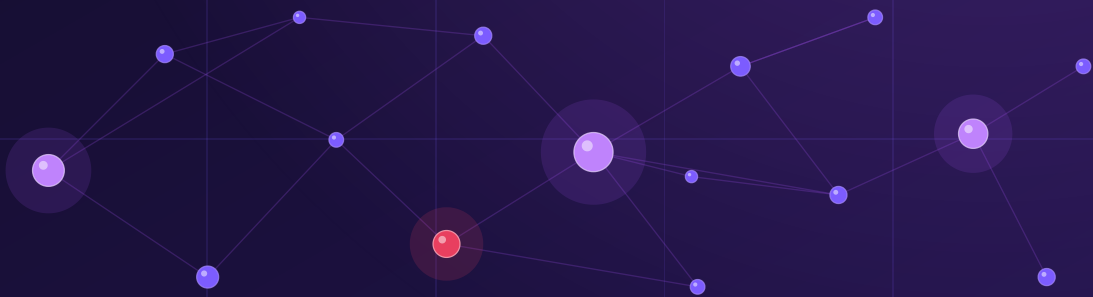


JUNE 2026 REPORT

THE STATE OF THE CYBER THREAT

The first half of 2026, read through our threat-watch data.



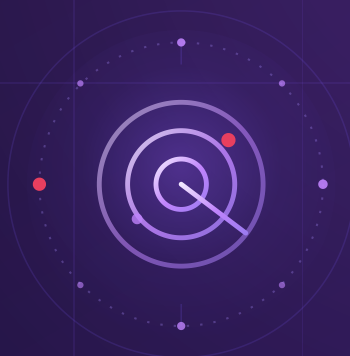
JANUARY TO JUNE 2026

LUKSMENTIS

Sovereign cyber watch · luksmentis.com

CONTENTS

00	A semester of reckoning Editorial: what our data says	3
01	The age of consolidation Ransomware: fewer groups, more victims	5
02	One supplier, dozens of victims Third parties & OAuth: the ShinyHunters saga	8
03	Cyber as a weapon Geopolitics: reprisals and infrastructure	11
04	The inventory of the semester Data breaches: from France to resale	15
05	What is actually exploited Vulnerabilities: KEV over CVSS	19
06	The AI that industrialises theft Cross-cutting: the multiplier of trends	22
07	Priorities and outlook What it means for security teams	24



00 • EDITORIAL

A SEMESTER OF RECKONING

What our data says

64 000

major cyber signals consolidated over six months

LuksMentis watch • Jan to Jun 2026

A SEMESTER OF RECKONING

What our data says

The first half of 2026 will not be remembered for a single attack, but for three underlying shifts that reinforce one another: a ransomware market that **concentrates** around a handful of actors, the return of cyber as an extension of geopolitical conflict, and the industrialisation, through artificial intelligence, of the theft and resale of data.

Our watch has consolidated nearly **64,000 major cyber signals** since 1 January 2026: incidents, vulnerability disclosures, data breaches, group claims. From that flow, we continuously recons-

truct **incidents** linking an identified attacker to a named victim: more than 14,500 to date, covering 10,200 distinct organisations. This raw material, and not a selection of spectacular events, is what informs the pages that follow.

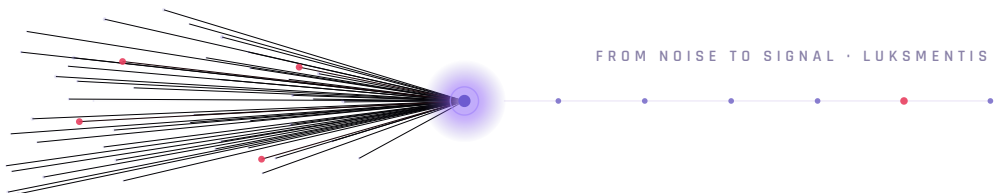
The overall picture is clear. Ransomware and data theft saturate the landscape; edge devices (VPNs, firewalls) remain the favoured entry point; and a single weak link, a supplier or a forgotten OAuth token, is now enough to compromise dozens of organisations in cascade. This report breaks these dynamics into six chapters, each grounded in our figures and set against the major sector reports.

The semester in figures (LuksMentis, January to June 2026)

INDICATOR	VALUE
Qualified cyber signals	nearly 64,000
Reconstructed incidents (attacker to victim)	14 500
Distinct named victims	10 200
Ransomware claims (leak sites)	1,592 / 79 groups
Actively exploited CVEs tracked (KEV)	1 629
of which weaponised in ransomware	327

LuksMentis watch · luksmentis.com · June 2026

A note on method. Our figures reflect a **watch**, not an exhaustive census of the global threat. Our system captures a very large volume of raw signals every day; we analyse, cross-check and triage them to use only information from verifiable sources and to discard the background noise. The figures here therefore cover that qualified flow, not the raw collection. We reason in rankings and shares rather than absolute volumes. Finally, attribution of a group or a country often relies on open sources: it indicates who **claims** or is credited with an attack, not judicial proof.





01 · RANSOMWARE

THE AGE OF CONSOLIDATION

Fewer groups, more victims

71 %

of victims concentrated by the top 10 ransomware groups

ScienceDirect · Q1 2026

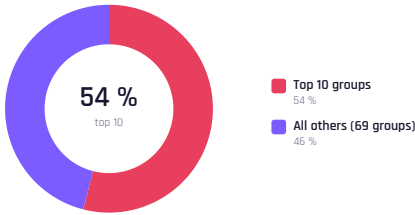
THE AGE OF CONSOLIDATION

Fewer groups, more victims

IN BRIEF After two years of fragmentation, the ransomware market reconcentrates: fewer groups, but more industrial, and more victims.

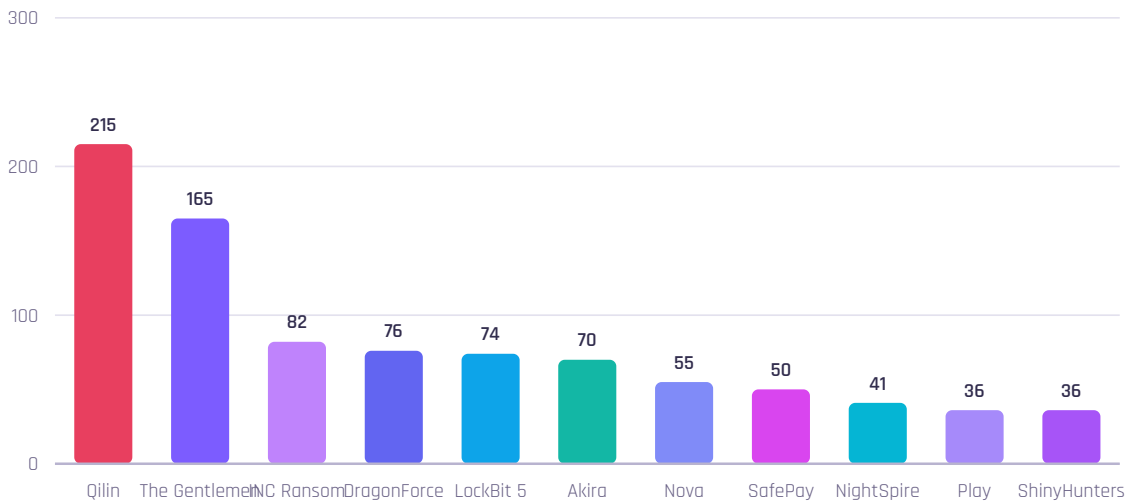
For two years the ransomware market had **fragmented**: the takedowns of LockBit and ALPHV/BlackCat had scattered affiliates into a myriad of small franchises. The first half of 2026 reverses the trend. The market **reconcentrates** around a handful of industrial actors. Globally, the first quarter of 2026 saw more than 2,100 victims listed on leak sites, and the top 10 groups now account for roughly **71% of victims**, up from 57% (ScienceDirect).

Our sample confirms it in its own measure. Across 1,592 claims observed on leak sites since late January, spread over 79 groups, the ten most active account for **54%** of victims. The gap with the global 71% reflects our collection coverage; the **direction** is the same: value shifts towards the top of the ranking.



Concentration: share of the top 10 groups

LuksMentis watch · 2026 leak-site sample (vs 71% of the global market, ScienceDirect) · luksmentis.com · June 2026



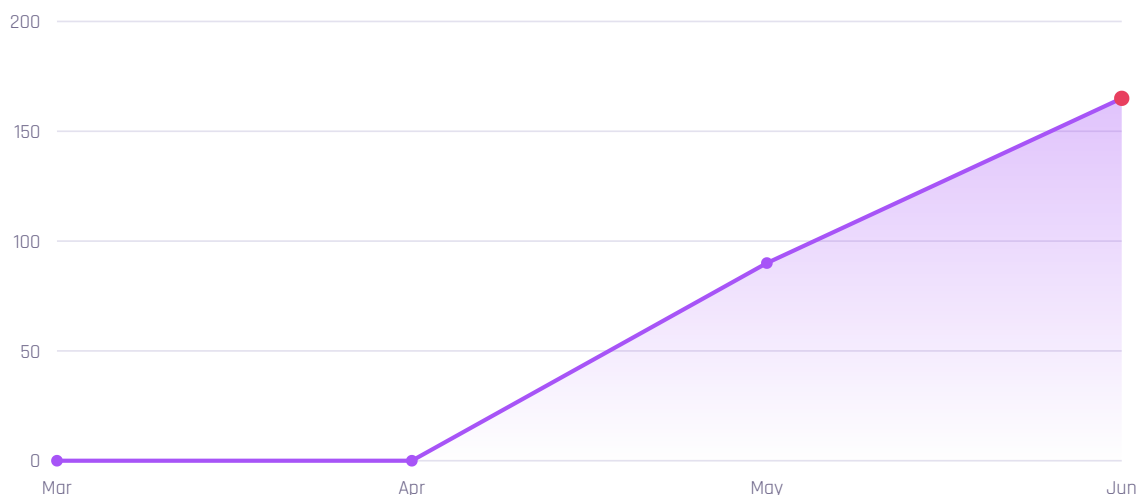
Top ransomware groups by claims (leak sites, 2026)

LuksMentis watch · leak-site claims, January to June 2026 (1,592 total) · luksmentis.com · June 2026

At the top, **Qilin** stands out as the most prolific group, a third consecutive quarter of dominance. Its aggressive affiliate model and its permanence make it the centre of gravity of the market. Behind it, the ranking mixes established names (INC Ransom, DragonForce, Akira, Play) with a new generation of franchises (Nova, SafePay, NightSpire), a sign of an ecosystem reshaping rather than calming down.

The Gentlemen: the revelation of the semester

No trajectory illustrates this reshaping better than **The Gentlemen**. Emerging in August 2025, the group went from around thirty victims in the last quarter of 2025 to **182 in the first quarter of 2026**, climbing to second most active actor. In our own leak-site tracking it also ranks second, with 165 claims. Its signature: a professional, almost corporate approach, and heavy exploitation of edge devices (FortiOS, SonicWall VPN, Cisco ASA). It is the typical 2026 newcomer: not a band of amateurs, but a seasoned organisation industrialising initial access through infrastructure flaws.



The Gentlemen surge: claimed victims, cumulative monthly 2026

LuksMentis watch · cumulative leak-site claims (the group only enters our tracking in spring 2026) · luksmentis.com · June 2026

This landscape lines up precisely with our study « [Anatomy of attacker groups](#) », which already mapped the dominance of financial actors and the rise of newcomers. The consolidation observed here is its logical sequel: ransomware-as-a-service matures, and in a criminal economy, maturity means concentration.

What it changes. Against a concentrated market, defense gains clarity: monitoring the TTPs of the top ten groups covers most of the real risk. But concentration also increases each dominant actor's **capacity**, more affiliates, more tools, more pressure. Patching edge devices is no longer hygiene, it is the front line.

KEY TAKEAWAYS

- 01** The ransomware market reconcentrates: fewer groups, but more industrial.
- 02** The top 10 captures roughly 71% of global victims, up from 57%.
- 03** Defense priority shifts towards the dominant actors and their access vectors.



02 · THIRD PARTIES & OAUTH

ONE SUPPLIER, DOZENS OF VICTIMS

The ShinyHunters saga

237

reconstructed incidents for ShinyHunters, the most present actor in the corpus

LuksMentis watch · H1 2026

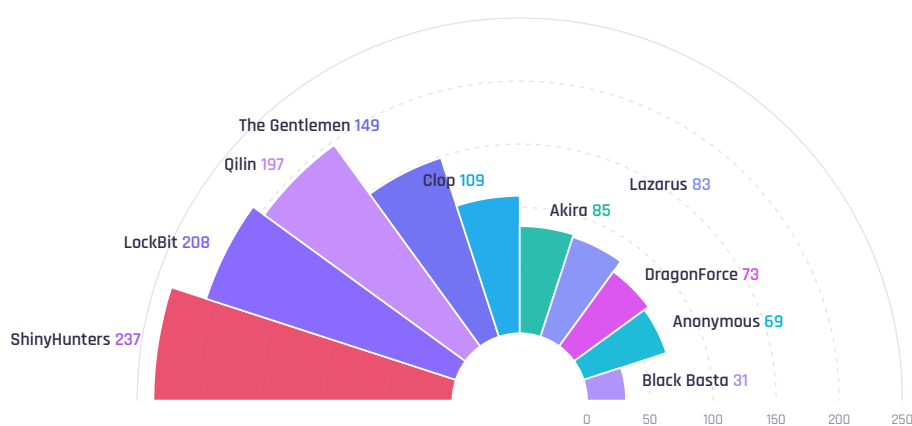
ONE SUPPLIER, DOZENS OF VICTIMS

The ShinyHunters saga

IN BRIEF Compromise no longer targets the fortress but its suppliers: a single OAuth token at a trusted third party is enough to expose dozens of organisations.

If one actor sums up the through-line of 2026, it is **ShinyHunters**. In our data, across all reconstructed incidents, it is the most

present group in the corpus, ahead of LockBit and Qilin. Its hallmark is not encryption, but **large-scale data theft**, often via a trusted third party.



Most active actors, across all reconstructed incidents

LuksMentis watch · attributed incidents (named groups, excluding generic labels) · luksmentis.com · June 2026

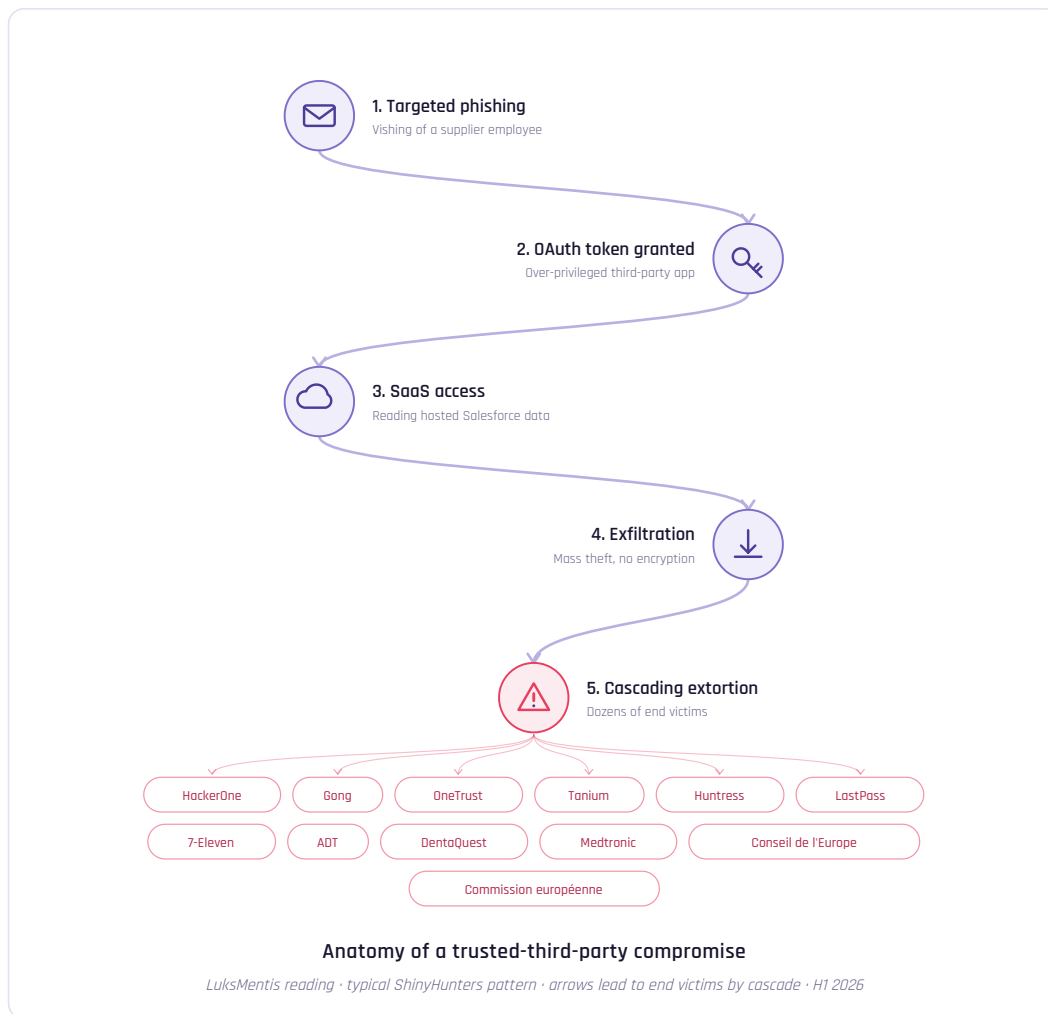
The modus operandi that defined the semester comes down to one word: **OAuth**. After the 2025 Salesloft Drift wave, a third-party app connected to Salesforce whose stolen tokens exposed more than 700 organisations, the mechanism repeated in 2026. In June, a group operating as Icarus exploited an OAuth integration via the Klue tool to siphon Salesforce data from several security firms themselves: HackerOne, Gong, OneTrust, Tanium, Huntress, LastPass. ShinyHunters also hit 7-Eleven, and Medtronic confirmed a claimed theft of more than 9 million records.

These names are not theoretical for us: they are among the victims our watch attributed to ShinyHunters this semester, Instructure, 7-Eleven, ADT, DentaQuest, the Council of Europe, Medtronic, the European Commission. The common denominator is never the victim's fortress, but the **excessive permission** once granted to a third-party application.

The weak link is not in the fortress

This is exactly the thesis of [our article on third-party security](#): nearly one in three breaches now involves a third party (30%, up from 15% a year earlier per Verizon's 2025 DBIR), and these intrusions are the slowest to detect, 267 days on average (IBM). Data is no longer stolen by breaching a wall, but by borrowing a **trust tunnel** you opened yourself. A forgotten OAuth token, a never-revoked service account: the aggravating factor is organisational before it is technical.

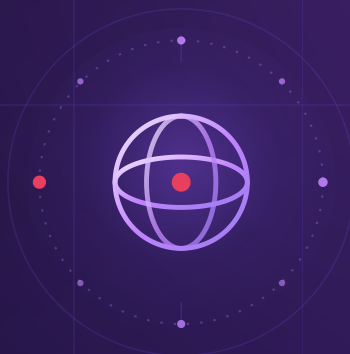
What it changes. The attack surface has shifted to SaaS and integrations. Inventory your OAuth connectors, apply least privilege to third-party apps, rotate and revoke secrets, demand verifiable guarantees from suppliers (ISO 27001, SOC 2): these are no longer comforts, they are the new foundations.



How to read this diagram. A trusted supplier is first compromised by phishing; an over-permissive OAuth token then opens access to its SaaS data. The attacker exfiltrates en masse, without encryption, then triggers the leverage effect: a single intrusion at the supplier propagates in cascade to dozens of end clients. This is the typical pattern of the ShinyHunters saga.

KEY TAKEAWAYS

- 01** Risk has shifted from the fortress to suppliers and SaaS integrations.
- 02** A single over-privileged OAuth token can expose dozens of organisations in cascade.
- 03** Inventory connectors, apply least privilege, demand verifiable guarantees (ISO 27001, SOC 2).



03 · GEOPOLITICS

CYBER AS A WEAPON

Reprisals, hacktivism, infrastructure

36 %

of attributed incidents involve state espionage or
hacktivism

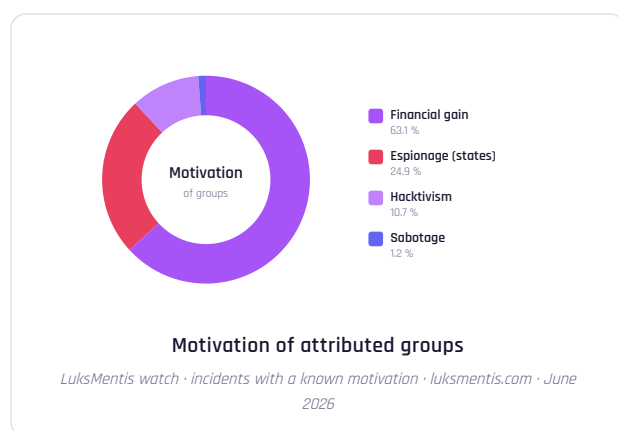
LuksMentis watch · H1 2026

CYBER AS A WEAPON

Reprisals, hacktivism, infrastructure

IN BRIEF Financial gain still dominates, but state espionage and hacktivism are rising: more than a third of attributed incidents now carry a geopolitical dimension.

The overwhelming majority of attacks remain motivated by **financial gain**: 63% of the groups we attribute act for money. But the first half of 2026 saw a motivation long thought secondary resurface, geopolitics. State espionage (25%) and hacktivism (11%) now make up more than a third of attributed incidents.



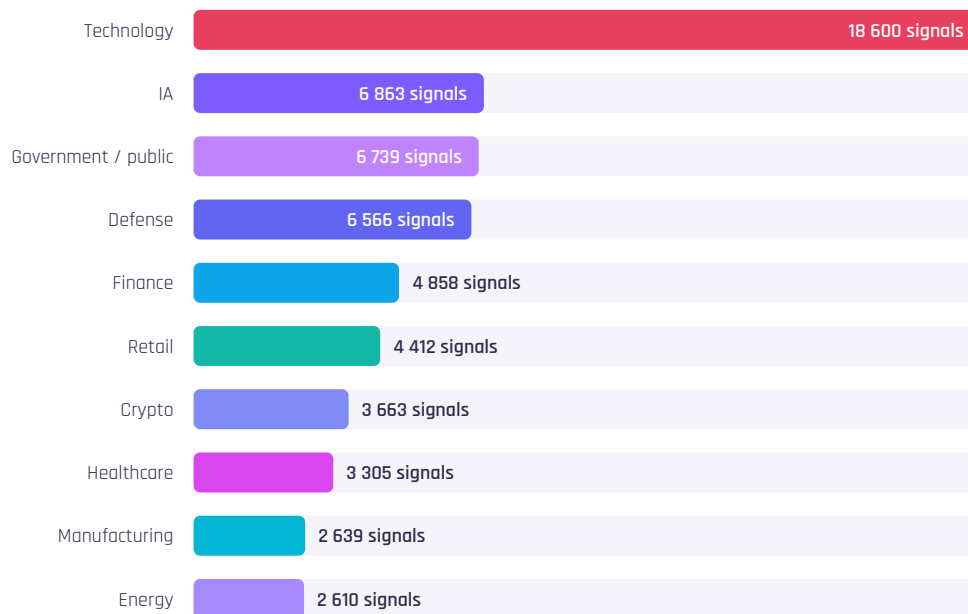
The trigger is known: after the February 2026 US-Israeli strikes on Iranian targets, researchers observed a wave of cyber reprisals and hacktivist campaigns against Israel, the United States and

their allies. In March, medical technology firm Stryker suffered an attack linked to a pro-Iranian hacktivist group, with employees watching their machines wiped in real time. Our base reflects this activity: Anonymous remains the leading hacktivist label in our corpus, followed by pro-Russian collectives such as NoName057(16) and Killnet.

In parallel, **Russia** remains the most imminent threat to European critical infrastructure, with confirmed attacks capable of hitting the EU's energy and water systems. On origin attribution, our mapping of state groups brings out a dozen groups linked to **China** (espionage), a Russian core spanning espionage, financial operations and sabotage, and Iranian and North Korean clusters.

The target shifts towards vital functions

This tension shows in the targeted sectors. Beyond technology, which dominates mechanically, **defense** and **energy** weigh heavily in our flow, two sectors where an intrusion carries not just market value but strategic value. The blurring between common crime and state operation, where a « financial » group sometimes serves as cover for a state, is one of the most worrying developments of the semester.



Most targeted sectors (signal volume, H1 2026)

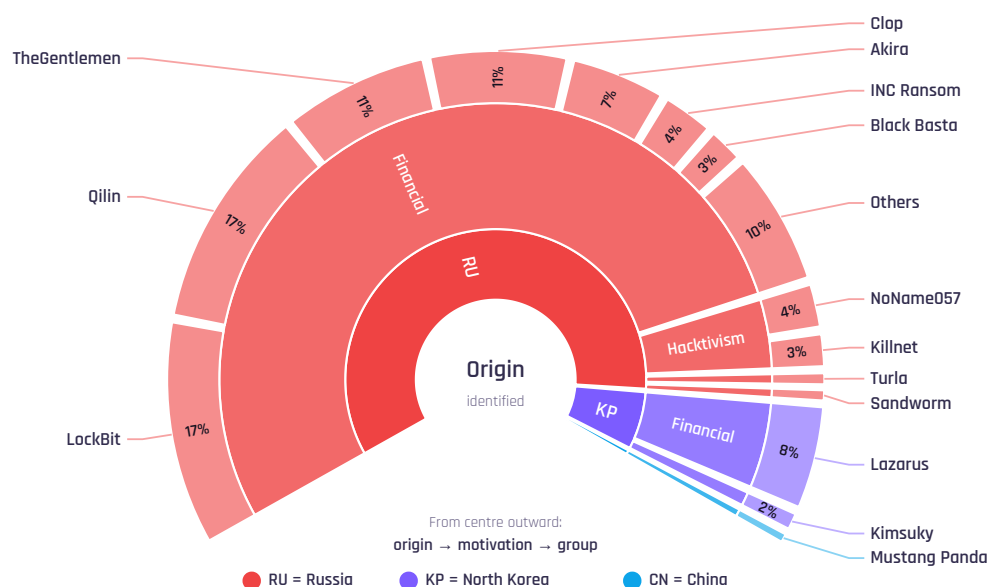
LuksMentis watch · sectorised signals (multiple tagging possible) · luksmentis.com · June 2026

What it changes. For infrastructure operators, the threat is no longer only extortion but **sabotage**. Network segmentation (OT/IT), continuity plans and readiness for a destructive wipe (wiper) leave the realm of theory.

Origin, motivation, group. Across incidents whose origin is identifiable, three national logics stand out:

- **Russia:** mostly financial (the ransomware ecosystem: LockBit, Qilin, Clap...), with a pro-Russian hacktivist fringe (NoName057, Killnet) and a touch of state sabotage (Sandworm).
- **North Korea:** almost exclusively financial (Lazarus), complemented by espionage (Kimsuky).
- **China:** an assumed espionage profile (Mustang Panda).

In short, financial crime is overwhelmingly Russophone, intelligence gathering Chinese and North Korean, and sabotage remains a rare state signature. This reading extends our study « [Anatomy of attacker groups](#) ».



Origin → motivation → group (main groups)

LuksMentis watch · main groups whose origin is identifiable · 14 June 2026 · luksmentis.com

KEY TAKEAWAYS

- 01 Financial gain remains the majority (63%), but geopolitics is clearly rising.
- 02 State espionage and hacktivism make up more than a third of attributed incidents.
- 03 Critical infrastructure becomes an assumed target for reprisals.



04 · DATA BREACHES

THE INVENTORY OF THE SEMESTER

From France to the resale market

61 %

of the semester's qualified incidents are data breaches

LuksMentis watch · H1 2026

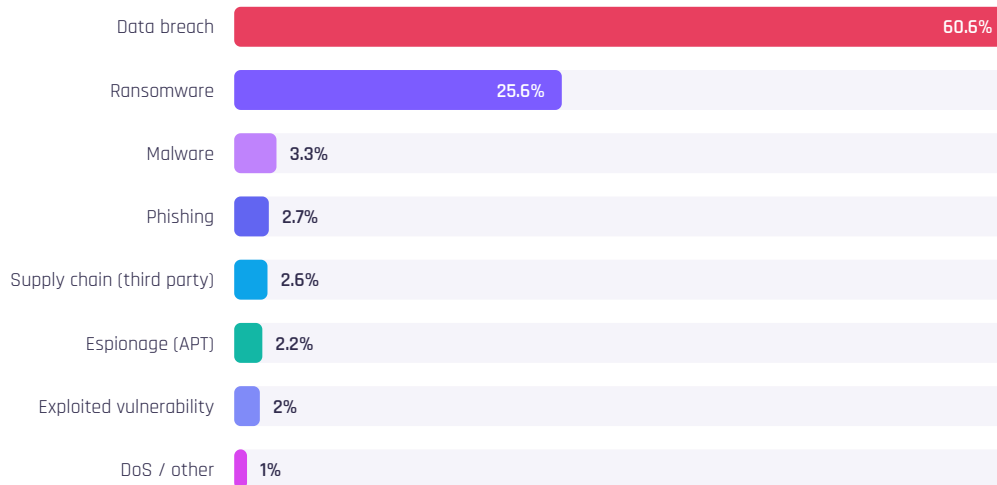
THE INVENTORY OF THE SEMESTER

From France to the resale market

IN BRIEF 2026 is the year stealing data takes precedence over encrypting it: the breach becomes the leading incident type of the semester.

The data breach is, by far, the leading incident type we reconstruct: it represents **61%** of the qualified incidents of the semester,

ahead of ransomware (26%). 2026 is the year stealing data takes precedence over encrypting it.



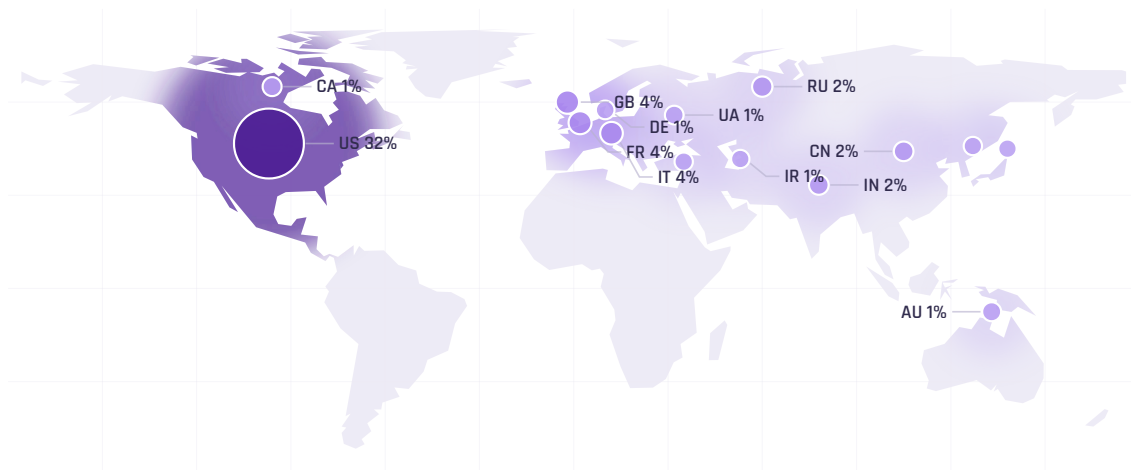
Incident breakdown by attack type (H1 2026)

LuksMentis watch · dominant type of reconstructed incidents (about 6,300 incidents) · luksmentis.com · June 2026

The scale of the standout cases is staggering. France Titres (ANTS) disclosed on 20 April 2026 a breach of **11.7 million accounts** on the ants.gouv.fr portal, with the arrest of a 15-year-old suspect. Internationally: Telus (700 TB claimed by ShinyHunters), Under Armour (72 million accounts), Match Group, and the French national bank-account registry. One case will stand as a major warning: a health-care breach exposed the **fingerprints and palm-print biometrics**

of 1.8 million people, data that, unlike a password, cannot be reset.

France is no blind spot in this picture: it is the **fourth most present country** in our geolocated flow, as [our study on France's place](#) already documented. Far from being spared, it is a prime target.



Where the threat concentrates: most targeted countries (H1 2026)

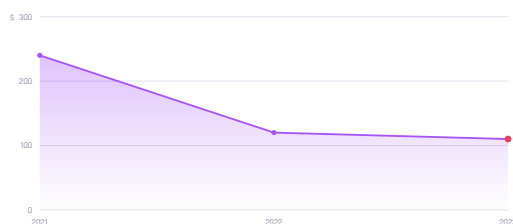
LuksMentis watch · share of geolocated signals · luksmentis.com · June 2026

The price of stolen data: a market that splits

What becomes of this data? It is resold, and its price tells a story. Dark-web price indexes (Privacy Affairs) show a **steady erosion** of bulk-data prices: a stolen payment card backed by a \$5,000 balance was worth \$240 in 2021, only \$110 in 2023. The cause is massive oversupply: more than 2.8 billion compromised credentials circulated on the markets in 2025, fed by infostealers.

But the market does not collapse: it **splits in two**. On one side, raw data (PII, context-less cards) becomes a commodity sold for a few dollars. On the other, what is rare and directly monetisable gains value: a verified crypto account trades for \$200 to \$400, privileged admin access tops \$1,000, and a full medical record is worth about ten times a payment card. Biometric data, for its part, still es-

caping any public pricing grid, its market is opaque, which is not reassuring.



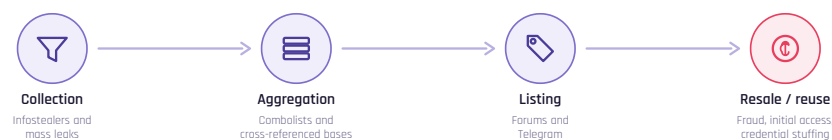
The price of a stolen payment card (balance up to \$5,000) collapses

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

The stolen-data market splits in two (2025 ballpark)

RESOLD DATA	INDICATIVE PRICE	TREND
Raw identity / PII (name + email)	under \$15	down (oversupply)
Payment card with CVV	\$10 to \$40	down
Full identity (fullz)	\$20 to \$100	down
Medical / health record	\$250 to \$310	stable (10x a card)
Verified crypto account	\$200 to \$400	up (scarcity)
Admin / privileged access	over \$1,000	up (premium)

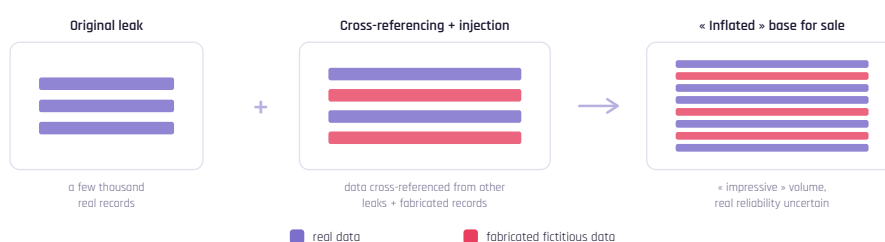
Sources : Privacy Affairs (2023) ; Biometric Update, deepstrike/Constella (2025-2026) · luksmentis.com · June 2026



The journey of stolen data, from collection to resale

LuksMentis reading · resale market · H1 2026

« **Inflation** » in practice. Some operators never break into the target company's systems. They start from credentials already leaked elsewhere, test them en masse across many services (credential stuffing) and keep only those that still work, most often because the victim reused the same password. They then assemble a base that looks entirely authentic: the « proof » sample contains real active accounts, but none actually comes from the company's system. This fabricated base is then resold, or used to demand a ransom by pretending an intrusion that never happened.



Infostealer: how a few real leaks are « inflated » for resale

LuksMentis reading · a bulky base mixes cross-referenced real data and fabricated records · H1 2026

KEY TAKEAWAYS

- 01 The data breach is the leading incident type of the semester (61%).
- 02 Stealing data now takes precedence over encrypting it.
- 03 The resale market is structuring, from cheap PII to premium access.



05 · VULNERABILITIES

WHAT IS ACTUALLY EXPLOITED

KEV over CVSS

28 %

of actually exploited flaws are rated « medium » or « low »
in CVSS

LuksMentis watch · 3,867 CVEs

WHAT IS ACTUALLY EXPLOITED

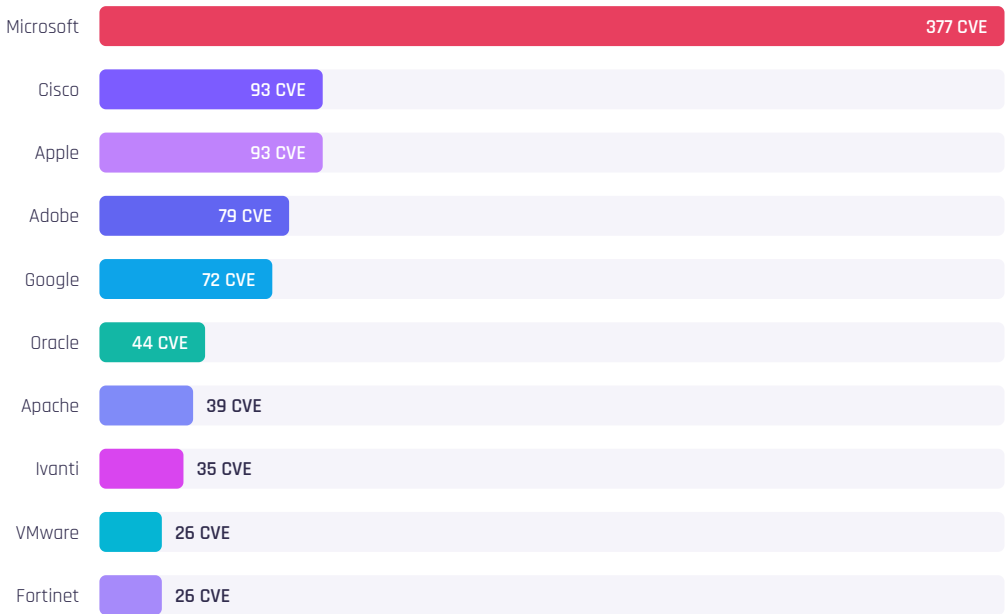
KEV over CVSS

IN BRIEF Risk is not read in the CVSS score but in real-world exploitation: the KEV catalog redraws patching priorities.

In March 2026, attackers actively exploited FortiGate firewalls as an initial access vector, via recent flaws including **CVE-2026-24858**. A campaign dubbed ClickFix compromised more than 700 sites by exploiting a critical SQL injection (CVE-2026-26980) in the

Ghost CMS. Two reminders that a vulnerability is not an abstraction: it is the raw material of initial access.

Our mirror of CISA's KEV catalog tracks **1,629 vulnerabilities** confirmed as actively exploited, of which 327 are already weaponised in ransomware campaigns. The breakdown by vendor maps the entry points of the moment.

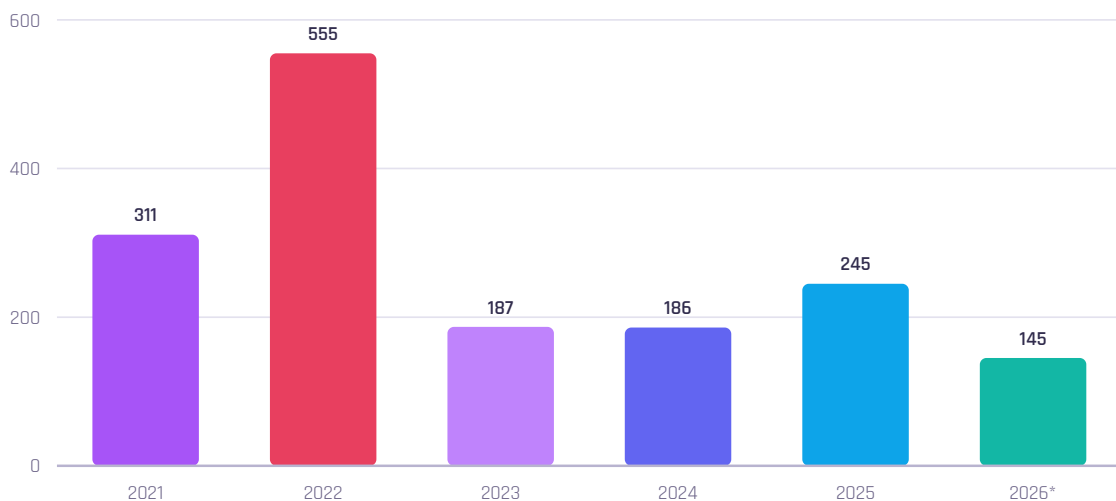


Vendors most represented in the KEV catalog

LuksMentis watch · KEV mirror (all years) · luksmentis.com · June 2026

Microsoft dominates by historical volume, but it is **edge devices** that make the news: Cisco, Ivanti and Fortinet concentrate the recent additions. In the first half of 2026 alone, we watched a cascade of Cisco Catalyst SD-WAN, FortiClient EMS and FortiOS flaws

enter the KEV, exactly the products The Gentlemen and others exploit to get in. 145 CVEs have been added to the catalog since January.

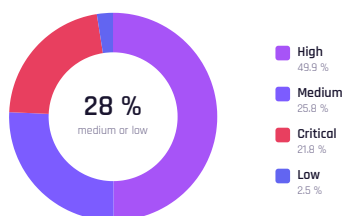


Actively exploited vulnerabilities added to the catalog (per year)

LuksMentis watch · mirror of CISA's KEV catalog (1,629 CVEs tracked) · luksmentis.com · June 2026

The CVSS score does not measure risk

The most important point of this chapter is not a volume, it is a method. Our base counts more than 440 CVEs published in 2026, all rated « high » or « critical », yet across all the flaws we track, nearly **28% are rated « medium » or « low »**. CVSS severity, computed in isolation, says nothing about real-world exploitation.

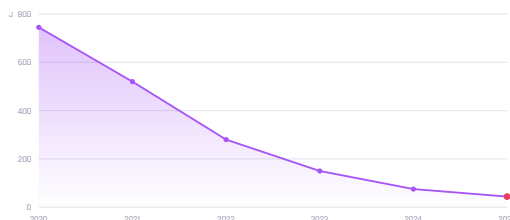


CVE breakdown by CVSS v3 severity

LuksMentis watch · 3,867 scored CVEs · luksmentis.com · June 2026

This was already the thesis of [our analysis on minor vulnerabilities](#), published in early June: fewer than one in five « critical » vulnerabilities is actually exploited, while « medium » flaws become the decisive link in an attack chain. A few weeks later, CISA confirmed this analysis in the clearest way. Its new directive **BOD 26-04**,

« **Prioritizing Security Updates Based on Risk** », revoked the historic BOD 22-01 to base prioritisation no longer on the CVSS score, but on real risk: asset exposure, presence in the KEV catalog, exploit automation capability and technical impact. That the agency explicitly keeps **exploit automation** as a criterion echoes our finding about the effect of AI word for word. The right question is no longer « is this flaw critical? », but « is it exploited, exposed, and reachable? ».



Average time to exploit

Source: Flashpoint, N-Day Vulnerability Trends (-94% in 5 years) · luksmentis.com · June 2026

Because AI has rewritten the equation. The average time to exploit fell from 745 days in 2020 to 44 days in 2025 (Flashpoint), and an autonomous agent can now exploit a known flaw for a few dollars. The stock of « minor » vulnerabilities an organisation leaves lying around is no longer a dormant risk: it is compound-interest debt.



06 · CROSS-CUTTING

THE AI THAT INDUSTRIALISES THEFT

The multiplier of every trend

96 %

successful exfiltration rate in Q1 2026, AI at the helm

Infosecurity Magazine · Q1 2026

THE AI THAT INDUSTRIALISES THEFT

The multiplier of every trend

IN BRIEF AI does not create a new threat: it accelerates and industrialises all the others, from sorting stolen data to exploiting flaws.

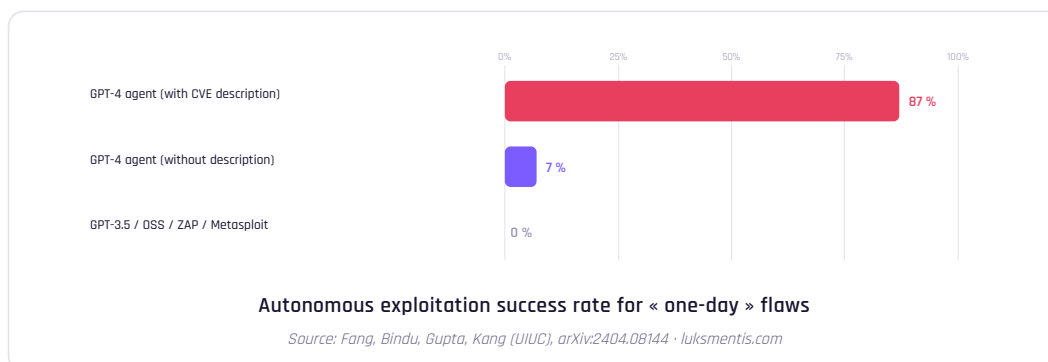
One force runs through the previous five chapters: **artificial intelligence**. It does not create a new threat; it **accelerates** and **automates** all the others. In the first quarter of 2025, the successful exfiltration rate reportedly reached 96%, with an average of 743 GB stolen per undisclosed incident, and criminal platforms like Lo-tAI or ClawdBot show how AI now automates the sorting and prioritisation of stolen data.

On the attacker side, AI lowers the cost of exploitation (chapter 5), sorts infostealer logs in seconds to extract high-value access (chapter 4), and multiplies OAuth reconnaissance (chapter 2). On

the defense side, it finds flaws faster than they can be fixed: Anthropic's Glasswing program identified more than 10,000 critical or high vulnerabilities in two months, of which more than 99% were unpatched at announcement. Discovery is no longer the bottleneck, **remediation** is.

This new surface has its own risk framework, detailed in [our OWASP LLM overview](#): prompt injection, data leakage to LLMs, over-autonomous agents, poisoned RAG. Securing the **internal use** of AI has become a discipline in its own right, on a par with securing a classic information system.

What AI changes in practice. A GPT-4-based agent exploited, on its own, 87% of a set of « one-day » flaws from the CVE description alone, where GPT-3.5, eight open-source models and the ZAP and Metasploit scanners scored 0%. Deprived of the description, the rate drops to 7%: AI excels at exploiting a known flaw far more than at discovering a new one. Average cost of a successful exploit: \$8.80, versus \$25 for a human pentester, and the agent is massively parallelisable.



KEY TAKEAWAYS

- 01 AI does not invent a threat: it accelerates and automates all the others.
- 02 Time to exploit collapses, from 745 days in 2020 to 44 days in 2025.
- 03 Sorting stolen data, exploiting flaws, exfiltration: everything industrialises.



07 · FOR THE TEAMS

PRIORITIES AND OUTLOOK

What it means for security teams (CISOs)

KEV

focus effort where attack chains actually break

Guiding principle · BOD 26-04

PRIORITIES AND OUTLOOK

What it means for security teams (CISOs)

IN BRIEF Focus effort where attack chains actually break, rather than stacking tools downstream.

What to make of this overview? The priorities that emerge for security leaders are not a checklist: they follow directly from what the semester showed, and obey a single principle, focus effort where attack chains actually break, rather than stacking tools downstream.

The first door to close remains the **edge**. VPNs, firewalls and gateways concentrate the initial access of dominant groups; a thorough inventory, a patch applied within days whenever a flaw enters the KEV, and Internet exposure cut to the strict minimum are worth more than any defense added later. In the same move, it becomes vital to **regain control of third-party integrations**: map OAuth connectors, impose least privilege, rotate and revoke secrets, demand verifiable guarantees (ISO 27001, SOC 2) from critical suppliers. One in three breaches now runs through a third party; granted trust is not a security control.

On vulnerabilities, the reflex to install is to **prioritise by exploitability rather than by CVSS**, crossing KEV status, public exploit and EPSS score: a « medium » flaw actually exploited must come be-

fore a « critical » one isolated behind several layers of segmentation. The geopolitical escalation calls in parallel for **preparing for the destructive**: for sensitive operators, the wiper scenario is no longer theoretical, which brings immutable backups, genuinely tested restoration and OT/IT separation back to the fore.

Facing AI-driven industrialisation, finally, two stances stand out. First, **treat any stolen data as already resold**: rather than hoping a leak stays confidential, bet on detecting the use of compromised credentials and on phishing-resistant authentication. Second, **govern internal AI use**, that is, frame what staff and agents can do with LLMs before that surface becomes a blind spot. Beyond these priorities, a more structural avenue is worth raising: for the most critical data, the best protection against a third party's failure is still not to depend on it, by reinternalising what can be.

No organisation is invulnerable. But, as we wrote about third-party security, you cannot claim victimhood if you have not put the means in place to protect yourself. The first half of 2026 does not say the threat is unstoppable: it says where to put the effort.

SOURCES CITED

LuksMentis watch (primary data, June 2026 queries).

Verizon, 2025 Data Breach Investigations Report (third-party share).

IBM, Cost of a Data Breach Report 2025 (cost, supply-chain dwell time).

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

Rapid7, 2026 Global Threat Landscape Report.

Privacy Affairs, Dark Web Price Index (2021 to 2023 editions).

Biometric Update; deepstrike, Constella (resale prices and infostealers, 2025-2026).

CISA, BOD 26-04 « Prioritizing Security Updates Based on Risk » (revokes BOD 22-01); KEV catalog: [cisa.gov](https://www.cisa.gov).

ScienceDirect (ransomware consolidation, top-10 concentration).

Infosecurity Magazine (exfiltration rate, stolen volumes).

Trade press: PurpleSec, La Nouvelle Tribune, Facteria, Quiver Quantitative, Techtime, Franceinfo.

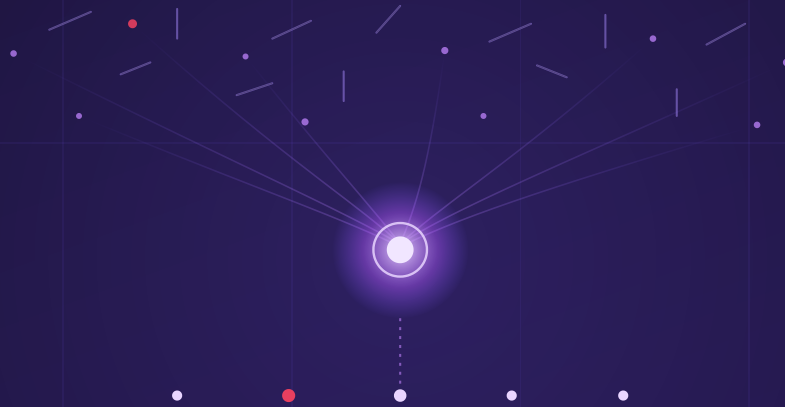
LuksMentis articles: Anatomy of attacker groups; Third-party security; Minor vulnerabilities; OWASP LLM overview (luksmentis.com/blog).

About this report

Report produced by LuksMentis from its proprietary cyber threat watch (nearly 64,000 qualified signals from January to June 2026) and the external sources listed above. Figures marked « LuksMentis watch » rely on our internal data. Attribution often relies on open sources and has no value as judicial proof. © LuksMentis 2026, luksmentis.com, reproduction and reuse subject to authorisation.

LUKSMENTIS

CYBER THREAT INTELLIGENCE



SCRAPE THE NOISE. EXTRACT INTELLIGENCE.

Get the essentials of the cyber threat, **free, every day.**

Sign up for free · luksmentis.com

Free newsletter · daily digests.

luksmentis.com · Sovereign cyber watch

© LuksMentis 2026 · Reproduction and reuse subject to authorisation