateformes en facilitant la vente**.

Les places de marché illicites offrent en effet aux délinquants l'avantage d'un relatif anonymat. Elles leur permettent de commercialiser ou d'échanger des produits variés comme des informations volées, des contenus illicites, des armes, des explosifs ou des produits stupéfiants.

Lorsque les transactions sont réalisées en actifs numériques, leur traçage, la saisie de fonds, et l'identification de leurs propriétaires peuvent être techniquement plus complexes que pour les flux financiers traditionnels.

L'émergence et la diversification des places de marché ont permis aux cyberdélinquants de mettre en place des processus de vente relevant quasiment du commerce en ligne (catalogue avec descriptif, stock en temps réel, avis clients, notes des vendeurs, etc).

Le travail des enquêteurs facilité

La LOPMI permet désormais aux enquêteurs de réaliser des investigations plus poussées dans le cadre des **enquêtes sous pseudonyme (ESP)**.

Les enquêteurs peuvent procéder à un **achat de confiance** en réalisant la transaction d'un produit ou d'un service illicite afin de recueillir de nouveaux indices et traces de la commission des faits (article 230-46 3e du Code de procédure pénale).

Les enquêteurs peuvent également réaliser un **coup d'achat**, c'est-à-dire prendre un rendez-vous avec le vendeur sans toutefois que la vente ne soit consommée, en vue de son interpellation en flagrant délit (article 230-46 4e du Code de procédure pénale).

Ces deux techniques sont soumises à l'autorisation préalable du procureur de la République ou du juge d'instruction saisi des faits.

> « Afin de gagner plus rapidement la confiance des suspects, les enquêteurs peuvent désormais mettre à leur disposition des moyens juridiques, financiers, logistiques, de dépôt, d'hébergement, de conservation et de télécommunication. »

De plus, la LOPMJ permet, pour les enquêtes ou informations relatives à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement, de **procéder à l'activation à distance d'un appareil électronique**, à l'insu ou sans le consentement de son propriétaire ou de son possesseur, aux seules fins de procéder à sa localisation en temps réel (article 230-34-1 du Code de procédure pénale).

Cette géolocalisation, par exemple d'un véhicule connecté, peut être réalisée grâce aux moyens de l'État soumis au secret de la défense nationale.

Enfin, sur le plan financier, les enquêteurs peuvent désormais, après accord du procureur de la République ou du juge d'instruction, **procéder à la saisie d'actifs numériques par tout moyen** (article 706-154 du Code de procédure pénale). Ce régime est calqué sur celui des actifs bancaires afin d'offrir une saisie rapide et facilitée. Les actifs numériques étant particulièrement volatiles et fongibles, une telle mesure permet de suivre plus rapidement et d'identifier plus facilement les bénéficiaires de la commission d'infractions dissimulées.

Apports juridiques, réglementation et doctrine

Loi d'orientation et de programmation du ministère de l'Intérieur :

23 JANVIER 2023

Deux nouvelles infractions spécifiques cyber sont créées (voir page précédente).

Le quantum des peines est aggravé.

Les moyens d'enquête relatifs à la cybercriminalité (enquête sous pseudonyme, saisie d'actifs numériques) sont renforcés.

Cour de cassation, chambre criminelle - affaire ENCROCHAT - n°22-83.613

4 AVRIL 2023

Cet arrêt permet désormais aux services d'enquête d'exploiter les données criminelles captées sans produire d'attestation de sincérité, dans le cas de figure où les données captées ne sont pas chiffrées et donc reçues en clair sur le dispositif permettant de les capter. Les indications techniques relatives au processus de captation étant couvertes par le secret de la défense nationale, les enquêteurs ne sont pas tenus d'exposer lesdites techniques.

Cour de cassation, chambre criminelle - affaire ENCROCHAT - n°22-84.475

10 MAI 2023

Il s'agit du premier arrêt affirmant que l'attestation de sincérité n'est pas requise dès lors que les données captées n'étaient pas chiffrées. Le service d'enquête ayant procédé à la captation n'est pas tenu de remettre une attestation de sincérité des résultats transmis.

Loi d'orientation et de programmation du ministère de la Justice :

20 NOVEMBRE 2023

Les enquêteurs ont désormais la possibilité de mettre en œuvre une géolocalisation en temps réel par activation à distance de la puce GPS d'un appareil numérique.

Digital Service Act (DSA)

17 FÉVRIER 2024

ENTRÉE EN VIGUEUR APPLICABLE DÈS LE 25 AOÛT 2023 POUR LES «TRÈS GRANDS MOTEURS DE RECHERCHE»

La Commission européenne a ouvert en décembre 2023 la première procédure contre la société X (ex-Twitter) pour des manquements présumés aux obligations de lutte contre les contenus illicites et de désinformation, des manquements aux obligations de transparence, et une interface utilisateur trompeuse.

Cour de justice de l'Union européenne - Grande chambre - M.N (Encrochat) - C-670/22 (Question préjudicielle allemande)

30 AVRIL 2024

Au sein de l'UE, dans le cadre d'une décision d'enquête européenne, le partage des éléments de preuves numériques entre États membres s'applique en matière de captation des données criminelles, quand bien même l'État récipiendaire (Allemagne) n'applique pas le même cadre juridique que l'État d'exécution (France). Toutefois, la possibilité d'exercer des recours contre la captation doit demeurer dans l'État d'exécution.

GENESIS MARKET

4 AVRIL 2023

Les faits :

La plateforme ***« genesis market »*** revendait des données personnelles et des solutions permettant à ses clients d'usurper l'identité de victimes et d'accéder illégalement à leurs comptes sans déclencher de mesures de sécurité. On dénombre 1,5 million de victimes et 80 millions de données personnelles volées.

L'enquête :

Lancée en 2019, cette opération a regroupé 17 pays dont la France représentée par l'Office Anti-Cybercriminalité (OFAC).

Les résultats :

- 200 perquisitions ;
- 119 interpellations dont 3 en France ;
- Fermeture de la plateforme.

FAUSSES CONVOCATIONS

19 JUIN 2023

Les faits :

Initiée en 2020, une campagne de **courriels frauduleux** usurpant l'identité de hautes personnalités policières et judiciaires a inondé les boîtes courriel de particuliers les accusant de faits graves et les menaçant de poursuites judiciaires en cas de non-paiement d'une prétendue amende.

L'enquête :

Dès octobre 2022, la France a ouvert un dossier EUROJUST afin de lutter contre ce phénomène aux côtés de partenaires européens. L'enquête a conduit des gendarmes à mener des investigations sur le sol ivoirien en coopération avec les autorités du pays et le soutien d'Interpol. Un réseau a été découvert en France. Les enquêteurs de l'OFAC, de l'UNCyber, de la section de recherches de Versailles et de la brigade de recherches de Nice ont interpellé plusieurs équipes de criminels pour le blanchiment d'extorsions représentant un préjudice de 3 millions d'euros.

Les résultats :

- 300 dépôts de plainte en France ;
- 8 équipes indépendantes identifiées ;
- 18 interpellations.

RAGNAR_LOCKER

16 AU 20 OCTOBRE 2023

Les faits :

Ragnar_Locker est un groupe criminel actif depuis 2019 spécialisé dans les cyber-attaques par rançongiciel. Ses membres pratiquent la double extorsion auprès des victimes en chiffrant leurs données et en les menaçant de les diffuser sur internet.

L'enquête :

Une démarche conjointe de la France et de plusieurs pays, soutenue par Europol, a permis de mener à bien plusieurs actions à l'encontre du groupe. En France, l'enquête était conduite par des gendarmes de l'Unité Nationale Cyber (UNCyber).

Les résultats :

- Fermeture d'un site *web* ;
- 4 interpellations en France, en Espagne et en Lettonie.

FRENCHIE

25 OCTOBRE 2023

Les faits :

Depuis 2019, un jeune Français revendait sur des forums cybercriminels des outils facilitant le déploiement de rançongiciels, l'extraction de données ou encore l'infection massive d'ordinateurs. Il les développait seul ou au sein de groupes de pirates informatiques.
Ces services criminels étaient ensuite vendus à chaque utilisation ou sous la forme d'un abonnement hebdomadaire.

L'enquête :

La Brigade de Lutte Contre la Cybercriminalité de la préfecture de Police de Paris a été à la manœuvre pour l'enquête.
Les activités illégales de cet acteur malveillant avaient été détectées au cours d'une autre enquête.

Les résultats :

- Interpellation du cybercriminel.

Saisies de :

- 70 000€ en crypto-actifs, d'un véhicule et de matériel numérique ;
- Condamnation à 4 ans de prison dont 2 avec sursis et à 50 000€ d'amende ;
- Confiscation de l'ensemble des saisies.

UNE MENACE GLOBALE

- 1ère apparition : **juin 2022**
- Des attaques dans **80 pays**
- Plus de **1 500 victimes**
- Préjudice de **100 millions de dollars**

UNE RÉPONSE INTERNATIONALE

- Coopération de 13 pays mise en place en janvier 2022 à EUROPOL
- Un préjudice évité estimé à 130 millions de dollars
- Plus de 300 clés de déchiffrement récupérées
- Démantèlement de l'infrastructure *HIVE* le 26 janvier 2023
- Un « *Sprint* » (réunion technique) s'est tenu à Orlando en février 2023
- Une saisie de crypto-actifs à hauteur de 570 000 euros

LES PRINCIPAUX ACTEURS DE LA COOPÉRATION INTERNATIONALE

Initiateurs du *takedown* - un des principaux serveurs sur leur territoire

L'autre principal serveur de l'infrastructure criminelle sur leur territoire

Désanonymisation des sites TOR qui a permis la localisation des serveurs

Reconstruction d'une partie de l'infrastructure *HIVE*
Identification des serveurs de contrôle dans le monde
Suivi de transactions en crypto-actifs des attaquants

Les autres acteurs :

ET SUR LE TERRITOIRE NATIONAL

- 1ère attaque : laboratoire pharmaceutique en juillet 2021
- Services enquêteurs : OFAC et DIPN de la Gironde (co-saisine)
- 59 victimes identifiées parmi lesquelles 27 ont déposé plainte
- Préjudice moyen estimé : 200 000 euros par victime (fourchette basse)
- Tous les secteurs d'activité sont touchés sur tout le territoire
- Récupération de déchiffreurs ayant notamment permis d'accompagner la remédiation du Conseil Départemental de Seine-Maritime en octobre 2022

Démantèlement de la plateforme de crypto-actifs Bitzlato

UNCyber
Direction des opérations et de l'emploi

bitzlato

ENQUÊTE

- Opération judiciaire internationale menée contre la plateforme Bitzlato le 18 janvier 2023
- Conduite sous le pilotage de l'Unité nationale cyber de la Gendarmerie nationale
- Montant estimé des fonds blanchis : 2 milliards d'euros

SAISIES

Cryptoactifs
21 000 000€

Numéraire
27 000€
31 000$

3 *véhicules*

EFFECTIFS ENGAGÉS

50 militaires de la gendarmerie

250 agents des forces de sécurité intérieure à l'échelle internationale

PARTENARIATS INTERNATIONAUX

EUROPOL EC3 European Cybercrime Centre

AP CYBORG

EC3 Forensic

Cyber intelligence team

PJ/SCID

FBI New-York et Miami

Guardia Civil-UCO

Cybercrime Division and Digital Forensic Laboratory

FIOD, cybercrime team Oost-Nederland

ÉTAPE 1

L'activité criminelle (cybercriminalité, rançongiciel, stupéfiants, pédocriminalité, etc.) génère un profit financier conséquent.

ÉTAPE 2

Les fonds illicites sont transférés sur la plateforme Bitzlato sous forme de *wallets* contenant des actifs numériques.

ÉTAPE 3

Ces transactions sont opacifiées grâce à Bitzlato et les actifs anonymisés.

ÉTAPE 4

Ces actifs sont soit échangés contre des roubles soit de nouveau transférés vers d'autres plateformes pour une nouvelle phase de blanchiment.

ÉTAPE 5

Ces fonds illicites financent d'autres activités criminelles et le train de vie des malfaiteurs.

04 Prospective

PROSPECTIVE

04

1 EN 2024, QUELLES ÉVOLUTIONS CYBERCRIMINELLES ?

A partir des tendances observées en 2023, se dégagent différents axes à suivre avec vigilance en 2024.

Sur les phénomènes cybercriminels

Atteintes aux systèmes d'information

L'année 2023 et le début 2024 ont été marqués par le **démantèlement de groupes opérant des rançongiciels** à la suite d'opérations internationales menées par les forces de l'ordre.

La plateforme de revendication et de vente de données (*DataLeak Site*) du groupe Hive a été fermée en janvier 2023. Le portail du groupe de rançongiciel Ragnar_Locker a été saisi en octobre 2023. Enfin, en février 2024, l'infrastructure de LockBit, le groupe de rançongiciel le plus offensif en France et dans le monde, a été démantelée.

Il conviendra de surveiller les **probables recompositions et réorganisations des cybercriminels** développant ou utilisant ces rançongiciels. Ces cyberattaques restent particulièrement lucratives avec des impacts critiques sur les victimes.

A noter : les **bases de données sensibles et/ou personnelles** sont la cible de nombreuses actions cybercriminelles. Des vols de données sont donc encore à anticiper.

Atteintes aux biens

Les atteintes aux biens, et en particulier les escroqueries, ont représenté la majorité des infractions cyber enregistrées en 2023 en France.

Les escrocs ont démontré l'année passée une capacité à **améliorer leurs compétences techniques.**

Ce perfectionnement devrait se poursuivre en 2024 et leur permettre de déployer des **escroqueries plus sophistiquées** notamment grâce à un recours généralisé aux *deepfakes*, ou bien d'investir d'autres terrains (rançongiciel, *botnets*, etc.)

Atteintes aux personnes

Une hausse des atteintes aux personnes et en particulier aux mineurs a été observée en 2023.

L'évolution de la pédocriminalité sera à surveiller en 2024. Il est important de prêter une attention spécifique aux évolutions des usages des jeunes en matière de réseaux sociaux pour anticiper les modes opératoires des cybercriminels.

Au fil des années, les préférences des plus jeunes diffèrent de leurs aînés et évoluent d'une tranche d'âge à l'autre.

Les pédocriminels s'adaptent en conséquence et font évoluer leurs modes opératoires en fonction du nouveau réseau en vogue. Une veille attentive s'impose en 2024 pour identifier quel pourrait être le prochain réseau social des jeunes ou à défaut les plateformes les plus utilisées, telles que les forums de jeux vidéos.

D'autre part, **l'implication de mineurs** dans des organisations cybercriminelles s'avère une tendance récurrente depuis plusieurs années. Elle reste à surveiller et à prendre en compte dans les démarches de prévention.

Un mode opératoire consiste pour les cybercriminels à se faire passer pour des jeunes mineurs de moins de 15 ans sur des forums de rencontre, à avoir des conversations de nature sexuelle avec leur cible allant jusqu'à lui fixer un rendez-vous.

Il s'agit en réalité d'un guet-apens afin d'extorquer la victime ainsi piégée. Cela s'accompagne parfois de publications sur les réseaux sociaux.

Politique et géopolitique

L'année 2023 a été marquée par les cyberattaques visant des entreprises ou des institutions françaises en résonance avec des événements sociaux, sociétaux et géopolitiques nationaux et internationaux.

Ces opérations malveillantes ont pris majoritairement la forme d'attaques par déni de service distribué (*DDoS*) ou de défigurations.

Ces attaques, menées par des acteurs isolés ou organisés, avaient pour objectif de faire passer un message revendicatif.

Elles ont essentiellement été le fait d'hacktivistes aux motivations politiques, religieuses ou bien encore sociétales.

La géopolitique, la politique en France mais aussi son actualité économique et sociale, ou encore la tenue de grands événements, constituent également des points de vigilance en 2024 car susceptibles de susciter des cyberattaques.

Une nouvelle recrudescence des attaques *DDoS* a été observée début 2024.

Sur les vecteurs facilitant la cybercriminalité

Les vecteurs utilisés par les cybercriminels évoluent au fil du temps et se combinent.

C'est par exemple le cas du **hameçonnage** *(phishing* en anglais). Celui-ci a été historiquement opéré par téléphone *(vishing*, contraction de *voice* et de *phishing)*, encore largement employé, et par courriel. S'est ensuite développé le *smishing*, contraction de SMS et de *phishing*.

Dernier venu, le ***quishing***, contraction de QR code et *phishing*, sera à suivre en 2024 s'agissant d'un phénomène émergent apparu en 2023.

La numérisation et l'interconnexion croissantes des systèmes ont continué en 2023 à apporter de nouvelles opportunités pour les cybercriminels.

Les **attaques par chaîne d'approvisionnement *(supply chain)*** seront ainsi de nouveau à surveiller avec attention en 2024.

> « En effet, le niveau de sécurité d'une organisation se mesure par rapport au maillon le plus faible de sa chaîne. »

Les cybercriminels ont conscience des opportunités liées à la chaîne d'approvisionnement.

L'attaque peut se faire par rebond d'une victime à une autre. Elle peut aussi provenir de la **compromission d'un logiciel distribué auprès de multiples organisations.**

FOCUS

L'exemple des crypto-actifs

Les cybercriminels ciblent désormais les réseaux numériques décentralisés comme les *blockchains* qui permettent d'**échanger de la valeur** sous forme de crypto-actifs **entre plusieurs adresses publiques**.

Le portefeuille (*wallet*) est un moyen d'accéder à une adresse publique.

Les **exploitations de failles dans les *smart contracts*** concernent les ***blockchains***, des réseaux numériques pour la plupart ouverts et publics. Une **erreur dans un *smart contract*** est donc visible par tous. Elle peut rapidement être exploitée à des **fins malveillantes** et relève autant d'individus isolés, jouant sur un effet d'opportunité, que de groupes organisés.

De 2021 à 2023, d'après les données publiques disponibles concernant les *blockchains*, le **cumul total des cinq principales exploitations malveillantes s'élèverait à plusieurs milliards de dollars.**

Les crypto-actifs échangés *via* des *smart contracts* le sont majoritairement dans le cadre de la **finance décentralisée**, dite *DeFi (Decentralized Finance)*. Celle-ci suit la valorisation totale des crypto-actifs, déjà en hausse en 2024, ce qui impliquera une vigilance renforcée.

Au-delà des *smarts contracts*, la cybercriminalité liée aux crypto-actifs repose principalement sur les escroqueries.

Parmi celles-ci, de **faux services financiers**, imitant les services légitimes, incitent l'utilisateur de crypto-actifs à signer une transaction qui autorise en réalité l'attaquant à vider le portefeuille de la cible. L'opération est alors réalisée grâce un **logiciel malveillant** nommé « ***draineur*** ».

Sur l'année 2023, ces « *wallets drainers* » ont dérobé plusieurs centaines de millions de dollars à des centaines de milliers de victimes dans le monde, dont des Français.

Sur les modes opératoires et les supports utilisés

Intelligence Artificielle

En 2023, l'**Intelligence Artificielle** (IA) a été utilisée de façon conséquente à des fins criminelles.

En matière d'escroqueries, les IA génératives seront de plus en plus utilisées en 2024 pour créer des vidéos mais aussi du texte plus varié, plus vraisemblable pour les opérations de *phishing*, et donc plus **difficile à détecter**. Se dessine ensuite l'**automatisation** d'une partie des tâches dans les années à venir, donc la démultiplication du nombre de victimes potentielles atteignables par chaque escroc.

L'intelligence artificielle devrait continuer à ouvrir de **nouvelles perspectives criminelles**, notamment en accroissant les possibilités de manipulation de l'information. La capacité à générer une illustration, une photo dite « ultra réaliste » *(text-to-image)* ou une vidéo rend de plus en plus vraisemblables des événements et/ou des personnes qui ne le sont pas. Cela permettra de faciliter les escroqueries, le harcèlement moral, de toucher la réputation d'une personne, et plus généralement de désinformer.

D'autre part, **créer des identités fictives** est un usage de l'IA générative appelé à se renforcer dans les prochaines années. Les groupes criminels organisés, qui s'adaptent rapidement aux évolutions techniques, pourraient y recourir pour faciliter l'**ouverture de comptes** par des personnes non-existantes, en vue de faciliter le **blanchiment** d'opérations financières illicites.

Ainsi, l'IA au service des criminels démultiplie largement les possibilités et les opportunités d'attaques tout en démocratisant les capacités de réalisation.

Des services criminels plus accessibles

Une **démocratisation** de la cybercriminalité a enfin été observée en 2023. Celle-ci s'est d'abord traduite par le développement constant de la **cybercriminalité en tant que service** *(Cybercrime-as-a-Service* ou *CaaS)*, en particulier sur les forums cybercriminels. Ces services ne sont plus uniquement réservés à des cybercriminels expérimentés. Ils deviennent accessibles à de jeunes pirates informatiques disposant de peu de moyens.

Ces derniers peuvent mener des cyberattaques grâce à des guides et des outils de plus en plus simples d'utilisation. L'année 2023 a ainsi été marquée par le phénomène des rançongiciels disponibles clé en main (*Ransomware-as-a-Service* ou *RaaS*). La cybercriminalité en tant que service sera donc un axe à suivre avec attention en 2024.

D'autre part, des services autrefois disponibles sur le *darkweb* sont désormais aussi proposés *via* les **réseaux sociaux**. De faux documents (faux permis, faux résultats d'analyses sanguines par exemple) sont plus facilement accessibles. Cet accès à la cybercriminalité est facilité par une simplicité d'usage et un sentiment d'impunité. En 2024, cette tendance constituera un point de vigilance.

Se renseigner et prévenir

CYBER MALVEILLANCE .GOUV.FR

Prévenir et sensibiliser les internautes sur la cybersécurité.

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

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.

Construire sa sécurité cyber

ANSSI

Des guides pour durcir son matériel et son réseau et se préparer à une crise cyber.

Connaître et déployer les bonnes pratiques. Signaler des vulnérabilités.

MonAideCyber INNOVATION ANSSI

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

CNIL.

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

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

VOUS AVEZ UN DOUTE SUR UN E-MAIL ?

Signalez-le comme spam sur la plateforme :

signal spam

Réagir face à des atteintes cyber

Ma Sécurité
Application Grand Public

THESEE

La plainte en ligne pour les escroqueries sur internet.

En brigade de gendarmerie ou commissariat de police, par téléphone ou internet.

PHAROS

Signaler un contenu illicite sur internet.

PERCEV@L

Signaler des usages frauduleux d'une carte bancaire sur internet.

Plaintes et signalements

Réactions et aides

CYBER MALVEILLANCE .GOUV.FR

Assister les victimes de cybermalveillances.

CSIRT
RÉGIONAUX

Apporter des conseils et aider à trouver des prestataires.

ANSSI

Assister les entités essentielles et les entités importantes ou intervenir pour des faits très sensibles.

CNIL.

Prévenir en cas de fuite de données personnelles, réelle ou supposée.

Ma Sécurité
Application Grand Public

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

masecurite.interieur.gouv.fr[1]

THESEE

***THESEE** pour les escroqueries sur internet :*

service-public.fr/particuliers/vosdroits/N31138

PHAROS

***PHAROS** pour signaler des contenus illicites :*

internet-signalement.gouv.fr/PharosS1

PERCEV@L

***PERCEVAL** pour signaler une fraude à la carte bancaire :*

service-public.fr/particuliers/vosdroits/R46526

1. L'ensemble des plateformes du ministère de l'Intérieur peuvent être trouvées sur le lien suivant : https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne

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

cybermalveillance.gouv.fr

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

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

***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

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

cnil.fr

Adresse publique (crypto-actifs) :
Chaîne de caractères alphanumériques servant de point de référence pour l'envoi et la réception de crypto-actifs sur une *blockchain*.

Affiliés (*affiliates*) :
Cybercriminels qui mènent des cyberattaques, parfois sophistiquées, en utilisant des outils malveillants mis à disposition par des développeurs ou des concepteurs. Les gains générés par les affiliés sont partagés avec les développeurs *via* un système de commissions.

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

***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* :**
Contraction de « *bot* » et « *net* » qui signifie « réseau de robots ». Il s'agit d'un réseau de machines compromises administré par un ou plusieurs acteurs malveillants.

Cheval de Troie :
Logiciel malveillant de contrôle à distance.

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

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

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 numériques.

Cyberharcèlement :
Acte ou propos intentionnel d'un individu ou 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.

***Darkmarket* :**
Pages ou sites *web* proposant la vente de services ou objets, le plus souvent illicites, *via* le *darkweb*.

***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.

***Deepfake* (hypertrucage) :**
Technique de manipulation d'un contenu numérique basée sur l'intelligence artificielle. Elle permet notamment de créer de faux contenus rendant possible l'usurpation de l'identité d'une personne.

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, à l'aide d'un ordinateur.

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

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.).

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

Faux ordres de virement (FOVI) :
Mode opératoire qui consiste à détourner un virement vers le compte d'un malfaiteur, en se faisant passer par exemple pour un fournisseur de la victime.

Finance décentralisée (*DeFi*) :
Écosystème de services financiers s'appuyant sur la technologie *blockchain* et des *smart contracts* pour fonctionner de manière décentralisée, sans intermédiaires traditionnels.

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

Hameçonnage (*phishing*) :
Technique utilisée pour induire en erreur une cible et lui soutirer des informations personnelles (identifiant, mot de passe, identité, etc.) par l'envoi d'un courriel usurpant par exemple un site institutionnel.

***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.

LOPMI :
Loi d'orientation et de programmation du ministère de l'Intérieur.

LOPMJ :
Loi d'orientation et de programmation du ministère de la Justice.

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

***Malvertising* :**
Contraction de « *malicious* » et de « *advertising* », il s'agit d'une publicité trompeuse utilisée pour propager des logiciels malveillants.

Minage de crypto-actifs :
Action visant à sécuriser une *blockchain* en prêtant sa puissance de calcul ou en mettant en jeu des crypto-actifs de celle-ci, dans le but de générer de nouveaux blocs et de choisir l'ordre des transactions. Quand ils minent un bloc, les mineurs sont rétribués en crypto-actifs nouvellement créés et frais de transaction associés.

Minage de crypto-actifs malveillant (*cryptojacking*) :
Pratique malveillante consistant à utiliser la puissance de calcul d'un appareil à l'insu de son propriétaire pour miner des crypto-actifs.

Mixeur :
Service de mélange de crypto-actifs permettant de rompre le lien de traçabilité des transactions.

***Money mule* :**
Intermédiaire de transfert d'actifs, qui permet de blanchir des gains frauduleux.

***OTP* (*one-time password*) :**
Mot de passe à usage unique. Ces codes de sécurité qui se réinitialisent à chaque authentification fournissent une protection supplémentaire. Il s'agit d'une méthode utilisée dans l'authentification à deux facteurs (2FA).

***OTP bot* :**
Programme malveillant automatisé qui est utilisé par des cybercriminels pour contourner les systèmes d'authentification à deux facteurs (2FA) et accéder aux services en ligne de la victime.

***Pentest* (test d'intrusion, *penetration testing*) :**
Méthode d'évaluation de la sécurité d'un ou plusieurs composants informatiques qui consiste à simuler une attaque telle que pourrait la réaliser un acteur malveillant. L'objectif est d'identifier les vulnérabilités exploitables en vue de proposer un plan d'action.

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'achat ou de location d'un rançongiciel où une partie des gains perçus par un affilié est reversée aux développeurs du programme malveillant.

RGPD :
Règlement général sur la protection des données.

***Quishing* :**
Contraction de « QR code » et de « *phishing* ». Il s'agit d'hameçonnage réalisé par le biais de QR codes malveillants.

***SEO poisoning* :**
Technique visant à optimiser la visibilité d'une page ou d'un site *web* malveillants pour qu'ils apparaissent dans les premiers résultats de recherche.

***Sextorsion* :**
Extorsion, *via* internet, de faveurs (sexuelles ou financières) à la suite d'un chantage, notamment à la *webcam*.

***Smart contract* :**
Programme informatique autonome sur une *blockchain* qui s'exécute sans tierce partie selon des conditions préalablement définies.

***Smishing* :**
Mot issu de la contraction de « SMS » et de « *phishing* ». Il s'agit d'hameçonnage par SMS.

***Spoofing* :**
Usurpation d'une identité pour gagner la confiance de la victime, afin d'accéder à ses systèmes, de diffuser des logiciels malveillants, de dérober ses données et de capter des actifs numériques ou fiduciaires.

Système de traitement automatisé des 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.

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

Directeur de publication :
Général de division Christophe Husson

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

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

Sa rédaction a été réalisée par le CEntre d'analyse et de regroupement 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

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