DRÔLE DE BESTIAIRE

SAVEZ-VOUS PARLER LE LANGAGE CYBER ?

URGENCE CYBER REGION SUD >>>> LES PORTES OUVERTES >>>> 27 MAI 2025

Le ver
#LeColonisateur

Rôle : La propagation autonome d’un code malveillant (malware).

Symbole : Tel un ver de terre, le ver numérique rampe hors de vue, invisible et patient, creusant ses galeries dans les systèmes d'information, jusqu'à les rendre instables ou totalement inopérants.

Description : Créature numérique sans maître, le ver ne se contente pas d'infecter un hôte : **il se reproduit de lui-même, sans intervention humaine**, et s’insinue silencieusement dans d’autres systèmes connectés. Il progresse de proche en proche, comme une nappe de brouillard toxique s'étendant au gré des réseaux, exploitant les moindres interstices laissés ouverts par la négligence ou la faille.
Sa force réside dans sa capacité à agir en silence, sans commande directe, et à **transformer un simple incident en épidémie numérique à grande échelle**. Là où un virus a besoin d’un déclencheur, le ver se suffit à lui-même pour croître et proliférer.

Le renard (fox)

#L'infiltré

Rôle : L'exploitation furtive des vulnérabilités logicielles.

Symbole : Symbole de la **ruse** et la duplicité, le renard s'insinue dans les systèmes en se glissant sous le radar, exploitant les raccourcis, les oublis, les négligences humaines comme autant de brèches ouvertes sur l'invisible.

Description : Le renard numérique n'attaque pas de front : **il préfère les chemins détournés, les failles discrètes, les interfaces familières** que l'on oublie de surveiller. Souvent dissimulé dans des programmes légitimes ou des outils utilitaires (PDF reader, extensions de navigateur, exécutables inoffensifs en apparence), il revêt le masque du quotidien pour mieux dérober, observer ou préparer l'ouverture d'une porte dérobée.
Ce n'est ni un ver ni un cheval de Troie au sens strict : c'est un opportuniste, un parasite malin qui s'adapte à son environnement, joue de la ruse technique et se déplace avec élégance dans les marges du code.

Cerber
Le geôlier à #TroisTêtes

Rôle : Le blocage des données par chantage numérique (ransomware).

Symbole : Tel un chien mythologique posté à la frontière des mondes, Cerber **garde les données enfermées dans les ténèbres du chiffrement**, aboyant sans relâche jusqu'à ce qu'un tribut soit payé. Sa triple tête symbolise la terreur, la domination et l'opacité.

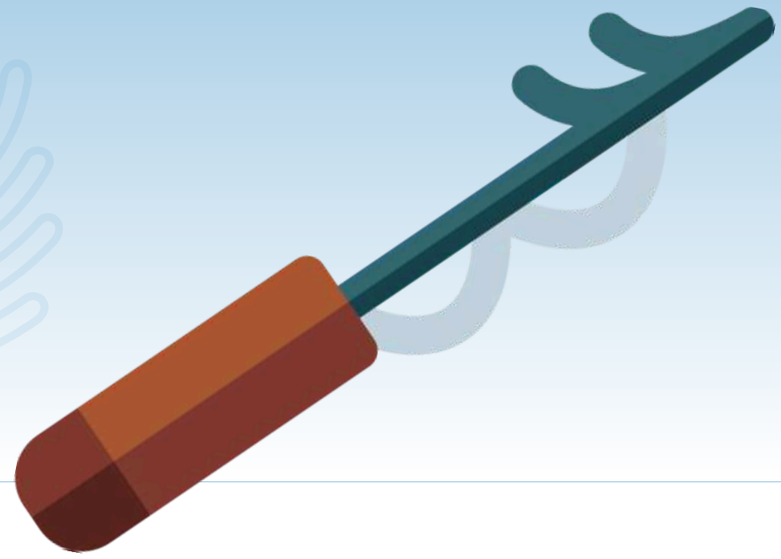
Description : Gardien féroce du royaume des fichiers chiffrés, Cerber capture les données et ne les relâche qu'en échange d'une rançon. Multiforme, il est difficile à abattre et souvent camouflé. Cerber se distingue par sa brutalité froide : il ne vole pas, il retient en otage.
Il ne cherche pas la discrétion, mais l'effroi immédiat, l'efficacité psychologique. Il sait que l'urgence panique plus sûrement que l'invisibilité.

L’hameçonneur
#Phishing

Rôle : Le vol de données par tromperie (phishing).

Symbole : Tel un pêcheur patient tapi sur la berge du réseau, l’hameçonneur ne force pas, il attire. Il jette ses lignes déguisées en messages anodins, imitant à la perfection l’allure d’un site, d’une institution, d’un collègue ou d’un proche. Ce qu’il veut ? Que vous mordiez à l’hameçon.

Description : L’hameçonneur ne brise aucune porte : il vous tend une clef, et vous l’acceptez de vous-même. Il s’introduit dans votre boîte mail ou votre téléphone sous la forme d’un message pressant, d’un lien séduisant, d’une urgence fabriquée. **C’est un voleur de confiance, un imitateur de la réalité**, qui prospère dans les automatismes humains : cliquer trop vite, faire confiance à un logo familier, répondre dans la précipitation.
Par sa nature, il **frappe à grande échelle**, inlassablement, jusqu’à ce qu’une proie se laisse prendre. Chaque clic erroné, chaque formulaire rempli, lui livre des identifiants, des accès, des secrets. Et parfois, un simple clic ouvre la voie à bien pire : intrusion, rançonnage, vol de données personnelles ou professionnelles.



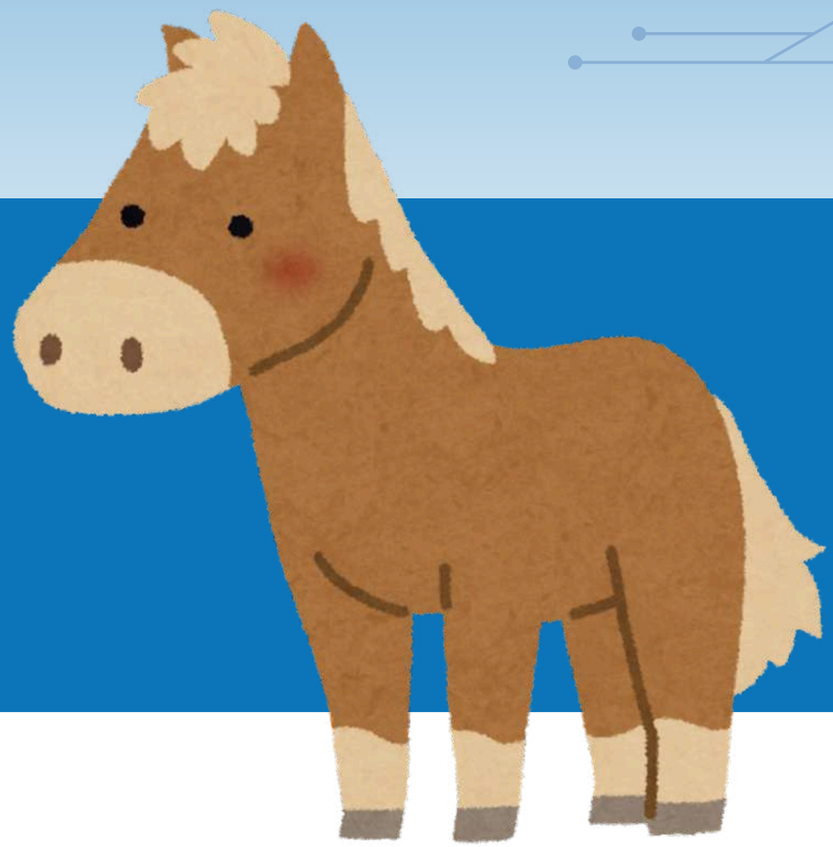
Le harponnage
#SpearPhishing

Rôle : Le vol ciblé par tromperie personnalisée (spear phishing).

Symbole : Là où l'hameçonneur lance des lignes au hasard, **le harponneur vise avec précision**. Il ne cherche pas la foule, mais une proie unique, souvent précieuse, isolée, influente. Sa flèche est soigneusement taillée, son message écrit sur mesure. Il est le chasseur d'élite du cyberespace, patient, calculateur, redoutablement efficace.

Description : Le harponnage ne repose pas sur la masse, mais sur l'intelligence de la manipulation. L'attaque est précédée d'une phase d'observation : l'**attaquant étudie sa cible**, ses habitudes, ses collègues, son vocabulaire, ses responsabilités. Puis il fabrique un message sur mesure, souvent indiscernable d'un vrai — un faux ordre de virement, une demande urgente du directeur, une invitation à renouveler un mot de passe.
Cette attaque ne vise pas un mot de passe générique, mais un accès stratégique : compte administrateur, interface sensible, boîte mail d'un cadre dirigeant. Une seule erreur, un seul clic, et l'intrusion est totale.
Le harponnage est l'arme privilégiée des attaques avancées (APT), des escroqueries au président, des campagnes de sabotage numérique. Il combine l'art du déguisement et la science du ciblage.

Se faire



"Se faire poné" (ou "se faire pwné") signifie, dans le langage geek ou gamer : se faire dominer, écraser, humilier, ou pirater.

En cybersécurité, l’expression est souvent utilisée pour dire que des identifiants ou des données ont été compromis.
"Le site s’est fait pwned" = Le site s’est fait pirater, il a perdu le contrôle de ses données.

A l’origine, "Pwned" est né d’une faute de frappe de "owned", dans le monde des jeux vidéo en ligne et du hacking. Sur un clavier QWERTY, les touches "O" et "P" sont côte à côte.

La pêche à la baleine #Whaling

Rôle : Attaque ultra-ciblée contre les hauts dirigeants (whaling).

Symbole : À la croisée de la ruse et de l'ambition, le chasseur de baleine ne vise pas les maillons faibles, mais les figures d'autorité : PDG, directeurs financiers, chefs de service. Sa proie n'est pas la plus exposée, mais la plus stratégique. C'est un prédateur de prestige, patient et méticuleux, qui n'attaque que lorsque le gain est à la hauteur du risque.

Description : Le chasseur de baleine vise les grandes figures : PDG, CFO, cadres dirigeants. Moins de cibles, mais des attaques préparées, personnalisées, et potentiellement très lucratives.

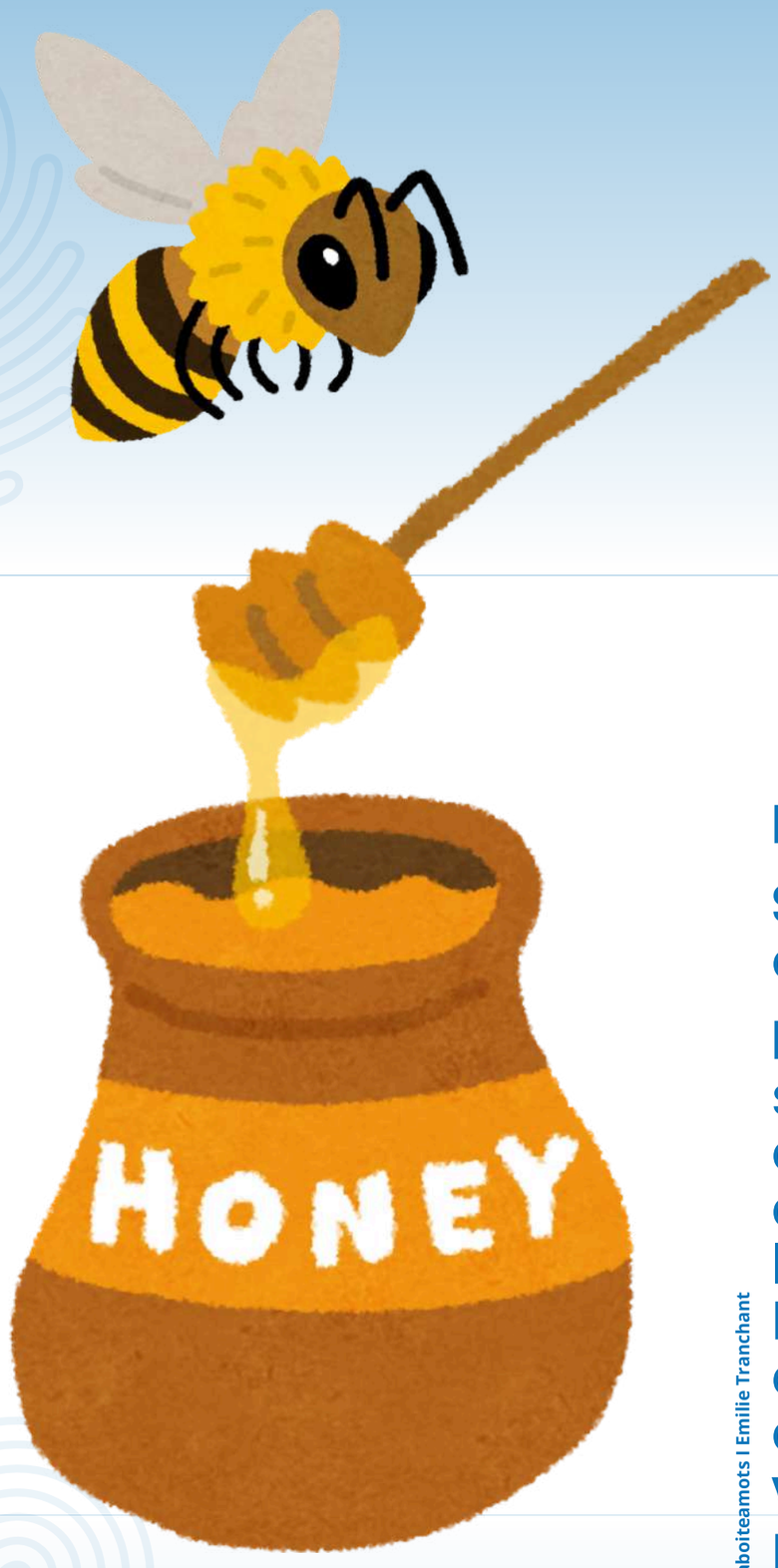
La pêche au chat
#Catphishing

Rôle : L'usurpation d'identité affective.

Symbole : Le chat incarne la manipulation : doux, attirant, familier, il mène son monde à la baguette.

Description : Le chat prend une apparence douce, séduisante, familière. Derrière le masque, un escroc. Il joue sur les émotions pour manipuler, extorquer ou déstabiliser. Il capte les fragilités affectives, comble les solitudes, suscite la confiance… pour mieux la trahir.

Il ne s'attaque pas à l'identité, mais à l'intimité. L'usurpateur ne cherche pas seulement à se faire passer pour un autre, il cherche à devenir le centre émotionnel de la victime. C'est un parasite empathique, un illusionniste numérique qui transforme le besoin de lien en levier de contrôle. Derrière l'écran, le visage projeté est une chimère : il n'a d'existence que pour séduire, piéger, voler — parfois l'argent, souvent la paix intérieure.



L’abeille et son #PotDeMiel

Rôle : Le “honeypot” est un **leurre défensif**.

Symbole : Il symbolise le piège raffiné et observation passive.

Description : Il attire les intrus par son parfum sucré. Mais ce miel est toxique : une fausse base de données, un faux accès, un leurre savamment conçu pour capturer les mouvements de l’assaillant sans qu’il s’en doute.
Le honeypot n’attaque pas — il observe, enregistre, analyse. Il inverse la logique du rapport de force : **l’agresseur croit pénétrer une cible vulnérable, alors qu’il est lui-même mis à nu**, piégé dans une architecture qui n’existe que pour le contenir.

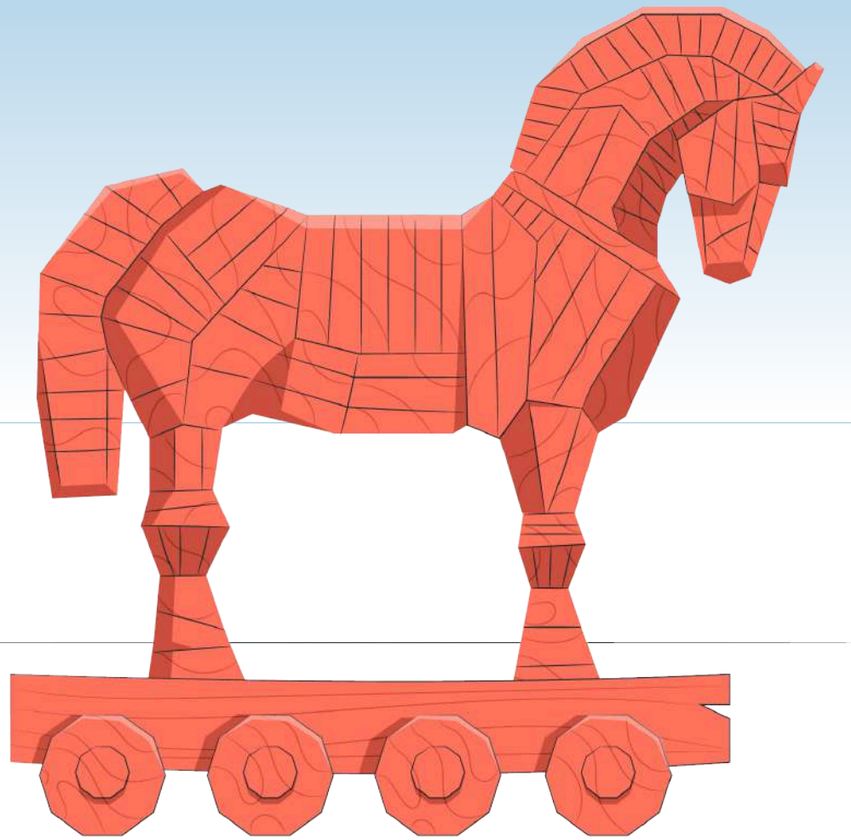
L’hydre
L’attaque #multi-tête

Rôle : La force brute ou la menace résiliante.

Symbole : L’hydre est le symbole de la démultiplication et de la résilience.

Description : Chaque fois qu’on coupe une tête — processus, point d’entrée, serveur — deux autres repoussent. **Cette menace n’avance pas masquée : elle frappe fort, frappe vite, mais surtout, elle revient.** C’est une attaque de saturation, de persistance, d’usure. Elle exploite la redondance, les failles systémiques, la fatigue défensive. La neutraliser une fois ne suffit pas : elle est pensée pour survivre, se reformer, s’adapter. On croit l’avoir arrêtée, mais elle se recompose ailleurs, sous une autre forme, parfois plus agressive encore.

Le cheval de Troie #FauxAllié



Rôle : La duplicité.

Symbole : Le cheval de Troie, comme dans la mythologie, incarne la ruse.

Description : Derrière une apparence inoffensive, ce cheval cache des agents malveillants. Le programme semble légitime, l'accès paraît anodin, la demande semble de confiance. Mais une fois introduit dans la forteresse numérique, il libère ses cavaliers : malwares, portes dérobées, scripts d'exécution, espionnage furtif. L'attaque ne force pas l'entrée : elle obtient le consentement, feint la légitimité, infiltre en douce. **C'est une trahison de l'intérieur, une ruse d'accès camouflée dans les plis de la normalité.**

Le zombie
#PerteDeContrôle

Rôle : Le zombie a pour mission de mener une attaque coordonnée (botnet) en prenant le contrôle.

Symbole : Le zombie symbolise l'absence de volonté, le détournement.

Description : La machine, une fois infectée, obéit sans conscience, ni question. Isolée, elle demeure anodine ; connectée à un essaim, elle devient une arme. **L'armée des zombies agit en meute** : attaques DDoS, spams massifs, vols de données, propagation silencieuse de malwares. Le botnet est une force sans visage, mobilisée à l'insu même de ceux qui la portent.
Ce défaut de volonté ne touche pas que les machines : **il s'étend aux utilisateurs,** souvent inconscients que leur terminal a été détourné. Le botnet prospère sur l'ignorance, la routine et l'indifférence. C'est une infrastructure fantôme, en sommeil, attendant le signal d'attaque.
La coordination, parfois décentralisée via des réseaux peer-to-peer, accentue le caractère insaisissable de la menace : nul ne perçoit l'assaut avant qu'il ne frappe, nul ne peut en localiser la source. Il incarne la figure moderne de la horde : innombrable, silencieuse, instrumentalisée.

Le rat #fouineur (trop) discret

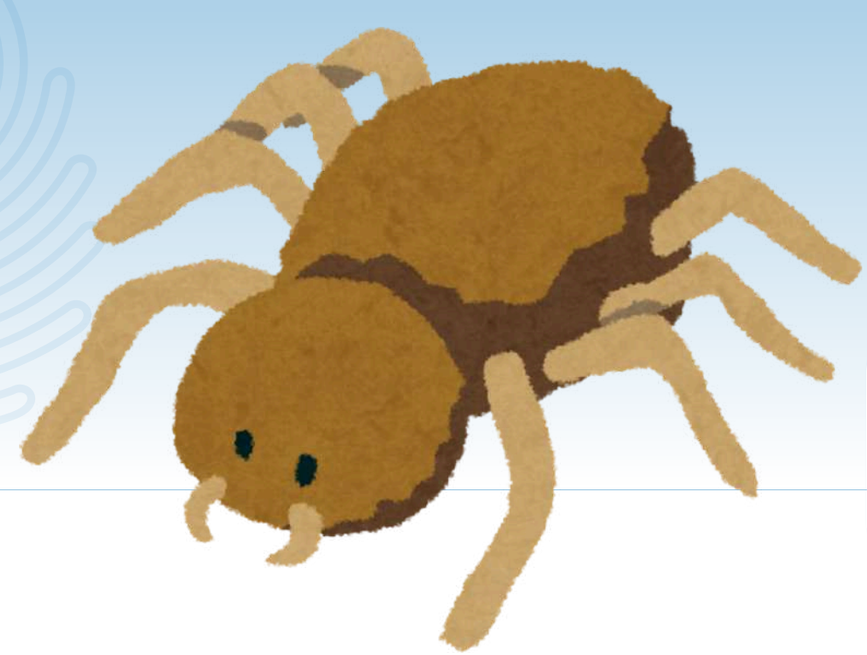
Rôle : L’intrusion invisible RAT (Remote Access Trojan).

Symbole : Symbole de l’infiltration, À l’image du rat, il agit dans le noir, longe les parois, se déplace dans les interstices du système sans déclencher d’alerte.

Description : Le RAT, ou cheval de Troie d’accès à distance, s’introduit discrètement dans le système, souvent dissimulé dans un fichier anodin : une pièce jointe, un lien apparemment légitime, un logiciel piraté. **Une fois installé, il ne fait pas de bruit. Il observe.** Il attend. Il ouvre une porte dérobée entre l’ordinateur infecté et son maître à distance. Ce dernier peut alors tout voir, tout entendre, tout contrôler : fichiers, webcam, clavier, microphone. Le RAT transforme la machine en marionnette, le réseau en théâtre d’opérations silencieuses. **C’est l’espion qui s’infiltre, prend le contrôle et reste invisible**, maître du dispositif sans jamais se montrer. Une présence fantôme dans l’ombre du numérique.

Le caméléon
#polymorphe

Rôle : Malware polymorphe, il joue sur la dissimulation.
Symbole : Le caméléon est le maître du camouflage.
Description : Il se fond dans le décor, épouse les teintes du familier, mime les apparences de la confiance. Le caméléon numérique n'impose rien : il suggère, il trompe. Un faux site bancaire, un courriel imitant l'administration, une application clonée jusqu'au moindre détail. **Tout semble authentique, tout semble normal.** Mais sous la peau trompeuse se cache le piège. Le but n'est pas de forcer, mais de séduire ; non d'attaquer frontalement, mais de faire croire. C'est l'art du phishing, du spoofing, de l'hameçonnage subtil. L'illusion fonctionne parce qu'elle rassure. **L'utilisateur ne se méfie pas** de ce qu'il croit reconnaître. Ainsi, le caméléon s'infiltre en douce, sans alerte, sans choc. Il n'imite pas pour divertir, mais pour tromper. C'est la menace qui avance masquée, déguisée en normalité.



L’araignée
La tisseuse du web

Rôle : L’exploration automatique du réseau.
Symbole : Vigilance, mémoire, omniprésence.
Description : L’araignée déploie méthodiquement sa toile sur l’ensemble du cyberespace. **Elle avance sans bruit, patiente, attentive**, en suivant les liens, en cartographiant les connexions, en capturant les contenus. Programmée pour explorer, elle indexe, recense, archive. Aux moteurs de recherche, elle fournit une image structurée du web, une mémoire vivante des pages, des relations et des flux. **Elle n’est pas, à l’origine, une menace : c’est un œil qui regarde tout, en silence.** Mais entre de mauvaises mains, elle devient un éclaireur redoutable. Car ce que l’araignée voit, d’autres peuvent l’exploiter. Certains crawlers malveillants copient des bases de données, détectent les failles, identifient les API mal protégées, aspirent des informations sensibles laissées sans défense. **L’araignée devient alors espionne,** sentinelle pour pirates, agent d’une future attaque. Son exploration, banale en apparence, peut annoncer une phase de reconnaissance préalable à l’intrusion. Elle n’attaque pas, elle prépare le terrain. C’est l’intelligence froide d’un processus automatisé, capable de couvrir l’ensemble du réseau avec une précision implacable.