RADICAL-SSI

PANORAMA DES MENACES CYBER 2025–2026

Partie 1 : Etude sur le système économique de la cybercriminalité

Radical SSI - Avril 2026

Note éditoriale

Ce document est une synthèse analytique construite à partir de sources publiques - ANSSI, CNIL, Cybermalveillance.gouv.fr, ENISA, presse spécialisée européenne - et de l'observation opérationnelle du paysage des menaces en 2025 et au premier trimestre 2026. Les faits illustratifs cités sont issus d'incidents avérés et documentés. Cette synthèse est destinée aux décideurs, CODIR, DSI, RSSI, mais aussi à toute personne souhaitant disposer d'une lecture stratégique des menaces actuelles, sans prérequis technique.

Table des matières

1 Introduction : la cybercriminalité est un système économique 3

2 Poser le problème : la monétisation du crime est structurante 5

3 Une taxonomie des attaques selon les modes de monétisation 7

3.1 La monétisation par la contrainte : l'extorsion directe 7
3.2 La monétisation par revente volontaire : les marchés secondaires de données 8
3.3 La monétisation par détournement de flux financiers 9
3.4 La monétisation par exploitation de ressources : cryptomining et botnets locatifs 10
3.5 La monétisation différée : persistance et valeur stratégique 12
3.6 La monétisation par destruction ou capture de valeurs symboliques 12
3.7 Au-delà de la monétisation : les attaques à finalité stratégique 14

4 La structure du marché criminel 17

4.1 La professionnalisation et la division du travail 17
4.2 Le financement de l'écosystème criminel 18
4.3 La liquidité différentielle des marchés 18
4.4 La liquidité spécifique des attaques supply chain 20
4.5 La convergence vers l'exfiltration comme choix rationnel 20

5 Les implications pour repenser une défense cyber 23

5.1 Dégrader le rendement plutôt que bloquer l'accès 23
5.2 Identifier ce qui rend une organisation cible rentable sur les marchés criminels 23
5.3 Utiliser la spécialisation des attaquants comme levier de Threat Intelligence 23
5.4 Deux limites à garder en tête 24

6 Conclusion : La cybercriminalité comme fait économique total 26

7 Lexique et notes 28

1 Introduction : la cybercriminalité est un système économique

La cybercriminalité n'est pas un phénomène technique, c'est un système mature, rationnel et doté de mécanismes internes de régulation. Comprendre ses logiques de monétisation est un préalable à toute stratégie de défense cohérente.

L'attaquant est un acteur économique. Il arbitre en permanence entre effort, risque et gain, en cherchant à minimiser le nombre de phases de son opération et à maximiser la fluidité de sa monétisation. C'est cet arbitrage, plus que la sophistication technique, qui détermine le choix de la cible et du mode opératoire.

Les modes de monétisation sont diversifiés et complémentaires. De l'extorsion directe par rançongiciel, jusqu'au détournement de flux financiers, l'écosystème criminel couvre un spectre complet de modèles économiques. Chacun correspond à un profil d'attaquant, une cible et un niveau de risque distincts.

La convergence que l'on constate actuellement vers l'exfiltration est un choix rationnel. Face aux rançongiciels dont le taux de conversion s'érode sous la pression réglementaire, l'exfiltration pure offre un rendement structurellement supérieur et un risque réduit : moins de phases, absence de friction avec la victime, marché secondaire fluide et discret. Et, une irréversibilité totale pour la victime.

L'écosystème de la cybercriminalité est industrialisé et résilient. La division du travail très forte a abaissé drastiquement le niveau de compétence requis pour mener des attaques sophistiquées. Cet écosystème est remarquablement résistant aux démantèlements : ses composants survivent aux individus.

Etudier la cybercriminalité sous l'angle de sa monétisation nous amène à concevoir trois implications défensives majeures :

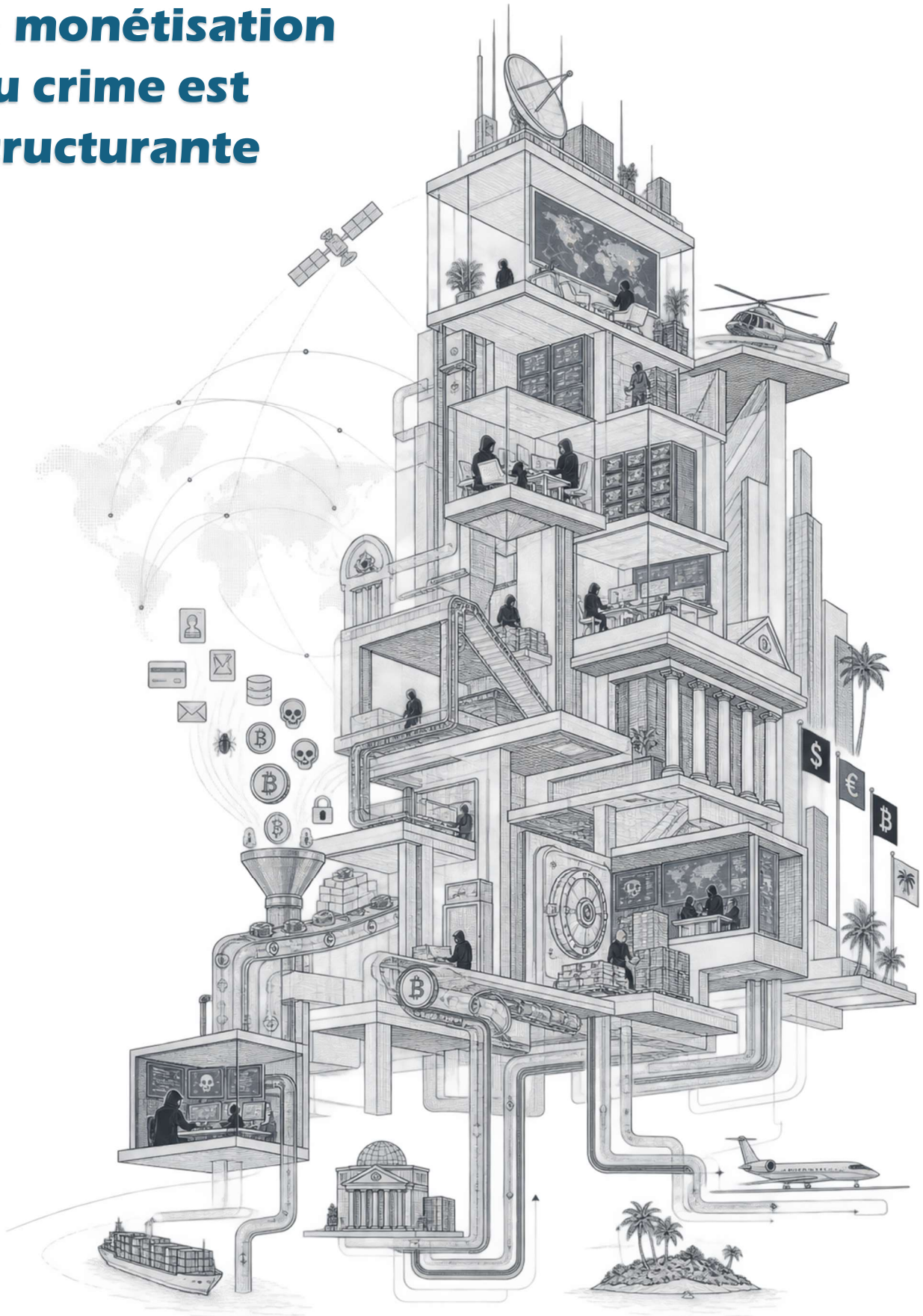
- Raisonner à dégrader le rendement de l'attaque plutôt qu'à la bloquer techniquement ;
- Identifier ce qui rend une organisation cible rentable aux yeux d'un attaquant rationnel ;
- Ne pas confondre silence et sécurité : les attaques les plus cruelles sont souvent celles qui ne se manifestent pas, nous vivons l'ère du « Low and slow ».

Au-delà de la simple logique de monétisation, l'écosystème cybercriminel obéit à des mécanismes économiques classiques de formation des prix, d'arbitrage des portefeuilles d'attaques et de recherche d'optimisation du rendement marginal.

La cybercriminalité ne se contente pas de générer des revenus, elle est un système économique.

Hervé RINDZUNSKI
CEO, Radical SSI

Poser le problème : la monétisation du crime est structurante



2 Poser le problème : la monétisation du crime est structurante

Les cybercriminels arbitrent entre effort, risque gain et liquidité

La cybercriminalité est souvent décrite à travers ses outils (phishing[1], rançongiciels[2], infostealers[3], botnets) ou ses victimes (hôpitaux, collectivités, grandes entreprises mais aussi individus insuffisamment préparés). Cette lecture, utile pour la réponse immédiate, occulte une réalité plus structurante : derrière la diversité des attaques, il y a toujours une logique de rendement.

L'attaquant, qu'il soit un adolescent opportuniste armé d'un kit acheté sur Telegram[4] ou un groupe criminel structuré opérant comme une franchise, est avant tout un acteur économique. Il arbitre en permanence entre trois variables :

- L'effort requis pour mener chaque phase de l'attaque ;
- Le risque encouru à chaque phase ;
- Le gain espéré.

C'est cet arbitrage, et non la sophistication technique, qui détermine le choix de la cible, du vecteur et du mode opératoire.

À ces trois variables s'ajoute implicitement une quatrième : la liquidité[5] du gain. Un modèle de monétisation peut être théoriquement rentable mais peu attractif s'il implique des délais longs, une incertitude sur la transaction ou une dépendance à un acheteur rare. Cette dimension explique en grande partie les choix tactiques observés en 2025.

Penser une nouvelle posture de défense selon la monétisation

Cette grille de lecture économique a une conséquence directe pour les défenseurs : une organisation qui raisonne uniquement en termes de blocage technique (pare-feu[6], détection, correctif, mitigation[7]) joue sur le terrain de l'attaquant.

A l'opposé, une organisation qui raisonne en termes de dégradation du rendement de l'attaque, c'est-à-dire qui vise à augmenter son coût ou réduire son gain change fondamentalement la nature du rapport de force.

L'allongement du délai constitue un levier défensif : ralentir l'attaquant, c'est augmenter son exposition et son coût. Mais ce levier a sa limite : les attaques dites « Low and Slow[8] » sont précisément conçues pour le neutraliser, en fragmentant l'activité malveillante sur des semaines ou des mois pour rester sous les seuils de détection.

Avant de décrire les menaces, leurs acteurs et leurs modes opératoires, il apparaît donc utile de dresser une taxonomie des modes de monétisation, car c'est la nature du gain espéré qui détermine, en dernière analyse, pourquoi une cible est choisie plutôt qu'une autre.

Cette taxonomie peut se lire selon un prisme transversal :

- Certains modes reposent sur une logique de capture : s'emparer de quelque chose qui a de la valeur (données, flux, ressources, accès) ;
- D'autres reposent sur une logique de destruction : détruire ou dégrader quelque chose dont la valeur réside dans son intégrité (réputation, confiance, continuité).

Les modes les plus sophistiqués combinent les deux.

Une taxonomie des attaques selon les modes de monétisation

3 Une taxonomie des attaques selon les modes de monétisation

3.1 La monétisation par la contrainte : l'extorsion directe

Le mode de monétisation le plus ancien, basé sur la menace

La monétisation contrainte est la forme la plus ancienne et la plus visible de cybercriminalité à but lucratif. Son principe est simple : l'attaquant crée une situation de dépendance ou de menace, puis exige un paiement pour y mettre fin.

C'est économiquement la moins efficiente des formes de monétisation : elle nécessite une interaction directe avec la victime, et d'établir un rapport de force qui génère des frictions considérables.

Ces modèles impliquent tous au minimum trois phases distinctes : l'attaque, la négociation et le paiement, avec un fort risque d'exposition durant la phase de négociation. C'est précisément cette friction inhérente à l'interaction contrainte avec la victime, qui pousse les acteurs les plus rationnels de l'écosystème criminel à migrer vers des formes de monétisation plus fluides.

La monétisation contrainte conserve néanmoins une efficacité opportuniste élevée dans certains contextes spécifiques : organisations fortement dépendantes à leur continuité opérationnelle, absence de sauvegardes exploitables, ou environnement réglementaire exposant fortement à une divulgation publique.

En particulier, l'inefficience structurelle de certaines des cibles peut permettre d'atteindre des rendements ponctuellement très élevés.

Les attaquants les plus structurés pratiquent ainsi une forme de qualification de la victime (une sorte de KYV, « Know Your Victim », par analogie au KYC des banques, « Know Your Customer ») : ils évaluent sa dépendance opérationnelle, sa capacité de restauration, son exposition réglementaire et sa probabilité de paiement avant de calibrer leur demande.

Quelques catégories de monétisation contrainte

Le rançongiciel classique	La menace de publication de données exfiltrées (double extorsion)
C'est l'archétype de la monétisation contrainte : les données ou systèmes de la victime sont chiffrés, rendant l'organisation incapable de fonctionner, et la clé de déchiffrement est monnayée. Le paiement est forcé, souvent en cryptomonnaie, et s'opère dans un contexte de pression temporelle maximale. Les autorités recommandent de ne pas payer (certaines juridictions commencent à l'interdire) ce qui érode mécaniquement le taux de conversion de ce modèle.	Elle reproduit la même structure que le rançongiciel classique mais sans chiffrement préalable : l'attaquant menace de diffuser des données sensibles si la rançon n'est pas versée. Les frictions sont identiques : victime sous contrainte, paiement visible, risque juridique. Le résultat est souvent similaire : une partie significative des victimes refuse de payer, quitte à subir la publication, ce qui tend à devenir l'attitude quasi unanimement conseillée face au rançongiciel classique également.

Le DDoS[9] rançonné	Le faux signalement réglementaire (variante émergente).
Ce mode obéit à la même logique sans exfiltration ni chiffrement : la menace d'interruption de service (ou juste la mise en œuvre durant un temps court servant d'avertissement) suffit. Ce modèle est particulièrement répandu contre les plateformes transactionnelles, les établissements financiers et les opérateurs de jeux en ligne, pour lesquels chaque minute d'indisponibilité a un coût direct et mesurable.	L'attaquant menace de dénoncer l'organisation aux autorités (CNIL, régulateurs sectoriels) pour une violation réelle ou fabriquée, en l'absence de paiement. La donnée n'est pas revendue ; c'est la menace de sanction institutionnelle qui est monétisée. Ce modèle est particulièrement efficace dans les secteurs fortement régulés, où le coût d'une procédure réglementaire, même infondée, peut dépasser celui de la demande d'extorsion.

3.2 La monétisation par revente volontaire : les marchés secondaires de données

Maintenant, on ne recherche plus le paiement auprès de la victime

À l'opposé de l'extorsion directe, la revente volontaire de données exfiltrées repose sur une transaction consentie entre vendeur et acheteur.

C'est structurellement un marché : il y a une offre, une demande, des prix, des intermédiaires et des mécanismes de confiance. C'est aussi, pour l'attaquant, un modèle bien plus fluide : le paiement est discret, définitif, et ne nécessite aucune interaction avec la victime.

La formation des prix sur ces marchés repose sur plusieurs facteurs déterminants : la fraîcheur des données (un accès valide aujourd'hui peut être obsolète demain), leur exclusivité (une base déjà diffusée perd vite de la valeur), leur exploitabilité directe (présence d'identifiants complets, absence de chiffrement) et leur potentiel de scalabilité (capacité à être utilisé massivement ou ciblé). Ces facteurs créent une forte volatilité des prix et incitent à une monétisation rapide.

La nature du bien vendu détermine le profil de l'acheteur, le prix et la liquidité de la transaction.

Quatre catégories de monétisation par revente volontaire de données exfiltrées

Les données nominatives et comportementales :	Les correspondances et messageries :
Noms, adresses, numéros de téléphone, IBAN, données de santé, historiques d'achat, données de profilage : ces bases alimentent des opérations de fraude secondaire, de phishing ciblé ou de re-victimisation. C'est le segment le plus liquide : les acheteurs sont nombreux, les prix unitaires faibles mais les volumes considérables. Ces bases sont désormais si abondantes que leur valeur unitaire s'érode : on peut anticiper à court terme l'émergence de revendications de violations mensongères, des attaquants cherchant à monétiser des données qu'ils ne possèdent pas réellement, tout comme une saturation du marché par une offre surabondante (ce qui pourra être un mécanisme de stabilisation).	Emails, messageries internes, comptes-rendus de réunions : ces données intéressent des acheteurs aux motivations très différentes : • Concurrents cherchant un avantage commercial ; • Adversaires cherchant des éléments compromettants ; • Presse d'investigation ; • Services de renseignement étrangers. Les trois premiers peuvent conclure des transactions discrètes et définitives ; les États paient rarement directement mais disposent d'intermédiaires. C'est un marché de gré à gré, peu liquide mais à prix élevés sur les cibles de valeur.

La propriété intellectuelle et les secrets industriels	Les données d'accès et d'infrastructure
Brevets non déposés, formules, code source, roadmaps R&D, résultats d'essais cliniques. L'acheteur est ici un concurrent direct ou un acteur étatique cherchant à combler un retard technologique. C'est le segment le moins liquide, les acheteurs potentiels sont rares et identifiables, parfois même à l'origine de la violation. C'est aussi celui où les prix unitaires sont sans commune mesure avec les autres catégories. La transaction est souvent longue à conclure et nécessite des intermédiaires spécialisés.	Credentials[10], clés API[11], certificats, accès VPN, sessions actives. Ces données ne sont pas revendues à des utilisateurs finaux mais à d'autres attaquants, via des Initial Access Brokers[12] (IAB). C'est le segment le plus mature et le plus organisé : les IAB sont des acteurs spécialisés qui évaluent, certifient et revendent des accès à des organisations compromises, souvent avec des garanties de validité. La liquidité est maximale : un accès à une grande entreprise se vend en quelques heures sur les forums spécialisés.

Ces marchés sont caractérisés par une asymétrie d'information structurelle : le vendeur connaît la qualité réelle du bien, l'acheteur ne peut souvent en vérifier qu'un échantillon. Cela explique l'émergence de mécanismes de réputation et d'intermédiation qui jouent un rôle équivalent à des agences de confiance dans les marchés légaux, au travers de places de marché et de tiers de confiance.

Un marché mature avec même un mécanisme stabilisateur : l'escrow[13]

Dans toutes ces transactions volontaires, le recours à un tiers de séquestre (escrow) est fréquent. L'acheteur dépose les fonds auprès d'un intermédiaire de confiance, qui les libère au vendeur une fois la livraison des données vérifiée. Ce mécanisme, directement inspiré du commerce légal en ligne, réduit le risque de défaut de paiement et contribue à professionnaliser et donc à fluidifier ce marché. Son existence est un indicateur de maturité : on ne construit des mécanismes de confiance que dans des marchés qui ont vocation à durer.

Ces marchés secondaires ont une propriété économique particulièrement défavorable aux victimes : la donnée vendue ne disparaît pas de la circulation après la première transaction. Elle peut être revendue, enrichie par croisement avec d'autres bases, puis revendue à nouveau.

La re-victimisation : la première exploitation peut être suivie d'autres

Une organisation victime d'une exfiltration n'est pas exposée une seule fois mais potentiellement de manière récurrente, à mesure que ses données circulent et s'agrègent dans l'écosystème. C'est le mécanisme de re-victimisation : la première attaque ne clôt pas l'exposition, elle l'ouvre.

Et, pour l'entreprise dont les fichiers ont été dérobés, l'effet « bad buzz » peut persister longtemps, surtout si l'origine de la fuite est aisée à deviner par les victimes ou leurs conseils. Cette persistance de la donnée volée sera traitée en détail dans le chapitre suivant.

3.3 La monétisation par détournement de flux financiers

S'introduire dans un système financier pour en modifier des paramètres

Ce mode de monétisation se distingue fondamentalement des précédents : la donnée n'est pas revendue, elle est utilisée comme outil pour intercepter ou rediriger des flux financiers légitimes. L'attaquant n'a pas besoin de créer un marché secondaire, il détourne à son profit un circuit existant, vers un ou des comptes aisément créables en ligne.

Les exemples ci-dessous exploitent tous la confiance que les organisations placent dans leurs propres processus. La donnée volée n'est pas une fin, c'est une clé qui ouvre un circuit financier légitime. C'est ce qui les rend particulièrement difficiles à détecter et à prévenir par des moyens purement techniques.

Ces modèles présentent une caractéristique économique déterminante : ils suppriment totalement la phase de marché. Le gain est capturé directement, sans dépendance à un acheteur, ce qui réduit fortement l'incertitude et explique leur attractivité croissante, notamment pour des acteurs intermédiaires disposant d'un accès mais pas d'une capacité à opérer sur des marchés criminels complexes.

La fraude au virement / Business Email Compromise (BEC[14])

L'attaquant compromet ou usurpe une messagerie professionnelle pour se substituer à un fournisseur, un dirigeant ou un partenaire dans une transaction en cours. Il modifie les coordonnées bancaires au dernier moment, et demande à ce que le paiement légitime soit dirigé vers un compte qu'il contrôle. La sophistication de cette attaque réside dans son invisibilité : aucun système n'est chiffré, aucune donnée n'est publiée, la victime a volontairement exécuté le virement. La détection est souvent tardive, le recouvrement rare.

La manipulation de référentiels de paiement

Variante plus silencieuse encore : l'attaquant accède aux systèmes comptables ou aux bases fournisseurs d'une organisation et modifie des IBAN dans les fiches tiers. C'est généralement l'œuvre d'un insider[15] ou d'un attaquant ayant acheté des données d'accès à un IAB, mais ce peut être aussi directement celle d'un attaquant de plus haut niveau. Le détournement des transactions est alors assez long à détecter. C'est une attaque particulièrement adaptée aux grandes organisations dont les processus de validation sont morcelés entre plusieurs équipes.

Le délit d'initié par exfiltration

L'attaquant accède à des informations financières non publiques — résultats trimestriels avant publication, opérations de fusion-acquisition en cours, décisions réglementaires anticipées — et les exploite sur les marchés financiers. La donnée n'est pas revendue ; elle est consommée. Ce mode est structurellement différent des précédents car l'attaquant est souvent son propre client final, ou agit pour le compte d'un commanditaire très ciblé. La traçabilité des flux financiers qui en résulte le rend théoriquement plus exposé — ce qui explique qu'il reste moins fréquent mais à très haute valeur unitaire.

Une variante : le sim swapping[16], les attaques sur les cartes SIM

Le sim swapping illustre une variante immédiate de ce détournement : en convainquant un opérateur téléphonique de transférer le numéro de la victime vers une carte SIM qu'il contrôle, l'attaquant intercepte les SMS d'authentification et vide directement les comptes bancaires ou les wallets[17] de cryptomonnaies associés. Aucune négociation, aucune revente : la monétisation est instantanée et définitive. C'est techniquement un vecteur d'ingénierie sociale, mais sa finalité économique l'inscrit pleinement dans la logique du détournement de flux.

3.4 La monétisation par exploitation de ressources : cryptomining[18] et botnets[19] locatifs

Faire travailler silencieusement des milliers de victimes à son avantage

L'exploitation de ressources est le mode de monétisation le plus discret de tous, et il est souvent sous-estimé. L'attaquant n'y vole pas de données, ne chiffre pas de systèmes, ne menace pas sa victime. Avec l'aide d'un malware[20], il s'approprie silencieusement une ressource : la puissance de calcul et la capacité réseau de l'organisation compromise. Les victimes ne sont alors qu'un moyen, pas une cible.

Cette appropriation de la puissance de calcul est silencieuse : elle survient lorsque son propriétaire légitime télécharge un logiciel corrompu ou spécifique, un malware, souvent à l'occasion d'une recherche sans aucun rapport sur le web. Une bonne illustration : un internaute cherche un petit outil pour effectuer une tâche qui lui paraît secondaire mais nécessaire à cet instant, comme fusionner deux fichiers pdf, ou extraire la bande son d'une vidéo. L'outil qu'il va télécharger effectue bien la fonction demandée, mais installe en même temps un autre logiciel qui va fonctionner de manière silencieuse.

Le malware étant déployé des milliers de fois, au gré des téléchargement volontaires par des utilisateurs bernés mais consentants, ces réseaux atteignent couramment des dizaines de milliers de postes.

Ces modes partagent une même structure économique : aucune interaction avec la victime, aucune négociation, aucune revente de données. Ils partagent aussi une même implication défensive : une organisation qui ne détecte aucune exfiltration et ne reçoit aucune demande de rançon n'est pas nécessairement saine. Elle peut être silencieusement exploitée.

Monétiser les ressources des victimes

L'émergence de ces modèles s'inscrit dans une logique de maximisation du rendement marginal[21] : une infrastructure compromise peut générer un revenu continu avec un coût opérationnel quasi nul. L'automatisation croissante des déploiements de malwares et l'orchestration centralisée des botnets accentuent encore cette dynamique.

Ces modèles présentent enfin une propriété stratégique importante : ils sont facilement abandonnables, même sachant que leur ROI est en général faramineux. Lorsque l'infrastructure compromise est détectée ou nettoyée, l'attaquant perd une source de revenu mais non son modèle économique. Il peut simplement déplacer l'exploitation vers d'autres ressources compromises.

Quelque cas d'usage d'un botnet

Le cryptomining	Le botnet locatif
Les machines compromises des victimes minent de la cryptomonnaie au profit de l'attaquant, qui en tire un gain direct et continu. Le programme de minage va consommer 15 à 20% de la puissance de calcul, et enverra directement ses résultats à l'attaquant. Repérable sur des réseaux d'entreprise, cette attaque est quasi indétectable sur un ordinateur personnel	Les machines compromises sont agrégées en un réseau loué à des tiers pour du spam, des attaques DDoS à la demande ou du credential stuffing[22]. Le bien vendu n'est pas une donnée mais une capacité. Ce marché est mature, tarifé et organisé : on loue un botnet comme on loue une infrastructure cloud, certains agrégeant plusieurs dizaines de milliers d'ordinateurs.

Les botnets : comment gagner de l'argent avec de faux humains :

La fraude à la publicité numérique	Les opérations d'influence ou de désinformation
Les botnets locatifs sont aussi massivement utilisés pour générer des clics ou des impressions publicitaires frauduleuses, facturées à des annonceurs légitimes. Ce marché représente plusieurs milliards de dollars annuels et constitue l'une des formes de	Un message souvent faux ou décontextualisé est injecté dans l'écosystème informationnel (X, TikTok, Instagram, etc.). Des milliers de comptes du botnet, pilotés par de vraies personnes dans des « fermes de contenu », vont alors le liker et le commenter pour le propulser artificiellement en

monétisation les plus discrètes et les plus stables de l'écosystème criminel. La victime dont les machines sont détournées n'en sait rien ; l'annonceur paie sans savoir qu'il rétribue un botnet ; seule la plateforme publicitaire intermédiaire pourrait détecter l'anomalie.	tendance. Les algorithmes des plateformes font le reste : ce qui semble viral devient viral. L'opinion suit le bruit, pas l'inverse. Un botnet d'influence ne cherche pas à convaincre, il cherche à saturer. Ces opérations sont commanditées et donc rémunérées.

La détection des botnets reste insuffisante, notamment parce que les intérêts économiques de modération des plateformes, des intermédiaires publicitaires et des annonceurs ne sont pas toujours parfaitement alignés.

3.5 La monétisation différée : persistance et valeur stratégique

S'introduire dans un réseau, s'y maintenir : un sport d'acteurs de haut niveau

Ce mode de monétisation est le plus patient de tous. L'attaquant ne cherche pas un gain immédiat mais profite d'une position qu'il a investie, et dont la valeur se réalisera plus tard. C'est une logique de capital, pas de revenu, basée sur une diminution du risque : l'attaquant vendeur restera discret et ne sera pas l'attaquant exploitant, qui lui risquera plus d'être repéré.

Ce modèle introduit aussi une logique de portefeuille : l'attaquant ne cherche pas uniquement un gain immédiat mais diversifie ses actifs (accès, données, positions persistantes) pour optimiser son rendement global dans le temps.

La monétisation est complexe : il n'est pas question de donner une publicité visible à des introductions dans des serveurs d'entreprise. Les places de marché dédiées sont confidentielles et la transaction est plus souvent initiée par une demande de service émise par un acteur financier ou étatique.

Comment exploiter l'introduction dans un réseau

La persistance vendue	L'espionnage stratégique à retour différé
L'attaquant ayant réussi à s'introduire dans un réseau d'entreprise y maintient discrètement un accès dans le temps et le revend à un tiers. La valeur réside dans la durée et la profondeur de l'accès : c'est un actif qui se déprécie lentement tant qu'il n'est pas détecté, qui peut se revendre plusieurs fois, mais qui peut disparaître soudainement.	L'exfiltration ne se monétise pas directement mais constitue un avantage dont le retour est géopolitique ou concurrentiel sans qu'il n'y ait toujours de « paiement » financier. C'est le mode privilégié des acteurs étatiques, mais aussi de certains grands groupes industriels pour lesquels l'avantage informationnel vaut plus que n'importe quelle transaction.

3.6 La monétisation par destruction ou capture de valeurs symboliques

S'attaquer aux valeurs symboliques capitalisables comme la réputation

Les modes précédents opèrent tous sur l'usage, le détournement, la vente ou la location de biens tangibles ou de flux mesurables.

Il existe une autre catégorie, structurellement différente : les valeurs symboliques capitalisables, c'est-à-dire des actifs immatériels dont la valeur économique est réelle mais indirecte, comme la confiance ou la réputation.

Dans certains secteurs, la réputation n'est pas seulement un actif : elle est la condition d'existence du modèle économique. Si on ne peut pas acheter la réputation d'une organisation sur un marché criminel, il est assez simple de revendre sa destruction… Cette destruction produit des effets économiques immédiats et durables : perte de clients, de donateurs, de partenaires, de licences réglementaires.

Ces valeurs symboliques capitalisables (confiance, réputation, etc.) sont particulièrement concentrées dans certains secteurs : plateformes de confiance, organisations caritatives, institutions de santé, acteurs financiers grand public. Pour ces organisations, la réputation n'est pas un actif parmi d'autres, c'est le fondement de leur modèle économique, et l'essentiel de leur valeur. Une attaque qui les prive de la confiance de leurs utilisateurs peut être plus dévastatrice qu'une exfiltration de données ou qu'un rançongiciel.

Comment s'attaquer aux valeurs symboliques : quelques exemples

La destruction commanditée de réputation
Un concurrent, un adversaire politique ou un acteur hostile paie pour qu'une attaque nuise à la réputation d'une organisation. Ce n'est pas de l'extorsion puisque la victime ne reçoit aucune demande. C'est du sabotage marchand : l'attaquant est un prestataire, le commanditaire est le bénéficiaire, et la victime n'a aucun interlocuteur à qui céder. C'est le mode le plus difficile à détecter et à attribuer, précisément parce qu'il ne génère aucun contact avec la victime.

La capture de réputation
L'attaquant usurpe l'identité d'une marque de confiance pour conduire des opérations frauduleuses en son nom : faux sites de collecte reproduisant l'interface d'une plateforme connue, faux emails de campagne au nom d'une ONG reconnue, fausses pages de dons exploitant la notoriété d'une institution. La valeur n'est pas détruite, elle est volée et retournée contre ses détenteurs et leurs publics. La victime subit une double perte : elle finance involontairement la fraude par sa réputation, et elle en supporte ensuite les conséquences en termes de confiance. C'est un mécanisme de « piggyback[23] économique » : l'attaquant s'appuie sur un capital de confiance existant pour réduire son coût d'acquisition.

La menace d'extorsion narrative
Distincte de la capture de réputation, et finalement proche de la monétisation par la contrainte et de l'extorsion directe, l'extorsion narrative repose sur la menace de construire ou d'amplifier un récit négatif, réel ou fictif. Ce mode reste émergent et encore difficile à distinguer de certaines formes d'influence ou de manipulation informationnelle. L'attaquant ne détient pas nécessairement de données compromettantes : il menace de fabriquer un scandale, de coordonner une campagne de dénigrement, ou de diffuser des éléments sortis de leur contexte. Le levier n'est pas la donnée, c'est la narration. Ce mode est particulièrement efficace contre les organisations dont la légitimité repose sur la

La contamination d'écosystème
Ce mode est principalement observé dans des logiques étatiques ou hybrides, mais peut être exploité (très rarement et indirectement) par des acteurs criminels. Là, l'attaque ne vise pas une organisation mais la confiance dans une catégorie entière. Compromettre une plateforme de collecte de fonds ne nuit pas seulement à cette plateforme mais peut fragiliser la confiance dans toutes les plateformes similaires. Ce mode est particulièrement recherché par les acteurs étatiques cherchant à déstabiliser des secteurs entiers, ou par des acteurs criminels cherchant à créer un vide de confiance qu'ils pourront occuper avec des alternatives frauduleuses.

confiance publique : associations, fondations, institutions culturelles ou de santé.	Les régulations ambitieuses comme DORA[24] ou NIS2[25] essayent aussi de les combattre.

Les spécificités des valeurs symboliques, et la difficulté à les défendre

Ces modes peuvent être analysés selon trois logiques économiques :

- Génération directe de revenus ;
- Transfert de valeur vers un tiers (dans les cas de sabotage commandité) ;
- Création d'un avantage compétitif indirect (déstabilisation d'un acteur ou d'un marché).

Quatre caractéristiques les différencient fondamentalement des modes précédents :

- L'attaquant n'a pas besoin de données pour nuire : la destruction de valeur symbolique peut être opérée sans aucune exfiltration, ce qui rend les défenses techniques classiques largement inopérantes ;
- Les effets sont durables et difficilement réversibles. Une réputation se construit en années et se détruit en heures. La restauration est lente, coûteuse et incertaine ;
- La victime peut être à la fois cible et vecteur : dans la capture de réputation notamment, c'est la notoriété de la victime qui est utilisée comme arme contre ses propres utilisateurs ;
- L'effet de levier est élevé : une attaque limitée peut produire des pertes économiques disproportionnées via la perte de confiance.

Face à ces modes, la défense technique est bien sûr nécessaire mais totalement insuffisante. Elle doit être complétée par une veille narrative, par la surveillance des usurpations d'identité, des campagnes de dénigrement, des faux sites, et par une capacité de réponse publique rapide, qui est une compétence organisationnelle distincte de la cybersécurité technique.

Il s'agit d'un changement de périmètre : la cybersécurité ne doit plus se contenter de protéger les systèmes, mais aussi de maintenir les conditions de la confiance. Les organisations les plus exposées seront celles qui n'ont pas intégré la gestion de crise réputationnelle dans leur plan de réponse aux incidents cyber.

3.7 Au-delà de la monétisation : les attaques à finalité stratégique

La stratégie, un domaine réservé aux grosses organisations et aux états

La grille économique développée dans ce chapitre permet d'analyser la grande majorité des attaques cyber observées. Elle a cependant ses limites, et l'honnêteté analytique impose de les nommer.

Tous les attaquants ne cherchent pas à monétiser. Certaines attaques obéissent à une logique stratégique, géopolitique ou idéologique dans laquelle le gain financier est absent, secondaire, ou simplement un moyen au service d'une finalité autre. Les traiter dans ce cadre serait forcer une grille sur des réalités qui n'y entrent pas.

Des exemples d'attaques à finalité stratégique

Quelques configurations méritent d'être mentionnées ici, sans être développées[26].

L'infiltration par faux employés	**Les attaques commanditées à finalité géopolitique**
Des acteurs étatiques, la Corée du Nord étant le cas le plus documenté, placent des ressortissants sous une fausse identité comme salariés à distance dans des entreprises étrangères. Le	Un État mandate un groupe criminel pour conduire une opération dont l'objectif est politique : déstabilisation, renseignement, ou sabotage. Le groupe peut en tirer un bénéfice

salaire perçu finance directement l'État commanditaire ; l'accès obtenu sert des objectifs de renseignement ou de sabotage à long terme. C'est un modèle hybride où la monétisation existe, certes, mais en étant une couverture et non la finalité.	criminel secondaire, mais la logique de l'opération n'est pas économique. L'ambiguïté entre criminalité organisée et opération étatique est ici délibérée : elle complique l'attribution et dilue la responsabilité.

La perturbation de marché comme arme	Le sabotage d'infrastructure
Certaines attaques visent non pas à extraire une valeur mais à détruire ou dégrader la capacité d'un acteur économique ou d'un secteur entier, au bénéfice indirect d'un concurrent ou d'un État adverse. La monétisation est exogène à l'attaque : elle se réalise dans l'économie réelle, pas dans l'écosystème criminel.	L'exemple le plus emblématique reste Stuxnet, arme logicielle conçue conjointement par les États-Unis et Israël pour détruire physiquement les centrifugeuses du programme nucléaire iranien. Aucune donnée exfiltrée, aucune rançon, aucun marché secondaire : la destruction était la finalité. Stuxnet a établi qu'une attaque cyber pouvait produire des effets cinétiques réels, franchissant une frontière que l'écosystème criminel n'a ni les moyens ni les raisons de franchir, mais que les acteurs étatiques ont désormais intégrée dans leur arsenal.

Les attaques à finalité stratégique ont bien tous les marqueurs de la stratégie

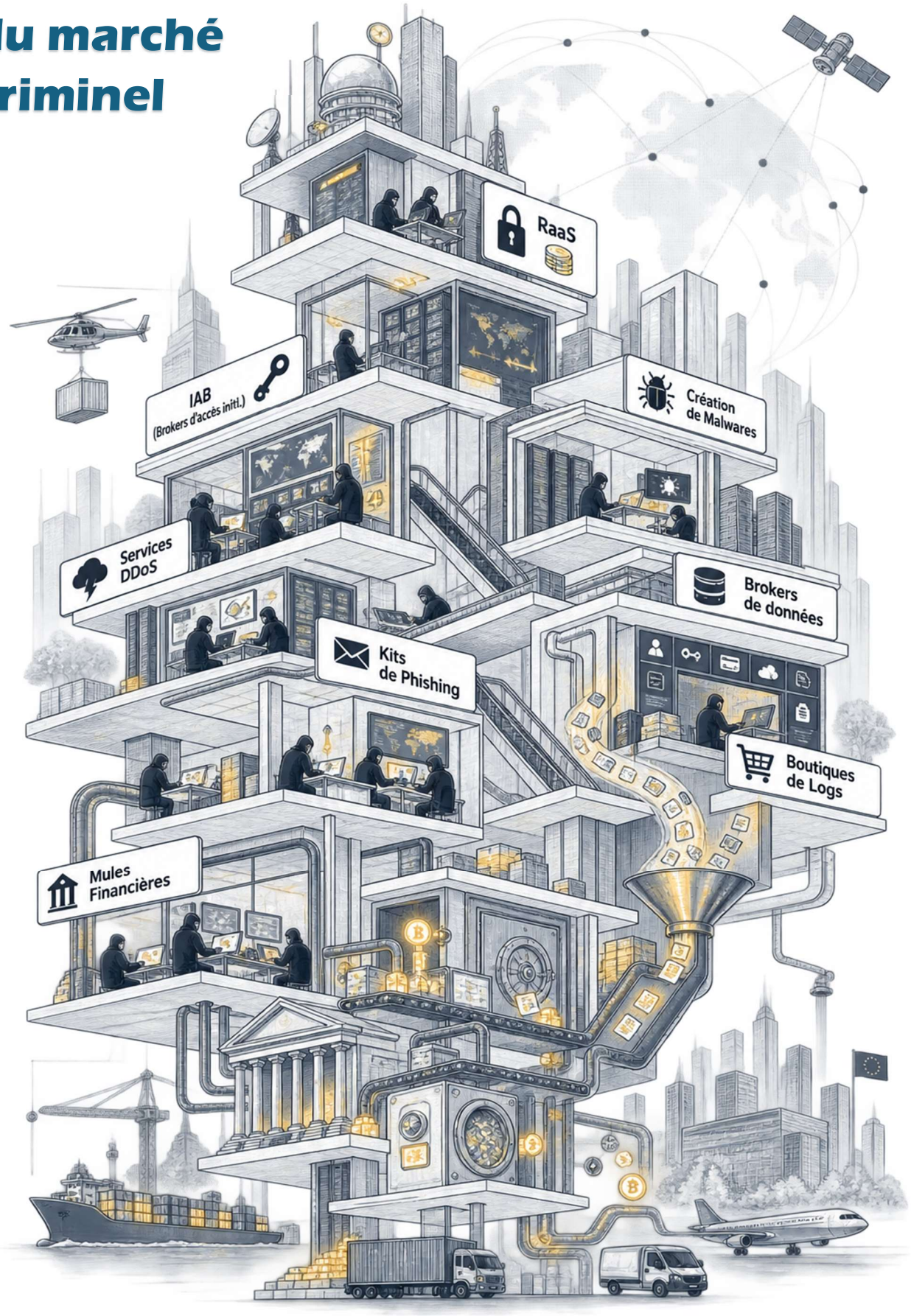
Ces configurations partagent plusieurs propriétés communes qui les rendent particulièrement difficiles à appréhender avec les outils défensifs classiques :

- La patience : le rendement n'est pas immédiat, ces modèles supposent un horizon temporel long et une capacité à différer la réalisation de la valeur.
- La dissimulation comme condition d'efficacité : contrairement au rançongiciel ou à l'extorsion, ces modèles perdent leur valeur s'ils sont détectés tôt. L'invisibilité n'est pas un avantage opérationnel, c'est une condition structurelle.
- La multiplicité des bénéficiaires : dans chacun de ces modèles, la valeur produite par l'attaque est capturée par plusieurs acteurs simultanément : commanditaire, exécutant, bénéficiaire indirect. Cette dispersion rend l'attribution et la réponse juridique particulièrement complexes.
- L'inadéquation des défenses classiques : ces modèles contournent ou neutralisent les défenses techniques périmétriques. Ils appellent des réponses organisationnelles, humaines et de renseignement que la cybersécurité technique seule ne peut pas fournir.

Surtout, elles n'ont pas de signal de monétisation détectable : pas de négociation, pas de marché secondaire, pas de demande de rançon.

C'est précisément ce silence qui les rend dangereuses et qui justifie qu'elles soient traitées séparément, avec les outils analytiques adaptés à leur nature réelle.

La structure du marché criminel



4 La structure du marché criminel

Les modes de monétisation décrits dans la section précédente ne fonctionnent pas isolément. Ils s'articulent en un écosystème structuré, avec une division du travail, des marchés différenciés et des mécanismes de régulation informels. Cet écosystème a achevé, en 2025, sa transformation en secteur industriel mature.

4.1 La professionnalisation et la division du travail

Une organisation professionnelle digne de l'industrie

La cybercriminalité organisée ne ressemble plus à l'image du hacker solitaire. Elle s'est fragmentée en rôles spécialisés et interdépendants :

- Les Initial Access Brokers (IAB) se spécialisent dans la pénétration initiale des réseaux et la revente des accès obtenus, sans les exploiter eux-mêmes.
- Les « ingénieurs de détournement » achètent un accès auprès d'un IAB et se spécialisent dans son exploitation technique : latéralisation dans le réseau, escalade de privilèges, exfiltration de bases de données. Ils sont le chaînon entre l'accès brut vendu par l'IAB et le bien monnayable, qu'il soit credentials enrichis, données exfiltrées, accès approfondi revendu à prix supérieur. C'est un rôle de prestation de service pure : l'ingénieur de détournement n'est pas propriétaire de l'attaque, il n'en est que le sous-traitant technique.
- Les développeurs conçoivent les outils (malwares, kits d'exploitation, infostealers, etc.) qu'ils vendent ou louent à d'autres acteurs. Ces outils, grâce entre autres à l'IA, gagnent en 2025 une nouvelle puissance : ils combinent de plus en plus souvent plusieurs mécanismes d'attaque comme kit de phishing + infostealer, ou infostealer + dropper[27] installant silencieusement un accès persistant, ou encore deepfake[28] vocal couplé à un BEC pour valider oralement un virement déjà initié par email frauduleux.
- Les blanchisseurs assurent la conversion et le transfert des gains, souvent via des chaînes de cryptomonnaies ou des mules financières.
- Les opérateurs RaaS[29] (Ransomware-as-a-Service) fournissent une infrastructure clé en main : en plus de fournir le logiciel et ses services (hébergement, paramétrage, support technique multilingue), ils fournissent les plateformes de négociation, d'encaissement et de transfert financier à des affiliés qui conduisent les attaques.
- Les affiliés louent ces infrastructures et conduisent les campagnes, sans nécessairement maîtriser les aspects techniques. On trouve là des dizaines de rôles spécialisés : phishers[30], scammeurs[31] [32], alloteurs[33], cashers[34], rédacteurs de leurres, testeurs de credentials, etc. qui constituent dans ce monde professionnel une base d'acteurs de petit niveau, mais très étendue.
- Les places de marché comme BreachForums[35] et ses équivalents constituent l'infrastructure commerciale de cet écosystème. Structurées comme des marketplaces e-commerce, elles proposent annonces tarifées, systèmes de réputation des vendeurs, modération des litiges et services d'escrow intégrés. Leurs administrateurs sont à la fois hébergeurs, modérateurs et percepteurs de commissions — un modèle économique parfaitement calqué sur celui des plateformes légales.

Une écologie criminelle : spécialisation, résilience, régénération

Cette division du travail a une conséquence directe : elle abaisse drastiquement le niveau de compétence requis pour mener une attaque sophistiquée, tout en diluant la responsabilité pénale entre de nombreux acteurs difficiles à relier.

Cette structuration est renforcée par un phénomène de plateformisation : des infrastructures techniques comme des forums, des messageries, des canaux privés et chiffrés jouent un rôle équivalent à celui de plateformes numériques légales, assurant acquisition de clients, support, gestion de réputation et résolution de litiges. Certains écosystèmes criminels fonctionnent ainsi comme de véritables SaaS[36] clandestins.

Cette structure a une seconde conséquence, souvent sous-estimée par les défenseurs : elle rend l'écosystème criminel remarquablement résilient aux démantèlements. Quand LockBit[37] est neutralisé, quand BreachForums est saisi, quand un groupe disparaît à la suite de dissensions internes, les rôles survivent aux individus : la nature a horreur du vide. Les développeurs migrent vers de nouvelles franchises, les affiliés se redistribuent, les places de marché se reconstituent sous de nouveaux noms. Démanteler un acteur ne détruit pas le marché : cela crée au plus une perturbation temporaire, parfois même une opportunité pour les concurrents.

4.2 Le financement de l'écosystème criminel

Un financement lui aussi industrialisé, multi étages

Pour être complet, il faut parler du financement de ce secteur et des investissements qui y sont consentis. Les outils, les infrastructures, les premières opérations ont un coût qui peut même parfois être significatif pour les opérations de haut niveau. Une partie de ce financement peut provenir de réinvestissements de gains antérieurs, mais une autre provient d'investisseurs criminels cherchant un retour sur investissement : commanditaires étatiques dotant des groupes affiliés, organisations criminelles traditionnelles diversifiant leurs activités vers le cyber, ou simplement acteurs fortunés de l'écosystème finançant de nouvelles franchises.

L'écosystème criminel dispose ainsi de mécanismes d'investissement et de réinvestissement qui rappellent, par certains aspects, le financement de l'innovation légale, ce qui explique en partie sa capacité à se reconstituer rapidement après démantèlement.

Des cols blancs mais aussi des liens avec les pires organisations criminelles

Enfin, une dimension plus sombre encore de ce financement mérite d'être mentionnée : le recours à la traite humaine comme mode d'approvisionnement en compétences techniques. Cette réalité est particulièrement documentée dans certains écosystèmes de fraude en ligne et d'escroquerie numérique, où des travailleurs recrutés sous contrainte produisent scripts, contenus, interfaces ou infrastructures opérationnelles.

Même si ce recours est plus présent dans les écosystèmes de scams, fraude en ligne, pig butchering[38], etc., des développeurs, recrutés sous de fausses promesses d'emploi ou directement enlevés, sont retenus dans des « fermes de développement » localisées dans des zones où l'État de droit est défaillant. Ils produisent sous contrainte les outils et infrastructures qui alimentent l'écosystème criminel mondial. C'est la face la plus violente d'un système qui, par ailleurs, se présente volontiers sous les traits rassurants d'une économie de marché organisée.

4.3 La liquidité différentielle des marchés

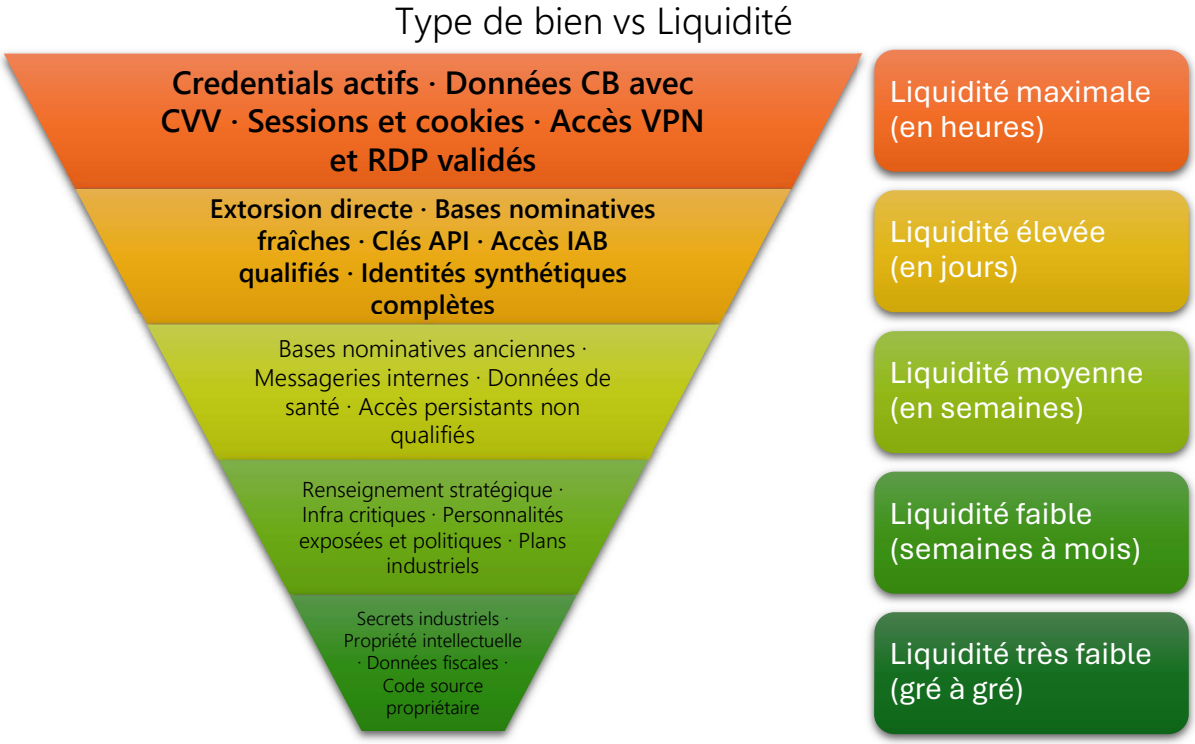
La liquidité comme choix principal

Tous les biens issus de la cybercriminalité ne se vendent pas avec la même facilité. On peut distinguer un gradient de liquidité.

À un extrême, les credentials et accès se vendent en quelques heures sur des forums spécialisés. C'est le marché le plus liquide, avec des prix standardisés et une demande permanente. Comme les données périment assez vite, les prix sont marqués par une forte tendance baissière, ce qui pousse les attaquants à automatiser massivement la collecte pour compenser la dépréciation unitaire. On a là un cercle auto-entretenu qui tire les prix vers le bas tout en élargissant le périmètre des attaques. Par contrecoup, des acteurs de plus en plus débutants peuvent mener des campagnes à périmètre de plus en plus large.

À l'autre extrême, les secrets industriels et la propriété intellectuelle nécessitent des semaines de négociation avec un acheteur rare et qui apporte un risque d'être identifié. C'est le marché le moins liquide, mais à valeur unitaire sans commune mesure. La période de risque pour l'attaquant primaire est limitée à la phase de négociation.

Entre les deux, les données nominatives, identifiants de carte de crédit ou documents d'identité constituent un marché de volume à prix largement décroissants, tandis que les correspondances et messageries forment un marché de gré à gré dont la valeur dépend entièrement de la cible.



La fraîcheur, l'exclusivité et l'exploitabilité directe peuvent faire monter un bien d'un niveau à l'autre.

Cette liquidité n'est pas uniquement fonction de la nature du bien, mais aussi de la profondeur du marché, du nombre d'acheteurs actifs et de la standardisation des produits. Plus un bien est standardisé, plus il devient liquide, mais aussi plus sa valeur unitaire tend à diminuer sous l'effet de la concurrence…

La liquidité comme choix pour une majorité d'attaquants

Cette liquidité différentielle explique les choix tactiques des attaquants : un groupe cherchant un gain rapide ciblera des credentials ; un groupe patient et bien équipé investira dans l'exfiltration de propriété intellectuelle. Mais pas uniquement : leur spécialisation les cantonne souvent à un ou deux segments de marché. Cette spécialisation constitue, pour les défenseurs, un levier de threat intelligence[39] encore sous-exploité : le type de données ciblées est souvent une signature du groupe attaquant.

La liquidité segmente les types d'attaques que peut subir une victime

Cette grille de liquidité a un corollaire du côté des victimes : toutes les organisations ne présentent pas le même profil d'attractivité selon les segments de marché :

- Une PME industrielle sera plus exposée au vol de propriété intellectuelle commandité par un concurrent qu'à une opération RaaS sophistiquée ;
- Une plateforme transactionnelle grand public sera prioritairement ciblée pour ses bases de credentials et ses flux financiers ;
- Un établissement de santé cumulera l'attractivité des données nominatives sensibles et la vulnérabilité opérationnelle qui rend le rançongiciel efficace.

Cette asymétrie entre profil d'attractivité et perception interne du risque est l'un des angles morts les plus fréquents dans les stratégies de défense.

4.4 La liquidité spécifique des attaques supply chain[40]

Les attaques supply chain occupent une place à part dans ce gradient : elles sont l'œuvre de techniciens de haute valeur, qui mûrissent et étudient leur projet. Elles ne ciblent pas un bien précis mais ouvrent un périmètre. En compromettant un fournisseur commun à de nombreuses organisations (que ce soit un composant logiciel, un prestataire d'infogérance, une brique d'authentification) l'attaquant jette un filet sans connaître à l'avance exactement ce qu'il va trouver.

C'est une logique d'investissement avec risque de perte en capital, mais aussi comparable à une pêche merveilleuse : le coût d'entrée est fixe, souvent quand même réduit, et le rendement potentiel est démultiplié. Elles peuvent être analysées comme un modèle d'investissement à fort effet de levier : un coût d'entrée unique permet d'accéder à un portefeuille de cibles, avec un rendement incertain mais potentiellement très élevé.

L'asymétrie explique l'attractivité croissante de ce vecteur pour les groupes disposant des compétences techniques élevées nécessaires.

4.5 La convergence vers l'exfiltration comme choix rationnel

Ces deux éléments, professionnalisation et liquidité différentielle, permettent de comprendre le pivot structurel décrit en introduction : le glissement du rançongiciel classique vers l'exfiltration pure n'est pas une mode, c'est un choix rationnel d'optimisation économique.

Ce mouvement ne correspond pas à une substitution complète mais à une hybridation des modèles. De nombreuses opérations combinent désormais exfiltration, chiffrement et pression informationnelle, cherchant à maximiser les leviers de monétisation plutôt qu'à en privilégier un seul. L'évolution observée est donc moins un pivot qu'une convergence.

L'exfiltration réduit le nombre de phases de l'attaque, supprime la friction de la négociation contrainte, ouvre un marché secondaire fluide et discret, et dilue le risque entre des acteurs spécialisés.

Face à un rançongiciel dont le taux de conversion s'érode sous la pression réglementaire et la résistance croissante des victimes, l'exfiltration offre un rendement ajusté au risque structurellement supérieur.

À cela s'ajoute un avantage structurel décisif : l'irréversibilité. Une victime de rançongiciel qui restaure ses sauvegardes reprend partiellement la main. Une victime d'exfiltration ne récupère jamais ses données : elles existent désormais hors de son contrôle, indéfiniment. Ce caractère irréversible renforce le levier de l'attaquant même en l'absence de paiement.

Un facteur structurant supplémentaire est la baisse continue du coût marginal de l'attaque, sous l'effet de l'automatisation et de l'IA. L'IA n'invente pas nécessairement de nouveaux modèles économiques criminels ; elle en réduit surtout les coûts d'entrée, accélère les cycles d'exploitation et augmente la scalabilité des opérations existantes. Cette évolution entraîne une augmentation massive de l'offre (attaques opportunistes, campagnes à grande échelle), une pression à la baisse sur les prix unitaires et une saturation progressive de certains segments de marché, notamment les données nominatives. Cette dynamique renforce la nécessité, pour les attaquants, de se différencier soit par le volume, soit par la spécialisation.

C'est cette logique, plus que n'importe quelle innovation technique, qui structure l'évolution de la menace en 2025.

Pour conclure, précisons que cette logique économique ne fonctionne pas dans un vide géographique. Elle prospère dans des zones de faible coopération judiciaire internationale, où les acteurs opèrent avec une quasi-impunité structurelle.

Cette impunité structurelle est renforcée par un vide juridique international : il n'existe pas de qualification pénale harmonisée de la cybercriminalité en droit international (ni de régime pénal international pleinement harmonisé et universellement appliqué en matière de cybercriminalité). La Convention de Budapest, seul instrument multilatéral existant, ne couvre qu'une partie des États et ses mécanismes d'entraide restent lents et conditionnels. Cette fragmentation juridique est un facteur structurant du marché criminel au même titre que la géographie : elle garantit aux acteurs opérant depuis certaines juridictions une quasi-impunité de fait, indépendamment de leur visibilité.

Cette dimension géopolitique et ses implications pour la coopération défensive sont traitées plus loin.

Les implications pour repenser une défense cyber

5 Les implications pour repenser une défense cyber

Comprendre la cybercriminalité comme système économique n'est pas qu'un exercice intellectuel, c'est se préparer à un changement de posture défensive. Il ouvre trois lignes d'action que la seule lecture technique ne permet pas d'identifier.

5.1 Dégrader le rendement plutôt que bloquer l'accès

La défense technique classique (souvent périmétrique, par pare-feu en entrée, segmentation de l'interne et détection par des sondes) joue sur le terrain de l'attaquant : elle cherche à bloquer l'accès. L'IA (un chapitre ultérieur détaille ses usages dans ce cadre) permet de faire évoluer cette défense périmétrique par l'analyse de signaux faibles et la mise au jour de patterns d'attaque. Mais nombre d'entreprises sont encore très en retard sur ce plan, voire ne le prennent pas en compte.

C'est nécessaire mais insuffisant. Une organisation qui raisonne en termes économiques cherchera à dégrader le rendement de l'attaque : augmenter son coût opérationnel, réduire la valeur des données accessibles, allonger les délais de chaque phase.

Un attaquant dont le rendement attendu est inférieur à son coût d'opération choisira une cible plus simple et surtout plus rentable. La défense devient alors une question de prix relatif, pas d'imperméabilité absolue.

Cette approche implique également d'agir sur la valeur économique des actifs exposés : réduction de la durée de vie des credentials, segmentation limitant la réutilisabilité des accès, ou encore diminution de la valeur exploitable des données en cas d'exfiltration. La défense ne consiste plus seulement à empêcher, mais à rendre inutile.

5.2 Identifier ce qui rend une organisation cible rentable sur les marchés criminels

La grille de liquidité différentielle des marchés est un outil de priorisation défensive.

Une organisation devrait être capable de répondre à la question : quelles sont mes données les plus liquides sur un marché criminel ? Quelles sont celles à valeur unitaire la plus élevée ?

Ce n'est pas nécessairement ce que le RSSI considère comme le plus sensible. Pourtant, un secret industriel peut valoir moins sur ce marché qu'une base de credentials fraîche, selon le profil des attaquants susceptibles de cibler l'organisation.

Cette analyse gagne à être formalisée comme une cartographie économique de l'exposition : quels actifs sont liquides, lesquels sont rares, lesquels sont directement monétisables sans transformation. Cette grille peut diverger significativement de la classification traditionnelle des données sensibles.

5.3 Utiliser la spécialisation des attaquants comme levier de Threat Intelligence

La division du travail et la spécialisation des groupes criminels constituent paradoxalement un avantage pour les défenseurs : chaque groupe laisse une signature, dans le type de données ciblées, les outils utilisés, les modes opératoires, les places de marché fréquentées.

Une organisation qui investit dans la Threat Intelligence peut anticiper les attaques probables en fonction de son secteur, de son profil de données et des groupes actifs sur son périmètre géographique.

Même si elle n'a d'utilité que pour les grandes structures, ou pour celles dont l'exposition justifie un ciblage avancé, c'est une posture proactive que la seule réponse aux incidents ne permet pas de construire.

5.4 Deux limites à garder en tête

Cette lecture économique a ses propres angles morts. Elle s'applique bien aux acteurs criminels rationnels et organisés. Elle s'applique moins bien aux attaquants idéologiques, aux hacktivistes, ou aux acteurs étatiques dont la logique est géopolitique et non financière. Bien qu'ils puissent aussi utiliser l'écosystème criminel comme infrastructure, commanditer des IAB, louer des botnets, ce qui brouille la frontière et complique la grille d'analyse, il existe pour eux d'autres grilles d'analyse, développées dans les chapitres suivants.

Enfin, même au sein du crime organisé, la rationalité économique n'est pas toujours parfaite : erreurs opérationnelles, conflits internes, escroqueries entre acteurs ou décisions opportunistes peuvent perturber ces équilibres. Le système est structuré, mais il reste fondamentalement instable à l'échelle micro.

Conclusion : la cybercriminalité comme fait économique total

6 Conclusion : La cybercriminalité comme fait économique total

Cette étude s'est construite sur un postulat : comprendre pourquoi une attaque a lieu avant de chercher comment elle se déroule. L'angle de la monétisation n'est pas un détour intellectuel, c'est certainement un chemin assez court vers une défense cohérente.

Ce qu'elle révèle est à la fois simple et dérangeant. La cybercriminalité n'est pas un phénomène chaotique alimenté par des acteurs imprévisibles. C'est un système économique mature, avec ses marchés, ses prix, sa division du travail, ses mécanismes de confiance et ses logiques d'investissement.

La cybercriminalité est un système qui alloue des ressources, optimise ses rendements et s'adapte aux contraintes réglementaires avec une agilité que beaucoup d'entreprises légales lui envieraient.

Cette maturité a une conséquence directe pour les défenseurs : les approches purement techniques ne suffisent plus. Bloquer un accès, corriger une vulnérabilité, détecter une intrusion, tout cela reste nécessaire, mais c'est accepter de jouer sur le terrain de l'attaquant.

L'enjeu est désormais de raisonner en termes de rendement relatif : rendre son organisation moins rentable à attaquer que la suivante, réduire la valeur liquide de ses actifs exposés, allonger les délais de chaque phase jusqu'à ce que le coût d'opération dépasse le gain espéré.

Trois convictions émergent de cette analyse, qui devraient structurer la posture défensive de toute organisation exposée.

La première est que le silence n'est pas la sécurité. Les attaques les plus coûteuses (exfiltrations silencieuses, persistances longue durée, exploitations de ressources, opérations à finalité stratégique) sont précisément celles qui ne se manifestent pas. L'absence d'alerte n'est pas une preuve d'intégrité ; c'est parfois la signature d'une compromission réussie.

La deuxième est que la valeur criminelle d'un actif n'est pas sa valeur métier. Un secret industriel peut valoir moins sur un marché criminel qu'une base de credentials fraîche. Une donnée perçue comme banale peut être hautement liquide. Trop peu d'organisations ont encore formalisé la cartographie économique de leur exposition (quels actifs sont liquides, lesquels sont rares, lesquels sont directement monétisables). C'est pourtant un exercice crucial aujourd'hui.

La troisième est que l'écosystème criminel est résilient par construction. Démanteler un groupe, saisir une place de marché, neutraliser un opérateur RaaS produit au mieux une perturbation temporaire. Les rôles survivent aux individus, les franchises se reconstituent, les affiliés se redistribuent. La résilience de l'attaquant doit appeler une résilience symétrique du défenseur, à sa capacité à absorber, détecter et se rétablir.

Ce document est la première partie d'un panorama plus large. Les chapitres suivants traiteront des moyens techniques d'attaque et de défense, des acteurs (états, groupes criminels organisés, hacktivistes, insiders), de leurs modes opératoires, et des secteurs les plus exposés.

Mais quelle que soit la menace considérée, la grille économique développée ici reste le premier filtre : comprendre ce que l'attaquant vient chercher, c'est déjà commencer à lui rendre la tâche plus difficile.

Lexique et notes

7 Lexique et notes

[1] **Phishing** : technique d'hameçonnage consistant à envoyer des messages frauduleux imitant des communications légitimes (banques, administrations, plateformes connues) pour inciter la victime à révéler ses identifiants ou cliquer sur un lien malveillant. Moyen d'attaque initial très usité et ouvrant la porte à de très nombreux types d'attaques.

[2] **Rançongiciel** : traduction française de "ransomware" : logiciel d'attaque qui chiffre les données d'une victime et exige une rançon en échange de la clé de déchiffrement.

[3] **Infostealer** : logiciel d'attaque silencieux conçu pour collecter automatiquement des données sensibles (identifiants, mots de passe, cookies, données bancaires) sur les machines compromises, puis les transmettre par un réseau à l'attaquant.

[4] **Telegram** : application de messagerie chiffrée largement utilisée par l'écosystème criminel pour la vente d'outils, de données et de services malveillants, en raison de sa politique de modération historiquement permissive.

[5] **Liquidité du gain** : au sens criminel, représente la facilité et la rapidité avec laquelle un bien volé peut être converti en argent. Un mot de passe se vend en heures ; un secret industriel peut nécessiter des semaines de négociation.

[6] **Pare-feu** : dispositif logiciel ou matériel filtrant les flux réseau entrants et sortants selon des règles prédéfinies, constituant la première ligne de défense périmétrique d'un système d'information.

[7] **Mitigation** : ensemble des mesures prises pour limiter l'impact d'une attaque en cours ou réduire la surface d'exposition d'un système, sans nécessairement en éliminer la cause.

[8] **Low and Slow** : caractéristique d'attaques dont une des techniques consiste à fragmenter l'activité malveillante sur une longue période (semaines, mois) pour rester sous les seuils de détection des systèmes de surveillance.

[9] **Distributed Denial of Service** (DDoS) : attaque visant à rendre un service indisponible en le saturant de requêtes simultanées émises depuis un grand nombre de machines, souvent un botnet.

[10] **Credential** : identifiant numérique permettant l'accès à un système : typiquement un couple nom d'utilisateur et mot de passe, mais aussi des certificats, tokens ou clés d'accès.

[11] **Clé API** : les clés API sont des identifiants techniques permettant à une application ou un service de s'authentifier auprès d'un autre service. Leur vol donne accès aux systèmes et données associés sans nécessiter de mot de passe utilisateur.

[12] **Initial Access Brokers** (IAB) : les IAB sont des acteurs criminels spécialisés dans l'intrusion initiale dans des réseaux d'entreprise, qui revendent ensuite cet accès à d'autres attaquants sans l'exploiter eux-mêmes.

[13] **Escrow** : mécanisme de tiers de séquestre : un intermédiaire de confiance détient les fonds jusqu'à la vérification de la livraison du bien. Utilisé dans les transactions criminelles pour réduire le risque de défaut de paiement entre parties qui ne se font pas confiance.

[14] **Business Email Compromise** (BEC) : type de fraude consistant à usurper ou compromettre une messagerie professionnelle pour détourner un virement bancaire en se faisant passer pour un dirigeant, un fournisseur ou un partenaire.

[15] **Insider** : personne disposant d'un accès légitime aux systèmes d'une organisation (employé, prestataire, sous-traitant) qui en abuse, volontairement ou sous contrainte, à des fins malveillantes.

[16] **Sim swapping** : catégorie d'attaque d'ingénierie sociale consistant à convaincre un opérateur téléphonique de transférer le numéro d'une victime vers une carte SIM contrôlée par l'attaquant, permettant d'intercepter ses SMS d'authentification.

[17] **Wallet** : application ou dispositif permettant de stocker et d'utiliser des cryptomonnaies. Contrairement à un compte bancaire, un wallet n'est rattaché à aucune institution financière : son contenu est accessible uniquement via une clé privée, ce qui en fait une cible privilégiée pour les attaquants.

[18] **Cryptomining** : utilisation de la puissance de calcul d'une machine pour générer (miner) de la cryptomonnaie. Lorsqu'elle est effectuée à l'insu du propriétaire via un malware, elle constitue un vol de ressources.

[19] **Botnet** : réseau de machines infectées par un malware et contrôlées à distance à l'insu de leurs propriétaires, utilisé pour mener des attaques coordonnées, du spam ou du cryptomining.

[20] **Malware** : contraction de "malicious software" : tout logiciel conçu pour nuire à un système, voler des données ou en prendre le contrôle à l'insu de son propriétaire.

[21] **Rendement marginal** : en économie, gain supplémentaire obtenu pour chaque unité additionnelle d'effort ou d'investissement. Appliqué ici à la logique des attaquants qui optimisent l'allocation de leurs ressources entre différentes cibles ou modes opératoires.

[22] **Credential stuffing** : attaque automatisée consistant à tester massivement des couples identifiant/mot de passe volés sur de nombreux services, en exploitant la tendance des utilisateurs à réutiliser les mêmes mots de passe, pour profiter de ce couple identifiant/mot de passe sur d'autres services.

[23] **Piggyback** : stratégie par laquelle un attaquant exploite la notoriété ou la réputation d'une organisation légitime pour réduire ses propres coûts d'acquisition de victimes, en se greffant sur la confiance existante.

[24] **Digital Operational Resilience Act** (DORA). Règlement européen entré en vigueur en 2025, imposant aux acteurs financiers des exigences strictes de résilience opérationnelle face aux risques numériques.

[25] **Network and Information Security directive, version 2** (NIS2). Directive européenne de 2023 étendant les obligations de cybersécurité à un périmètre élargi de secteurs et d'organisations, avec des sanctions renforcées.

[26] Elles feront l'objet d'une analyse distincte dans le Panorama de la Cybersécurité 2025-2026, consacré aux moyens techniques d'attaque et de défense, aux acteurs, à leurs modes opératoires, et aux secteurs les plus exposés.

[27] **Dropper** : malware dont la fonction première est d'installer discrètement un autre logiciel malveillant sur la machine compromise, servant de vecteur d'entrée pour une charge utile plus sophistiquée.

[28] **Deepfake** : contenu audio ou vidéo synthétique généré par intelligence artificielle pour imiter de manière convaincante la voix ou l'apparence d'une personne réelle, utilisé notamment pour des arnaques ou de la manipulation.

[29] **Ransomware-as-a-Service** (RaaS) : modèle commercial criminel par lequel des opérateurs fournissent à des affiliés une infrastructure clé en main pour mener des attaques par rançongiciel,

en échange d'une commission sur les gains. Ce modèle est calqué sur celui très populaire en informatique du SaaS (Software as a Service).

[30] **Phisher** : acteur criminel spécialisé dans les opérations de phishing.

[31] **Scam** : arnaque en ligne, généralement à grande échelle, visant à extorquer de l'argent ou des données personnelles à des victimes par tromperie.

[32] **Scammeur** : auteur de scams : individu spécialisé dans les arnaques en ligne, souvent de faible niveau technique, opérant à partir de scripts et de modèles fournis par d'autres acteurs de l'écosystème.

[33] **Alloteur** : acteur criminel spécialisé dans le tri, la segmentation et la valorisation de bases de données volées, afin de les vendre en lots adaptés aux différents acheteurs selon leur profil d'exploitation.

[34] **Casher** : acteur criminel chargé de convertir des gains illicites (cryptomonnaies, accès à des comptes bancaires compromis) en argent réel, souvent via des mules financières ou des réseaux de change informels.

[35] **BreachForums** : Place de marché criminelle en ligne assez connue, spécialisée dans la vente de données volées, de credentials et d'accès compromis. Saisie à plusieurs reprises par les autorités, elle s'est reconstituée autant de fois sous différentes formes.

[36] **Software as a Service** (SaaS) : modèle de distribution logicielle où l'application est hébergée dans le cloud et accessible par abonnement, sans installation locale. Certains écosystèmes criminels reproduisent ce modèle pour leurs outils d'attaque.

[37] **LockBit** : groupe criminel organisé et opérateur RaaS, l'un des plus actifs mondialement entre 2020 et 2024. Partiellement démantelé par les autorités en 2024, ses affiliés ont rapidement migré vers d'autres franchises.

[38] **Pig butchering** : type d'arnaque de long terme combinant manipulation affective (souvent via une application de rencontre) et incitation à investir dans une plateforme de cryptomonnaies frauduleuse. La victime est "engraissée" avant d'être "abattue" financièrement.

[39] **Threat intelligence** : discipline analysant du renseignement sur les menaces : collecte et analyse d'informations sur les groupes d'attaquants, leurs outils, leurs cibles et leurs modes opératoires, permettant d'anticiper les attaques plutôt que d'y réagir.

[40] **Supply chain** : les attaques « Supply chain » sont des attaques ciblant non pas une organisation directement, mais un fournisseur, un prestataire ou un composant logiciel tiers utilisé par cette organisation, pour atteindre indirectement un grand nombre de cibles.

Radical SSI :
36 avenue Franklin ROOSEVELT, 94300 VINCENNES
(+33) 1 41 74 69 66
contact@radical-ssi.fr
https://radical-ssi.fr/