MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2025

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2025

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Commandement du ministère
de l'Intérieur dans le cyberespace

SOMMAIRE

Édito 7

Chiffres clés 2024 8

Tendances majeures et évolutions de la cybercriminalité 9

1 Écosystème de la cybercriminalité 10

1 | Industrialisation de la cybercriminalité 12

2 | Modes de communication des cybercriminels 14

3 | Cybercriminalité en tant que service *(Cybercrime-as-a-Service)* 15

2 Modes opératoires des cybercriminels 18

1 | Principaux modes d'action 20

2 | Usage de nouvelles technologies à des fins malveillantes 31

3 | Modes opératoires hybrides 37

3 Retours d'enquêtes majeures et évolutions juridiques 40

1 | Évolutions juridiques 42

2 | Retours d'enquêtes majeures (OFAC, UNCyber et BL2C) 44

4 Nouvelles technologies et anticipation des cybermenaces 50

1 | L'usage de l'intelligence artificielle dans la prévention des menaces 52

2 | Internet des objets : un vecteur de risques émergents 54

Informations utiles 56

Lexique 60

Madame, Monsieur,

Ces dernières semaines, plusieurs enlèvements et tentatives d'enlèvements dans le monde de la cryptomonnaie en France ont été organisés. Après des mois de traque, leur commanditaire présumé a été arrêté au Maroc. Ce succès illustre tout aussi bien la métamorphose de la criminalité que l'évolution de la réponse que nous lui opposons.

Les criminels ont désormais pleinement investi le monde numérique. Tantôt terrain de chasse à part entière, tantôt prolongement du monde physique, la criminalité s'y développe à un rythme industriel et les criminels y mettent en commun leurs compétences. Au cœur du darknet ou par l'intermédiaire des messageries chiffrées, les trafiquants en tous genres côtoient les rançonneurs et les faussaires. Ils y complexifient leurs méthodes, anonymisent leurs circuits de décision.

Pour protéger nos concitoyens, nos entreprises mais aussi les intérêts de la nation qui peuvent être pris pour cibles par des hacktivistes, plus de 15 000 policiers et gendarmes spécialisés scrutent chaque jour le cyberespace pour traquer et trouver les criminels qui s'y sont réfugiés, et qui pensent pouvoir agir dans l'ombre, à l'abri des écrans.

Pour coordonner et renforcer leur action, nous avons institué, en décembre 2023, le Commandement du ministère de l'Intérieur dans le cyberespace, le COMCYBER-MI. Ce n'est pas une structure de plus : c'est une arme opérationnelle adaptée aux défis sécuritaires du numérique.

Cette réponse, nous allons la renforcer encore davantage dans les années à venir, en continuant à investir le champ des possibles que nous offrent les nouvelles technologies. Car avoir un coup d'avance, c'est le meilleur moyen de ne pas avoir une guerre de retard face aux criminels. Et leur rappeler que nulle part, l'impunité ne saurait prospérer.

Bruno RETAILLEAU
Ministre d'État, Ministère de l'Intérieur

CHIFFRES CLÉS 2024

348 000* atteintes numériques enregistrées en 2024

+74% *d'atteintes numériques en cinq ans*

65% d'atteintes aux biens

29,7% d'atteintes aux personnes

4,9% d'atteintes aux institutions et à l'ordre public

0,4% d'atteintes aux législations et règlementations spécifiques numériques

17 100 atteintes aux systèmes d'information en 2024

-13% *de saisines pour des cyberattaques par rançongiciel*

THESEE

107 331 plaintes ou signalements relatifs aux escroqueries sur internet enregistrés sur la plateforme Thésée

PHAROS

222 364 signalements de contenus illicites reçus par la plateforme Pharos

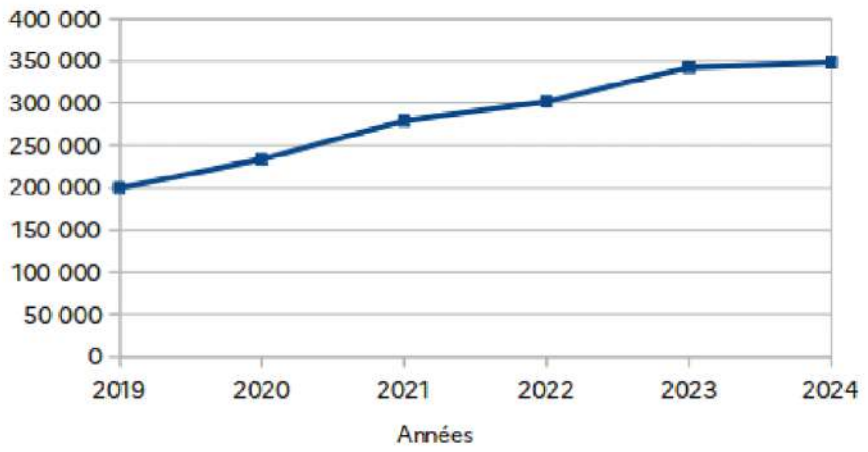
PERCEV@L

230 537 signalements d'usages frauduleux de cartes bancaires enregistrés par la plateforme Perceval

60 000

mis en cause pour des atteintes numériques

Nombre d'infractions constatées annuellement depuis 2019



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.

** Ce chiffre intègre les 50800 dépôts de plainte de la plateforme Thésée.*

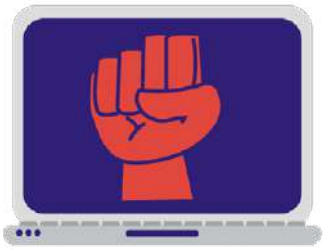
Rançongiciels

La menace liée aux rançongiciels demeure prédominante, bien que le nombre de plaintes déposées pour ce type d'attaque ait baissé de 13% en 2024 par rapport à l'année précédente[1].

Pour gagner en efficience et prévenir la détection par les dispositifs de sécurité, le chiffrement des données du système d'information de la victime est devenu de moins en moins systématique. Les attaquants ont désormais tendance à privilégier le vol et la menace de diffusion des données dans le but de contraindre les victimes à payer la rançon.

La hiérarchie des groupes de rançongiciels a connu plusieurs bouleversements. La mobilisation de services d'enquêtes internationaux contre *LockBit* en 2024 a mis à mal son hégémonie. Au niveau international, *RansomHub* a supplanté *LockBit* en nombre d'attaques constatées. Plusieurs groupes de rançongiciels très actifs ont émergé en 2024. Certains recyclent des codes sources ayant fuité, quand d'autres développent leur propre rançongiciel avec l'assistance de l'intelligence artificielle (IA).

Hacktivisme



Les conflits internationaux ont trouvé un écho important dans le cyberespace. 707 revendications d'attaques hacktivistes ont ainsi été recensées contre la France en 2024. Certaines organisations hacktivistes qui avaient l'habitude d'agir seules se sont alliées avec d'autres groupes considérés comme compatibles, donnant ainsi naissance à des coalitions dont certaines ciblent spécifiquement la France.

En parallèle, plusieurs cas d'attaques sous « faux drapeau » ont été observés.

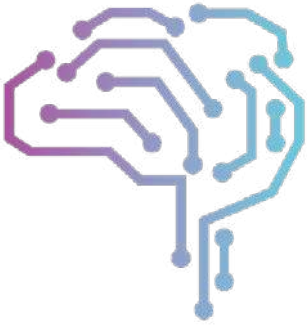
Concernant les modes d'action, les hacktivistes continuent de privilégier les attaques par déni de service distribué *(DDoS)* et les défigurations de sites internet. Dans le même temps, une multiplication des revendications d'atteintes envers des SCADA (systèmes industriels) est observée.

Vols de données

2024 est l'année de la prise de conscience par le plus grand nombre du danger que représentent les fuites de données. Plusieurs cas de vente de données personnelles de millions de Français survenus au cours de l'année écoulée ont été relayés dans les médias.

De leur côté, les cyberdélinquants ont compris les profits qu'ils pouvaient générer de la (re)vente de ces données. À tel point que certains n'hésitent pas à tenter de vendre des bases de données soit recyclées (déjà diffusées), soit créées par IA ou encore provenant de sources accessibles publiquement.

Intelligence artificielle



En 2024, l'évolution de l'intelligence artificielle, notamment des IA génératives s'est poursuivie, tant du côté de la protection contre les cybermenaces, que du côté des attaquants. Aujourd'hui l'IA constitue une menace comme une opportunité sans précédent dans le champ du cyberespace. Les technologies à base de grands modèles (*LLM : large modèle de langage, VLM : large modèle de vision, LAM : large modèle d'action*), peuvent tout à la fois être exploitées pour créer des logiciels malveillants comme pour mieux détecter les cybermenaces.

L'IA intervient également dans les attaques de type *DDoS*, décuplant leurs effets néfastes. Elle permet notamment la gestion d'attaques multivectorielles, s'adaptant aux cibles en temps réel en fonction des circonstances.

Alors qu'elle accroît l'accessibilité des criminels à des techniques sophistiquées, améliorant ainsi leur efficacité, elle nécessite d'être appréhendée par les forces de sécurité intérieure pour être en mesure de mieux lutter contre cette tendance de la criminalité.

1. Source Parquet du TJ Paris – 3ème Division – JIRS/JUNALCO – Section J3 - cybercriminalité

ÉCOSYSTÈME DE LA CYBERCRIMINALITÉ

1 | Industrialisation de la cybercriminalité 12

2 | Modes de communication des cybercriminels 14

3 | Cybercriminalité en tant que service *(Cybercrime-as-a-Service)* 15

1 ÉCOSYSTÈME DE LA CYBERCRIMINALITÉ

Les groupes cybercriminels font l'objet d'analyses quant à leurs modes opératoires. Ils sont composés d'individus disposant d'une technicité informatique ou d'une capacité financière qui leur est propre. Le travail des forces de sécurité consiste à les localiser afin de procéder à leur arrestation, le plus souvent dans le cadre d'une coopération internationale. Certains acteurs malveillants peuvent être catégorisés comme des amateurs *(script kiddies)* s'appropriant des outils clés en main, quand d'autres disposent d'une véritable expertise en matière de sécurité informatique.

Les cybercriminels répondent à trois motivations principales : l'appât du gain (rançongiciels, ventes de données), l'idéologie (défiguration de pages *Web*, cyberattaques par *DDoS*) ou l'orgueil (défi informatique, besoin de reconnaissance). Ils peuvent également être animés par d'autres ressorts : déviances (pédocriminalité) ou comportements toxiques (harcèlement). Ces acteurs malveillants peuvent agir seuls, mais le plus souvent le font de manière coordonnée. Si certains collaborent par opportunisme ou pour augmenter leurs capacités de nuisance, d'autres se sont constitués en véritables groupes criminels, disposant d'une organisation et de modes opératoires qui leur sont propres.

1 | Industrialisation de la cybercriminalité

Le champ de la criminalité numérique n'a cessé de croître depuis ces dix dernières années et a connu en 2024 un tournant significatif en matière d'appropriation des outils techniques et de répartition des tâches au sein des écosystèmes de la cybercriminalité. Cette étape d'industrialisation a marqué un tournant dans les interactions entre cybercriminels.

Pour mettre en œuvre leurs activités illicites, les acteurs malveillants bénéficient de nombreux outils (serveurs, logiciels malveillants, etc.) et de canaux de discussion (forums, messageries chiffrées, réseaux sociaux, etc.), leur permettant d'interagir entre eux et d'optimiser leurs actions. À titre d'exemple, sur les forums cybercriminels, il est possible d'acheter des accès à des serveurs d'entreprises ou encore de louer des logiciels malveillants pour mener des cyberattaques ou des escroqueries massives. Ces acteurs sont également en lien étroit avec les opérateurs du blanchiment, qui utilisent à la fois les systèmes traditionnels de la criminalité organisée et les crypto-actifs.

L'évolution de cet écosystème a conduit, sur le même principe qu'un marché économique légal, à une répartition, une automatisation et une rationalisation des tâches entre les acteurs de la cybercriminalité. Ainsi, certains groupes ou individus se sont spécialisés dans le développement d'outils malveillants, quand d'autres préfèrent se concentrer sur la vente d'accès initiaux ou de bases de données. Pour autant, tous ces acteurs malveillants sont interconnectés entre eux, par le biais de nombreux moyens de communication, principalement pour des motifs opportunistes. Ainsi, ils sont en mesure de sous-traiter certaines tâches ou de mettre à disposition des compétences au profit d'autres acteurs, en échange d'une rémunération.

Modélisation d'un écosystème cybercriminel

FOCUS

Narcotrafic en ligne

Le trafic de stupéfiants en ligne constitue un marché criminel qui a pris une ampleur inédite avec l'apparition de milliers de points de deal numériques. Le *darknet*, les forums cybercriminels, les messageries chiffrées ou encore les réseaux sociaux offrent aux groupes criminels organisés des alternatives à leurs trafics, qui sont à la fois des supports technologiques d'optimisation de leurs activités, mais également un moyen de repli face aux politiques antidrogues menées dans l'espace physique. Ces technologies favorisent les échanges sécurisés et participent au phénomène d'ubérisation du trafic de stupéfiants. Elles concernent tant la vente au détail pour les particuliers que de grosses quantités pour les narcotrafiquants.

2 | Modes de communication des cybercriminels

L'écosystème de la cybercriminalité peut sembler complexe compte tenu de la multitude d'acteurs malveillants. Toutefois, leurs activités peuvent être regroupées au sein de quatre catégories d'infrastructures de délinquance, leur permettant d'échanger au quotidien : les forums cybercriminels et canaux de discussion ouverts, les messageries chiffrées, les réseaux sociaux et la téléphonie.

Les forums cybercriminels jouent un rôle fondamental dans les interactions entre les acteurs malveillants liés à la cybercriminalité. Les échanges effectués par le biais de ces forums permettent aux cybercriminels d'échanger, d'acheter, de louer et de vendre des services (logiciels malveillants, accès initiaux, bases de données, recrutements de cybercriminels, partage de connaissance, etc.).

Bien que de nombreux forums cybercriminels disposent d'espaces de discussion couvrant un large spectre d'activités malveillantes, certains d'entre eux se sont spécialisés dans des types d'opérations spécifiques (cyberattaques par rançongiciels, vente de données, etc.).

Ces forums se déclinent en sous-forums dédiés par sujets et permettent parfois de cibler des communautés spécifiques, notamment par affinité de langue (francophones, russophones, anglophones, etc). Certains d'entre eux sont utilisés par un nombre restreint de groupes cybercriminels disposant de très hautes compétences techniques.

Les cybercriminels échangent également *via* les messageries chiffrées, qu'ils estiment plus sécurisées, pour évoquer des sujets plus sensibles (montants des transactions, recrutement des cybercriminels, etc.). Ces messageries ne permettent cependant pas à ces acteurs malveillants d'agir en toute impunité, puisque des opérations judiciaires de grande ampleur sont également menées sur ce type d'outils, à l'instar d'*Encrochat*[2] ou de *Ghost*[3] par la gendarmerie nationale et de *SkyECC*[4], par la police nationale. Plusieurs dizaines de milliers de criminels et cybercriminels ont ainsi pu être identifiés.

Par ailleurs, de nombreux cybercriminels utilisent à la fois les réseaux sociaux, qui permettent de cibler un grand nombre de victimes, et la téléphonie, pour échanger via des solutions chiffrées ou démarcher des victimes. Les cybercriminels et escrocs utilisent notamment des logiciels pour automatiser les campagnes massives d'escroqueries en ligne ou pour dérober des données, à caractère personnel ou financier.

Ces différents types de support de communication participent ainsi à renforcer et à sécuriser une partie des échanges entre les acteurs cybercriminels et font l'objet de démantèlements par les forces de sécurité intérieure spécialisées dans la lutte contre la cybercriminalité.

2. https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2020/retour-sur-l-affaire-encrochat
3. https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2024/les-gendarmes-cyber-chasseurs-de-ghost
4. https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

3 | Cybercriminalité en tant que service *(Cybercrime-as-a-Service)*

La cybercriminalité en tant que service ou *Cybercrime-as-a-Service (CaaS)*, consiste à mettre à disposition des compétences ou outils clés en main en échange d'une rémunération. Ces échanges sont principalement effectués sur des forums fermés, nécessitant parfois un transfert d'argent ou une interaction avec les administrateurs de la plateforme. Ce phénomène est surtout connu en tant que modèle fréquemment mis en œuvre par les groupes de rançongiciels. Il se rapporte néanmoins à d'autres aspects de la cybercriminalité.

Les principaux services proposés sur ces forums consistent à vendre, acheter ou louer :

- des vulnérabilités informatiques ou des accès initiaux, qui permettent notamment de compromettre la machine d'une victime ;
- des maliciels qui permettent l'infection, la prise de contrôle à distance de la machine de la victime ou encore le chiffrement de ses données ;
- des outils d'anonymisation tels que des serveurs d'attaque *(serveur de bulletproof hosting)* ;
- des compétences techniques humaines diverses.

Le *CaaS* est un terme générique également déclinable en sous-catégories :

Phishing-as-a-Service

un acteur fournit à un client des outils clé en main pour lancer une campagne d'hameçonnage ;

Malware-as-a-Service

location ou vente d'un logiciel malveillant, prêt à l'emploi, permettant de dérober les informations stockées sur un système d'information telles que des mots de passe ou clés privées (exemple des *infostealers*) ;

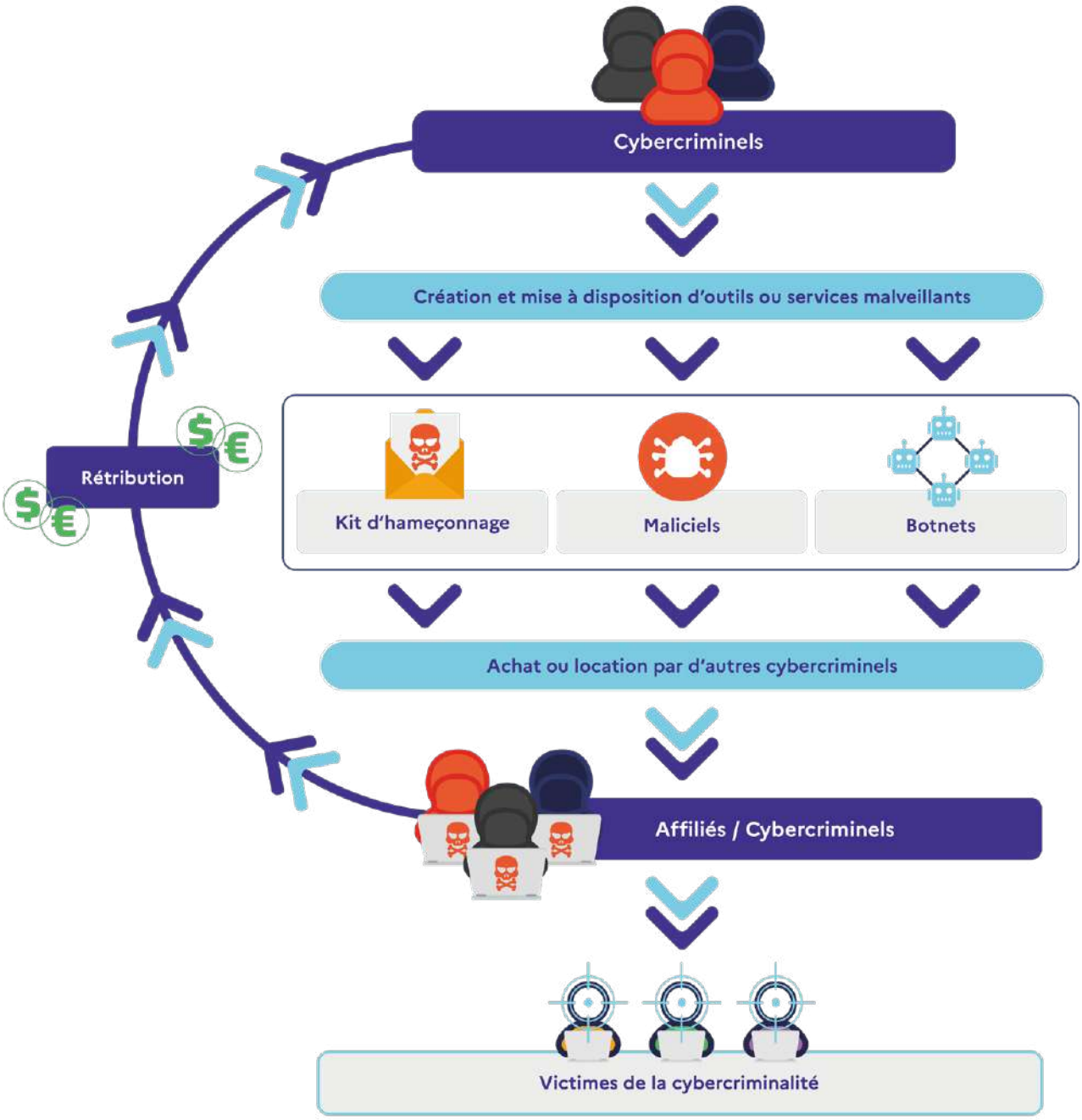
DDoS-as-a-Service

location d'un réseau de machines zombies afin de saturer un serveur ;

Ransomware-as-a-Service

fourniture d'outils permettant de déployer un rançongiciel sur le système d'information d'une cible.

L'activité de Cybercriminalité en tant que service devrait logiquement perdurer dans les prochaines années. Attirés par la perspective de gains financiers rapides, de plus en plus d'acteurs, notamment mineurs et jeunes adultes, se tournent vers ce type de prestation clé en main.



Modélisation de la cybercriminalité en tant que service

Rançongiciel en tant que Service *(RaaS)*

L'activité cybercriminelle liée aux rançongiciels est facilitée par le *CaaS*, permettant largement de mener des attaques de ce type. Le modèle administrateurs / affiliés, similaire à une structure d'entreprise, est mis en place entre les groupes de développeurs, éditant les logiciels malveillants et les affiliés qui en sont les utilisateurs. Les affiliés partagent ainsi une part des revenus criminels générés grâce aux cyberattaques par le biais de rétributions aux développeurs.

L'année 2024 a vu émerger de nouvelles familles de rançongiciels dont certaines sont particulièrement actives à ce jour *(RansomHub, Qilin, HellDown, apt73/bashe, Termite, etc.)*. Deux mouvements peuvent être observés : d'un côté, le groupe Termite revendiquant onze attaques du 17 novembre au 17 décembre 2024 avec une version modifiée du rançongiciel *Babuk*, dont le code source a fuité en 2021 et d'un autre côté, le groupe *FunkSec* , apparu fin 2024, revendiquant 85 attaques au niveau mondial en décembre, soit plus que tout autre groupe sur la même période. Il serait composé d'autodidactes, sans relations connues avec d'autres acteurs, ayant utilisé l'intelligence artificielle afin de développer leur rançongiciel et de concevoir leurs courriels d'hameçonnage. Ces deux approches démontrent la faculté d'adaptation des acteurs du domaine, intégrant notamment les apports récents de l'IA.

Certains changements ont néanmoins pu être observés au cours de l'année 2024. En effet, la famille de rançongiciel *LockBit* très active au premier semestre 2024, a été affaiblie grâce à l'action coordonnée des forces de l'ordre *(opération Cronos)*, réduisant ainsi le nombre d'attaques contre le territoire national sur le reste de l'année.

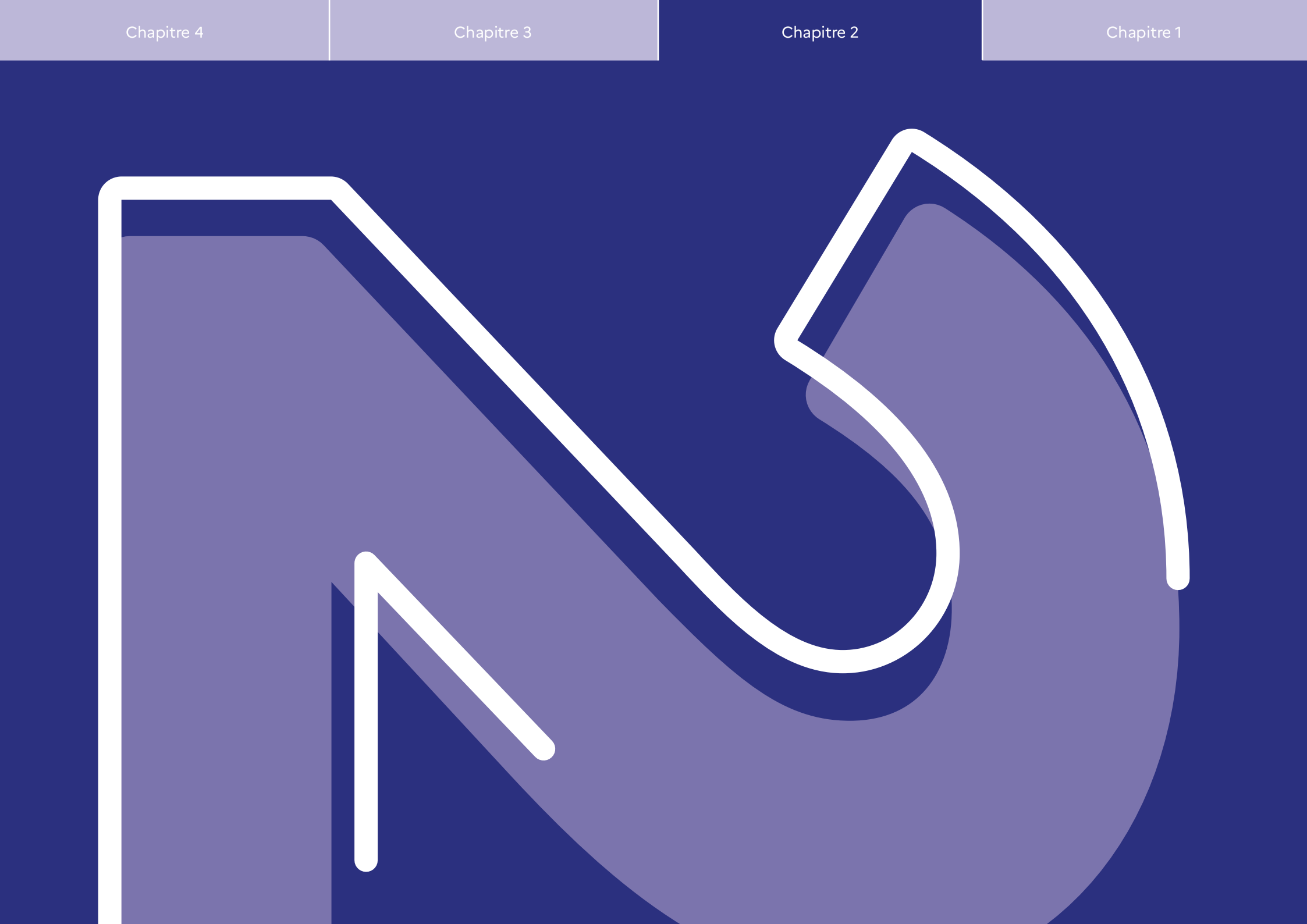
FOCUS

L'hébergement pare-balles *(Bulletproof Hosting)*

« L'hébergement pare-balles » ou *bulletproof hosting*, est un service de mise à disposition d'infrastructures techniques équivalent à un service d'hébergement *Web*, mais dont la finalité est d'offrir un support à des activités criminelles, telles que l'hébergement de logiciels malveillants, l'envoi massif de courriels d'hameçonnage ou encore l'hébergement de contenus illicites. Ce service est le plus souvent payable en cryptoactifs et constitue une activité lucrative pour ses administrateurs. Il permet ainsi d'offrir des capacités d'anonymisation et de facilitation d'activités criminelles, notamment en hébergeant des serveurs de contrôle à distance (C2), utilisés par exemple pour la gestion des *botnets*. Le service de *bulletproof hosting* va ainsi mettre à disposition un serveur faisant office d'hôte pour des individus ou entités souhaitant accomplir des activités illicites.

Les services de *bulletproof hosting* diffèrent selon leur localisation, leur prix, leur réputation et les contenus qu'ils acceptent.

Ce type d'hébergement reste un pilier pour un grand nombre de plateformes de cybercriminalité et constitue une solution durable si elle est localisée dans un pays où la législation et la coopération internationale sont insuffisantes. Concernant les activités illicites, les hébergeurs de serveurs *bulletproof* peuvent adopter une posture plus ou moins active. Ils s'engagent à protéger et anonymiser les identités et communications de leurs clients et mettent en place des protocoles et garanties. Ainsi, la plupart des services peuvent être payés en cryptoactifs et l'hébergeur investit dans des solutions lui permettant de masquer les adresses IP et les serveurs de ses clients.



MODES OPÉRATOIRES DES CYBERCRIMINELS

1 | Principaux modes d'action 20

2 | Usage de nouvelles technologies à des fins malveillantes 31

3 | Modes opératoires hybrides 37

2 MODES OPÉRATOIRES DES CYBERCRIMINELS

La cybercriminalité regroupe tous les crimes et délits commis contre ou à l'aide de systèmes informatiques. Elle prend des formes très variées : vols de données personnelles, escroqueries, piratages de comptes, rançongiciels ou encore usurpations d'identité.

En 2024, ces attaques ont continué à évoluer, devenant plus nombreuses, plus ciblées et plus difficiles à détecter, notamment grâce à l'usage de l'intelligence artificielle ou des crypto-actifs.

Cette partie du rapport présente les principales méthodes utilisées par les cybercriminels, en raison de leurs techniques, de leur organisation et des outils qu'ils emploient.

Elle met aussi en lumière la professionnalisation de certains groupes et l'apparition de services «prêts à l'emploi» accessibles même aux personnes peu expérimentées. Comprendre ces mécanismes est essentiel pour mieux identifier les menaces et adapter les mesures de protection, que l'on soit un citoyen, une entreprise ou une administration.

1 | Principaux modes d'action

Hameçonnage *(phishing)*

L'hameçonnage *(phishing)* est une technique utilisée pour induire en erreur une personne afin de lui dérober des fonds, des informations personnelles voire professionnelles, sensibles ou confidentielles (identifiants de connexion, données bancaires, documents classifiés, etc.).

Ce phénomène en constante augmentation demeure le vecteur de primo-infection le plus répandu en raison de sa simplicité d'exécution et de sa rentabilité et s'est perfectionné en 2024 avec l'appropriation de l'intelligence artificielle par les cybercriminels.

Outre de nombreux cas d'escroqueries, ce mode d'action permet de s'introduire dans les systèmes d'information, d'y exécuter un maliciel, d'extraire des données pour les publier, les revendre ou à des fins d'espionnage. Les auteurs de ces faits agissent principalement pour des motivations financières.

Avec plusieurs centaines de millions de tentatives d'hameçonnage par an, ce type d'attaque ne cesse d'augmenter dans le monde et repose essentiellement sur une criminalité de masse.

Plusieurs tendances se sont dessinées ces dernières années :

- les malfaiteurs semblent privilégier des campagnes massives d'hameçonnage, principalement par courriel ou *via* la téléphonie ;

- le *smishing (SMS phishing)* est en forte hausse depuis 2024 : il suppose la rédaction de textes concis, mais efficaces, envoyés depuis des applications de messagerie ou les logiciels de téléphonie. L'imprécision d'une notification du suivi d'un colis ou à l'inverse, un ordre succinct et précis d'une prétendue autorité incite plus facilement le destinataire à cliquer sur le lien ;

- les auteurs usent d'inventivité lors des campagnes d'hameçonnage afin que les documents en pièces jointes d'un courriel ou les liens de sites internet ne soient pas détectés comme malveillants ou à risque ;

- le *vishing (voice phishing)* : également en forte augmentation, les appels téléphoniques sont devenus quotidiens et ciblent l'ensemble de la population. Les auteurs innovent dans les discours employés et l'identité des organismes utilisés, par exemple lors des campagnes au faux conseiller bancaire. Ces campagnes s'accompagnent le plus souvent de l'usurpation d'une ligne téléphonique légitime *(spoofing)* ;

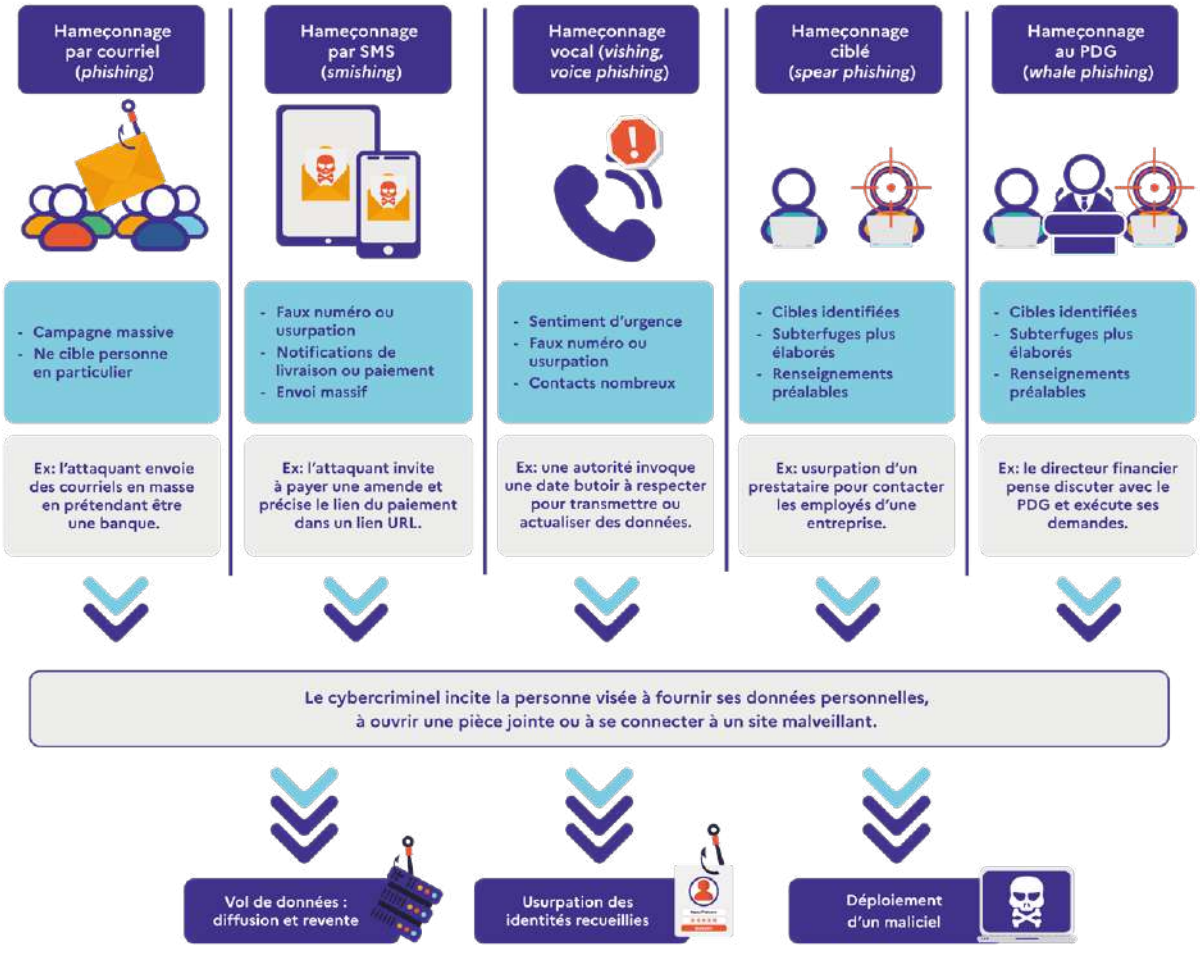
- le télétravail représente une source de compromission pouvant être exploitée par les cyber-criminels ;

- l'utilisation de l'intelligence artificielle permet aux acteurs malveillants de mettre en place des campagnes d'hameçonnage de plus en plus crédibles et difficiles à déceler par les victimes.

Le facteur humain représente le premier vecteur de compromission. Toutes les personnes possédant des appareils capables d'émettre et de recevoir des communications sont susceptibles d'être la cible d'une action frauduleuse. Les personnes physiques, à titre personnel ou professionnel, sont généralement touchées par des campagnes d'hameçonnage non ciblées et diffusées de manière large. Les personnes morales, au travers de leurs employés, cadres, prestataires et clients sont davantage victimes de campagnes ciblées. L'empreinte numérique d'une personne stratégique au sein d'une entreprise constitue souvent une porte d'entrée pour mettre en place une campagne d'hameçonnage ciblée *(spear phishing)*.

Enfin, ces campagnes d'hameçonnage, qui font appel à de l'ingénierie sociale, peuvent également constituer un point d'entrée pour mener des cyberattaques à l'encontre de systèmes d'information (rançongiciels, vols de données, etc).

Diverses méthodes existent pour induire en erreur les victimes :



Typologie des modes d'hameçonnage

Usurpation d'identité numérique *(spoofing)*

L'usurpation d'identité numérique *(spoofing)*, est une méthode utilisée par les cybercriminels pour se faire passer pour un organisme légitime. Cette technique permet d'usurper plusieurs supports numériques tels qu'une adresse courriel, une adresse IP, un site internet ou un numéro d'appel téléphonique. Ce mode opératoire est particulièrement difficile à détecter, car les attaquants font apparaître une adresse ou un numéro en apparence légitime.

Grâce à ces techniques, les cybercriminels établissent un lien de confiance avec leur cible et accèdent ainsi à des systèmes ou appareils, dans le but de voler des informations, d'extorquer de l'argent ou d'installer des logiciels malveillants sur l'appareil de la victime.

Les attaquants à l'origine de faits délictueux utilisant le *spoofing* téléphonique manipulent leurs victimes, en jouant sur la confiance qu'elles accordent aux numéros appelants qui apparaissent sur leurs téléphones. Le *spoofing* téléphonique sert principalement à la commission de trois faits : l'usurpation de numéros d'entreprises pour commettre des fraudes au président, les faux appels visant à déclencher les services d'urgence (appelés *swatting*) et les fraudes au faux conseiller bancaire.

Fraude au président

Les attaquants usurpent un numéro de téléphone pour tromper les victimes et obtenir des informations sensibles ou des virements. Le plus souvent, il s'agit d'usurper l'identité d'une personne dont les fonctions sont stratégiques pour l'entreprise (un président, un comptable habilité à réaliser des actions financières, une secrétaire ayant délégation ou encore un fournisseur ou un client).

Canular téléphonique *(swatting)*

Les attaquants utilisent le numéro de leurs victimes et simulent des situations d'urgence (fusillades, violences) pour déclencher l'intervention indue des forces de l'ordre, ce qui peut parfois conduire à des préjudices importants.

Faux conseiller bancaire

Les cybercriminels usurpent le numéro d'une banque et simulent des alertes de sécurité pour obtenir des données sensibles, valider des achats ou inciter à effectuer des virements bancaires au bénéfice de l'attaquant.

Mode opératoire des réseaux de cybercriminels spécialisés dans le *spoofing* téléphonique

Le *spoofing* occupe une place de plus en plus prépondérante dans le paysage des cybermenaces, tant par sa sophistication croissante, que par son rôle dans les affaires judiciaires qu'il peut rendre particulièrement complexes. Si le *spoofing* est largement intégré dans les menaces actuelles, ses mécanismes et implications sont généralement méconnus. Voici quelques clés pour comprendre le *spoofing* avec un éclairage particulier sur l'usurpation des numéros de téléphone ou « *spoofing* téléphonique ».

Pour réaliser des attaques avec des numéros de téléphone usurpés, les cybercriminels exploitent des outils légitimes conçus pour gérer les réseaux téléphoniques d'entreprises dont ils détournent les usages.

Les cybercriminels ont mis en place une véritable économie autour de l'usurpation de numéros avec une organisation quasi-professionnelle bénéficiant d'une image de marque. Ils proposent des services automatisés et personnalisables, avec des interfaces simplifiées pour choisir le numéro à usurper. Ils appliquent également une tarification structurée, incluant des abonnements et des crédits, facilitant ainsi l'accès à ces outils même pour des utilisateurs peu expérimentés.

Cette organisation bien rodée contribue à la massification des attaques de *spoofing*, rendant ces pratiques accessibles et efficaces à grande échelle.

Les logiciels de vol d'informations *(infostealers)*

Les *infostealers*, sont des logiciels malveillants conçus pour extraire des données particulièrement sensibles sur les appareils infectés, tels que les mots de passe, identifiants bancaires, recherches enregistrées dans l'historique du navigateur, et autres données personnelles.

L'utilisation de ce type de logiciel malveillant est en forte augmentation depuis plusieurs années et constitue l'une des menaces les plus critiques de l'année 2024. Commercialisés sous un modèle *Malware-as-a-Service (MaaS) via* des forums cybercriminels, voire des canaux de discussions ouverts, ces *infostealers* sont accessibles à des individus disposant de faibles compétences techniques.

L'utilisation des *infostealers* se déroule en quatre étapes :

L'infection :

Les *infostealers* pénètrent les systèmes *via* des pièces jointes malveillantes, des logiciels piratés ou des liens d'hameçonnage;

La collecte :

Une fois installés, les *infostealers* analysent l'appareil compromis pour extraire des données : identifiants, mots de passe, *cookies*, portefeuille de crypto-actifs, cartes bancaires, etc ;

Transmission :

Les données volées sont envoyées à un serveur contrôlé par les cybercriminels, souvent par le biais de canaux chiffrés pour éviter la détection ;

Exploitation :

Les données volées sont utilisées pour la fraude, la revente, l'usurpation d'identité ou comme levier pour des attaques avancées. Elles alimentent aussi de nouvelles campagnes d'hameçonnage, perpétuant un cycle de compromission.

Impacts d'une compromission par *infostealers*

Pour les individus

- Vol d'identité et usurpation de comptes en ligne ;
- Pertes financières directes (comptes bancaires, crypto-actifs) ;
- Atteinte à la vie privée.

Pour les organisations

- Compromission de systèmes d'information *via* des identifiants volés ;
- Porte d'entrée pour des attaques plus sophistiquées ;
- Fuites de données confidentielles et atteinte à la réputation ;
- Coûts associés aux violations de données et non-conformité réglementaire.

FOCUS

Opération Magnus[5]

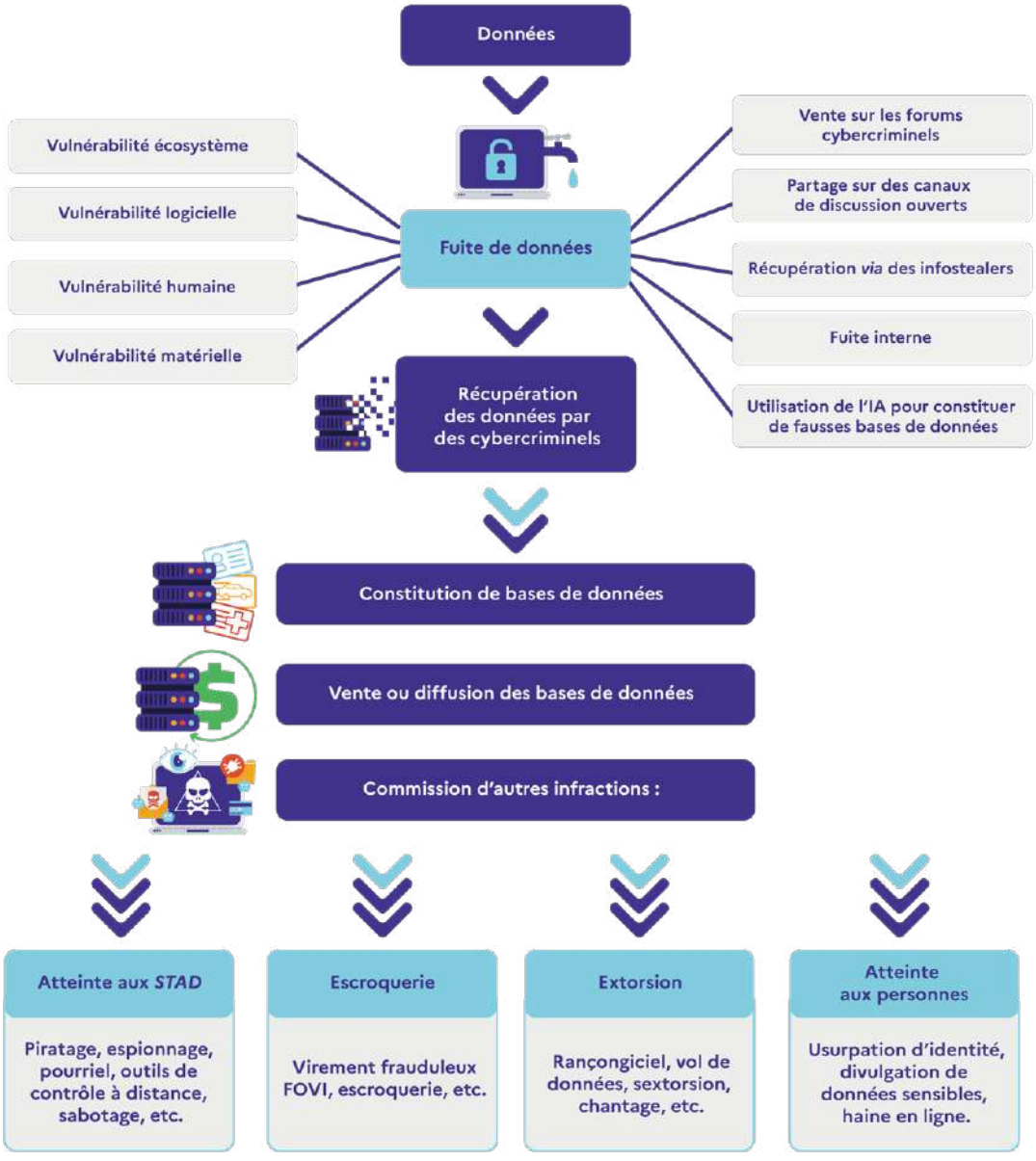
En octobre 2024, l'opération Magnus a été menée pour démanteler les réseaux des *infostealers RedLine* et *META*. Menée conjointement par plusieurs pays et coordonnée par Eurojust, elle a conduit à la saisie de serveurs, de noms de domaine et de chaînes *Telegram* utilisés par ces groupes cybercriminels. A noter qu'il existe des dizaines d'*infostealers* sur les marchés cybercriminels.

5. https://www.eurojust.europa.eu/news/malware-targeting-millions-people-taken-down-international-coalition

L'exploitation des fuites de données

Phénomène cybercriminel qui a particulièrement marqué l'année 2024, l'exploitation des *« fuites de données »* ou *« dataleaks »* consiste pour des cybercriminels à pirater ou récupérer puis diffuser ou vendre des bases de données volumineuses sur des forums cybercriminels ou des canaux de discussion.

Ces bases, constamment enrichies, contiennent un nombre important d'informations qui permettent notamment de mener des cyberattaques (piratages de serveurs ou de comptes personnels, rançongiciels, espionnage, etc.) ou des escroqueries massives ou ciblées (faux investissements, *carding*, FoVI, etc.). Des milliards de données sont ainsi disponibles sur Internet telles que des identifiants et des mots de passe, des données personnelles et financières et peuvent concerner tant les particuliers que les entreprises et les administrations. Une partie significative de ces données est due au piratage de serveurs mal protégés ou à l'infection d'appareils par le biais d'*infostealers*.



Modélisation de l'exploitation des fuites de données

Dans le cadre d'attaques par rançongiciel, les données dérobées sur les systèmes d'information des victimes sont parfois mises à disposition sur des *« data leak sites »*, dénommés parfois *« wall of shame »* ou « mur de la honte ». Ce sont des sites ou des blogs hébergés principalement sur le *darkweb* où sont publiées les données dérobées des organisations refusant de payer la rançon. En 2024, le commandement du ministère de l'Intérieur dans le cyberespace a relevé 235 revendications en lien avec un vol de données concernant des victimes françaises.

Les acteurs de la menace

Le vol et la vente de données acquises frauduleusement attirent plusieurs types d'attaquants :

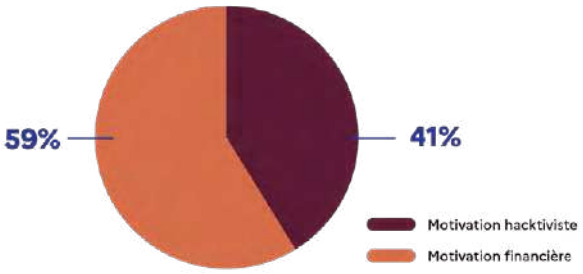
Un acteur malveillant débutant qui, cherchant à accroître sa réputation, recycle des bases de données obtenues dans des diffusions précédentes ou génère des bases de données fallacieuses en utilisant l'IA. Agissant par opportunisme, il propose ces informations à la vente ou s'en attribue le vol.

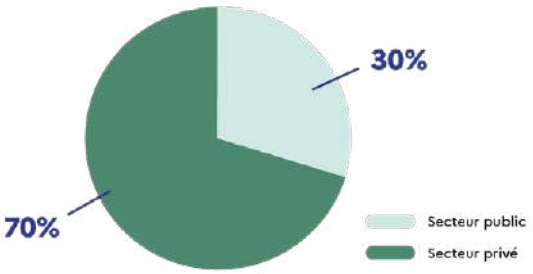
Un acteur confirmé maîtrisant les techniques d'intrusion qui opère seul ou au sein d'un groupe. Certains acteurs isolés peuvent agir par défi ou pour leur satisfaction personnelle. De nature imprévisible, leurs motivations diffèrent autant que leurs compétences techniques.

Les acteurs de la menace agissent en fonction de motivations diverses. L'appât du gain constitue le principal motif de leurs agissements. La revente des données collectées s'avère une activité potentiellement lucrative selon leur degré de confidentialité et de rareté.

Le vol de données est également observé chez les hacktivistes. L'objectif est d'attenter à la réputation d'organismes ou de pays ciblés lors des campagnes d'attaques. Ces opérations interviennent généralement au sein des alliances de circonstance formées par des groupes profitant d'un effet de masse et des capacités techniques de chacun.

Enfin, les fuites de données peuvent être le fait d'autres facteurs plus marginaux : défi personnel, vengeance contre un employeur, voire négligence. Une exposition involontaire des données résultant d'une diffusion accidentelle sur Internet, de la perte d'une clé *USB* par un employé ou d'un système de sécurité mal configuré, présente des impacts potentiellement critiques.

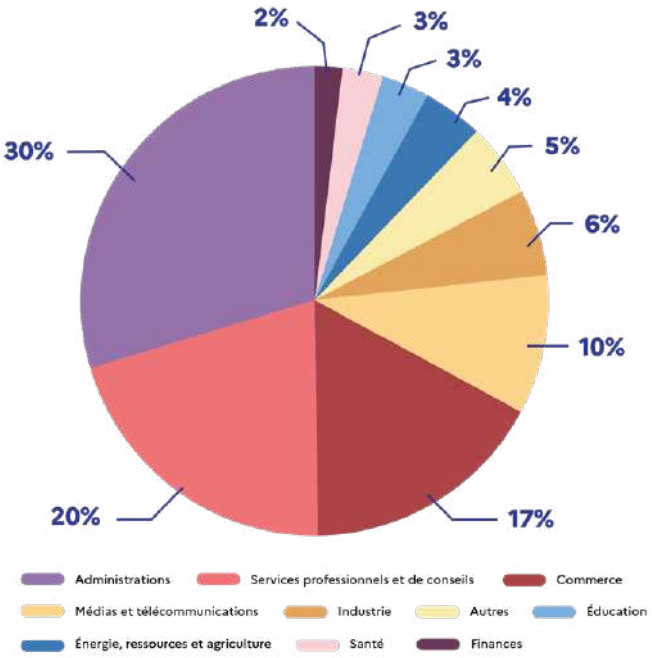


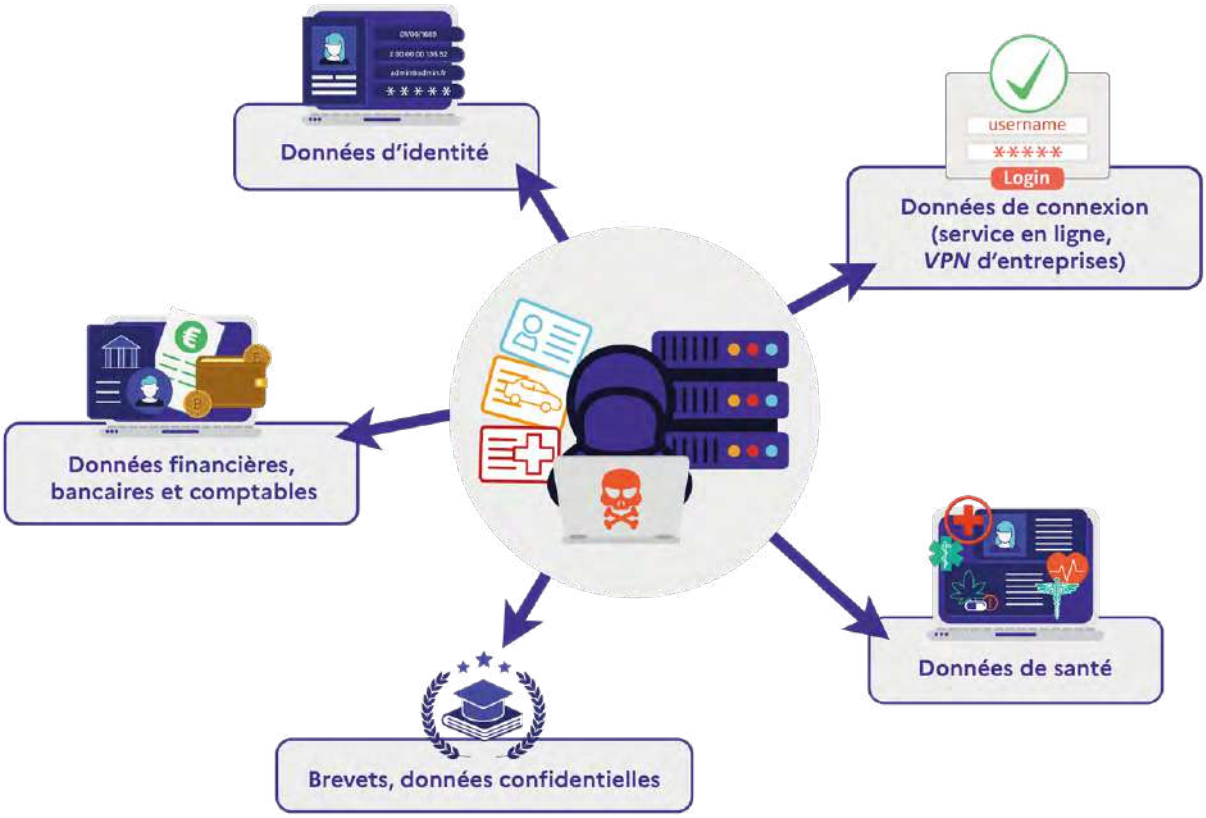


Secteurs et types de données concernés

D'après les mises à disposition de données volées constatées en 2024 par le commandement du ministère de l'Intérieur dans le cyberespace, aucun secteur n'est épargné par ce phénomène. Néanmoins, les administrations apparaissent comme des cibles privilégiées, constituant 30% de la totalité des fuites de données revendiquées.

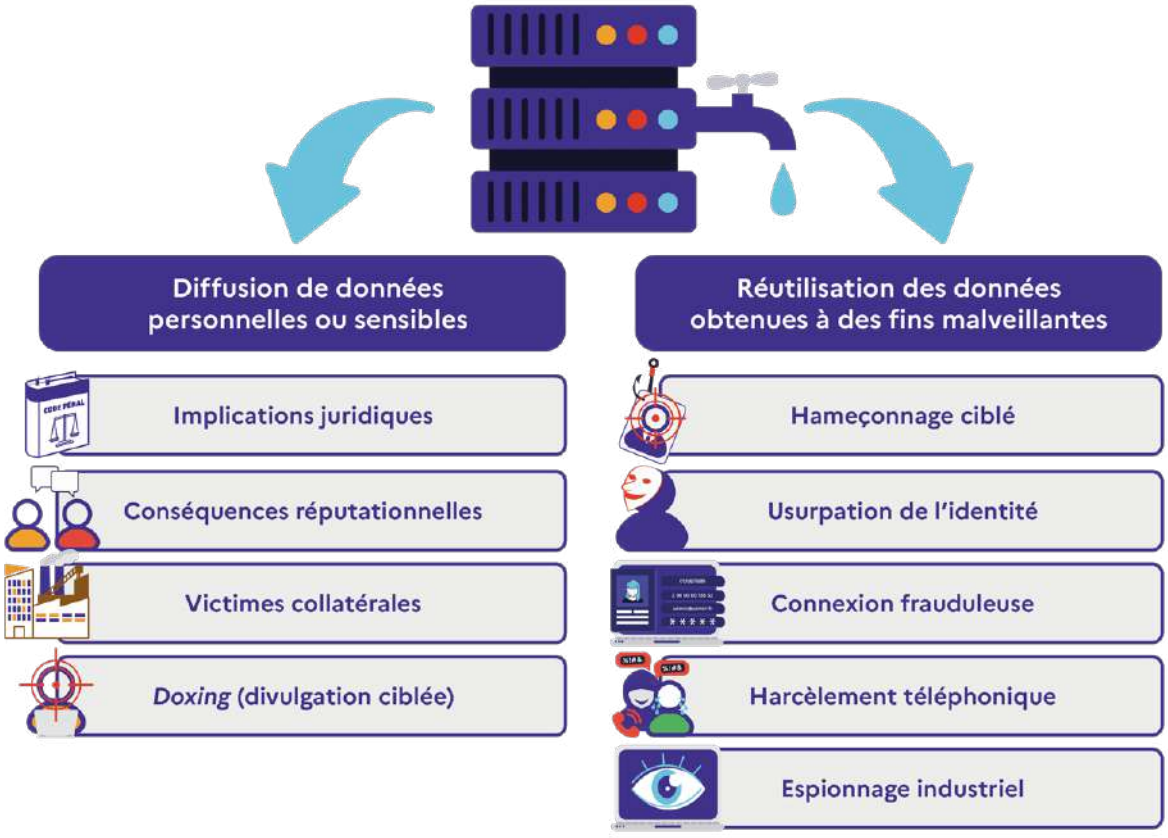
Les types de données varient en fonction des cibles (administrations, entreprises publiques, commerces en ligne, télécommunications, assureurs, etc).





Typologie des données volées

Les conséquences d'une fuite de données peuvent être multiples et impacter à la fois les organismes ciblés, les clients et usagers, ainsi que les partenaires dans la chaîne logistique *(supply chain)* d'approvisionnement.



Exploitation des données par les acteurs malveillants

Rançongiciels *(ransomware)*

Le rançongiciel *(ransomware)* peut être défini comme un logiciel malveillant bloquant l'accès à un ordinateur ou à ses fichiers par chiffrement des données afin d'exiger le paiement d'une rançon pour déchiffrer les données de la victime.

Les attaques par rançongiciel sont le fait d'une cybercriminalité organisée aux structures protéiformes et évolutives. L'un des modèles économiques développé est celui du *Ransomware-as-a-Service (RaaS)*. Il met à disposition un logiciel malveillant, des outils et des compétences humaines auprès d'affiliés en contrepartie du reversement d'un pourcentage de la rançon. Ce système permet également de mener des cyberattaques complexes, même pour des individus d'un niveau technique modéré.

En Europe, près de la moitié des cyberattaques par rançongiciel concernerait une TPE-PME dont l'activité peine à se maintenir ensuite, au risque de faire faillite.

Typologie des attaques et modes opératoires

Les groupes cybercriminels qui se sont spécialisés dans les rançongiciels ont globalement une approche similaire dans le *modus operandi* de leurs cyberattaques. Il existe cependant des variantes et des caractéristiques qui leur sont propres et qui permettent de les différencier, au-delà des dénominations de souches de rançongiciels qu'ils utilisent. L'année 2024 a marqué un tournant dans la composition des groupes malveillants principalement à la suite des actions coordonnées des forces de l'ordre ayant permis l'arrestation de plusieurs individus.

À noter que si les groupes se distinguent par la dénomination des rançongiciels *(LockBit, 8Base Ransomhub, Qilin,* etc.), les acteurs cybercriminels n'y sont pas toujours rattachés de manière exclusive, certains administrant ou utilisant plusieurs rançongiciels à la fois, visant plusieurs cibles différentes.

Des méthodes coexistent et se complètent pour atteindre les victimes :

La chasse au gros gibier *(Big game hunting)* :

Elle consiste à mener des actions ciblées de haute technicité sur des organisations importantes disposant de moyens élevés.

Les attaques de masse :

Actions opportunistes sur des cibles vulnérables.

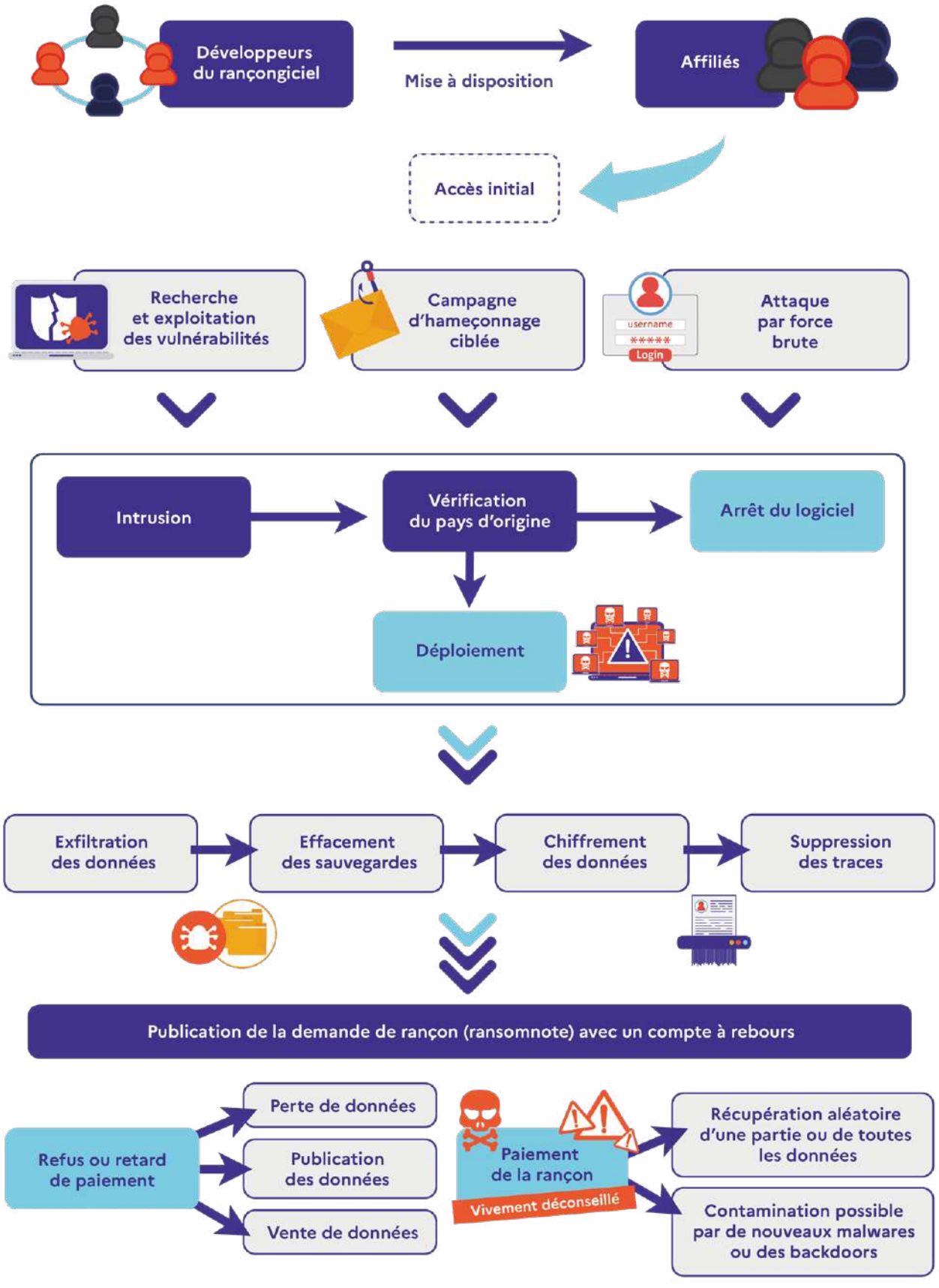
Les techniques d'infiltration dans les systèmes d'information d'une victime sont variées :

- **Passage par des courtiers en accès initiaux *(initial access brokers)*** qui fournissent des accès informatiques piratés à des sociétés depuis des forums cybercriminels.

- **Attaques par la chaîne logistique *(supply chain)* :** *via* des sous-traitants supposés moins protégés et permettant d'accéder indirectement à la société ciblée.

- **Ingénierie sociale *(social engineering)* :** par des techniques de manipulation ou de ruse, la victime est invitée à fournir des données ou à réaliser des actions sur incitation de l'attaquant.

- **Recours à des employés d'une organisation *(insiders)*** agissant par opportunisme financier ou par volonté de nuire.



Modélisation d'une cyberattaque par rançongiciel

La technique la plus répandue parmi les groupes actifs de rançongiciels est la double extorsion, devant la triple extorsion, plus récente :

La double extorsion : technique qui comprend le chiffrement des données qui sont par ailleurs dérobées et que les cybercriminels menacent de diffuser depuis leur plateforme ou sur des canaux de discussion ouverts.

La triple extorsion s'est fortement répandue depuis ces trois dernières années. Cette méthode consiste à ajouter, au chiffrement des données et à la menace de parution en ligne, l'interruption de l'activité et du réseau au moyen d'une attaque par déni de service distribué *(DDoS)*.

Certains groupes rançonnent uniquement les victimes en les menaçant de diffuser leurs données, sans même avoir chiffré les serveurs. La demande de rançon transmise à la victime est toujours accompagnée de menaces de vente ou de divulgation d'informations.

Un nouveau mode opératoire constaté en 2024 est la mise en place de deux comptes à rebours affichés sur la page *darkweb* du groupe cybercriminel. Par exemple, un compte à rebours avec menace de vente des données dans les trois prochains jours et un autre avec menace de diffusion gratuite des données dans les sept prochains jours.

Chaque groupe ou affilié est libre d'agir au moyen de méthodes sophistiquées et uniques. Les techniques utilisées sont pensées pour exercer une pression psychologique auprès des victimes, en les plaçant dans un état de sidération et de résignation afin qu'elles acceptent de payer la rançon qui s'effectue le plus souvent en crypto-actifs.

En outre, les cybercriminels adaptent le montant demandé à la capacité potentielle de la cible à payer la rançon. Ainsi, les victimes seraient théoriquement en mesure de payer.

FOCUS

Les courtiers d'accès initiaux

Les « courtiers en accès initiaux » *(initial access brokers)* sont des acteurs malveillants qui se spécialisent dans la découverte de vulnérabilités permettant d'avoir un premier accès dans le réseau informatique de la victime et la revente à d'autres groupes réalisant les cyberattaques (exfiltration de données, rançongiciels, etc.). La répartition des gains peut se faire par montant fixe en achetant les accès ou par rétribution d'une commission une fois que la cyberattaque aura donné lieu au paiement d'une rançon.

Ce type d'organisation illustre le niveau de spécialisation et de structuration de la menace. Certains forums cybercriminels se sont spécialisés dans la revente de ces accès, au sein desquels il existe un système de notation des utilisateurs. Le plus souvent, ces « courtiers » obtiennent l'accès aux réseaux des victimes par la détection de vulnérabilités informatiques, le vol d'identifiants *via* des *infostealers* ou des campagnes d'hameçonnage ciblées. Dans la plupart des ventes observées, les accès proposés prennent la forme d'accès distants « *RDP*[6] », « *VPN*[7] » ou d'accès à une solution de cybersécurité de la cible, notamment son pare-feu. Ces accès peuvent être vendus pour des montants pouvant osciller entre quelques centaines d'euros et plusieurs dizaines de milliers d'euros, selon le type de vulnérabilité ou le profil de la cible.

Réseaux de robots ou *botnets*

Les réseaux de robots, *botnets* ou réseaux zombies sont des réseaux d'équipements numériques reliés à Internet (ordinateurs, serveurs, objets connectés, etc.), infectés et pilotés par des cybercriminels au moyen de serveurs de contrôle à distance *(command & control)*.

Certains *botnets* peuvent être constitués de plusieurs millions de machines infectées et considérés comme des armes informatiques.

6. Remote Desktop Protocol
7. Virtual Private Network (réseau privé virtuel)

Les *botnets* peuvent constituer un support pour plusieurs types de cyberattaques :

Cyberattaques par *DDoS* :

surcharger les serveurs par du trafic réseau, à partir d'une multitude de supports informatiques infectés, au point de rendre le service indisponible ;

Diffusion de logiciels malveillants :

infection du support informatique pour se propager sur d'autres supports et ainsi augmenter l'efficacité du *botnet* ;

Bourrage d'identifiants *(credential stuffing)* par force brute

exécuter automatiquement des programmes forçant l'authentification par l'exploitation de données de connexion connues ;

Crypto-minage :

détourner frauduleusement un ordinateur et sa capacité de calcul pour miner des crypto-actifs en arrière-plan.

Mis en place par des groupes cybercriminels disposant d'une expertise technique avancée, des botnets sont aussi proposés à la location dans le cadre de la cybercriminalité en tant que service *(Cybercrime-as-a-service)*. Des plateformes sont ainsi gérées afin de mettre à disposition ces outils criminels en échange d'un paiement. Ce phénomène peut être particulièrement lucratif pour ses administrateurs, mais certaines cyberattaques sont également commises pour des revendications idéologiques.

Modélisation du fonctionnement d'un botnet

2 | Usage de technologies à des fins malveillantes

De nombreuses infractions sont commises par le biais de l'utilisation de technologies dont le développement est légitime, mais qui sont détournées par les cybercriminels pour améliorer leurs cyberattaques. C'est le cas notamment de l'intelligence artificielle et des crypto-actifs.

Intelligence artificielle : innovations criminelles

L'intelligence artificielle offre des nouvelles opportunités aux délinquants pour accroître la quantité comme l'efficacité des cyberattaques.

Les *deepfakes*, qui permettent de créer des contenus audio et visuels très réalistes, ont rapidement trouvé leur place dans l'arsenal des cybercriminels. Ces derniers exploitent l'IA pour automatiser et intensifier leurs activités malveillantes.

Les grands modèles[8] de langage sont utilisés pour rédiger des courriels d'hameçonnage *(phishing)* ou des vidéos compromettantes extrêmement convaincantes, adaptés au comportement et/ou au profil des victimes. Ces modèles offrent de nouvelles opportunités criminelles en permettant de déjouer les protections des systèmes d'information et la vigilance humaine en générant des attaques inédites. Ce nouveau panorama criminel engage les forces de sécurité intérieure dans une lutte asymétrique.

Les outils d'IA sont aussi la cible d'attaques. Parmi les méthodes les plus communes, la technique d'empoisonnement des données *(data poisoning)*, consiste à polluer les jeux de données utilisées pour entraîner les modèles d'apprentissage et permet ainsi, soit de fausser totalement les résultats, soit de contrôler le comportement prédictif du modèle entraîné. Il est alors possible de corrompre le modèle et les capacités de classification, de détection ou de prédiction.

Les *deepfakes*, une menace en pleine expansion

Les *deepfakes* sont des contenus falsifiés (vidéos, audios, photos) capables de reproduire l'apparence ou la voix d'une personne avec un réalisme déconcertant. En 2024, cette technologie s'est largement démocratisée, permettant à des individus malveillants de créer des contenus falsifiés utilisés à des fins criminelles.

Un *deepfake* peut résulter de différentes techniques :

Remplacement du visage d'une personne par celui d'une autre dans un contenu existant *(face swap)* ;

Utilisation d'un contenu déjà existant afin de faire tenir des propos fictifs à un individu *(facial reenactment)* ;

Création d'un contenu entièrement généré par l'IA, incluant l'image et/ou la voix d'un individu, sans se baser sur des images ou vidéos préexistantes (synthèse intégrale).

8. Large Language Model (LLM), Vision Language Model (VLM), Large Action Model (LAM)

Les *deepfakes*, quels usages ?

Désinformation

La création de contenus trompeurs peut permettre d'influencer les opinions, perturber des processus démocratiques ou semer la confusion médiatique. Les Jeux Olympiques de 2024 ont notamment été le théâtre de ce type de tentative.

Fraude et escroquerie

Les cybercriminels exploitent les *deepfakes* pour usurper des identités et tromper des particuliers ou des organisations.

Atteinte à la réputation

Les *deepfakes* sont utilisés pour générer des contenus diffamatoires, parfois à caractère pornographique, ciblant des personnes ou des entités dans un but de chantage ou de sabotage.

Pour le grand public, distinguer un *deepfake* d'un contenu authentique devient un défi quotidien. Les outils de détection existants, bien qu'efficaces dans certains cas, peinent à suivre l'évolution rapide des algorithmes.

Des applications grand public, mais aussi de véritables plateformes de *Deepfake-as-a-Service (DFaaS)* sont apparues, permettant à quiconque de créer des *deepfakes* sans compétences techniques facilitant leur utilisation à des fins malveillantes.

Nouvelles stratégies de *phishing* et assistance aux cybercriminels

L'hameçonnage « augmenté » par l'IA

L'hameçonnage *(phishing)*, attaque consistant à duper les victimes à travers des courriels ou messages frauduleux, a atteint un nouveau niveau d'efficacité grâce à l'IA en 2024. Adossés aux données publiques disponibles (profils sur les réseaux sociaux, informations issues de fuites de données), les cybercriminels utilisent l'IA pour générer des courriels personnalisés et crédibles, simulant des entités légitimes.

L'adoption de l'IA permet de rendre la détection plus difficile et d'augmenter le taux de réussite des campagnes de *phishing* réalisées à grande échelle.

Quelques exemples clés :

***Phishing* de masse par IA :**

Génération automatisée de milliers de courriels de *phishing* personnalisés imitant diverses institutions avec adaptation intelligente selon les réponses des victimes.

Hameçonnage ciblé *(spear phishing)* :

Courriel personnalisé basé sur l'analyse IA des données professionnelles publiques d'un décideur au sein d'une organisation, intégrant des références précises à son secteur et ses projets.

Hameçonnage vocal *(vishing)* :

Appel frauduleux utilisant une voix synthétisée d'un supérieur hiérarchique pour exiger un transfert urgent, sur un compte détenu par le cybercriminel.

Assistance aux cybercriminels

Les grands modèles de langage *(LLM)* permettent d'optimiser les activités des cybercriminels, transformant des novices en véritables acteurs malveillants et permettant aux experts de démultiplier leur champ d'action.

Exemples d'apports clés :

Création de scripts d'exploitation :

Génération automatique de scripts malveillants pour cibler des vulnérabilités connues ou émergentes.

Analyse accélérée de code :

Analyse de bases de code volumineuses pour repérer des failles plus rapidement qu'un humain.

Adaptation de logiciels malveillants :

Aide à la modification de code malveillant existant pour le rendre compatible avec de nouvelles cibles.

Potentiel et limites

Des programmes autonomes (agents) basés sur des *LLM* parviennent déjà à exécuter des cyber attaques complexes avec un taux de succès élevé.

Ces agents, conçus pour interagir avec des logiciels tiers et exécuter des commandes, exploitent des vulnérabilités documentées pour mener des actions malveillantes. Toutefois, leurs performances chutent drastiquement lorsque ces informations sont absentes.

Il reste, à ce jour, difficile d'évaluer précisément la maturité de ces usages au sein de l'écosystème cybercriminel ainsi que la part réelle d'automatisation par IA dans les cyberattaques. Cependant, le niveau de performance comme le nombre d'attaques par l'IA va certainement s'accroître.

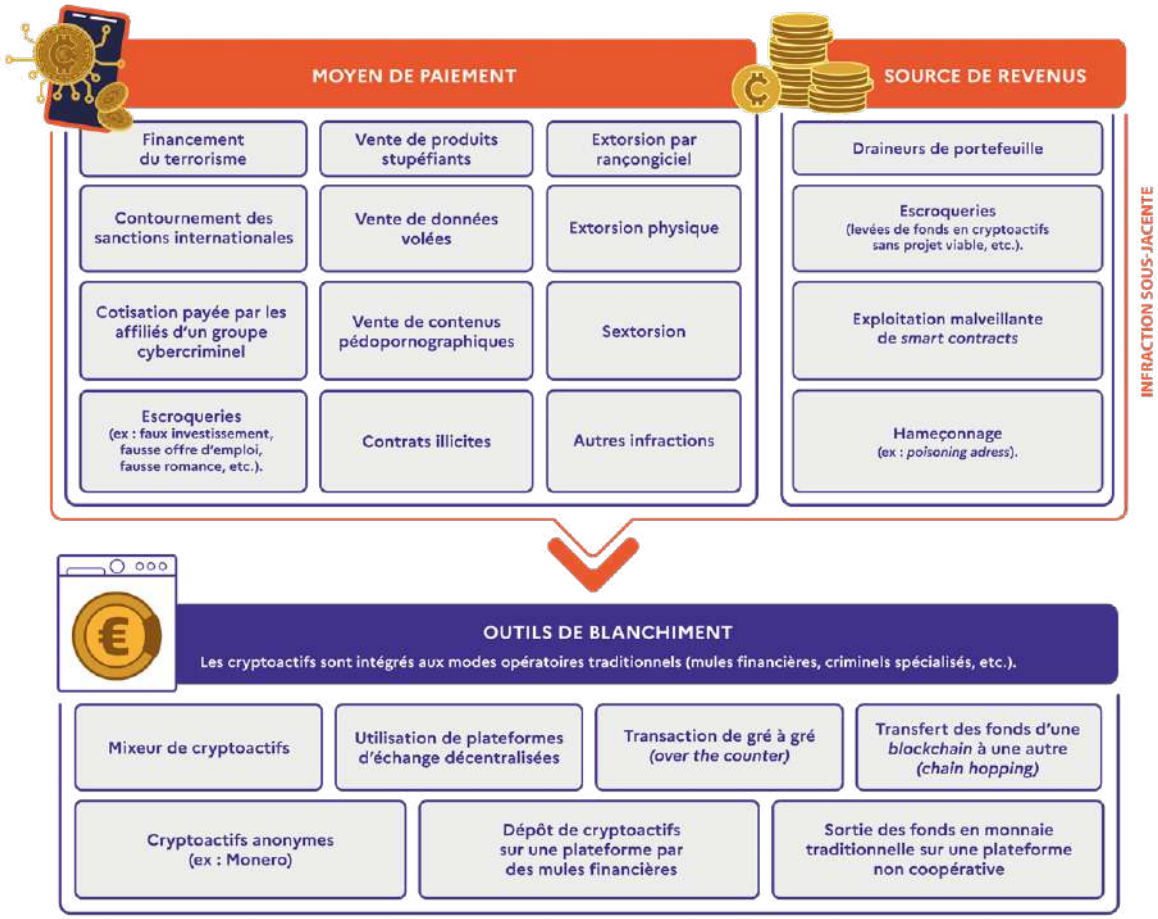
L'intelligence artificielle offre donc de belles perspectives aux cyberdélinquants. Fort heureusement, l'IA est également une arme capable de réagir avec efficacité et célérité dans la lutte contre la cybercriminalité.

Crypto-actifs et cybercriminalité

L'utilisation des crypto-actifs par les cybercriminels a connu un essor important depuis ces dix dernières années : financement des campagnes de cyberattaques par déni de service pour mettre hors service des sites Internet, paiements d'une rançon lors d'une cyberattaque par rançongiciel ou sur des forums cybercriminels (achat de bases de données, de logiciels malveillants, trafic de stupéfiants, etc.).

Si la majeure partie des transactions en crypto-actifs est légale, cette technologie serait utilisée dans des activités illicites à hauteur de plusieurs milliards de dollars par an au niveau mondial dont une partie significative concerne le blanchiment d'argent.

Leur utilisation à des fins illicites peut être classée en trois principales catégories : constituer un moyen de paiement, une source directe de revenus ou un outil de blanchiment.



Typologie des usages illicites des crypto-actifs

Les crypto-actifs comme moyen de paiement :

Les crypto-actifs les plus échangés tels que le *Bitcoin (BTC)* et les *stablecoins* peuvent être opportunément utilisés pour commettre de nombreuses infractions. Parfois, en complément du système financier traditionnel, ils sont utilisés pour la vente de produits stupéfiants ainsi que le commerce de données et de moyens de paiement volés.

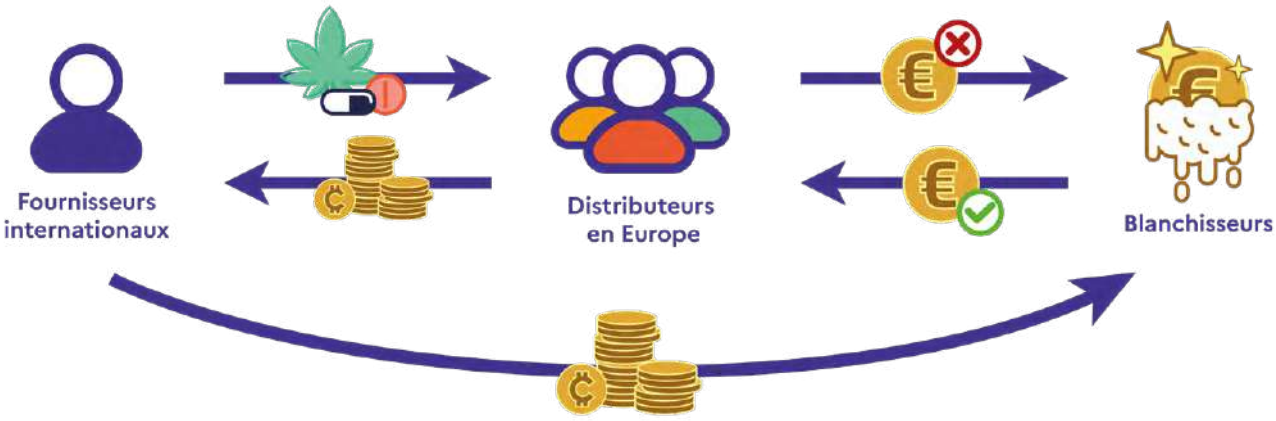
Ce commerce illégal s'effectue notamment sur les forums qui tiennent lieu de places de marché occultes. Un autre cas d'usage criminel est également lié aux crypto-actifs : la vente de contenus relevant de l'exploitation sexuelle des mineurs.

Dans le cas d'attaques coordonnées par déni de service distribué *(DDoS)* ou par rançongiciel *(ransomware)*, les groupes cybercriminels peuvent collecter des fonds auprès de leurs affiliés.

Les crypto-actifs comme source de blanchiment :

En matière de blanchiment d'argent, les criminels ont intégré les évolutions technologiques parmi l'éventail des outils à leur disposition. Pour tenter d'opacifier l'origine illégale des fonds, ils combinent les mixeurs de crypto-actifs (qui mélangent les montants initiaux *via* de multiples transactions réparties sur un grand nombre d'adresses publiques), les échangeurs instantanés (pour convertir des fonds entre deux crypto-actifs) et des crypto-actifs permettant des transactions anonymisées.

En plus de ces procédés, l'analyse des transactions des *blockchains* démontre que les criminels savent transférer leurs fonds d'une *blockchain* à l'autre *(chain hopping)* pour essayer d'opacifier leurs opérations.



Modélisation d'un schéma de blanchiment

Les escroqueries en lien avec les crypto-actifs

L'année 2024 constitue une année marquée par une forte évolution des escroqueries liées aux crypto-actifs qui peuvent être utilisés comme prétexte, comme moyens ou être l'objet même de l'infraction.

Un des modes opératoires les plus courants est le faux investissement. Cette méthode consiste à collecter des fonds, auprès de la victime, au prétexte de les investir pour son compte dans un ou plusieurs crypto-actifs. Les malfaiteurs se présentent comme des professionnels et vont jusqu'à usurper l'identité de plateformes d'échange de crypto-actifs légitimes, pour certaines notoires. Les escrocs promettent des rendements élevés pour s'attacher la confiance des victimes. Dans les cas où l'ingénierie sociale est la plus élaborée, un site internet voire une application affiche facticement l'encours des fonds « investis » par la victime qui visualise ainsi ses « gains » et est encline à investir davantage. La victime finit par perdre confiance et se rendre compte de l'escroquerie lorsqu'elle ne peut pas retirer ses fonds sous divers prétextes (frais de retrait, taxes, sécurisation du portefeuille, bogue informatique, etc.).

La fausse romance :

Désigne les techniques exploitant les sentiments et émotions de la victime pour lui soutirer des crypto-actifs dans le cadre d'une relation amoureuse simulée. Cette méthode peut opportunément combiner manipulation psychologique et schémas d'investissements frauduleux : *via* une application de messagerie, un réseau social ou une application de rencontre, le malfaiteur engage une discussion avec la victime, prétextant souvent une erreur, pour nouer une relation à distance avec l'objectif de collecter des fonds. Les transactions peuvent être faites par la victime sous divers prétextes (frais médicaux à payer, opportunité d'investissement immanquable, etc.).

Le faux emploi :

Ce procédé consiste à exploiter l'appât du gain et/ou le manque de ressources financières de la victime. Le contact se fait *via* une application de messagerie par une personne inconnue proposant un travail en ligne : des tâches simples sont demandées à la victime, telles que l'évaluation de produits sur un site marchand ou le partage de publicités, pour laquelle elle se voit promettre une rémunération. Pour débloquer les sommes promises, sous divers prétextes, le faux employeur demande à la victime de lui envoyer des crypto-actifs.

Création de jetons (Tokens) ou de memecoins :

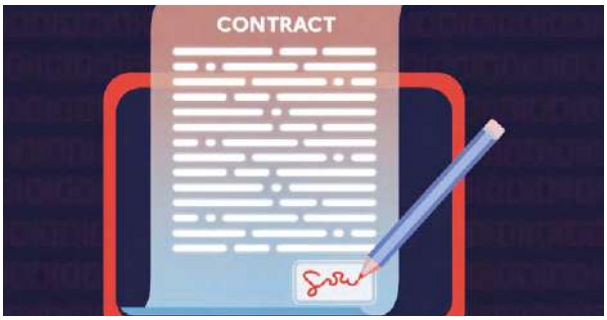
Sur une *blockchain* prévue pour cela, notamment *Ethereum* et *Solana*, ce procédé conduit de nombreuses victimes crédules à « investir » dans des crypto-actifs sans valeur fondamentale. Dans de nombreux cas, les créateurs de projet peuvent gonfler artificiellement le prix des actifs pour attirer les victimes puis revendre soudainement l'ensemble de jetons avant ces dernières.

Les escroqueries ayant pour objet les crypto-actifs

Dans certains cas, la finalité de l'infraction est de dérober les crypto-actifs de la victime. Souvent rattachés par simplification aux vols de crypto-actifs, les draineurs de portefeuilles et les exploitations de *smart contracts* relèvent pourtant *stricto sensu* de manœuvres visant à tromper le détenteur des fonds pour ensuite lui soustraire ses crypto-actifs et donc à une forme techniquement avancée d'escroquerie.

Draineur de portefeuille :

Il s'agit d'un ensemble de manœuvres visant à obtenir la permission de vider le portefeuille de crypto-actifs (au sens technique, c'est-à-dire une ou plusieurs adresses publiques sur une *blockchain*) de la victime. Elle est concrétisée par un *deceptive smart contract*, qui induit en erreur l'utilisateur. Comme un *smart contract* légitime, il s'agit d'un programme qui automatise une ou plusieurs transactions si une condition est réunie, par exemple le don de jetons *(tokens)* alloués en récompense à une action *(airdrop)* ou l'octroi d'un jeton non-fongible *(Non Fungible Token)* après la participation à un évènement *(proof of attendance)*.



Exploitation de *smart contracts* :

La finance décentralisée *(decentralized finance, dite DeFi)* est un écosystème au sein des crypto-actifs visant à recréer un système financier ouvert. Celui-ci repose sur un ensemble de *smart contracts*. Certains protocoles peuvent permettre de gérer au sein de leurs *smart contracts* des centaines de millions ou des milliards de crypto-actifs. Une erreur dans le code d'un protocole ou des manipulations par ingénierie sociale, peuvent permettre à des acteurs malveillants d'en dérober tout ou partie. En 2024, plus de 2,2 milliards de dollars auraient été dérobés suite à l'exploitation de failles dans des *smart contracts* ou directement sur une *blockchain*.

FOCUS

Utilisation des crypto-actifs par les narcotrafiquants

Les crypto-actifs permettent d'élargir les sources de revenus et de faire évoluer les méthodes d'achat, de vente et de blanchiment d'argent des groupes criminels organisés, notamment en matière de trafic de stupéfiants. La vente « au détail » de produits stupéfiants peut déjà être effectuée en crypto-actifs, que ce soit sur des places de forums cybercriminels et d'autres supports de communication tels que les messageries ou applications sur téléphone. Il est probable que ce phénomène suive la croissance du secteur des crypto-actifs et son adoption par un nombre de plus en plus important d'utilisateurs. En amont, le commerce « de gros » des stupéfiants est significativement effectué en crypto-actifs stables *(stablecoins)*.

3 | Modes opératoires hybrides

Si la cybercriminalité agit dans l'espace numérique, ses effets peuvent parfois se traduire dans le monde réel.

Nous constatons de plus en plus d'attaques hybrides mêlant actions physiques et cyber, comme l'extorsion violente de crypto-actifs, le sabotage d'infrastructures numériques ou encore la diffusion ciblée d'informations personnelles *(doxing)*. Ces phénomènes traduisent une porosité croissante entre la sphère numérique et la réalité concrète. Ils illustrent aussi l'évolution des menaces vers des logiques plus violentes, idéologiques ou déstabilisatrices.

Extorsion physique de crypto-actifs

Les détenteurs de crypto-actifs constituent des cibles pour certains groupes criminels organisés qui utilisent des méthodes violentes pour pouvoir soutirer les crypto-actifs de leurs victimes (séquestration, menaces physiques, tortures, etc.).

Si le phénomène était déjà observé au cours de salons et conférences spécialisées à l'étranger, il progresse en France, à mesure que les criminels utilisent de nouveaux moyens numériques pour identifier leurs cibles.

Les personnes disposant d'une certaine notoriété ou d'ancienneté dans le secteur (influenceurs, dirigeants de plateformes de crypto-actifs, etc.), ou leur proche, sont prises pour cible du fait de leur apparente richesse.

Sabotages physiques d'infrastructures réseaux

Bien que moins visible et moins médiatisé, le sabotage physique d'infrastructures numériques constitue une menace critique, notamment en raison de la forte dépendance numérique du monde actuel. Ces attaques visent directement les équipements physiques essentiels au fonctionnement des réseaux de communication et des systèmes d'information de la société.

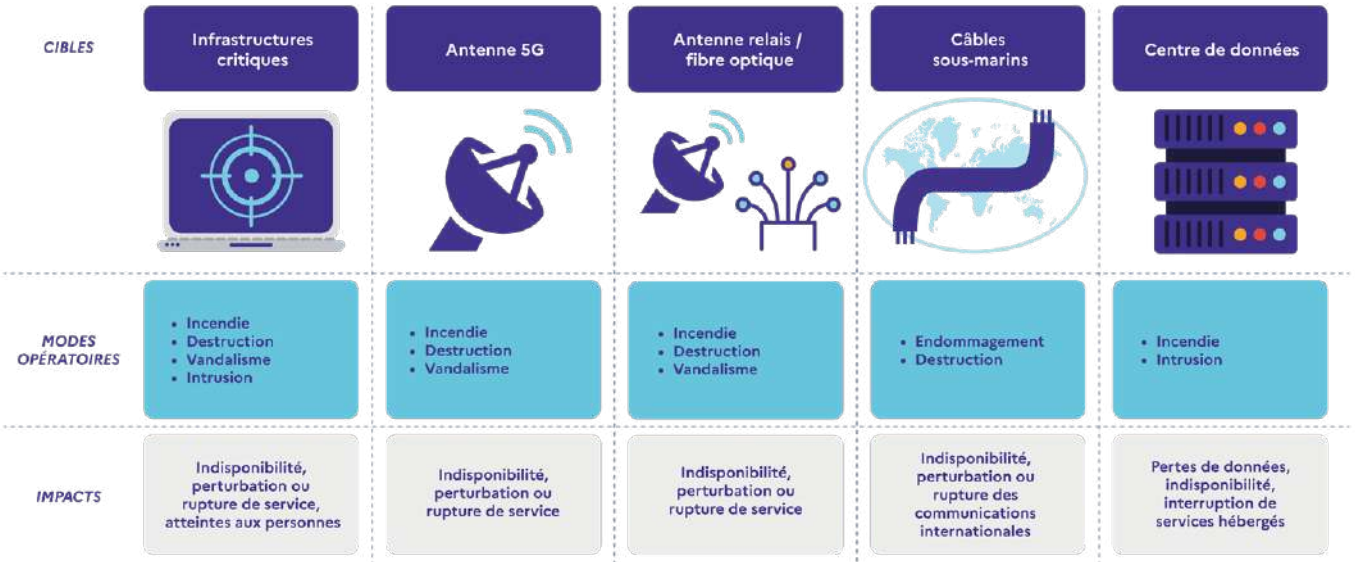
Les enjeux d'une telle menace sont multiples :

- **Géopolitique :** le sabotage peut être utilisé comme un outil de guerre hybride ;
- **Économique :** il peut générer des pertes financières importantes ;
- **Idéologique :** le sabotage peut être un vecteur utilisé pour promouvoir une idéologie ou un moyen d'expression de groupes hacktivistes ;
- **Sécuritaire :** ces actions peuvent fragiliser la sécurité (interruption de communications sensibles, services d'urgence, secteurs d'importance vitale, etc.).

Les modes opératoires varient en fonction des cibles, mais se traduisent généralement par une atteinte aux biens (vandalisme, destruction, incendie, etc.) physiquement ou numériquement. L'éventail de profils des auteurs est large, comprenant des groupes hacktivistes ainsi que des groupes criminels.

Le sabotage impacte l'infrastructure cible, ainsi que tous les services qui lui sont associés : services de communication, services Internet, services essentiels, etc.

Il constitue donc une menace grandissante notamment sur les infrastructures critiques et nécessite une surveillance et une redondance des systèmes pour limiter les impacts sur des services essentiels.



Modes opératoires liés aux sabotages d'infrastructures réseaux

Divulgation de données personnelles *(doxing)*

Le *doxing* illustre de quelle manière des atteintes dans l'espace numérique peuvent avoir des impacts sur la sécurité physique des personnes en conduisant notamment à des actes de harcèlement ou des agressions.

Le *doxing* est un phénomène associé au cyberharcèlement : cette attaque consiste à dévoiler ou à transmettre des données personnelles, telles que le nom, le prénom, les coordonnées, le lieu de vie ou de travail d'un individu, de manière à lui nuire ou à nuire à sa famille, voire à ses biens. Le terme *doxing* vient de la contraction entre le mot « doc » ou « document » et le verbe « *dropping* », faisant allusion au fait de transmettre des informations. L'infraction de *doxing* est réprimée par le Code pénal, depuis 2021.

Pour autant, ce phénomène n'est pas nouveau : le *doxing* a pu tout d'abord être observé dans la sphère cybercriminelle des années 1990. En effet, cette méthode était constatée dans le cadre de rivalités entre cybercriminels, permettant de rompre l'anonymat de ces individus.

Les acteurs malveillants continuent à ce jour de se *« doxer »* entre eux, généralement par vengeance ou par rivalité.

Le *doxing* s'est cependant étendu au-delà du monde cybercriminel et s'applique désormais à un grand nombre de cas d'usage. La population y recourant est généralement plutôt jeune et les informations sont diffusées sur les réseaux sociaux ou sur des forums dédiés à la publication de données personnelles, dans une logique de cyberharcèlement.

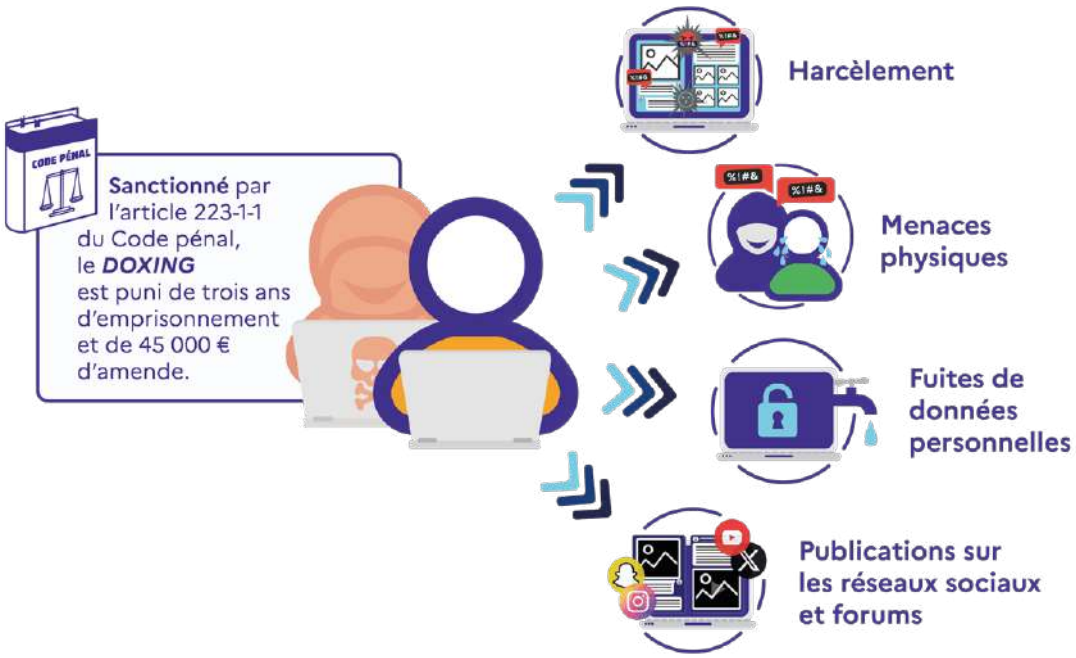
Le *doxing* est également prisé par les hacktivistes qui recourent à ce mode opératoire pour des motifs idéologiques. Ces actions peuvent s'inscrire dans le cadre de conflits internationaux où des acteurs souhaitent déstabiliser ou mettre en danger des personnes. Par exemple, dans le cadre du conflit russo-ukrainien, des actions de *doxing* sont menées fréquemment pour déstabiliser les forces adverses.

De la même manière, des cybercriminels avaient divulgué sur des canaux de discussion l'identité d'athlètes israéliens dans le cadre des Jeux olympiques de Paris 2024. On observe alors une transformation du risque numérique vers un risque physique pour les individus concernés.

Posant des questions d'éthique, le *doxing* a pour particularité d'être parfois pratiqué par des individus pensant agir de manière morale qui vont *« doxer »* des personnes considérées comme déviantes ou criminelles. Certains groupes ou individus isolés travaillent par exemple au *« doxing »* de supposés pédocriminels afin de « rendre justice » par eux-mêmes ou de tenter d'aider les enquêtes en cours. Cependant, ce phénomène constitue le plus souvent une entrave à ces enquêtes et participe à la commission de crimes et délits tels que la diffusion de contenus pédocriminels et des agressions physiques, parfois sur des personnes désignées à tort.

Si le phénomène est, à ce jour, difficile à quantifier et à qualifier, on observe tout de même que le *doxing* se généralise dans la sphère cybercriminelle et devient en parallèle une pratique idéologique.

Pour contrer ce phénomène, il est nécessaire de sensibiliser les internautes aux risques auxquels ils s'exposent en partageant leurs données personnelles en ligne et les encourager à maintenir un bon niveau d'hygiène numérique au quotidien afin de limiter les risques de fuites de données.



Modes opératoires liés au doxing

RETOURS D'ENQUÊTES MAJEURES ET ÉVOLUTIONS JURIDIQUES

1 | Évolutions juridiques 42

2 | Retours d'enquêtes majeures (OFAC, UNCyber et BL2C) 44

3 RETOURS D'ENQUÊTES MAJEURES ET ÉVOLUTIONS JURIDIQUES

1 | Évolutions juridiques

Lutte contre la cybercriminalité : une régulation en constante évolution

La cybercriminalité redessine en permanence les contours de la criminalité classique. Face aux défis du numérique, l'Union européenne a adopté plusieurs textes visant à renforcer la sécurité et à encadrer les nouvelles technologies.

Trois réglementations majeures illustrent cette volonté :

- **La directive NIS2**[9], qui renforce la cybersécurité des secteurs critiques et impose de nouvelles obligations aux entreprises et administrations.
- **Le RIA**[10], qui pose un cadre juridique pour l'intelligence artificielle en fonction de son niveau de risque.
- **Le règlement MICA**[11] , qui vise à encadrer les crypto-actifs et à protéger les investisseurs.

Un cadre juridique renforcé pour la cybersécurité et l'innovation

Directive NIS2 : un renforcement de la cybersécurité

Adoptée en janvier 2023 et entrée en vigueur le 17 octobre 2024 au niveau européen, la directive NIS2 vise à renforcer la cybersécurité en élargissant son champ d'application à des secteurs critiques tels que les administrations publiques, les collectivités territoriales et le domaine spatial. Elle impose des obligations accrues aux secteurs déjà couverts, notamment la banque, la santé, l'énergie, les transports et les services *cloud*.

A minima, 15 000 entités en France seraient concernées, classées en deux catégories : les entités essentielles (EE) et les entités importantes (EI), en fonction de leur domaine, taille et chiffre d'affaires.

La directive impose des mesures techniques (protection des infrastructures, chiffrement, audits, sauvegardes) et humaines (formations obligatoires). Les incidents cyber doivent être signalés sous 72 heures (24 heures pour les plus graves) avec des rapports détaillés. Les sanctions en cas de non-respect peuvent atteindre 10 millions d'euros ou 2% du chiffre d'affaires mondial.

L'ANSSI accompagne cette régulation et propose un espace en ligne dédié : MonEspaceNIS2 (monespacenis2.cyber.gouv.fr).

RIA : encadrer l'intelligence artificielle

Le cadre juridique en matière d'IA a récemment évolué avec l'arrivée du RIA (règlement européen sur l'Intelligence Artificielle). Cette réglementation, entrée en vigueur le 2 août 2024, est un enjeu majeur pour les forces de sécurité afin de prévenir toute asymétrie entre les possibilités criminelles et les capacités des forces de l'ordre.

Le RIA adresse l'IA par les cas d'usage auquel il associe un niveau de risque. Il classe les systèmes selon quatre niveaux de risque:

- Risque inacceptable: interdiction des usages dangereux comme le *scoring social*.
- Risque élevé: usage strictement encadré, notamment pour la surveillance biométrique.
- Risque spécifique: exigences de conformité en matière de transparence et de qualité des données.
- Risque minimal: simple obligation d'information des utilisateurs.

Le texte prévoit une gouvernance européenne avec la création du Bureau de l'IA et impose des sanctions pouvant atteindre 7% du chiffre d'affaires mondial ou 35 millions d'euros.

Cette mise en œuvre s'étalera jusqu'en 2026, en veillant à conjuguer éthique et innovation.

9. Network and Information Security
10. Règlement européen sur l'IA
11. Markets in Crypto-Assets

Règlement MICA : encadrer les crypto-actifs

En vigueur depuis le 30 décembre 2024, le règlement MICA vise à encadrer le marché des crypto-actifs et à protéger les investisseurs.

Il distingue trois catégories de crypto-actifs :

- Utilitaires : permettent d'accéder à un service.
- Adossés à un actif.
- Liés à une devise officielle.

Les NFT[12] restent en dehors du champ du règlement, sauf si des critères spécifiques sont définis par l'ESMA *(European Securities and Markets Authority)*. Les prestataires de services de crypto-actifs (PSCA), tels que les plateformes d'échange et les portefeuilles numériques, doivent désormais obtenir une autorisation européenne pour opérer.

Le texte renforce la protection des consommateurs en imposant un droit de rétractation et une information claire. Il interdit les pratiques frauduleuses telles que le délit d'initié et la manipulation de marché, alignant ainsi la réglementation des crypto-actifs sur les règles boursières.

Ces trois réglementations réaffirment la volonté de l'Union européenne de sécuriser le numérique tout en encadrant l'innovation et en renforçant la confiance des utilisateurs. Elles impliquent des investissements importants pour les entreprises, les collectivités et les services de l'État, pour construire un écosystème européen numérique sûr et innovant.

Lutte contre la cybercriminalité : une régulation en constante évolution

Deux décisions de justice récentes ont un impact significatif sur le cadre légal de la cybersécurité et de la protection des données personnelles en Europe. Elles concernent l'exploitation des données numériques dans le cadre des enquêtes judiciaires et l'utilisation des informations accessibles sur Internet.

CJUE, Gr. ch., 4 octobre 2024 (Affaire C-548/21)

La Cour de justice de l'Union européenne (CJUE) a posé un cadre strict sur l'exploitation des données contenues dans un téléphone portable lors d'une enquête judiciaire. Selon cette décision, l'autorisation d'un juge ou d'une autorité indépendante est désormais requise pour accéder aux données d'un téléphone, sauf en cas d'urgence justifiée comme un risque imminent pour la sécurité publique ou une menace terroriste.

Cette jurisprudence bouleverse les pratiques actuelles en France, où dans certains cas le procureur de la République pouvait autoriser ces accès sans contrôle judiciaire indépendant. Désormais, les enquêteurs doivent informer le propriétaire du téléphone dès que possible, sauf si cela compromet l'enquête en cours.

Ce revirement pourrait impacter les enquêtes de flagrance, menées sous l'autorité du procureur de la République, qui n'est pas un magistrat du siège et ne bénéficie donc pas des garanties d'indépendance exigées par la Cour de Justice de l'Union Européenne (CJUE). Des ajustements du Code de procédure pénale français seront nécessaires pour se conformer à cette jurisprudence.

Cass. Crim., 30 avril 2024, n°23-80.962

Cette décision de la Cour de cassation porte sur la collecte d'informations disponibles en sources ouvertes sur Internet. La Cour a jugé que le fait qu'une donnée soit accessible publiquement en ligne ne signifie pas qu'elle puisse être exploitée sans cadre légal.

Dans cette affaire, un enquêteur privé, mandaté par un directeur de la sécurité d'une entreprise, avait collecté des informations personnelles issues de réseaux sociaux et de bases de données publiques pour profiler des individus, sans les en informer. La Cour a estimé que cette collecte était déloyale et illicite car elle était réalisée à l'insu des personnes concernées et dans un but détourné.

Cette décision rappelle que la transparence et la loyauté sont essentielles en matière de traitement des données personnelles. Même si une information est librement accessible en ligne, son usage doit respecter les principes du *Règlement Général sur la Protection des Données (RGPD)*. Toute collecte de données personnelles doit être réalisée avec le consentement de la personne concernée ou dans le cadre strict défini par la loi.

12. Non Fungible Token

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

OPÉRATION CRONOS (LOCKBIT)

Apparition **fin 2019 initialement sous le nom «ABCD»**

Développé selon le modèle de **ransomware-as-a-service**

300 plaintes de victimes françaises recensées fin 2024

Plus de **7000 cyberattaques** réussies entre juin 2022 et février 2024

Cible tous types d'entités : hôpitaux, collectivités territoriales, transports, etc.

Des **milliards d'euros de préjudice**, et des centaines de millions de dollars rançonnés

Les faits :

Actif depuis 2019, le groupe cybercriminel opérant des rançongiciels a ciblé de nombreuses entreprises, des hôpitaux et des administrations publiques en France et à travers le monde.

L'enquête :

En 2020, la section J3 du parquet de Paris a ouvert une enquête, diligentée par la gendarmerie nationale. Une *taskforce* internationale a été constituée incluant la France sous la coordination d'Europol et d'Eurojust.
En février 2024, l'opération Cronos a permis de neutraliser une partie du réseau du groupe criminel. Cette action a visé les serveurs utilisés pour le déploiement des rançongiciels et les flux financiers associés, tout en identifiant plusieurs individus impliqués dans son fonctionnement.

LES RÉSULTATS DE L'OPÉRATION

34 serveurs saisis

Gel de plus de 200 comptes de crypto-actifs

2 individus interpellés

Sanctions contre l'administrateur LockBitSupp, notamment par le gel d'avoirs criminels

LES PRINCIPAUX ACTEURS DE LA COOPÉRATION INTERNATIONALE

UNE RÉPONSE INTERNATIONALE

- En 2020 une enquête a été ouverte par la section J3 du Parquet de Paris. Les investigations ont été confiées au C3N, actuelle division des opérations de l'Unité Nationale Cyber.
- Une *taskforce* internationale a rapidement été mise en place et a donné lieu, en octobre 2022, à l'interpellation d'un affilié sur territoire canadien.
- En février 2024, une opération internationale baptisée Cronos impulsée par la France et coordonnée par EUROPOL perturbe les opérations du groupe *LockBit*.
- L'opération a été menée à bien grâce à la coopération de 14 pays dans le monde.

OPÉRATION ENDGAME

Lancée en mai 2024, l'opération ENDGAME visait à démanteler plusieurs réseaux de botnets utilisés pour propager des logiciels malveillants à grande échelle. Plusieurs botnets ont ainsi été mis hors service, dont *IcedID, Smokeloader, Pikabot* et *Bumblebee*. Impliquées dans des campagnes de cybercriminalité affectant des millions de systèmes à travers le monde, ces infrastructures servaient notamment à déployer des rançongiciels et à exfiltrer des données sensibles. Ces cyberattaques ont eu des répercussions directes sur des secteurs critiques, notamment des établissements de santé. Coordonnée par Europol et Eurojust, l'enquête a permis de cartographier les infrastructures de commande et de contrôle (C2) des *botnets* et d'identifier les principaux opérateurs impliqués. Les autorités ont retracé les flux financiers associés à ces activités criminelles, mettant au jour des circuits de blanchiment via des crypto-actifs.

LES RÉSULTATS DE L'OPÉRATION

Plus de 100 serveurs neutralisés

Gel de 99 portefeuilles de crypto-actifs contenant plus de 70 millions d'euros

Interpellation de 4 mis en cause dont 3 par les autorités françaises

16 perquisitions

Prise de contrôle sur plus de 2 000 domaines liés à la distribution des logiciels malveillants

Émission de 10 mandats d'arrêt internationaux

EFFECTIFS ENGAGÉS

Coordonnée par l'OFAC, cette enquête faisait l'objet d'une co-saisine par la section de lutte contre la cybercriminilaté (J3) de l'office, de la BL2C et de l'UNCyber.

- Identification de l'administrateur *« SystemBC »*.
- Cartographie des infrastructures en collaboration avec l'ANSSI.
- Coordination du démantèlement de dizaines de serveurs de contrôle.

- Identification d'un acteur principal du dropper *BumbleBee*.
- Coopération avec les autorités arméniennes pour auditionner un individu et procéder à des perquisitions.

- Cible : le service cybercriminel PIKABOT est un injecteur complexe fonctionnant en *malware-as-a-service (MaaS)*. Il était loué par des cybercriminels pour diffuser d'autres programmes malveillants tels que des rançongiciels ou des outils d'exfiltration de données.
- Identification et arrestation en Ukraine de l'administrateur principal de PIKABOT ainsi que d'un complice, deux ressortissants ukrainiens, grâce à une étroite coopération policière internationale.
- Interpellations et perquisitions aux domiciles de l'administrateur et d'un complice, en Ukraine, avec les autorités locales.
- Saisie et démantèlement décisifs de l'infrastructure technique de PIKABOT, comprenant deux serveurs distants clés localisés en Ukraine, permettant l'arrêt immédiat des opérations criminelles.

Coordonée par Europol et Eurojust

Etats membres de l'UE ayant participé

Etats non membres de l'UE ayant participé

Autorités impliquées dans le centres de coordination de l'opération

PLASTIC DEFENSE

Les faits :

En février 2024, une opération judiciaire, menée par l'Unité Nationale Cyber, a permis de mettre fin aux agissements d'individus soupçonnés de faire partie d'un important trafic d'armes fabriquées par des imprimantes 3D. Une affaire inédite en France, résolue grâce à un travail coordonné entre les enquêteurs français et belges.

L'enquête :

En novembre 2022, le C3N, le Centre de lutte contre les criminalités numériques (aujourd'hui devenu la division des opérations de l'Unité Nationale Cyber), identifie sur le darknet un profil francophone, un jeune de 26 ans, proposant à la vente des armes imprimées en 3D. Un mode de fabrication accessible à beaucoup de personnes et qui permet de produire des armes intraçables et capables de tuer.

Les résultats :

- Interpellations de 2 administrateurs et d'une douzaine d'individus.
- Saisies du matériel (imprimantes 3D, ordinateurs, etc.) et de plusieurs milliers d'euros.
- Saisie de plusieurs dizaines d'armes imprimées en 3D et de munitions de différents calibres.

FRANCE TRAVAIL

Les faits :

Le 12 mars 2024, la section J3 du parquet de Paris saisissait la Brigade de Lutte contre la Cybercriminalité (BL2C) suite à une intrusion massive dans le système d'information de France Travail (ex-Pôle Emploi). Près de 43 millions de personnes étaient potentiellement concernées par le vol de données sensibles telles que numéros de sécurité sociale, coordonnées, identifiants, dates et lieux de naissance, exposant les victimes à des risques élevés d'arnaques par SMS et courriel.

L'enquête :

Les investigations révélaient que du 6 février au 5 mars 2024, les auteurs avaient usurpé l'identité d'agents habilités de Cap emploi en contactant le support technique de France Travail afin de réinitialiser leurs mots de passe. Une fois connectés, ils exfiltraient massivement les don-nées vers des serveurs externes, en utilisant des techniques d'anonymisation (VPN, numéros ON/OFF). L'analyse poussée des traces numériques et téléphoniques permettait toutefois d'identifier les suspects.

Les résultats :

- Le 17 mars 2024, trois jeunes individus âgés d'une vingtaine d'années étaient interpellés simultanément à leurs domiciles respectifs.
- L'exploitation des matériels saisis confirmait leur implication directe.
- Interpellations de deux individus en lien avec des faits d'enlèvement, séquestration et extorsion en bande organisée.

COCO

Les faits :

En juin 2024, la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO) a fait fermer la plateforme de chat Coco.gg. Il est reproché à celle-ci de faciliter des activités criminelles et notamment des faits liés à la pédocriminalité, au proxénétisme, et au trafic de stupéfiants.

L'enquête :

Cette enquête, ouverte en décembre 2023 est confiée à l'Unité Nationale Cyber (UNCyber) et à l'Office National Anti-Fraude (ONAF) en lien avec le COMCYBER-MI et des autorités sous la coordination d'Eurojust. Celle-ci a permis d'identifier des administrateurs, et de remonter les flux financiers. Entre janvier 2021 et mai 2024, 23 051 procédures judiciaires ont été ouvertes, impliquant 480 victimes identifiées.

Les résultats :

- Fermeture de la plateforme coco.gg et saisie des serveurs.
- Gel des comptes bancaires associés à la plateforme.
- Arrestation du fondateur de la plateforme.

EPSILON

Les faits :

De 2023 à 2024, trois entreprises françaises subissaient des cyber attaques, entraînant le vol de plusieurs millions de données clients. Les informations sensibles extraites (identifiants, mots de passe, numéros de cartes bancaires, crypto-actifs) étaient ensuite revendues sur un forum cybercriminel. Une des entreprises victimes avait également reçu une demande de rançon de 15 bitcoins, à laquelle elle n'avait pas cédé.

L'enquête :

L'enquête, confiée à la brigade de lutte contre la cybercriminalité (BL2C), permettait de déterminer que ces cyberattaques avaient été réalisées par le biais d'un logiciel malveillant (« *infostealer* ») dénommé *EPSILON*, conçu pour récupérer automatiquement les données sensibles sur les postes infectés. Le groupe cybercriminel administrant ce logiciel malveillant avait revendiqué ces attaques, ainsi que le piratage du compte X de BFMTV/RMC, à des fins de propagande et d'autopromotion.

Les résultats :

- Trois membres d'*EPSILON* étaient interpellés les 4 et 5 juin 2024 et mis en examen.
- Saisie de nombreux matériels numériques ainsi que l'accès à l'infrastructure du groupe.
- Saisie d'actifs numériques d'un montant de plusieurs milliers d'euros.
- Interpellation de deux autres membres importants du groupe en décembre 2024.

GHOST

Les faits :

En septembre 2024, en partenariat avec Europol, plusieurs pays européens, le FBI, le Centre de lutte contre les criminalités numériques (C3N), qui constitue aujourd'hui la division des opérations de l'Unité Nationale Cyber, et le COMCYBER-MI, ont procédé au démantèlement de la solution de chiffrement *GHOST*, qui était majoritairement utilisée par des groupes criminels organisés.

L'enquête :

Issu d'une saisine judiciaire de la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO), le démantèlement de la plateforme *GHOST* est le résultat d'une enquête au long cours menée par l'UNCyber et le COMCYBER-MI, qui ont joué un rôle prépondérant.

Ce travail très technique a été mené pendant plus d'un an au sein du Centre national d'expertise numérique (CNENUM) du COMCYBER-MI, et plus précisément dans le laboratoire de rétro-conception qui dispose de nombreux experts aux compétences rares.

Les résultats :

- Mise à l'arrêt d'une plateforme majoritairement utilisée par des groupes criminels organisés.
- Arrestation de 51 personnes en lien avec la criminalité organisée, principalement en lien avec le narcotrafic.
- Plusieurs assassinats ciblés déjoués.
- Saisies d'avoirs criminels et de stupéfiants.

POWER OFF

Les faits :

En décembre 2024, des plateformes illégales servant à mener des attaques par déni de service distribué *(DDoS)* contre des organisations ont été mises à l'arrêt à la suite d'une coopération judiciaire internationale.

Moyennant paiement, ces plateformes permettaient de paralyser des services de quelques minutes à quelques heures.

L'enquête :

L'opération baptisée *PowerOFF* a été menée sous la coordination d'Europol, avec la participation de 15 pays, dont la France, avec l'implication de l'Office anti cybercriminalité (OFAC).

Les investigations ont permis d'identifier les administrateurs des plateformes, ainsi que des centaines d'utilisateurs ayant commandité ou mené des attaques *DDoS via* ces services.

Les résultats :

- Saisie de 27 plateformes de *DDoS*.
- Arrestation de 3 administrateurs, notamment en France et en Allemagne.
- Identification de plus de 300 utilisateurs de ces services, exposés à des poursuites judiciaires.

SIM SWAPPING

Les faits :

En 2023, deux plaintes révélaient des attaques cybercriminelles visant des détenteurs de crypto-actifs. Ces derniers avaient été victimes de « *SIM swapping* », une technique consistant à détourner leur numéro de téléphone mobile par usurpation d'identité pour obtenir une nouvelle carte SIM. Ce procédé permettait aux criminels de contourner la double authentification par SMS et ainsi de vider les comptes numériques des victimes.

L'enquête :

Confiée à la Brigade de Lutte contre la Cybercriminalité (BL2C), l'enquête démontrait l'implication d'un groupe criminel structuré, composé de dix individus. Ciblant spécifiquement des détenteurs d'actifs numériques abonnés chez un même opérateur téléphonique, les criminels bénéficiaient de la complicité d'un prestataire interne pour activer les nouvelles cartes SIM. Une fois le contrôle des lignes obtenu, les codes reçus par SMS permettaient le transfert des crypto-actifs vers des comptes bancaires dits « taxis », contrôlés par d'autres complices. Plus de 200 victimes potentielles étaient identifiées, dont une trentaine ayant déjà porté plainte.

Les résultats :

- 10 suspects interpellés simultanément sur tout le territoire national et en outre-mer.
- À l'issue des investigations complémentaires et après l'exploitation approfondie des matériels saisis, trois auteurs secondaires faisaient l'objet d'une composition pénale, tandis que les sept principaux mis en cause étaient renvoyés devant la cham-bre correctionnelle du TJ de Paris.

MATRIX

Les faits :

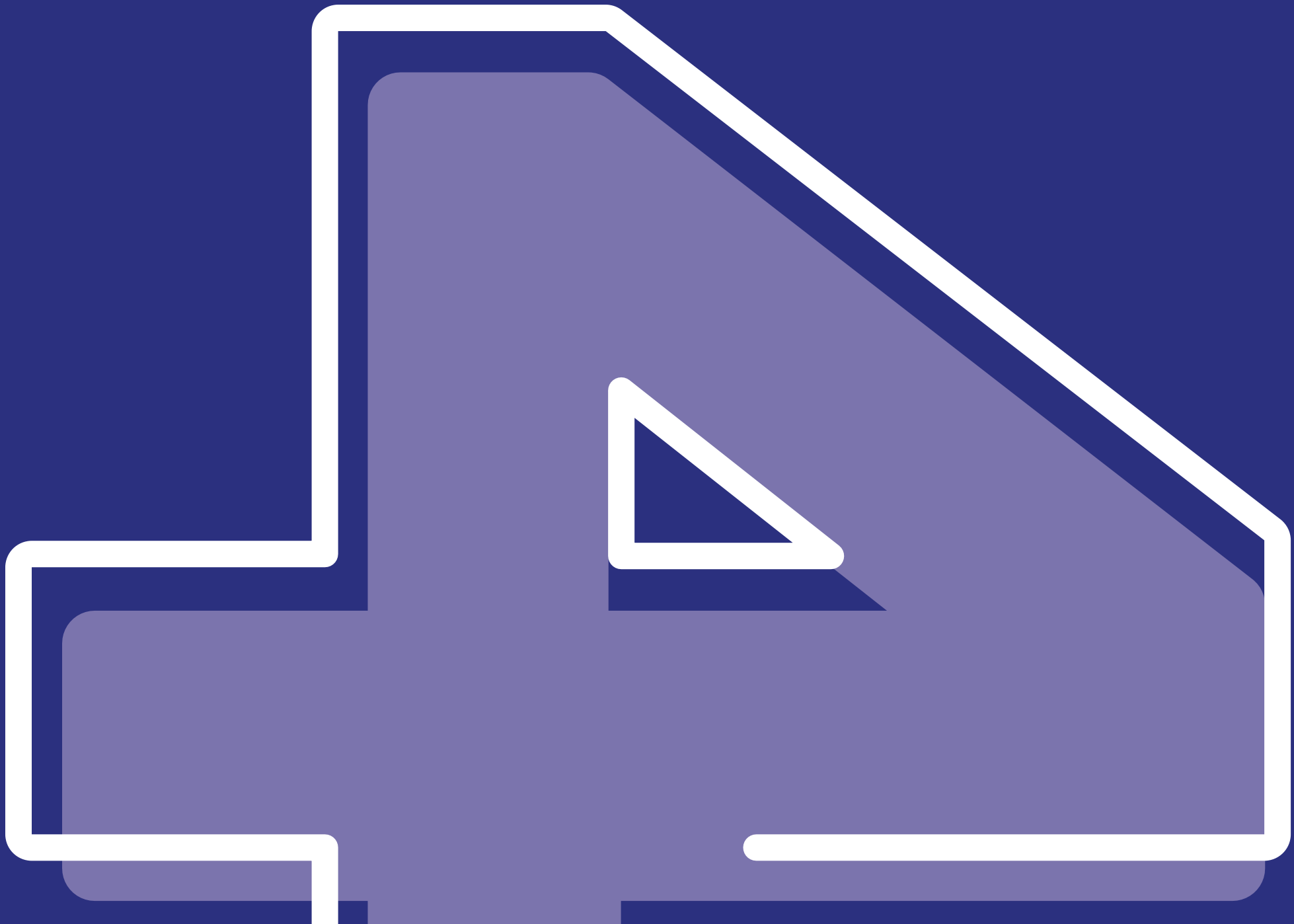
Découverte il y a quatre ans par les policiers néerlandais, *Matrix* était une messagerie chiffrée conçue et utilisée à des fins criminelles. Pour accéder à cette messagerie, les utilisateurs devaient s'équiper de téléphones coûtants entre 1 300 et 1 600 euros. La messagerie servait de canal de communication pour toutes formes de criminalités organisées comme des trafics de stupéfiant.

L'enquête :

Une enquête coordonnée par les agences européennes Europol et Eurojust, impliquant l'OFAC (Office anti-cybercriminalité) a permis d'intercepter et de déchiffrer plus de 2,3 millions de messages dans 33 langues. L'infrastructure Matrix reposait sur plus de 40 serveurs répartis dans plusieurs pays dont la France.

Les résultats :

- Démantèlement de la messagerie.
- Arrestation de trois individus originaires des pays de l'Est, dont une se trouvant à Paris.
- Saisie d'une villa en Espagne estimée à 15 millions d'euros, de 4 véhicules de luxe, 145 000 euros en numéraire et 500 000 euros en crypto-actifs.



PROSPECTIVE SUR L'ÉVOLUTION DES CYBERMENACES

1 | L'usage de l'intelligence artificielle dans la prévention des menaces 52

2 | Internet des objets : un vecteur de risques émergents 54

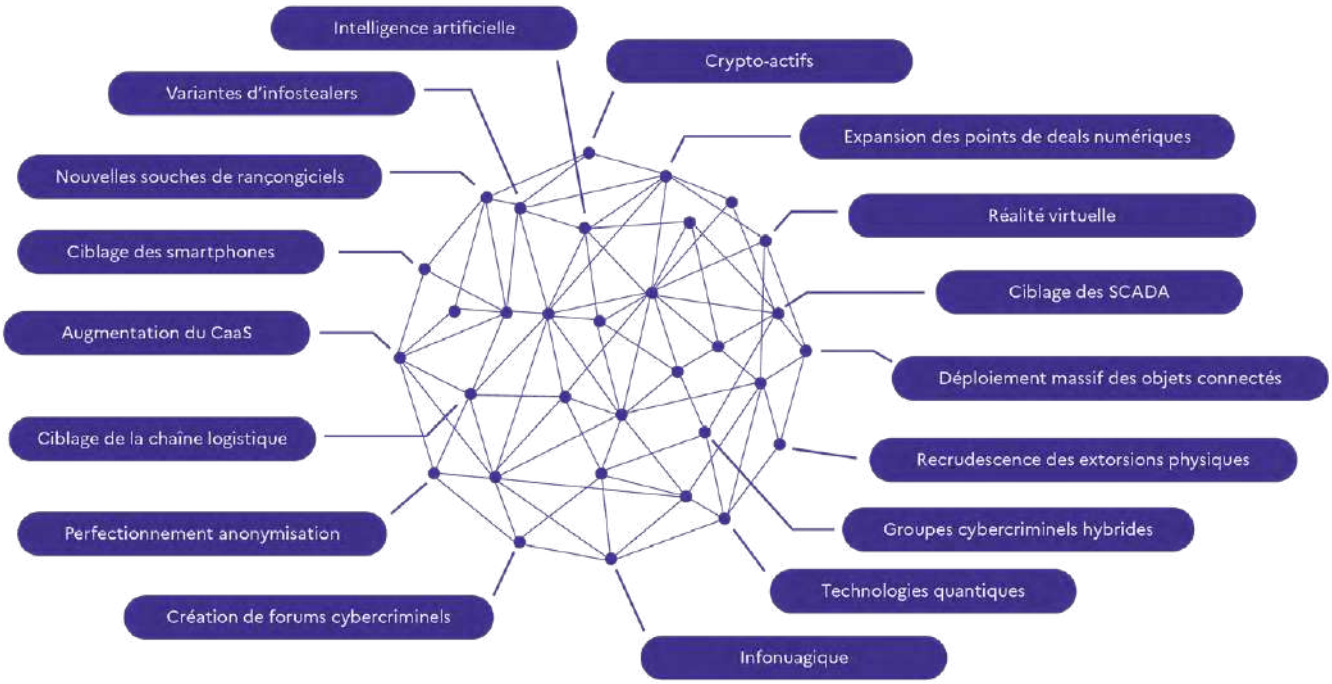
4 PROSPECTIVE SUR L'ÉVOLUTION DES CYBERMENACES

Dans un monde où les technologies et les usages évoluent à un rythme accéléré, les cybermenaces se transforment et se complexifient, rendant la prévention plus indispensable que jamais. Pour anticiper les risques de demain, il ne suffit plus de réagir : il faut comprendre et se préparer.

Cette partie du rapport s'attache à explorer les tendances émergentes et les technologies critiques.

Elle met en lumière le rôle central de l'intelligence artificielle dans la détection des menaces futures et les risques systémiques liés à la généralisation des objets connectés.

Ces approches complémentaires visent à doter les services de l'État, les acteurs privés et les citoyens d'une vision éclairée et proactive afin de renforcer collectivement la résilience du pays face aux menaces de demain.



L'évolution des cybermenaces

1 | L'usage de l'intelligence artificielle dans la prévention des menaces

Le recours à l'intelligence artificielle, pour avoir un impact positif, nécessite de s'inscrire dans une vision stratégique afin d'éviter des mésusages et de développer une IA responsable au profit de la protection des citoyens.

Son déploiement répond à un double impératif : garantir une sécurité numérique souveraine et neutraliser les attaques émergentes dans le respect du cadre éthique et juridique.

La stratégie CapIA, développée depuis quatre ans, adopte une approche collaborative où l'intelligence artificielle soutient le travail des enquêteurs sans remettre en cause leur capacité décisionnelle. Cette stratégie, qui inclut notamment le COMCYBER-MI, vise à construire une IA de confiance au service de la sécurité des citoyens.

Stratégie

L'IA, bien que détournée par les cybercriminels, est aussi un outil essentiel pour protéger les systèmes d'information, révéler les impostures ou encore détecter les comportements malveillants. Face aux menaces des IA génératives *(deepfakes, phishing)*, le commandement du ministère de l'Intérieur s'est inscrit dans la stratégie CapIA, développée au sein de la Gendarmerie et embrassant la polysémie de l'IA.

Il ne peut être envisagé d'exploitation de l'IA sans la construction de piliers solides appuyant la stratégie. Ils constituent la confiance fondatrice d'une innovation responsable, soutenable et durable. Quatre piliers structurent une approche de l'IA sur l'ensemble de sa chaîne de valeur garantissant sa performance technologique et celle de l'organisation qu'elle sert.

Ces piliers sont :

Une IA souveraine :

La capacité à maîtriser et développer ces outils au niveau national ou européen est essentielle et nécessite de s'engager dans la voie de la recherche et du développement appliqués ;

Une IA maîtrisée :

En développant une politique de gestion des talents et un registre de formation allant de l'acculturation (revue Cultur'IA) à la formation niveau expert (création de la chaire IA et Sécurité), l'objectif est d'appréhender les limites et les opportunités de l'exploitation de l'IA. Il s'agit également d'en avoir une connaissance approfondie afin de satisfaire aux exigences d'explicabilité vis-à-vis du citoyen comme des représentations parlementaires nationale et européenne ;

Une IA responsable :

La Gendarmerie notamment a publié dès 2021 une charte éthique pour les applications en IA qui s'inscrivent dans les valeurs de l'institution. Elle est par ailleurs engagée dans les enjeux de la réglementation européenne des usages de l'IA comme de l'expérimentation de son exploitation dans le cadre des grands évènements ;

Une IA partagée :

Il est essentiel dans le champ de la sécurité intérieure de ne pas demeurer en vase clos. Le COMCYBER-MI a engagé des partenariats avec le monde académique comme le monde industriel ou associatif. L'enjeu est d'expliquer, d'échanger et d'améliorer les usages face à des exploitations criminelles toujours plus imaginatives.

Des outils innovants au service de la détection et de la protection

L'intelligence artificielle offre une capacité inégalée à traiter des masses de données hétérogènes (texte, image, vidéo, voix) pour identifier des menaces imperceptibles à l'œil humain. Parmi les initiatives clés figure le projet *Authentik IA*. Développé en interne au sein du COMCYBER-MI par une équipe pluridisciplinaire (ingénieurs IA, juristes, alternants), ce projet a pour objectif d'identifier les médias synthétiques afin de faciliter la reconnaissance des *deepfakes*, en croisant des marqueurs techniques et contextuels détectés dans ces médias.

Dans le cadre de la détection d'images d'exploitation sexuelle de mineurs, le projet ODIP[13] (Outil de Détection des Images Pédopornographiques) visant à assister les enquêteurs dans la matérialisation de l'infraction est en cours de développement. Doublement primé lors des *Datacraft awards* de 2024, ce projet comporte deux étapes majeures :

- la création des représentations numériques de contenus d'exploitation sexuelle de mineurs qui permettent de détecter du contenu illicite sans le visualiser ;
- l'entraînement du modèle d'IA à partir de ces représentations vectorielles, afin qu'il soit en capacité d'identifier automatiquement ce contenu lors de l'analyse d'un support numérique.

Ce projet, développé en interne par le COMCYBER-MI, répond à la nécessité de soustraire les enquêteurs à l'exposition traumatique de contenus sensibles et à optimiser radicalement le traitement des preuves numériques.

13. https://www.numerama.com/cyberguerre/1900240-nos-outils-ia-permettent-deja-deviter-des-traumatismes-entretien-avec-le-general-de-gendarmerie-en-charge-de-lia.html

La formation et l'acculturation comme piliers de la stratégie CapIA

Au-delà de la mise en place d'outils d'IA avancés, l'usage et la maîtrise de ces innovations reposent également sur un solide dispositif de formation allant de l'acculturation au doctorat. Dans ce cadre, la stratégie CapIA définit les axes de formation en conformité avec le RIA qui impose la formation du personnel d'une organisation mettant en œuvre de l'IA. Entre le niveau de sensibilisation de l'ensemble du personnel du COMCYBER-MI et le niveau expert, CapIA met en place des formations courtes au profit des enquêteurs spécialisés.

Afin de pérenniser cette transmission de savoir, la revue bimestrielle Cultur'IA (accessible en ligne[14]) offre quant à elle une approche théorique et pratique, abordant à la fois les aspects juridiques, les évolutions technologiques ainsi que les applications concrètes dans le domaine de la sécurité.

Parallèlement, l'établissement d'une chaire « IA et Sécurité », portée aujourd'hui par un partenariat entre le COMCYBER-MI et l'Institut Supérieur d'Électronique de Paris (ISEP), vise à structurer des parcours doctoraux et à renforcer les compétences des cadres et des futurs experts. Ces initiatives pédagogiques et partenariales illustrent à la fois l'engagement pour l'innovation et pour une compréhension approfondie des outils déployés, garantissant ainsi que les acquis technologiques demeurent solidement ancrés dans une réflexion éthique et opérationnelle robuste.

La stratégie CapIA dans laquelle s'inscrit le COMCYBER-MI vise une ambition protectrice des libertés individuelles comme du modèle de société démocratique en offrant une plus grande efficacité dans la lutte contre la criminalité.

2 | Internet des objets : un vecteur de risques émergents

L'Internet des Objets (IdO), plus souvent connu sous son acronyme anglais *IoT (Internet of Things)*, concerne l'ensemble des objets connectés qui collectent et échangent des données et fournissent des services dans nos vies de tous les jours. Ces objets, souvent équipés de capteurs, peuvent traiter des informations pour déclencher des actions ou les transmettre. L'IdO, désigne spécifiquement des objets capables de fonctionner en réseau. Cela peut correspondre à des capteurs d'humidité, des capteurs de fenêtres, thermomètres, serrures, climatiseurs, véhicules connectés. Le marché des objets connectés se caractérise par son expansion extrêmement rapide, avec une estimation de 45 milliards d'objets connectés dans le monde d'ici 2030, qui auront un impact significatif sur nos modes de vie.

Malgré ses nombreux avantages, l'IdO représente une menace toujours plus importante. En effet, ces objets, collectant une très grande quantité de données sensibles, se révèlent être vulnérables aux cyberattaques. Les risques liés à leur sécurité, au respect de la vie privée et à l'interconnexion de ces dispositifs rendent leur gestion critique. L'augmentation du nombre d'objets connectés soulève des préoccupations à propos des atteintes à la vie privée, des violations de données et des failles de sécurité qui pourraient être exploitées par des cybercriminels.

De plus, ces objets connectés peuvent être détournés de leurs usages premiers afin de réaliser des actions malveillantes de type *DDoS* et espionnage en mobilisant leur puissance de calcul et leurs fonctionnalités.

Usages et évolutions

Les objets connectés formant l'Internet des Objets (IdO) sont présents dans divers secteurs : industrie, agriculture, automobile, santé ou encore domotique. L'IdO transforme notre quotidien et offre de nombreuses possibilités d'amélioration et de gestion des tâches. Ces utilisations sont également de plus en plus interconnectées avec des solutions d'intelligence artificielle.

Il se distingue par sa facilité de déploiement, de mise en œuvre et sa capacité d'adaptation aux besoins et leurs évolutions. Il permet l'automatisation des tâches, un gain de productivité, une optimisation des ressources. Il offre une accessibilité à distance et facilite la prise de décision.

À titre d'exemple, le déploiement de l'IdO dans le domaine de l'agriculture permet d'optimiser la gestion de serres en offrant des informations en temps réel sur les conditions telles que la température, l'humidité et l'éclairage. Ces données permettent d'ajuster les paramètres de gestion de la serre selon des critères définis et modifiables pour optimiser les conditions de culture.

14. https://www.calameo.com/books/0027192924fd5d12ea20e

Risques et exploitation

Dans le domaine de la cybersécurité, des failles sont quotidiennement détectées. La quantité et la variété d'objets connectés nous entourant ne faisant qu'augmenter, les risques numériques sont par conséquent d'autant plus présents. Des millions de vulnérabilités informatiques sont détectées chaque année sur des objets connectés.

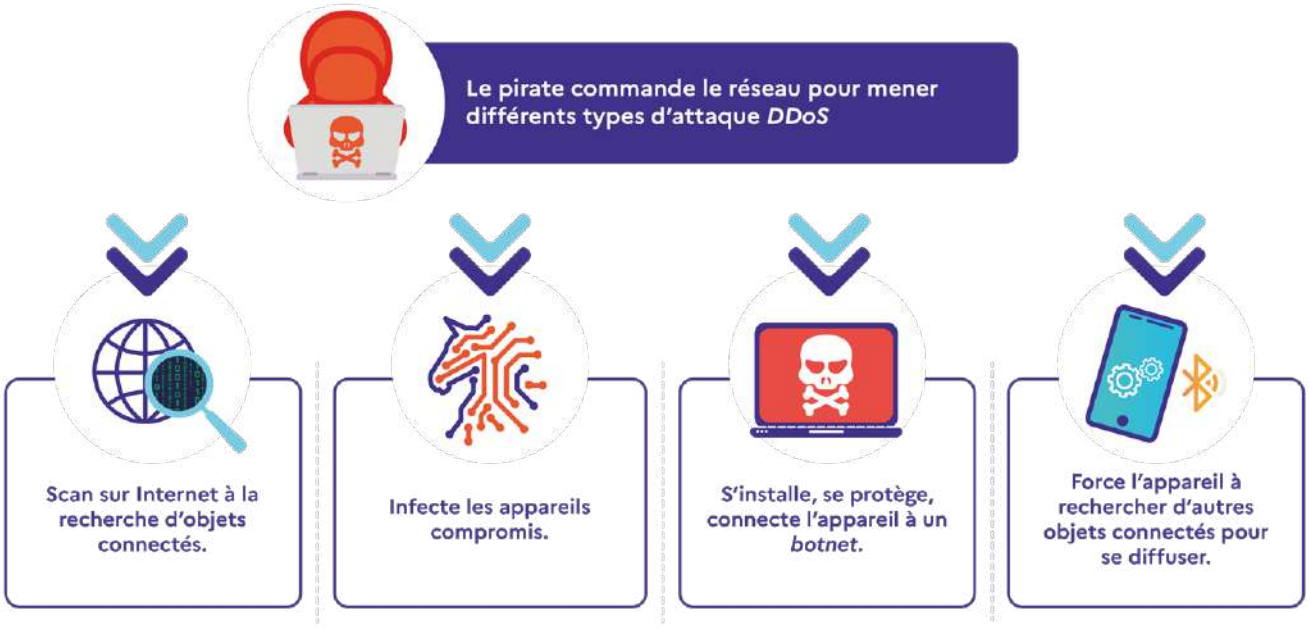
Les risques liés à l'Internet des Objets incluent une mauvaise prise en compte de la sécurisation dès la conception des objets et de leurs moyens de communication. Des mauvaises pratiques d'utilisateurs, comme l'utilisation de mots de passe faibles ou l'oubli de mise à jour des produits, aggravent ces risques.

L'exploitation criminelle de l'IdO se divise en deux grandes catégories : cybercriminalité et délinquance traditionnelle.

Les cybercriminels utilisent des outils pour pirater les objets connectés et les plateformes de connexions dans le but par exemple de créer des *botnets* pour perpétrer des attaques *DDoS*, de mener des campagnes d'hameçonnage, d'espionner, de voler des données ou encore d'accéder aux réseaux informatiques sur lesquels ils sont déployés.

La délinquance traditionnelle, utilise ces objets pour optimiser ses trafics, espionner, harceler ou faciliter des cambriolages et vols de voitures.

L'Internet des objets offre de nombreuses opportunités, mais soulève des défis en matière de sécurité, de vie privée et d'impact écologique. Bien que des règlementations telles que le RGPD, NIS2 ou encore le *Cyber Resilience Act* puissent limiter certains risques, l'accroissement du nombre d'objets connectés produits et utilisés générera une surface d'attaque de plus en plus importante.



Modélisation d'une cyberattaque via les objets connectés

Se renseigner

CYBER MALVEILLANCE .GOUV.FR

Prévenir et sensibiliser les internautes sur la cybercriminalité.

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 renforcer son système d'information 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.

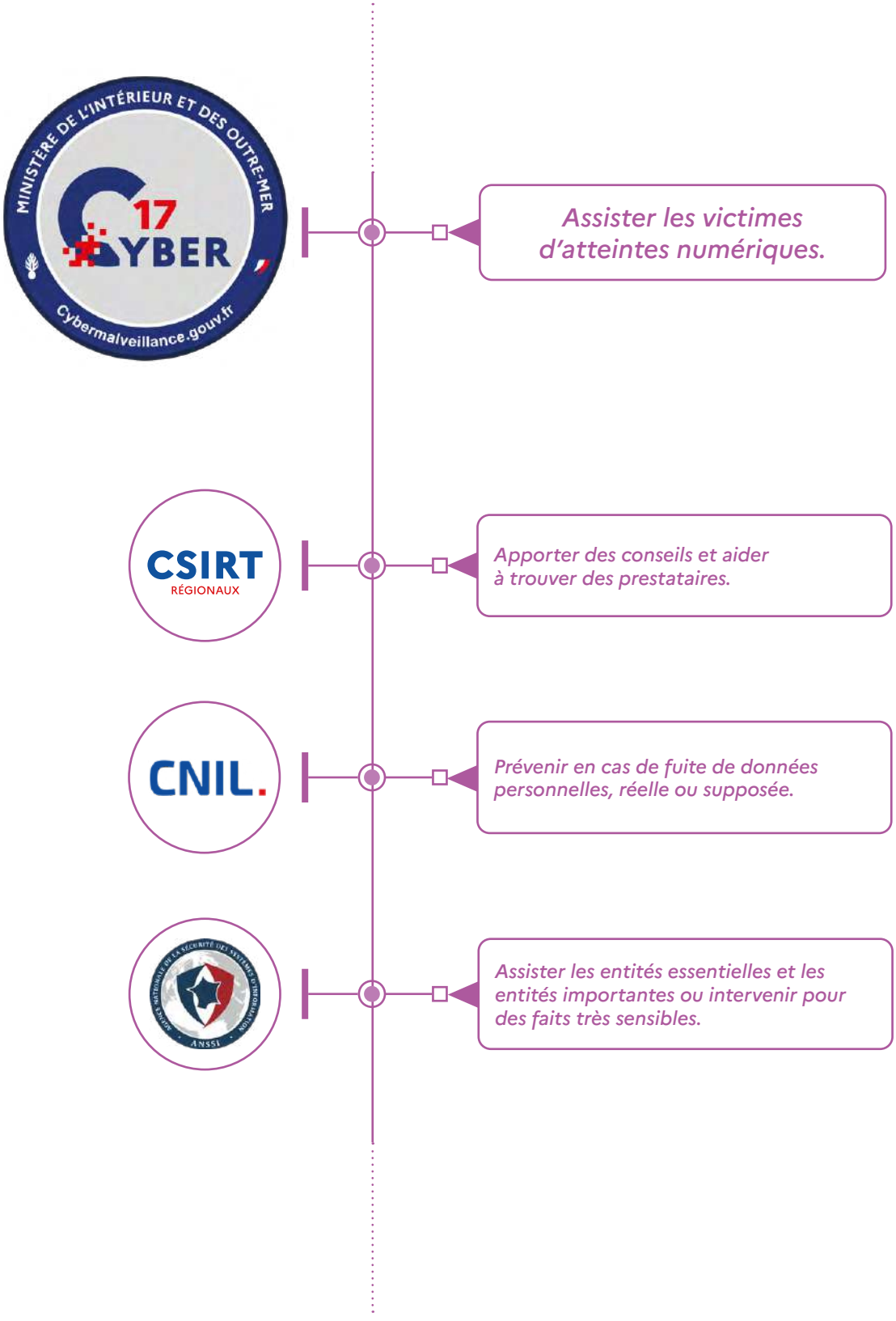
Se renseigner sur les données personnelles, l'exercice de ses droits ou faire un MOOC sur le RGPD.

VOUS AVEZ UN DOUTE SUR UN E-MAIL ?

Signalez-le comme spam sur la plateforme :

signal spam

Réagir face à des atteintes numériques



MA SÉCURITÉ

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

masecurite.interieur.gouv.fr

Ma Sécurité
Application Grand Public

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 :*

https://17cyber.gouv.fr/

CYBERMALVEILLANCE.GOUV.FR

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

cybermalveillance.gouv.fr

CSIRT
RÉGIONAUX

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

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

CNIL.

CNIL

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

cnil.fr

LEXIQUE

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.

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

Attaques sous « faux drapeau » :
Attaque trompeuse visant à faire croire qu'elle provient d'un autre acteur (pays ou groupe) pour dissimuler l'origine d'une cyberattaque ou porter atteinte à un acteur tiers.

***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, etc.).

***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.

Bourrage d'identifiants (*Credential Stuffing*) :
Attaque consistant à tester automatiquement des combinaisons d'identifiants et mots de passe volés, pour vérifier s'ils fonctionnent et mener une cyberattaque.

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

Chasse au gros gibier (*Big Game Hunting*) :
Stratégie de cyberattaque ciblant de grandes entreprises ou institutions pour exiger des rançons ou obtenir des gains très élevés *via* des techniques sophistiqués.

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

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

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

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 constitué par l'interconnexion mondiale 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.

***Doxing* :**
Révélation publique non autorisée d'informations personnelles sur une personne (nom, adresse, téléphone), souvent pour l'intimider ou la harceler.

***Dataleaks (fuites de données)* :**
Divulgation malveillante ou accidentelle de données sensibles (courriels, mots de passe, données bancaires, etc.).

***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.

***DDoS-as-a-Service (DaaS)* :**
Consiste à mettre à disposition ou louer des logiciels dédiés à la mise en œuvre de cyberattaques par *DDoS*. Les attaquants peuvent être rétribués pour mener certaines cyberattaques, en échange d'une preuve.

***Deepfake-as-a-Service (DfaaS)* :**
Service fournissant des vidéos truquées générées par IA *(deepfakes)* à la demande, accessibles même aux non-techniciens *via* des plateformes spécialisées payantes.

***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 ou plusieurs supports informatiques.

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

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.).

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

Empoisonnement des données
***(Data Poisoning)* :**
Altération volontaire des données d'entraînement d'un modèle d'IA pour biaiser ses résultats ou créer des comportements non voulus.

***ESMA (European Securities and Markets Authority)* :**
Autorité européenne supervisant les marchés financiers de l'Union européenne, veillant à leur stabilité et à la protection des investisseurs.

***Face swap* :**
Technique de modification d'images et vidéos où les visages de deux personnes sont échangés.

***Facial reenactment* :**
Technique de *deepfake* reproduisant les expressions faciales d'un individu en temps réel sur un autre visage.

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

Faux conseiller bancaire :
Escroc se présentant comme un employé de banque pour soutirer des informations financières ou obtenir des validations de virements sous prétexte d'une procédure de « sécurité ».

Faux emplois :
Annonces d'emplois frauduleuses visant à obtenir des données sensibles (RIB, pièces d'identité) ou escroquer de l'argent *via* de faux frais.

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.

Faux président :
Arnaque où un malfaiteur usurpe l'identité du dirigeant d'une entreprise pour exiger un virement bancaire.

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

G7 :
Le (« groupe des 7 ») est un groupe de discussion et de partenariat économique qui réunit chaque année les chefs d'État et de gouvernement des 7 pays parmi les plus industrialisés au monde (France, États-Unis, Canada, Japon, Royaume-Uni, Italie, Allemagne).

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 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.

ICANN (Internet Corporation for Assigned Names and Numbers) :
Organisation à but non lucratif et reconnue d'utilité publique rassemblant des participants du monde entier qui œuvrent à la préservation de la sécurité, la stabilité et l'interopérabilité de l'Internet.

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

***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.

***Ingénierie sociale* :**
Technique de manipulation psychologique exploitant la confiance ou l'ignorance dans un but malveillant. Ce mode opératoire est utilisé pour mener des escroqueries mais également des cyberattaques.

***Insiders* :**
Individus internes à une organisation (employés, sous-traitants) exploitant leur accès légitime dans un but malveillant.

***IoT / IdO (Internet of Things / Internet des Objets)* :**
Réseau d'objets connectés (montres, capteurs, appareils domestiques) capables de collecter et transmettre des données *via* Internet.

***LAM (Large Action Model)* :**
Modèle d'IA conçu pour planifier et exécuter des actions complexes, souvent utilisé pour automatiser des tâches pratiques dans des environnements logiciels ou physiques.

***LLM* (Large Language Model) :**
Modèle d'intelligence artificielle entraîné sur d'importants volumes de texte pour comprendre, générer ou résumer du langage naturel.

***Logiciel Open Source* :**
Logiciel dont le code source est entièrement accessible sur internet gratuitement. Il est potentiellement modifiable et réutilisable. Beaucoup de logiciels utilisés par les cybercriminels sont open source.

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 logiciels malveillants prêts à l'emploi, souvent avec support technique.

***Memecoins* :**
Crypto-actifs de memes (ex : *Dogecoin, Shiba Inu*), créés sans objectif technologique mais pouvant prendre de la valeur *via* la spéculation.

Minage de crypto-actifs :
Action visant à sécuriser une *blockchain* en prêtant sa puissance de calcul 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. Ce procédé est légal mais certains cybercriminels utilisent la puissance de calcul des machines de leurs victimes pour qu'elles minent des crypto-actifs à leur *insu*, au profit du malfaiteur.

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

Modus operandi (mode opératoire) :
Méthode ou mode opératoire utilisé de manière récurrente par un groupe ou un individu pour commettre des cyberattaques ou des fraudes.

NFT (Non-Fungible Token) :
Jeton numérique créé sur une *blockchain*, représentant une œuvre, un objet virtuel ou un droit.

***Phishing-as-a-Service (PhaaS)* :**
Vente de *kits* ou services d'hameçonnage clé en main sur des forums cybercriminels, messageries chiffrées ou autre.

Rançongiciel *(ransomware)* :
Logiciel malveillant de demande de rançon par chiffrement de données 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.

RDP *(Remote Desktop Protocol)* :
Protocole permettant la connexion à distance à un ordinateur.

RGPD :
Règlement général sur la protection des données.

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

RIA (Rich Internet Application) :
Applications *web* offrant une expérience utilisateur proche des logiciels installés, avec interactions dynamiques (ex. : *Google Docs, Figma*).

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.

***Script kiddies* :**
Hackers débutants utilisant des outils disponibles sur Internet sans comprendre leur fonctionnement, souvent pour mener des cyberattaques peu critiques.

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

***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*.

***Spearphishing* :**
Hameçonnage ciblé visant une personne ou entité précise, avec un message personnalisé. Ce mode opératoire est particulièrement utilisé pour infecter le support informatique de la victime et mener une cyberattaque.

***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.

***Swatting* :**
Appel malveillant destiné à faire intervenir indûment les forces de l'ordre ou de sécurité civile (ex : fausse alerte à la bombe).

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.

Typosquattage *(typosquatting)* :
Action malveillante qui consiste à déposer un nom de domaine très proche d'un autre nom de domaine, pour commettre des escroqueries ou des cyberattaques.

Vishing *(voice phishing)* / Hameçonnage vocal :
Escroquerie téléphonique utilisant l'ingénierie sociale pour inciter la victime à fournir des données sensibles ou effectuer des actions qui lui seront nuisibles.

VLM (Very Large Model) :
Modèle d'IA de nouvelle génération, encore plus vaste que les LLM, avec des milliards de paramètres, souvent multimodal (texte, image, code).

VPN (Virtual Private Network) :
Réseau privé virtuel créant un tunnel chiffré entre l'utilisateur et un serveur. Cette technologie permet notamment de changer d'adresse IP.

***Wallet* :**
Interface (logicielle ou matérielle) permettant d'accéder et de gérer des crypto-actifs liés à une ou plusieurs adresses publiques.

NOTES

Directeur de publication :
Général de division Christophe Husson

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 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

Illustration couverture :
Image générée avec Freepik IA et utilisée conformément à la licence Freepik. (www.freepik.com)

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