RAPPORT JUIN 2026

L'ÉTAT DE LA MENACE CYBER

Le premier semestre 2026 lu à travers les données de notre veille.

JANVIER À JUIN 2026

LuksMentis

Veille cyber souveraine · luksmentis.com

Sommaire

00 **Un semestre de bascule** 3
Édito : ce que disent nos données

01 **L'ère de la consolidation** 5
Ransomware : moins de groupes, plus de victimes

02 **Un fournisseur, des dizaines de victimes** 8
Tiers & OAuth : la saga ShinyHunters

03 **La cyber comme arme** 11
Géopolitique : représailles et infrastructures

04 **L'inventaire du semestre** 15
Fuites de données : de la France à la revente

05 **Ce qui est réellement exploité** 19
Vulnérabilités : le KEV plutôt que le CVSS

06 **L'IA qui industrialise le vol** 22
Transversal : le multiplicateur des tendances

07 **Priorités et perspectives** 24
Ce que ça implique pour les équipes sécurité

00

00 · ÉDITO

Un semestre de bascule

Ce que disent nos données

64 000

signaux cyber majeurs consolidés en six mois

Veille LuksMentis · janv. à juin 2026

00 · ÉDITO

Un semestre de bascule

Ce que disent nos données

Le premier semestre 2026 ne restera pas dans les mémoires pour une attaque unique, mais pour trois mouvements de fond qui se renforcent mutuellement : un marché du ransomware qui se concentre autour d'une poignée d'acteurs, le retour de la cyber comme prolongement d'un conflit géopolitique, et l'industrialisation, par l'intelligence artificielle, du vol et de la revente de données.

Notre veille a consolidé près de **64 000 signalements cyber majeurs** depuis le 1er janvier 2026 : incidents, divulgations de vulnérabilités, fuites de données, revendications de groupes. De ce flux, nous reconstruisons en continu des **incidents** reliant un attaquant identifié à une victime nommée : plus de 14 500 à ce jour, portant sur 10 200 organisations distinctes. C'est cette matière première, et non une sélection d'événements spectaculaires, qui éclaire les pages qui suivent.

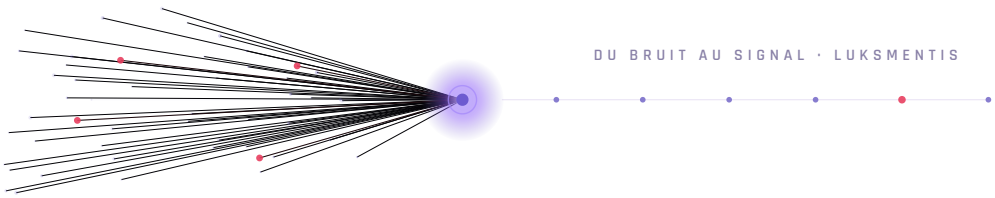
Le constat d'ensemble est net. Le ransomware et la fuite de données saturent le paysage ; les éditeurs de bordure (VPN, pare-feux) restent la porte d'entrée privilégiée ; et un même maillon faible, un fournisseur, un jeton OAuth oublié, suffit désormais à compromettre des dizaines d'organisations en cascade. Ce rapport décline ces dynamiques en six chapitres, chacun adossé à nos chiffres et mis en perspective avec les grands rapports du secteur.

Le semestre en chiffres (base LuksMentis, janvier à juin 2026)

INDICATEUR	VALEUR
Signalements cyber qualifiés	près de 64 000
Incidents reconstitués (attaquant vers victime)	14 500
Victimes nommées distinctes	10 200
Revendications ransomware (leak-sites)	1 592 / 79 groupes
CVE activement exploitées suivies (KEV)	1 629
dont instrumentalisées en ransomware	327

Veille LuksMentis · luksmentis.com · juin 2026

Note de méthode. Nos chiffres reflètent une veille, pas un recensement exhaustif de la menace mondiale. Notre dispositif capte chaque jour un très grand volume de signaux bruts ; nous les analysons, recoupons et trions pour n'exploiter que des informations issues de sources vérifiables et écarter le bruit de fond. Les chiffres présentés ici portent donc sur ce flux qualifié, pas sur la collecte brute. Nous raisonnons en classements et en parts plutôt qu'en volumes absolus. Enfin, l'attribution d'un groupe ou d'un pays repose souvent sur des sources ouvertes : elle indique qui revendique ou est crédité d'une attaque, pas une preuve judiciaire.



01 · RANSOMWARE

L'ère de la consolidation

Moins de groupes, plus de victimes

71 %

des victimes concentrées par le top 10 des groupes ransomware

ScienceDirect · T1 2026

01 · RANSOMWARE

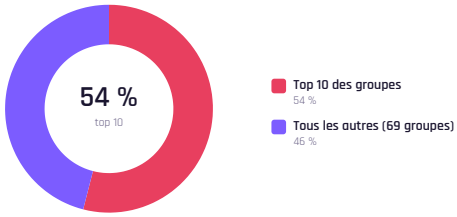
L'ÈRE DE LA CONSOLIDATION

Moins de groupes, plus de victimes

EN BREF Après deux ans de fragmentation, le marché du ransomware se reconcentre : moins de groupes, mais plus industriels, et davantage de victimes.

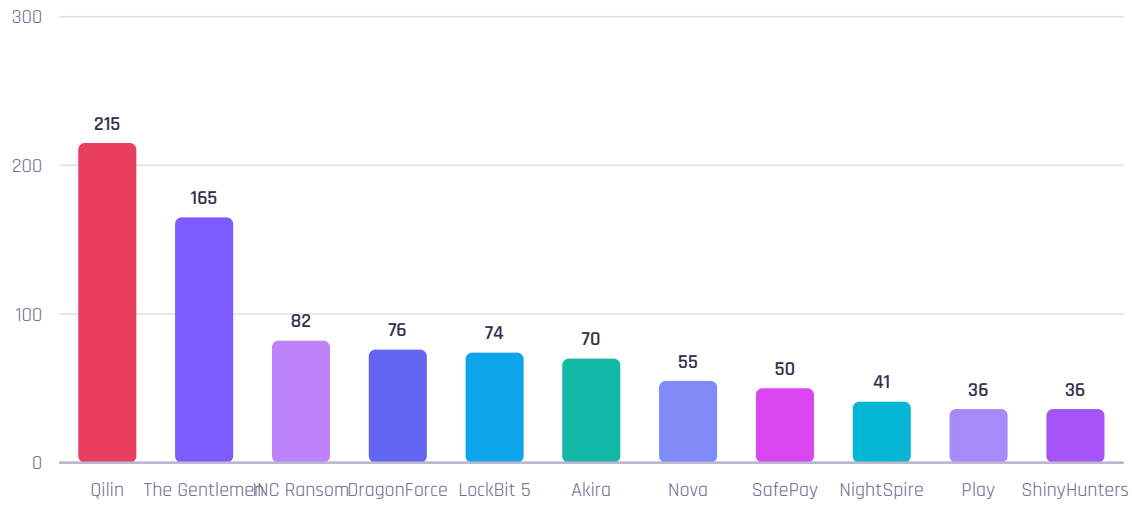
Pendant deux ans, le marché du ransomware s'était fragmenté : le démantèlement de LockBit et d'ALPHV/BlackCat avait dispersé les affiliés vers une myriade de petites franchises. Le premier semestre 2026 inverse la tendance. Le marché se **reconcentre** autour d'une poignée d'acteurs industriels. À l'échelle mondiale, le T1 2026 a vu plus de 2 100 victimes listées sur les sites de fuite, et le top 10 des groupes concentre désormais environ **71 % des victimes**, contre 57 % auparavant (ScienceDirect).

Notre échantillon le confirme à sa mesure. Sur 1 592 revendications relevées sur les leak-sites depuis fin janvier, réparties entre 79 groupes, les dix plus actifs concentrent **54 %** des victimes. L'écart avec les 71 % du marché mondial tient à la couverture de notre collecte ; la direction, elle, est la même : la valeur se déplace vers le haut du classement.



Concentration : part du top 10 des groupes

Veille LuksMentis · échantillon leak-sites 2026 (à comparer aux 71 % du marché mondial, ScienceDirect) · luksmentis.com · juin 2026



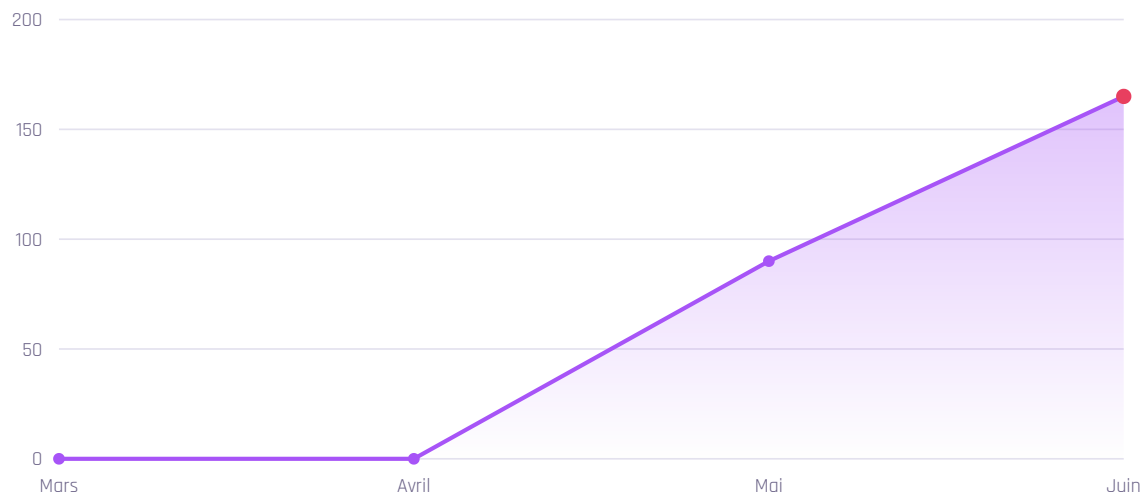
Top des groupes ransomware par revendications (sites de fuite, 2026)

Veille LuksMentis · revendications leak-sites, janvier à juin 2026 (1 592 au total) · luksmentis.com · juin 2026

En tête, **Qilin** s'impose comme le groupe le plus prolifique, troisième trimestre consécutif de domination. Son modèle d'affiliation agressif, sa permanence et sa capacité à absorber les affiliés orphelins en font le centre de gravité du marché. Derrière, le classement mêle des noms installés (INC Ransom, DragonForce, Akira, Play) et une nouvelle génération de franchises, Nova, SafePay, NightSpire, symptôme d'un écosystème qui se recompose plus qu'il ne se calme.

The Gentlemen : la révélation du semestre

Aucune trajectoire n'illustre mieux cette recomposition que celle de **The Gentlemen**. Apparu en août 2025, le groupe est passé d'une trentaine de victimes au dernier trimestre 2025 à **182 au premier trimestre 2026**, se hissant au rang de deuxième acteur le plus actif. Dans notre propre suivi leak-sites, il occupe également la deuxième place, avec 165 revendications. Sa signature : une approche professionnelle, presque corporate, et l'exploitation massive d'équipements de bordure, FortiOS, SonicWall VPN, Cisco ASA. C'est le profil type du nouvel entrant 2026 : pas un collectif d'amateurs, mais une organisation rodée qui industrialise l'accès initial par les failles d'infrastructure.



L'irruption de The Gentlemen : victimes revendiquées, cumul mensuel 2026

Veille LuksMentis · revendications leak-sites cumulées (le groupe n'entre dans notre suivi qu'au printemps 2026) · luksmentis.com · juin 2026

Ce paysage recoupe précisément notre étude « Anatomie des groupes d'attaquants », qui cartographiait déjà la domination des acteurs financiers et la montée des nouveaux entrants. La consolidation observée ici en est la suite logique : le ransomware-as-a-service mûrit, et la maturité, dans une économie criminelle, signifie la concentration.

Ce que ça change. Face à un marché concentré, la défense gagne en lisibilité : surveiller les TTP des dix premiers groupes couvre la majorité du risque réel. Mais la concentration accroît aussi la capacité de chaque acteur dominant, plus d'affiliés, plus d'outils, plus de pression. Patcher les équipements de bordure n'est plus une hygiène, c'est la première ligne.

Ce qu'il faut retenir

01 Le marché du ransomware se reconcentre : moins de groupes, mais plus industriels.

02 Le top 10 capte environ 71 % des victimes mondiales, contre 57 % auparavant.

03 La priorité de défense se déplace vers les acteurs dominants et leurs vecteurs d'accès.

02

02 · TIERS & OAUTH

Un fournisseur, des dizaines de victimes

La saga ShinyHunters

237

incidents reconstitués pour ShinyHunters, l'acteur le plus présent du corpus

Veille LuksMentis · H1 2026

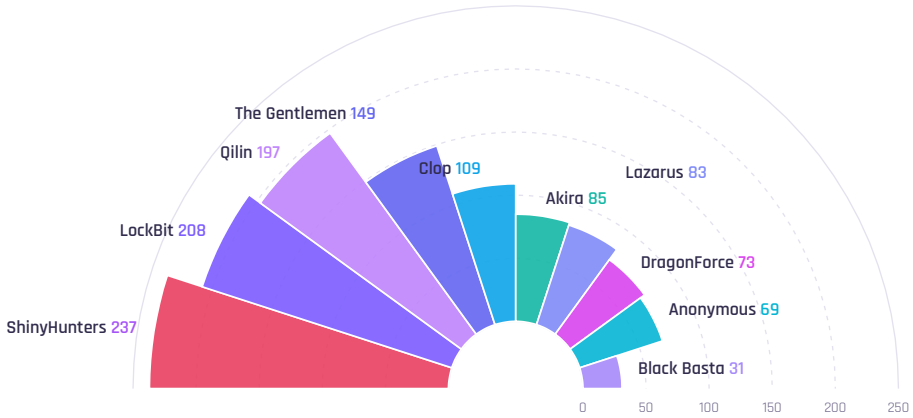
02 · TIERS & OAuth

Un fournisseur, des dizaines de victimes

La saga ShinyHunters

> **EN BREF** La compromission ne vise plus la forteresse mais ses fournisseurs : un jeton OAuth chez un tiers de confiance suffit à exposer des dizaines d'organisations.

Si un acteur résume le fil rouge de 2026, c'est **ShinyHunters**. Dans nos données, tous incidents reconstitués confondus, c'est le groupe le plus présent du corpus, devant LockBit et Qilin. Sa marque de fabrique n'est pas le chiffrement, mais le vol de données à grande échelle, souvent via un tiers de confiance.



Acteurs les plus actifs, tous incidents reconstitués confondus

Veille LuksMentis · incidents attribués (groupes nommés, hors libellés génériques) · luksmentis.com · juin 2026

Le mode opératoire qui a défini le semestre tient en un mot : OAuth. Après la vague Salesloft Drift de 2025, une application tierce connectée à Salesforce dont les jetons volés ont exposé plus de 700 organisations, la mécanique s'est reproduite en 2026. En juin, un groupe opérant sous le nom d'Icarus a exploité une intégration OAuth via l'outil Klue pour siphonner des données Salesforce de plusieurs entreprises de sécurité elles-mêmes - HackerOne, Gong, OneTrust, Tanium, Huntress, LastPass. ShinyHunters a par ailleurs frappé 7-Eleven, et Medtronic a confirmé un vol revendiqué de plus de 9 millions d'enregistrements.

Ces noms ne sont pas théoriques pour nous : ils figurent parmi les victimes que notre veille a attribuées à ShinyHunters ce semestre, Instructure, 7-Eleven, ADT, DentaQuest, le Conseil de l'Europe, Medtronic, la Commission européenne. Le dénominateur commun n'est jamais la forteresse de la victime finale, mais la **permission excessive** accordée un jour à une application tierce.

Le maillon n'est pas dans la forteresse

C'est exactement la thèse que développe notre article sur la sécurité des tiers : près d'une compromission sur trois implique désormais un tiers (30 %, contre 15 % un an plus tôt selon le DBIR 2025 de Verizon), et ces intrusions sont les plus lentes à détecter - 267 jours en moyenne (IBM). La donnée n'est plus volée en perçant un mur, mais en empruntant un tunnel de confiance qu'on a soi-même ouvert. Un jeton OAuth oublié, un compte de service jamais révoqué : le facteur aggravant est organisationnel avant d'être technique.

> **Ce que ça change.** La surface d'attaque s'est déplacée vers le SaaS et les intégrations. Inventorier ses connecteurs OAuth, appliquer le moindre privilège aux applications tierces, faire tourner et révoquer les secrets, exiger des garanties vérifiables de ses fournisseurs (ISO 27001, SOC 2) : ces gestes ne sont plus du confort, ce sont les nouvelles fondations.

Anatomie d'une compromission par un tiers de confiance

Lecture LuksMentis · schéma type de la saga ShinyHunters · les flèches mènent aux victimes finales par effet de cascade · H1 2026

Comment lire ce schéma. Un fournisseur de confiance est d'abord compromis par hameçonnage ; un jeton OAuth trop permissif ouvre alors l'accès à ses données SaaS. L'attaquant exfiltre en masse, sans chiffrement, puis actionne l'effet de levier : une seule intrusion chez le fournisseur se propage en cascade vers des dizaines de clients finaux. C'est le schéma type de la saga ShinyHunters.

Ce qu'il faut retenir

01 Le risque s'est déplacé de la forteresse vers les fournisseurs et les intégrations SaaS.

02 Un seul jeton OAuth surprivilégié peut exposer des dizaines d'organisations en cascade.

03 Inventorier les connecteurs, appliquer le moindre privilège, exiger des garanties vérifiables (ISO 27001, SOC 2).

03

03 · GÉOPOLITIQUE

La cyber comme arme

Représailles, hacktivisme, infrastructures

36 %

des incidents attribués relèvent de l'espionnage d'État ou de l'hacktivisme

Veille LuksMentis · H1 2026

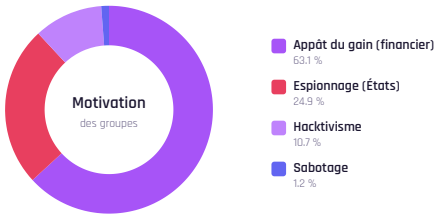
03 · GÉOPOLITIQUE

La cyber comme arme

Représailles, hacktivisme, infrastructures

> **EN BREF** L'appât du gain domine encore, mais l'espionnage d'État et l'hacktivisme remontent : plus d'un tiers des incidents attribués ont désormais une dimension géopolitique.

L'écrasante majorité des attaques reste motivée par l'**appât du gain** : 63 % des groupes que nous attribuons agissent pour l'argent. Mais le premier semestre 2026 a vu remonter une motivation qu'on croyait secondaire, la géopolitique. Espionnage d'État (25 %) et hacktivisme (11 %) forment désormais plus d'un tiers des incidents attribués.



Motivation des groupes attribués

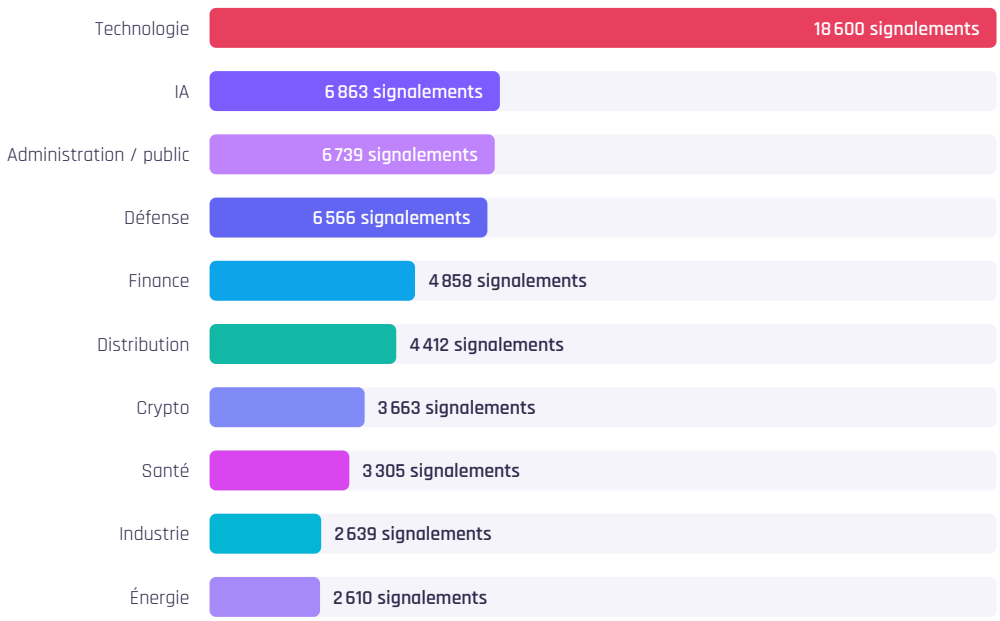
Veille LuksMentis · incidents à motivation connue · luksmentis.com · juin 2026

Le déclencheur est connu : après les frappes américano-israéliennes de février 2026 contre des cibles iraniennes, les chercheurs ont observé une vague de représailles cyber et de campagnes hacktivistes visant Israël, les États-Unis et leurs alliés. En mars, l'entreprise de technologie médicale Stryker a subi une attaque liée à un groupe hacktiviste pro-iranien, des employés voyant leurs postes effacés en temps réel. Notre base reflète cette activité : Anonymous reste le premier libellé hacktiviste de notre corpus, suivi de collectifs pro-russes comme NoName057(16) et Killnet.

En parallèle, la **Russie** demeure la menace la plus imminente pour les infrastructures critiques européennes, avec des attaques confirmées capables de toucher les systèmes énergétiques et hydrauliques de l'UE. Côté attribution d'origine, notre cartographie des groupes étatiques fait ressortir une douzaine de groupes liés à la **Chine** (espionnage), un noyau russe couvrant à la fois l'espionnage, l'opération financière et le sabotage, et des clusters iranien et nord-coréen.

La cible se déplace vers les fonctions vitales

Cette tension se lit dans les secteurs visés. Au-delà de la technologie, qui domine mécaniquement, la **défense** et l'**énergie** pèsent lourd dans notre flux, deux secteurs où une intrusion n'a pas qu'une valeur marchande, mais une valeur stratégique. Le brouillage entre criminalité crapuleuse et opération étatique, où un groupe « financier » sert parfois de couverture à un État, est l'une des évolutions les plus inquiétantes du semestre.



Secteurs les plus visés (volume de signalements, H1 2026)

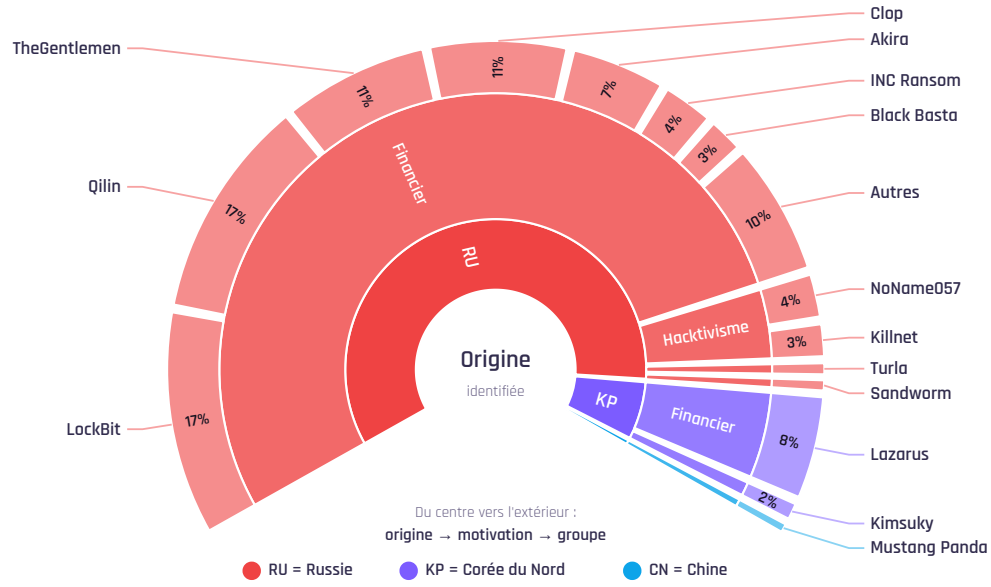
Veille LuksMentis · signalements sectorisés (étiquetage multiple possible) · luksmentis.com · juin 2026

Ce que ça change. Pour les opérateurs d'infrastructures, la menace n'est plus seulement l'extorsion mais le sabotage. La segmentation OT/IT, les plans de continuité et la préparation à un effacement destructif (wiper) sortent du registre théorique.

Origine, motivation, groupe. Sur les incidents dont l'origine est identifiable, trois logiques nationales ressortent :

- **Russie** : surtout financière (l'écosystème rançongiciel : LockBit, Qilin, Clop…), avec une frange hacktiviste pro-russe (NoName057, Killnet) et une pointe de sabotage étatique (Sandworm).
- **Corée du Nord** : presque exclusivement financière (Lazarus), complétée d'espionnage (Kimsuky).
- **Chine** : un profil d'espionnage assumé (Mustang Panda).

En somme, la criminalité financière est massivement russophone, le renseignement chinois et nord-coréen, et le sabotage reste une signature étatique rare. Cette lecture prolonge notre étude « Anatomie des groupes d'attaquants ».



Origine → motivation → groupe (principaux groupes)

Veille LuksMentis · principaux groupes dont l'origine est identifiable · 14 juin 2026 · luksmentis.com

Ce qu'il faut retenir

01 L'appât du gain reste majoritaire (63 %), mais la géopolitique remonte nettement.

02 Espionnage d'État et hacktivisme forment plus d'un tiers des incidents attribués.

03 Les infrastructures critiques deviennent une cible de représailles assumée.

04

04 · FUITES DE DONNÉES

L'inventaire du semestre

De la France au marché de la revente

61 %

des incidents qualifiés du semestre sont des fuites de données

Veille LuksMentis · H1 2026

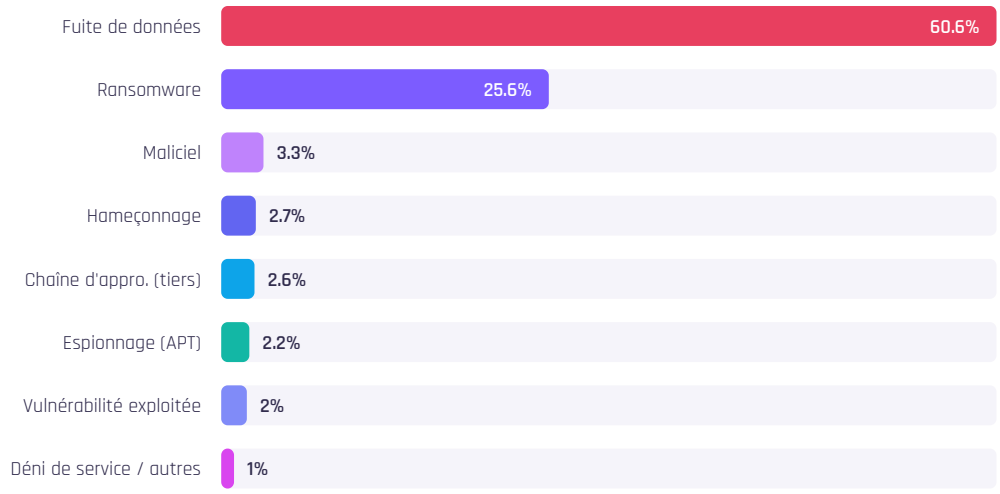
04 · FUITES DE DONNÉES

L'INVENTAIRE DU SEMESTRE

De la France au marché de la revente

EN BREF 2026 est l'année où voler la donnée prime sur la chiffrer : la fuite devient le premier type d'incident du semestre.

La fuite de données est, de loin, le premier type d'incident que nous reconstruisons : elle représente **61 %** des incidents qualifiés du semestre, devant le ransomware (26 %). 2026 est l'année où voler la donnée prime sur la chiffrer.

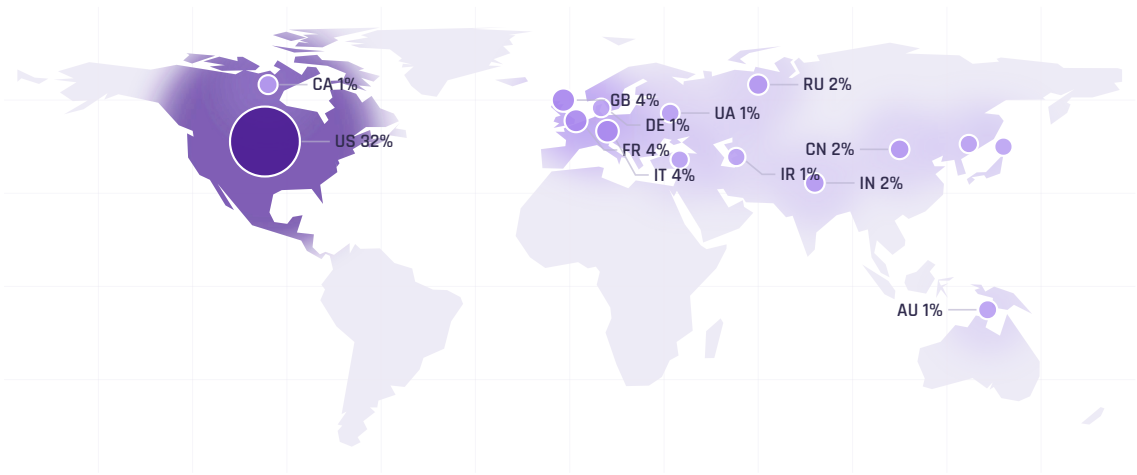


Composition des incidents par type d'attaque (H1 2026)

Veille LuksMentis · type dominant des incidents reconstitués (environ 6 300 incidents) · luksmentis.com · juin 2026

L'ampleur des cas marquants donne le vertige. France Titres (ANTS) a révélé le 20 avril 2026 un accès aux données de **11,7 millions de comptes** du portail ants.gouv.fr, avec l'arrestation d'un suspect de 15 ans. À l'international : Telus (700 To revendiqués par ShinyHunters), Under Armour (72 millions de comptes), Match Group, ou encore le registre national des comptes bancaires français. Un cas restera comme un signal faible majeur : une brèche dans le secteur de la santé a exposé les **empreintes digitales et palmaires biométriques de 1,8 million de personnes**, une donnée qu'on ne peut pas, contrairement à un mot de passe, réinitialiser.

La France n'est pas un angle mort de ce paysage : elle est le **quatrième pays le plus présent** dans notre flux géolocalisé, ce que documentait déjà notre étude sur la place de la France. Loin d'être épargnée, elle est une cible de premier plan.



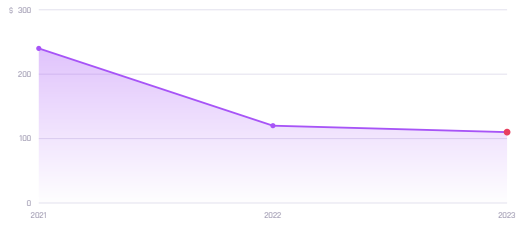
Où la menace se concentre : pays les plus visés (H1 2026)

Veille LuksMentis · part des signalements géolocalisés · luksmentis.com · juin 2026

Le prix de la donnée volée : un marché qui se scinde

Que deviennent ces données ? Elles se revendent, et leur prix raconte une histoire. Les index de prix du dark web (Privacy Affairs) montrent une **érosion continue** des tarifs de la donnée de masse : une carte bancaire volée adossée à un solde de 5 000 dollars valait 240 dollars en 2021, elle n'en vaut plus que 110 en 2023. La cause est une surabondance massive : plus de 2,8 milliards d'identifiants compromis circulaient sur les marchés en 2025, alimentés par les infostealers.

Mais le marché ne s'effondre pas : il se **scinde en deux**. D'un côté, la donnée brute (PII, cartes sans contexte) devient une commodité bradée à quelques dollars. De l'autre, ce qui est rare et directement monétisable prend de la valeur : un compte crypto vérifié se négocie 200 à 400 dollars, un accès administrateur privilégié dépasse les 1 000 dollars, et un dossier médical complet vaut environ dix fois une carte bancaire. La donnée biométrique, elle, échappe encore à toute grille de prix publique : son marché est opaque, ce qui n'est pas rassurant.



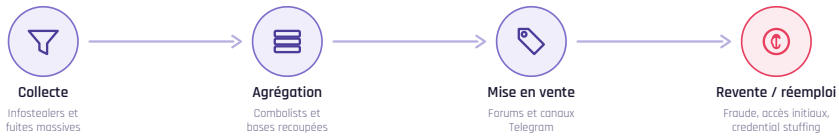
Le prix d'une carte bancaire volée (solde jusqu'à 5 000 $) s'effondre

Source : Privacy Affairs, Dark Web Price Index (éditions 2021, 2022, 2023) · luksmentis.com · juin 2026

Le marché de la donnée volée se scinde en deux (ordres de grandeur 2025)

DONNÉE REVENDUE	PRIX INDICATIF	TENDANCE
Identité brute / PII (nom + e-mail)	moins de 15 $	en baisse (surabondance)
Carte bancaire avec CVV	10 à 40 $	en baisse
Identité complète (« fullz »)	20 à 100 $	en baisse
Dossier médical / santé	250 à 310 $	stable (10 fois une carte)
Compte crypto vérifié	200 à 400 $	en hausse (raréfaction)
Accès admin / privilégié	plus de 1 000 $	en hausse (premium)

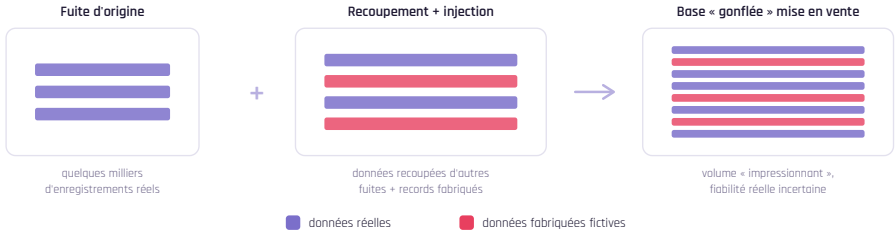
Sources : Privacy Affairs (2023) ; Biometric Update, deepstrike/Constella (2025-2026) · luksmentis.com · juin 2026



Le parcours de la donnée volée, de la collecte à la revente

Lecture LuksMentis · marché de la revente · H1 2026

Le « gonflage » en pratique. Certains opérateurs ne s'introduisent jamais dans le SI de l'entreprise visée. Ils partent d'identifiants déjà fuités ailleurs, les testent en masse sur de nombreux services (credential stuffing) et ne gardent que ceux qui fonctionnent encore, le plus souvent parce que la victime a réutilisé le même mot de passe. Ils assemblent alors une base qui a tout l'air authentique : l'échantillon « de preuve » contient de vrais comptes actifs, mais aucun ne provient réellement du système de l'entreprise. Cette base fabriquée est ensuite revendue, ou sert à réclamer une rançon en faisant croire à une intrusion qui n'a jamais eu lieu.



Infostealer : comment quelques fuites réelles sont « gonflées » pour la revente

Lecture LuksMentis · une base volumineuse mêle données réelles recoupées et records fabriqués · H1 2026

Ce qu'il faut retenir

01 La fuite de données est le premier type d'incident du semestre (61 %).

02 Voler la donnée prime désormais sur la chiffrer.

03 Le marché de la revente se structure, de la PII à bas prix aux accès premium.

05

05 · VULNÉRABILITÉS

Ce qui est réellement exploité

Le KEV plutôt que le CVSS

28 %

des failles réellement exploitées sont notées « moyenne » ou « basse » au CVSS

Veille LuksMentis · 3 867 CVE

05 · VULNÉRABILITÉS

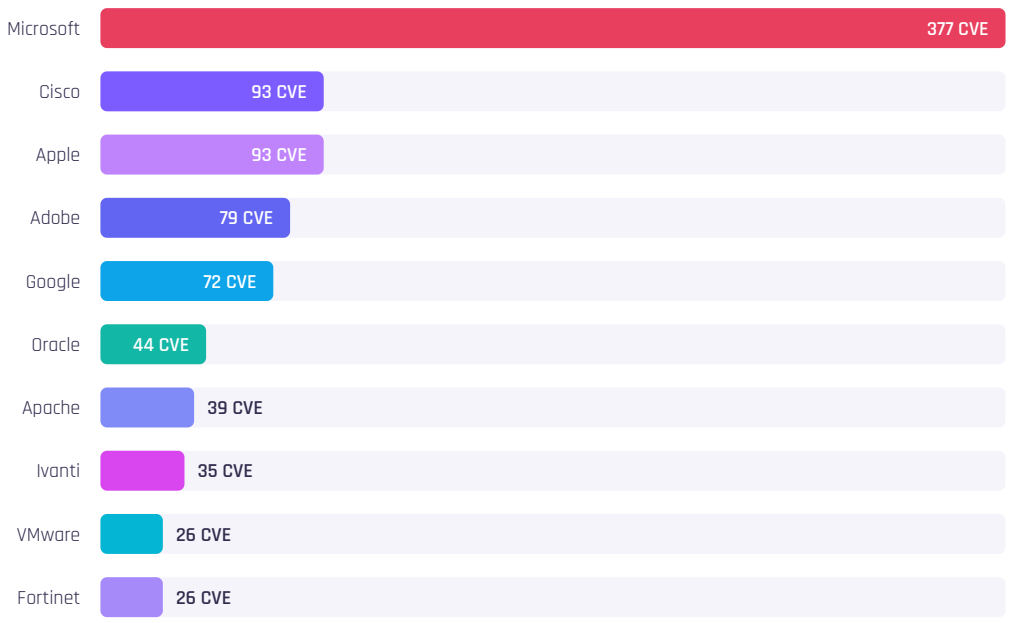
Ce qui est réellement exploité

Le KEV plutôt que le CVSS

EN BREF Le risque ne se lit pas dans le score CVSS mais dans l'exploitation réelle : le catalogue KEV redessine les priorités de correction.

En mars 2026, les attaquants ont activement exploité les pare-feux FortiGate comme vecteur d'accès initial, via des failles récentes dont **CVE-2026-24858**. Une campagne baptisée ClickFix a, elle, compromis plus de 700 sites en exploitant une injection SQL critique (CVE-2026-26980) dans le CMS Ghost. Deux rappels que la vulnérabilité n'est pas une abstraction : c'est la matière première de l'accès initial.

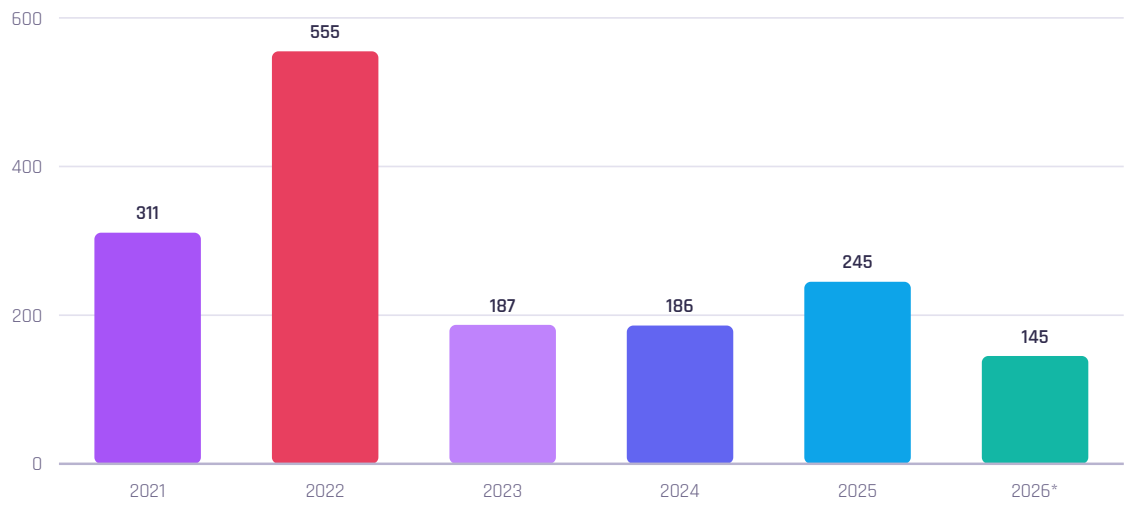
Notre miroir du catalogue KEV de la CISA suit **1 629 vulnérabilités confirmées comme activement exploitées**, dont 327 déjà instrumentalisées dans des campagnes de ransomware. La répartition par éditeur dessine la carte des points d'entrée du moment.



Éditeurs les plus représentés dans le catalogue KEV

Veille LuksMentis · miroir KEV (tous millésimes) · luksmentis.com · juin 2026

Microsoft domine par volume historique, mais ce sont les **équipements de bordure** qui font l'actualité : Cisco, Ivanti, Fortinet concentrent les ajouts récents. Sur le seul premier semestre 2026, nous avons vu défiler au KEV une cascade de failles Cisco Catalyst SD-WAN, FortiClient EMS et FortiOS, exactement les produits que The Gentlemen et consorts exploitent pour entrer. 145 CVE ont été ajoutées au catalogue depuis janvier.

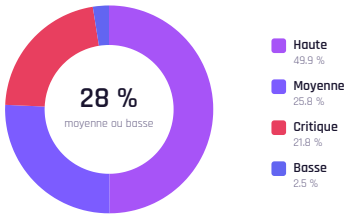


Vulnérabilités activement exploitées ajoutées au catalogue (par an)

Veille LuksMentis · miroir du catalogue KEV de la CISA (1 629 CVE suivies) · luksmentis.com · juin 2026

Le score CVSS ne mesure pas le risque

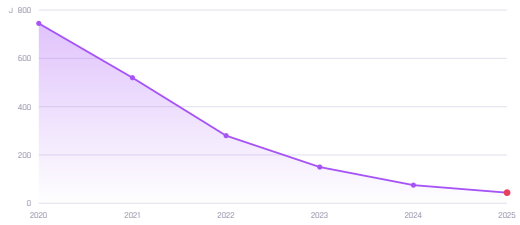
Le point le plus important de ce chapitre n'est pas un volume, c'est une méthode. Notre base compte plus de 440 CVE publiées en 2026, toutes notées « haute » ou « critique », mais parmi l'ensemble des failles que nous suivons, près de **28 % sont notées « moyenne » ou « basse »**. Or la sévérité CVSS, calculée en isolation, ne dit rien de l'exploitation réelle.



Répartition par sévérité des CVE dotées d'un score CVSS v3

Veille LuksMentis · 3 867 CVE scorées · luksmentis.com · juin 2026

C'était déjà la thèse de notre analyse sur les vulnérabilités mineures, publiée début juin : moins d'une vulnérabilité « critique » sur cinq est réellement exploitée, tandis que des failles « moyennes » deviennent le maillon décisif d'une chaîne d'attaque. Quelques semaines plus tard, la CISA est venue conforter cette analyse de la façon la plus nette qui soit. Sa nouvelle directive **BOD 26-04, « Prioritizing Security Updates Based on Risk »**, a révoqué l'historique BOD 22-01 pour fonder la priorisation non plus sur le score CVSS, mais sur le risque réel : exposition de l'actif, présence au catalogue KEV, capacité d'automatisation de l'exploit et impact technique. Que l'agence retienne explicitement l'automatisation de l'exploit comme critère rejoint mot pour mot notre constat sur l'effet de l'IA. La bonne question n'est plus « cette faille est-elle critique ? », mais « est-elle exploitée, exposée, et atteignable ? ».



Délai moyen avant exploitation (time to exploit)

Source : Flashpoint, N-Day Vulnerability Trends (-94 % en 5 ans) · luksmentis.com · juin 2026

Car l'IA a réécrit l'équation. Le délai moyen avant exploitation est passé de 745 jours en 2020 à 44 jours en 2025 (Flashpoint), et un agent autonome peut désormais exploiter une faille connue pour quelques dollars. Le stock de vulnérabilités « mineures » qu'une organisation laisse traîner n'est plus un risque dormant : c'est une dette à intérêts composés.

06

06 · TRANSVERSAL

L'IA qui industrialise le vol

Le multiplicateur de toutes les tendances

96 %

taux d'exfiltration réussie au T1 2026, l'IA à la manoeuvre

Infosecurity Magazine · T1 2026

06 · TRANSVERSAL

L'IA qui industrialise le vol

Le multiplicateur de toutes les tendances

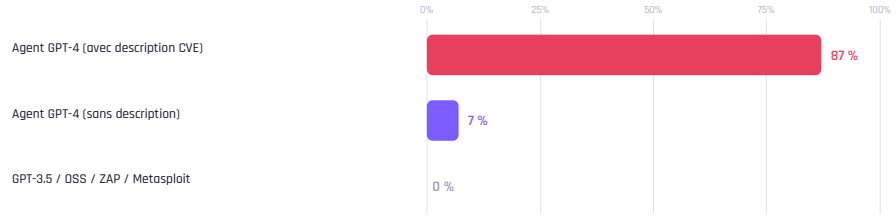
EN BREF L'IA ne crée pas de nouvelle menace : elle accélère et industrialise toutes les autres, du tri des données volées à l'exploitation des failles.

Une force traverse les cinq chapitres précédents : l'**intelligence artificielle**. Elle ne crée pas de nouvelle menace ; elle accélère et automatise toutes les autres. Au premier trimestre 2026, le taux d'exfiltration réussie aurait atteint 96 %, avec en moyenne 743 Go volés par incident non divulgué, et des plateformes criminelles comme LotAI ou ClawdBot montrent comment l'IA automatise désormais le tri et la priorisation des données volées.

Côté attaquant, l'IA abaisse le coût de l'exploitation (chapitre 5), trie les logs d'infostealers en quelques secondes pour en extraire les accès à forte valeur (chapitre 4), et démultiplie la reconnaissance OAuth (chapitre 2). Côté défense, elle découvre les failles plus vite qu'on ne les corrige : le programme Glasswing d'Anthropic a identifié plus de 10 000 vulnérabilités critiques ou élevées en deux mois, dont plus de 99 % non corrigées à l'annonce. La découverte n'est plus le goulot d'étranglement, la remédiation l'est.

Cette nouvelle surface a son propre référentiel de risques, que détaille notre panorama OWASP LLM : injection de prompt, fuite de données vers les LLM, agents trop autonomes, RAG empoisonné. Sécuriser l'usage de l'IA en interne est devenu une discipline à part entière, au même titre que sécuriser un SI classique.

Ce que l'IA change concrètement. Un agent bâti sur GPT-4 a exploité seul 87 % d'un jeu de failles « one-day » à partir de la seule description CVE, là où GPT-3.5, huit modèles open source et les scanners ZAP et Metasploit obtenaient 0 %. Privé de la description, le taux tombe à 7 % : l'IA excelle à **exploiter** une faille connue, bien plus qu'à en **découvrir** une nouvelle. Coût moyen d'un exploit réussi : 8,80 dollars, contre 25 pour un pentester humain, et l'agent est massivement parallélisable.



Taux de réussite d'exploitation autonome de failles « one-day »

Source : Fang, Bindu, Gupta, Kang (UIUC), arXiv:2404.08144 · luksmentis.com

Ce qu'il faut retenir

01 L'IA n'invente pas de menace : elle accélère et automatise toutes les autres.

02 Le délai avant exploitation s'effondre, de 745 jours en 2020 à 44 jours en 2025.

03 Tri des données volées, exploitation des failles, exfiltration : tout s'industrialise.

07

07 · POUR LES ÉQUIPES

Priorités et perspectives

Ce que ça implique pour les équipes (RSSI)

KEV

concentrer l'effort là où les chaînes d'attaque se brisent réellement

Principe directeur · BOD 26-04

07 · POUR LES ÉQUIPES

Priorités et perspectives

Ce que ça implique pour les équipes sécurité (RSSI)

> **EN BREF** Concentrer l'effort là où les chaînes d'attaque se brisent réellement, plutôt que d'empiler des outils en aval.

Que faire de ce panorama ? Les priorités qui se dégagent pour les responsables sécurité ne forment pas une liste de cases à cocher : elles découlent directement de ce que le semestre a montré, et obéissent à un même principe : concentrer l'effort là où les chaînes d'attaque se brisent réellement, plutôt que d'empiler des outils en aval.

La première porte à refermer reste la **bordure**. VPN, pare-feux et passerelles concentrent l'accès initial des groupes dominants ; un inventaire exhaustif, un correctif appliqué sous quelques jours dès qu'une faille entre au KEV, et une exposition Internet réduite au strict nécessaire valent mieux que n'importe quelle défense ajoutée ensuite. Dans le même mouvement, il devient vital de **reprendre la main sur les intégrations tierces** : cartographier les connecteurs OAuth, leur imposer le moindre privilège, faire tourner et révoquer les secrets, exiger des fournisseurs critiques des garanties vérifiables (ISO 27001, SOC 2). Un tiers sur trois est désormais dans la boucle des compromissions ; la confiance accordée n'est pas un contrôle de sécurité.

Sur les vulnérabilités, le réflexe à installer est de **prioriser par l'exploitabilité plutôt que par le CVSS**, en croisant statut KEV, exploit public et score EPSS : une faille « moyenne » réellement exploitée doit passer avant une « critique » isolée derrière plusieurs couches de segmentation. La montée géopolitique impose en parallèle de **se préparer au destructif** : pour les opérateurs sensibles, le scénario du wiper n'est plus théorique, ce qui remet au premier plan les sauvegardes immuables, la restauration réellement testée et la séparation OT/IT.

Face à l'industrialisation par l'IA, enfin, deux postures s'imposent. D'abord, **considérer toute donnée volée comme déjà revendue** : plutôt que d'espérer qu'une fuite reste confidentielle, miser sur la détection d'usage des identifiants compromis et sur une authentification résistante à l'hameçonnage. Ensuite, **gouverner l'usage interne de l'IA**, c'est-à-dire encadrer ce que collaborateurs et agents peuvent faire avec les LLM avant que cette surface ne devienne un angle mort. Au-delà de ces priorités, une piste plus structurante mérite d'être posée : pour les données les plus critiques, la meilleure protection contre la défaillance d'un tiers reste encore de ne pas en dépendre, en réinternalisant ce qui peut l'être.

Aucune organisation n'est invulnérable. Mais, comme nous l'écrivions à propos de la sécurité des tiers, on ne peut pas se revendiquer victime si l'on n'a pas mis les moyens de se protéger. Le premier semestre 2026 ne dit pas que la menace est imparable : il dit où porter l'effort.

Sources citées

Veille LuksMentis (données primaires, requêtes juin 2026).

Verizon, 2025 Data Breach Investigations Report (part des tiers).

IBM, Cost of a Data Breach Report 2025 (coût, délai supply chain).

Flashpoint, N-Day Vulnerability Trends (time to exploit).

Rapid7, 2026 Global Threat Landscape Report.

Privacy Affairs, Dark Web Price Index (éditions 2021 à 2023).

Biometric Update ; deepstrike, Constella (prix de revente et infostealers, 2025-2026).

CISA, BOD 26-04 « Prioritizing Security Updates Based on Risk » (révoque BOD 22-01) ; catalogue KEV : cisa.gov.

ScienceDirect (consolidation du ransomware, concentration du top 10).

Infosecurity Magazine (taux d'exfiltration, volumes volés).

Presse spécialisée : PurpleSec, La Nouvelle Tribune, Factoria, Quiver Quantitative, Techtime, Franceinfo.

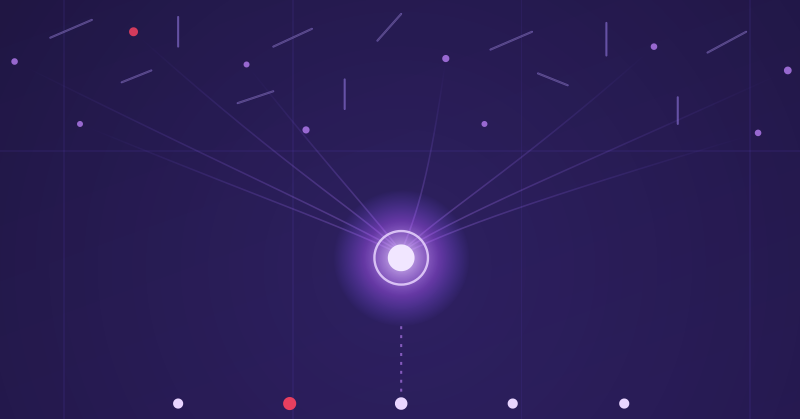
Articles LuksMentis : Anatomie des groupes d'attaquants ; Sécurité des tiers ; Vulnérabilités mineures ; Panorama OWASP LLM (luksmentis.com/blog).

À propos de ce rapport

Rapport produit par LuksMentis à partir de sa veille cyber propriétaire (près de 64 000 signalements qualifiés de janvier à juin 2026) et des sources externes listées ci-dessus. Les figures marquées « Veille LuksMentis » s'appuient sur nos données internes. Les attributions reposent souvent sur des sources ouvertes et n'ont pas valeur de preuve judiciaire. © LuksMentis 2026, luksmentis.com, reproduction et réexploitation soumises à autorisation.

LuksMentis

CYBER THREAT INTELLIGENCE



Scrape the noise.
Extract intelligence.

Recevez gratuitement **l'essentiel de la menace cyber**, chaque jour.

S'inscrire gratuitement · luksmentis.com

Newsletter gratuite · résumés quotidiens.

---

luksmentis.com · Veille cyber souveraine

© LuksMentis 2026 · Reproduction et réexploitation soumises à autorisation