ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Panorama de les ciberamenaces al quart trimestre del 2025

TLP: WHITE

GENER 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	30/01/2026	03/02/2026

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

L'informe següent té com a objectiu oferir una visió actualitzada del panorama de les ciberamenaces corresponent al quart trimestre de l'any 2025, amb l'objectiu d'identificar les amenaces clau que afecten les organitzacions i els governs, comparar aquestes dades amb les dels trimestres anteriors per arribar a conclusions clares i analitzar l'evolució del panorama al llarg de l'any 2025.

Per elaborar aquest informe s'han recopilat i analitzat dades globals i específiques d'Espanya. Gràcies a això, es podrà comprendre millor al ciberespai i prestar atenció als indicadors més rellevants per a Andorra, a causa de la proximitat geogràfica, econòmica amb Espanya i l'exposició a dinàmiques geopolítiques europees.

Al llarg d'aquest informe s'analitzaran els ciberatacs registrats el quart trimestre de l'any 2025, l'evolució dels ciberatacs l'any 2025 per trimestres, un estudi comparatiu de ciberamenaces ocorregudes el 2025 entre Andorra i la Unió Europea, els països més afectats en el quart trimestre, els actors d'amenaça més actius en el quart trimestre, les tècniques amb un impacte més gran, i els sectors més impactats i atacats del quart trimestre.

També es presentarà de manera detallada i específica el panorama de ciberamenaces a Espanya durant el quart trimestre del 2025, amb èmfasi en l'hacktivisme i el cibercrim.

Per acabar, s'exposaran les conclusions i els escenaris més probables del futur.

3. TENDÈNCIES I EVOLUCIÓ DE LES CIBERAMENACES

A l'apartat següent, s'analitzaran els ciberatacs registrats el quart trimestre del 2025 a nivell global, analitzarem tots els ciberatacs registrats l'any 2025 separats pels diferents trimestres i analitzarem un estudi comparatiu de les ciberamenaces ocorregudes el 2025 entre Andorra i la Unió Europea. També s'analitzaran els actors d'amenaça més actius, les tècniques amb més impacte i els sectors industrials més impactats i atacats.

3.1. Ciberatacs registrats durant el quart trimestre del 2025

Durant el quart trimestre del 2025 es van registrar 4.166 ciberatacs a nivell mundial, cosa que ha suposat una pujada del 4,5 % respecte dels registrats durant el tercer trimestre de l'any.

El volum de ciberatacs continua sent molt elevat i supera el nombre d'atacs del tercer trimestre que se situava en una mitjana superior dels 40 ciberatacs diaris, al quart trimestre arriba a una mitjana propera als 45 ciberatacs, cosa que reflecteix un increment de l'activitat maliciosa aquest darrer trimestre de l'any.

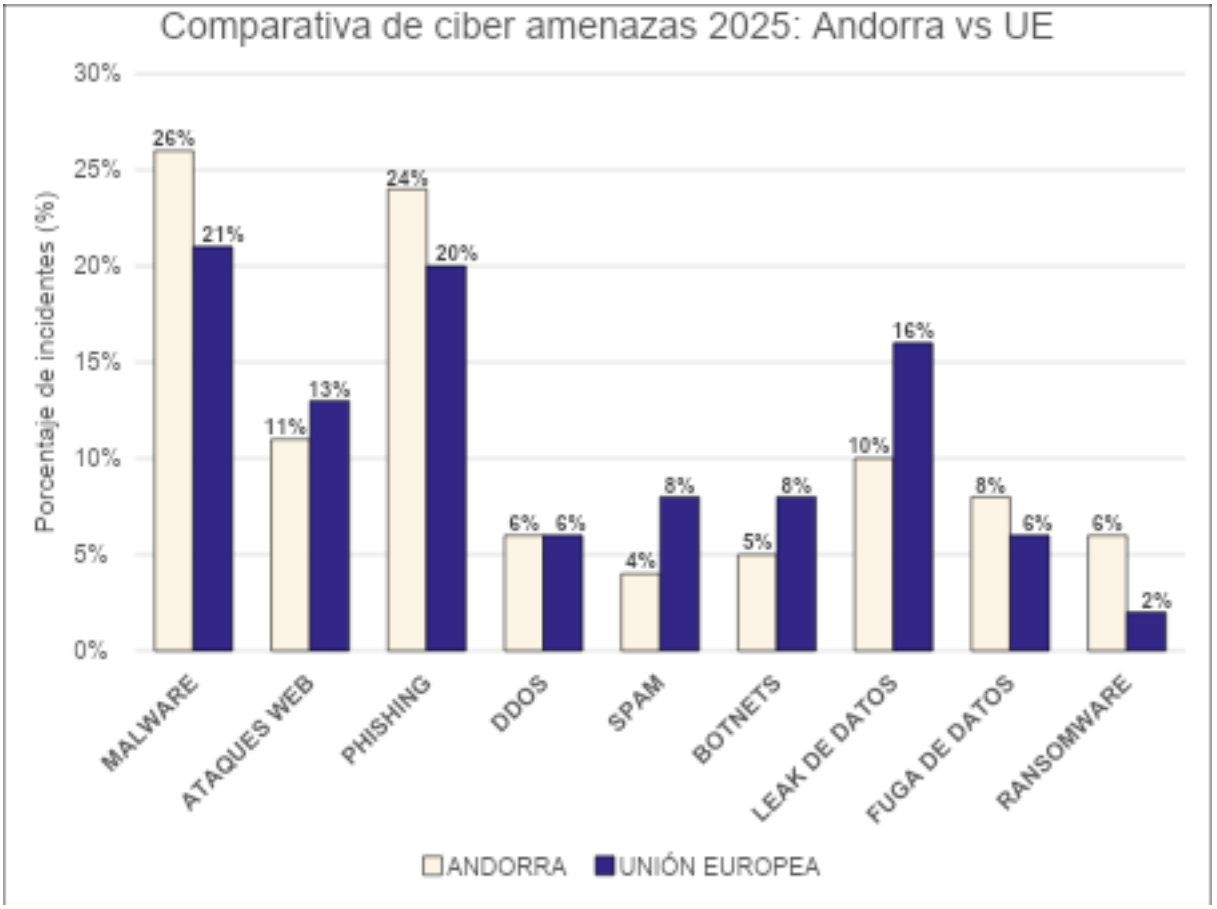
3.2. 18.671 ciberatacs el 2025: quina ha estat la seva evolució?

El gràfic següent mostra el nombre de ciberatacs registrats a nivell mundial al llarg d'aquest any 2025, distribuït per trimestres. El primer trimestre de l'any 2025 representa el volum d'atacs més elevat amb 6.373 ciberatacs, a partir del segon s'observa una disminució significativa del 34 %, amb 4.147 ciberatacs, en el tercer trimestre amb 3.985 els ciberatacs tornen a patir una caiguda del 3,9 %, i per finalitzar l'any s'observen 4.166 ciberatacs amb una pujada del 4,5 %. En general, les dades indiquen una caiguda forta després del primer trimestre i una estabilització a final d'any.

Gràfic 1 – Nombre d'atacs registrats a nivell mundial l'any 2025 dividit per trimestres

3.3. Comparativa de les ciberamenaces el 2025: Andorra vs. Unió Europea

Tot seguit, s'exposarà una taula amb dades comparatives de les ciberamenaces a Andorra i la Unió Europea corresponents a l'any 2025 proporcionades per l'Agència de la Unió Europea per a la Ciberseguretat (ENISA).



Gràfic 2 – Comparativa de les ciberamenaces el 2025: Andorra vs. Unió Europea (Ref. ENISA)

El gràfic proporcionat per l'Agència de la Unió Europea per a la Ciberseguretat (ENISA), mostra que Andorra el 2025 ha tingut un perfil més concentrat i amb més ciberamenaces conegudes o comunes que la mitjana de la Unió Europea, ja que en codi maliciós amb un 26 % i pesca amb un 24 % dominen clarament i superen els percentatges europeus. Aquestes dades podrien indicar que Andorra té més exposició a infeccions de codi maliciós directes i enginyeria social amb pesca en usuaris o organitzacions petites.

El programari de segrest i la fuga de dades són proporcionalment més presents al panorama andorrà, mentre que les amenaces massives com el correu brossa, *botnets*, atacs web o *leak* de dades són més freqüents en el panorama europeu.

3.4. Països més atacats

S'ha elaborat un *top ten* de països més afectats pels ciberatacs el quart trimestre, els Estats Units una vegada més es mantenen com el país més atacat del món i tornen a ocupar el lloc més alt del rànquing dominant molt per sobre dels altres països, igual que el primer, segon i tercer trimestre.

Andorra no ocupa el *top ten* de països més atacats, però a causa de la proximitat amb països com Espanya i França podria patir un efecte de danys col·laterals significatius, és per això que és important analitzar els països veïns:

- Espanya, amb 152 atacs, se situa al lloc 5, pujant 2 llocs del TOP 10 després d'ocupar el setè lloc el trimestre anterior.
- França, es consolida al lloc 2 amb 203 ciberatacs registrats, pujant un lloc del TOP 10 després d'ocupar el tercer lloc el trimestre anterior.

	PAÍS	Nombre d'atacs	% TOTAL
1	Estats Units	1210	29,0 %
2	**França**	**203**	**4,9 %**
3	Ucraïna	163	3,9 %
4	Itàlia	156	3,7 %
5	**Espanya**	**152**	**3,6 %**
6	Alemanya	149	3,6 %
7	Japó	148	3,6 %
8	Canadà	143	3,4 %
9	Bèlgica	125	3,0 %
10	Unió dels Emirats Àrabs	105	2,5 %

Taula 1 - TOP 10 de països més afectats per ciberatacs durant el quart trimestre

3.5. Actors d'amenaça més actius

L'actor d'amenaces més actiu durant aquest quart trimestre, igual que el primer, el segon i el tercer, ha estat novament el grup NoName057(16), a qui se li atribueixen 596 ciberatacs. Qilin i Akira com ja va succeir al primer, segon i tercer trimestres, tornen a formar part d'aquest rànquing, i s'erigeixen en els grups de programari de segrest (*ransomware*) amb més impacte aquest any 2025.

A continuació, exposarem el TOP 5 dels actors d'amenaça amb més atacs en aquest darrer trimestre de l'any 2025.

	ACTOR D'AMENAÇA	MÈTODE	CATEGORIA	Nombre d'atacs
1	NoName057(16)	DDoS	Hacktivisme	596
2	Qilin	Programari de segrest	Cibercrim	374
3	Akira	Programari de segrest	Cibercrim	195
4	Keymous+	DDoS	Hacktivisme	152
5	Cl0p	Programari de segrest	Cibercrim	84

Taula 2 - Top 5 d'actors més actius d'amenaça durant el quart trimestre

3.6. Tècniques amb més impacte

La taula següent detalla les tècniques d'atac amb més severitat emprades el quart trimestre de l'any 2025. Aquesta taula ajuda a comprendre quins vectors d'atac van ser més impactats i quins mètodes són prioritaris per a la mitigació i la prevenció de riscos.

	TÈCNIQUES	Nombre d'atacs	% TOTAL
1	Vulnerabilitats	250	5,7 %
2	Codi maliciós	1961	44,6 %
3	Múltiples tècniques	81	1,8 %
4	No revelat	819	18,6 %
5	Atacs web	9	0,2 %

Taula 3 – Tècniques amb més impacte durant el quart trimestre

3.7. Sectors més impactats

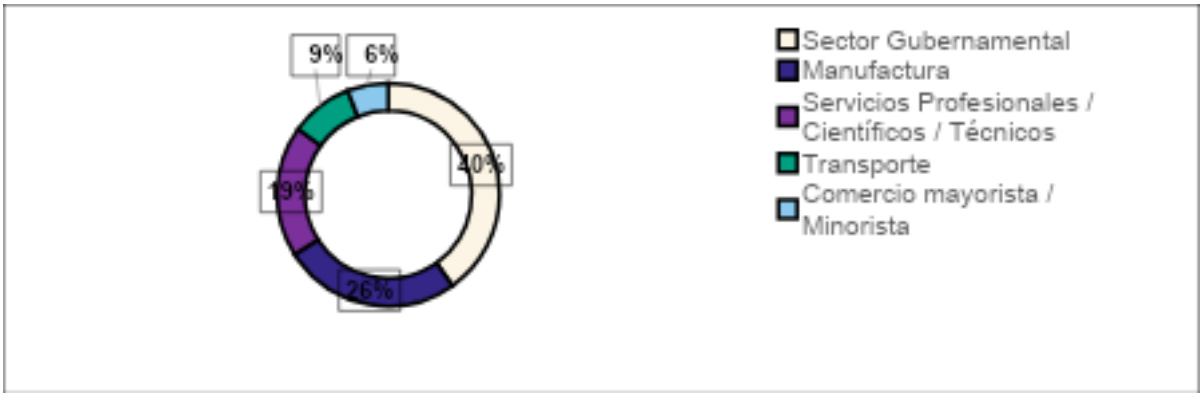
Aquesta taula mostra els sectors més afectades pels ciberatacs durant el quart trimestre de l'any 2025. Ens permet identificar quins sectors enfronten més severitat d'incidents i la proporció d'atacs sobre el total registrat.

	SECTOR	Nombre d'atacs	% TOTAL
1	Salut	194	29,3 %
2	Serveis professionals / Científics / Tècnics	416	62,7 %
3	Comerç majorista / detallista	277	41,8 %
4	Agricultura / Pesca	15	2,3 %
5	Manufactura	581	87,6 %

Taula 4 – Sectors més impactats durant el quart trimestre

3.8. Sectors més atacats

A l'anterior taula relacionada amb els sectors mostràvem els més impactats del quart trimestre de l'any, tot seguit mostrem el gràfic que mostra els sectors més atacats per volum de ciberatacs durant el quart trimestre de l'any 2025. Això ens permet identificar quins sectors han estat els més atacats, no els més impactats.



Gràfic 3 – Sectors més atacats durant el quart trimestre

4. PANORAMA DE CIBERAMENACES D'ESPANYA

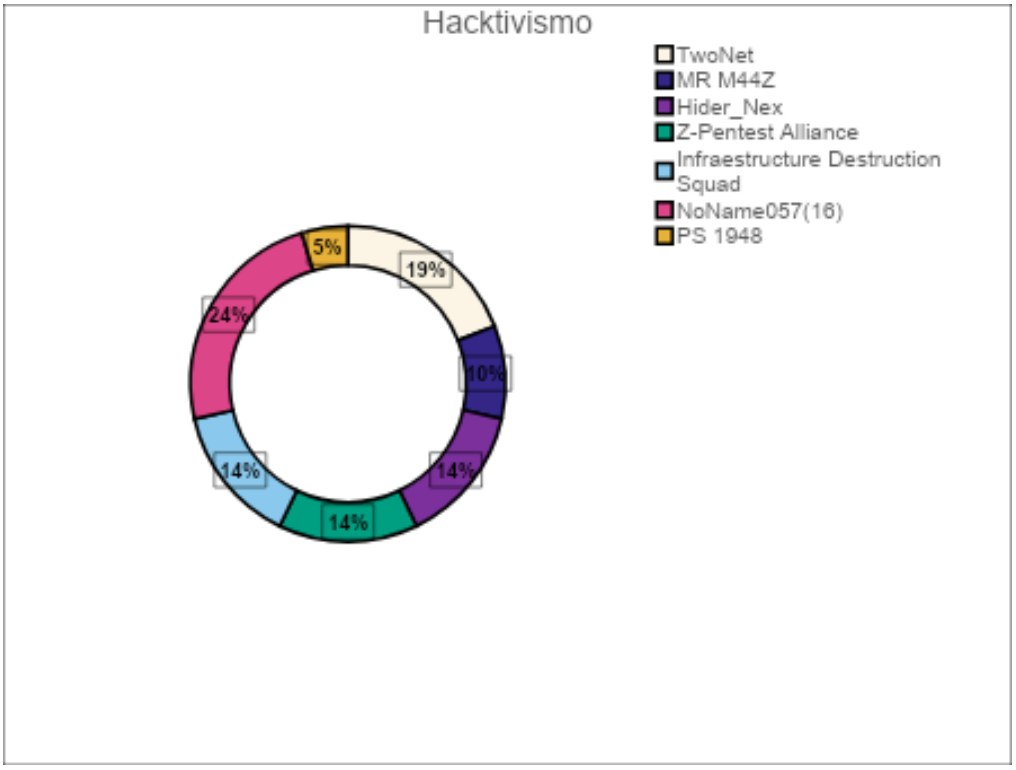
L'apartat següent de l'informe ofereix una anàlisi completa del panorama de ciberamenaces a Espanya del quart trimestre del 2025, on s'analitzarà l'activitat del hacktivisme i el cibercrim, inclosos els incidents de programari de segrest i venda d'accessos.

4.1. Hacktivisme

A continuació, analitzarem el panorama de l'hacktivisme durant el quart trimestre de 2025. Aquest trimestre en comparació amb el tercer veiem que els atacs hacktivistes perden pes, i passen de 163 ciberatacs a 21. Aquesta gran baixada de ciberatacs hacktivistes és perquè actors d'amenaça com a NoName057(16) i Z-Pentest han concentrat més els atacs en altres països membres de l'OTAN.

4.1.1 Ciberatacs hacktivistes

A partir de les dades recopilades, durant el quart trimestre del 2025 s'han detectat els següents grups que van realitzar atacs amb motivació hacktivista. El grup més actiu durant aquest període va ser NoName057(16), amb un 24 % dels atacs registrats, seguit molt de prop per TwoNet amb un 19 %.



Gràfic 4 - Grups hacktivistes més actius a Espanya durant el quart trimestre del 2025

4.1.1.1. Octubre

A l'octubre es van detectar 5 grups involucrats en atacs hacktivistes. Aquest mes es pot apreciar una activitat distribuïda i diversificada, sense cap actor que domini ni destaqui per sobre d'un altre.

	ACTOR D'AMENAÇA	Nre. d'atacs	% TOTAL
1	TwoNet	4	30,77 %
2	Hider_Nex	3	23,08 %
2	Z-Pentest Alliance	3	23,08 %
3	MR M44Z	2	15,38 %
4	Infraestructure Destruction Squad	1	7,69 %

Taula 5 - Grups hacktivistes actius a Espanya durant l'octubre del 2025

4.1.1.2. Novembre

Al novembre, NoName057(16) es proclama com el principal actor, encara que ho fa amb 5 atacs, no com a l'anterior trimestre, que en va fer 91. Grups com Infraestructure Destruction Squad i PS 1948 apareixen amb un atac cadascun.

	ACTOR D'AMENAÇA	Nre. d'atacs	% TOTAL
1	NoName057(16)	5	71,43%
2	Infraestructure Destruction Squad	1	14,29%
3	PS 1948	1	14,29%

Taula 6 - Activitat de grups de ransomware a Espanya el novembre de 2025

4.1.1.3. Desembre

Al desembre, només es detecta un atac per part del grup Infraestructure Destruction Squad.

	ACTOR D'AMENAÇA	Nre. d'atacs	% TOTAL
1	Infraestructure Destruction Squad	1	100 %

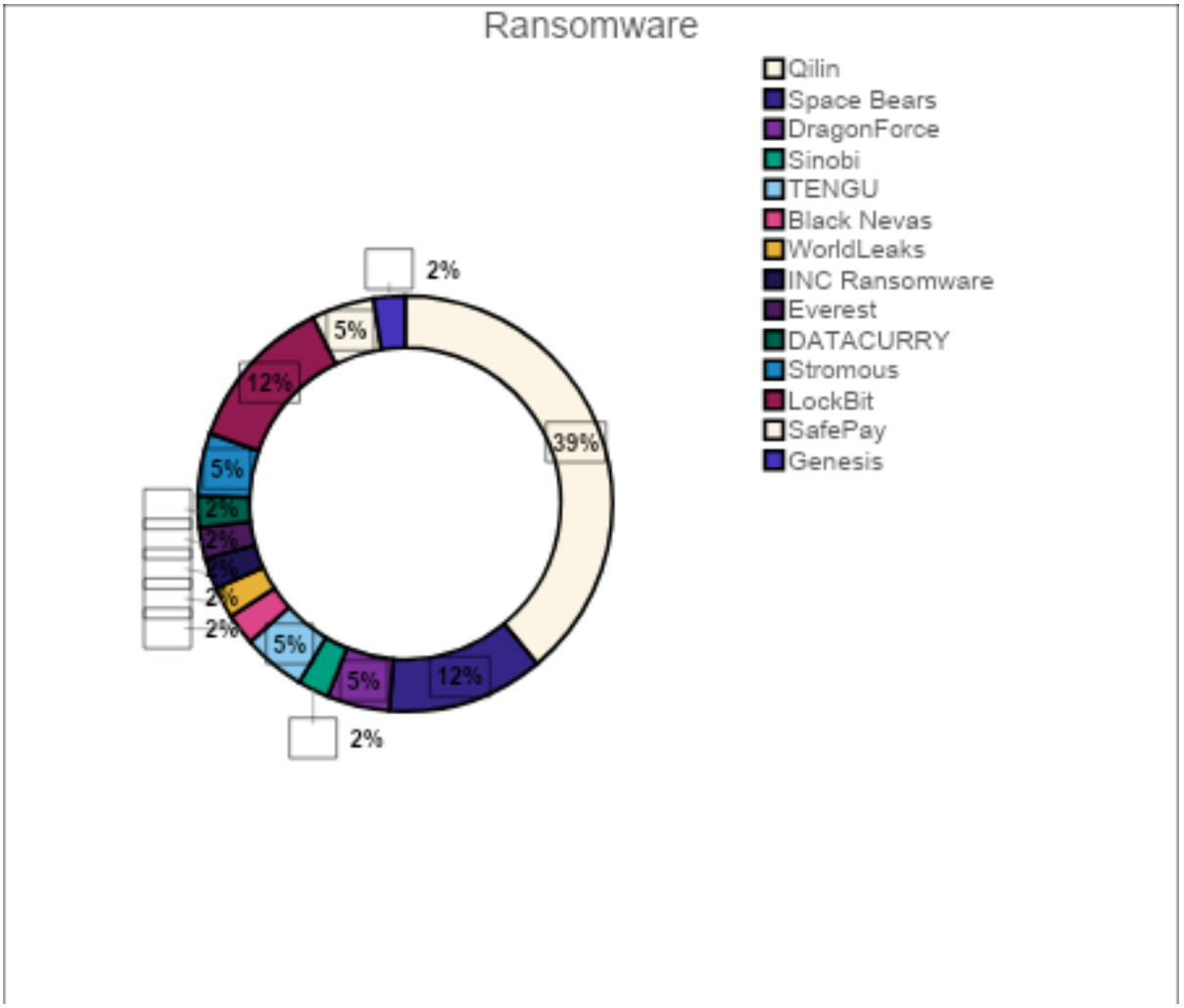
Taula 7 - Grups hacktivistes actius a Espanya durant el desembre de 2025

4.2. Cibercrim

A continuació, analitzarem el panorama del cibercrim durant el quart trimestre del 2025. Aquest trimestre en comparació al tercer veiem que s'han incrementat aquest tipus d'atacs, passant de 30 al tercer trimestre a 48 al quart trimestre, augmentant un 60 %.

4.2.1. Incidents de programari de segrest

El grup més actiu durant aquest trimestre va ser novament Qilin, que passa de 7 ciberatacs al tercer trimestre a 16 ciberatacs al quart trimestre. A partir de les dades recopilades, durant el quart trimestre de 2025 s'han detectat els grups següents que van realitzar atacs de tipus ransomware:



Gràfic 5 - Grups de programari de segrest més actius durant el quart trimestre del 2025

4.2.1.1. Octubre

A l'octubre, el grup Qilin domina el panorama amb un terç dels atacs registrats, un 37,50%. La resta d'activitat està molt distribuïda, i és que 6 grups diferents han fet almenys un atac de tipus ransomware.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Qilin	6	37,50 %
2	Space Bears	4	25,00 %
3	DragonForce	2	12,50 %
3	TENGU	2	12,50 %
4	Sinobi	1	6,25 %
4	Qilin	1	6,25 %

Taula 8 - Activitat de grups de ransomware a Espanya l'octubre del 2025

4.2.1.2. Novembre

Al novembre, Qilin destaca lleugerament com l'actor més actiu, la resta dels actors presenten una participació similar amb un ciberatac cadascun.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Qilin	2	28,57 %
2	Space Bears	1	14,29 %
2	WorldLeaks	1	14,29 %
2	INC Ransomware	1	14,29 %
2	Everest	1	14,29 %
2	DATACURRY	1	14,29 %

Taula 9 - Activitat de grups de ransomware a Espanya el novembre de 2025

4.2.1.3. Desembre

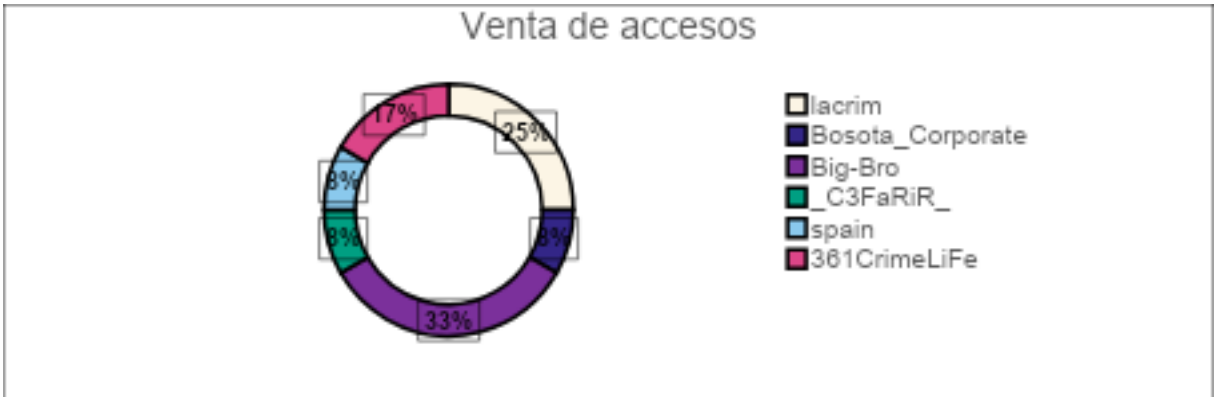
Al desembre, l'activitat es concentra principalment a Qilin amb un 44,44%, seguit de LockBit amb un 27,78%. La resta de grups presenta una participació menor.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Qilin	8	44,44 %
2	LockBit	5	27,78 %
3	Stromous	2	11,11 %
3	SafePay	2	11,11 %
4	Genesis	1	5,56 %

Taula 10 - Activitat de grups de ransomware a Espanya el desembre de 2025

4.2.2. Venda d'accessos

A partir de les dades recopilades, durant el quart trimestre del 2025 s'han detectat els grups següents que van fer vendes d'accés. El grup més actiu durant aquest trimestre va ser Big-Bro, tal com va passar anteriorment al tercer trimestre de l'any.



Gràfic 6 - Grups més actius en vendes d'accés durant el quart trimestre del 2025

4.2.2.1 Octubre

A l'octubre, l'activitat és limitada. Només s'observa un accés compromès per part de l'actor 361CrimeLiFe.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	361CrimeLife	1	100,00 %

Taula 11 - Distribució de vendes d'accés per grup durant l'octubre del 2025

4.2.2.2. Novembre

Al novembre, apareixen dos nous actors lacrim i Big-Bro.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	lacrim	2	66,67 %
2	Big-Bro	1	33,33 %

Taula 12 - Distribució de vendes d'accés per grup durant el novembre del 2025

4.2.2.3. Desembre

Al desembre, l'activitat es concreta a Big-Bro amb un 42,86 %, mentre que la resta dels grups tenen una participació similar amb un 14,29 % cadascun.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	Big-Bro	3	42,86 %
2	lacrim	1	14,29 %
2	_C3FaRiR_	1	14,29 %
2	Bosota_Corporate	1	14,29 %
2	spain	1	14,29 %

Taula 13 - Distribució de vendes d'accés per grup durant el desembre del 2025

5. CONCLUSIONS

Després d'haver analitzat el panorama de les ciberamenaces del quart trimestre de l'any 2025 i observant la situació geopolítica actual, ens fa pensar que per al pròxim període de l'any (T1 2026) s'esperi un increment notable de ciberatacs a Europa, principalment motivat per les negociacions de pau en curs de les guerres Ucraïna/Rússia i Gaza/Israel.

A més, la intervenció recent dels Estats Units a Veneçuela podria arribar a activar atacs hacktivistes prorussos/iranians o pro-Maduro contra els interessos occidentals.

Aquest escenari ens convida a continuar atents a les diferents mètriques i dades del panorama de ciberamenaces, ja que l'impacte podria ser significatiu. El cost anual del cibercrim ja s'estima al voltant dels 10,5 bilions de dòlars, i un repunt en atacs motivats per la geopolítica podria accelerar àmpliament aquesta tendència, cosa que afectaria notablement sectors clau com ara l'energia, el transport, les finances i els governs.

Amb això, l'informe tanca l'anàlisi del quart trimestre de l'any 2025 i obre la porta a la vigilància proactiva aquest any nou 2026 que, com ja hem esmentat, està marcat per una inestabilitat geopolítica persistent, per noves ciberamenaces i per grups cibercriminals que estan en evolució constant.

6. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.