ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

El panorama de les ciberamenaces 1T 2026

TLP: WHITE

ABRIL 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	29/04/2026	30/04/2026

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

Aquest informe té com a objectiu analitzar i oferir una visió actualitzada sobre el panorama de les ciberamenaces corresponent al primer trimestre de l'any 2026, amb una atenció especial a aquelles amenaces que puguin tenir un impacte significatiu en el context d'Andorra. Atesa la limitada informació i disponibilitat de dades específiques sobre el país andorrà, s'inclourà una anàlisi més completa del país veí, Espanya, a causa de la proximitat geogràfica, els llaços i l'operativa propera.

Durant el primer trimestre de l'any, l'ecosistema de les ciberamenaces ha estat molt influenciat per factors geopolítics, perquè l'increment de l'activitat de grups hacktivistes ha estat fortament associat al conflicte de l'Orient Mitjà. També s'ha observat un augment molt significatiu en el volum de les ciberamenaces globals, com també una focalització més gran en sectors estratègics, especialment el sector governamental.

Per a l'elaboració d'aquest informe s'han recopilat i analitzat les principals tendències globals, incloent-hi l'evolució dels atacs, els actors d'amenaça més actius, les tècniques més predominants i els sectors més impactats i atacats.

Per acabar, les conclusions de l'anàlisi s'exposaran juntament amb els escenaris més probables d'evolució a futur del panorama de les ciberamenaces.

3. TENDÈNCIES I EVOLUCIÓ DE LES CIBERAMENACES A NIVELL GLOBAL

A l'apartat següent, s'analitzaran les principals tendències i l'evolució de les ciberamenaces a nivell global del primer trimestre de l'any 2026. Centrarem una atenció especial al volum de ciberatacs registrats, la seva evolució des d'escenaris d'estabilitat fins a possibles repunts, els països més afectats, els actors d'amenaça més actius, les tècniques amb més impacte i els sectors industrials més atacats. També es detallarà una referència breu al context geopolític internacional actual, en concret el conflicte de l'Orient Mitjà, a causa de la seva influència en l'augment de les ciberamenaces a nivell global.

3.1. Ciberatacs registrats el primer trimestre del 22026

Durant el primer trimestre del 2026 es van registrar 6.418 ciberatacs a nivell mundial, cosa que ha suposat una pujada del 54 % respecte als registrats durant el quart trimestre de l'any 2025.

El volum de ciberatacs continua sent molt elevat i mostra un increment considerable respecte a períodes anteriors. La mitjana aproximada de ciberatacs diaris ja s'aproxima a 71, els trimestres anteriors de l'any 2025, se situaven en una mitjana superior als 40 ciberatacs el tercer trimestre i propera als 45 al quart, cosa que reflecteix un increment exponencial de l'activitat maliciosa.

3.2. De l'estabilitat al repunt, així han evolucionat els atacats globals

Al llarg de l'any 2025 es van registrar un total de 18.671 ciberatacs a nivell mundial, la qual cosa mostra variacions al llarg dels diferents trimestres. Després d'una lleugera recuperació el quart trimestre del 2025, el primer trimestre del 2026 ha experimentat un repunt significatiu. Aquest augment confirma una tendència a l'alça a l'inici del 2026, i reforça la preocupació pel creixement de les amenaces emergents al panorama global.

Gràfic 1 – Nombre d'atacs registrats a nivell mundial per trimestres

3.3. Actors d'amenaça més actius

L'actor d'amenaces més actiu durant el primer trimestre de l'any 2026, igual que tot l'any 2025, ha estat novament el grup NoName057(16), a qui se li atribueixen 595 ciberatacs. Qilin al segon lloc, torna a formar part d'aquest rànquing, i s'erigeix en l'únic grup de programari de segrest amb més impacte aquest primer trimestre de l'any 2026.

A continuació, exposarem el TOP 5 dels grups amb més atacs en el primer trimestre de l'any 2026.

	ACTOR D'AMENAÇA	MÈTODE	CATEGORIA	NRE. D'ATACS
1	NoName057(16)	**DDoS**	**Hacktivisme**	595
2	Qilin	**Programari de segrest**	**Cibercrim**	285
3	Keymous+	**DDoS**	**Hacktivisme**	136
4	Conquerors Electronic Army	**DDoS**	**Hacktivisme**	91
5	DieNet	**DDoS**	**Hacktivisme**	84

Taula 1 - Top 5 d'actors d'amenaça més actius durant el primer trimestre

A més dels actors d'amenaça al TOP5, altres actors han tingut un gran impacte aquest darrer trimestre. Actors d'amenaça com Cl0p (programari de segrest) i 313 Team (hacktivisme) han destacat per les campanyes dirigides a sectors estratègics i en el conflicte de l'Orient Mitjà.

3.4. Països més atacats

S'ha elaborat un top ten de països més afectats pels ciberatacs el primer trimestre, els Estats Units novament 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 tot l'any 2025.

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 169 atacs, se situa al lloc 6, i baixa un lloc del TOP 10 després d'ocupar el cinquè lloc el trimestre anterior.
- França, es consolida al lloc 3 amb 351 ciberatacs registrats, i descendeix un lloc del TOP 10 després d'ocupar el segon lloc el trimestre anterior.

	PAÍS	NRE. D'ATACS	% TOTAL
1	Estats Units	1481	23,1%
2	Israel	567	8,8%
3	**França**	**351**	**5,5%**
4	Alemanya	214	3,3%
5	Gran Bretanya	185	2,9%
6	**Espanya**	**169**	**2,6%**
7	Itàlia	147	2,3%
8	Canadà	134	2,1%

9	Japó	133	2,1%
10	Kuwait	126	2,0%

Taula 2 - Top 10 de països més afectats per ciberatacs durant el primer trimestre

3.5. Tècniques amb més impacte

La taula següent detalla les tècniques d'atac amb més severitat emprades el primer trimestre de l'any 2026. 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	NRE. D'ATACS	% TOTAL
1	Vulnerabilitats	166	2,6%
2	Programari maliciós	2181	34,0%
3	Múltiples tècniques	117	1,8%
4	No revelat	1874	29,2%
5	Robatori d'identitat / *Cracking* de comptes	22	0,3%

Taula 3 – Tècniques amb més impacte durant el primer trimestre

3.6. Sectors industrials més impactats

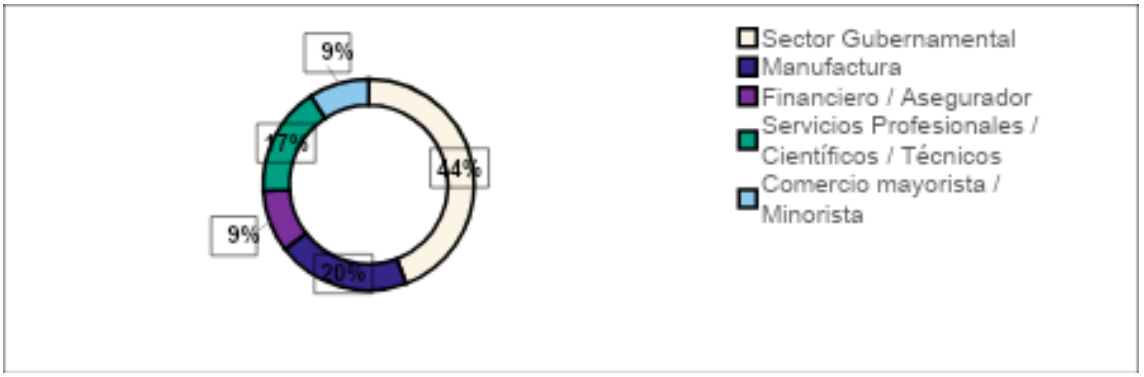
Aquesta taula mostra els sectors més afectats per ciberatacs durant el primer trimestre de l'any 2026. Ens permet identificar quins sectors han hagut d'enfrontar-se amb incidents més greus i la seva proporció d'atacs sobre el total registrat.

	SECTOR	NRE. D'ATACS	% TOTAL
1	Salut	272	30,4%
2	Serveis professionals / científics / tècnics	549	61,3%
3	Comerç majorista / detallista	442	49,3%
4	Agricultura / pesca	180	20,1%
5	Manufactura	635	70,9%

Taula 4 – Sectors industrials més impactats durant el primer trimestre

3.7. Sectors industrials més atacats

A l'anterior taula relacionada amb sectors mostràvem els més impactats del primer trimestre de l'any 2026, tot seguit mostrem el següent gràfic que mostra les indústries més atacades per volum de ciberatacs. Això ens permet identificar quins sectors han estat els més atacats, que no vol dir que hagin estat els més impactats.



Gràfic 1 – Sectors industrials més atacats durant el primer trimestre

3.8. Conflicte de l'Orient Mitjà

Durant el període analitzat del conflicte de l'Orient Mitjà durant el primer trimestre, es van registrar 1098 ciberatacs relacionats amb ell. El DDoS va ser la tècnica predominant (1002 atacs), la qual cosa representa més del 91 % del total. Israel va ser el país més afectat, i va concentrar el 45,8 % dels atacs (486 incidents), seguit per Kuwait (10,7 %) i Bahrain (7,2 %). La majoria dels atacs van ser duts a terme per grups de hacktivisme, principalment contra objectius governamentals, militars i del sector financer.

3.8.1. Tècniques més utilitzades

	TÈCNIQUES	NOMBRE D'ATACS
1	DDoS	1002
2	No revelat	89
3	Programari maliciós	5
4	Múltiples tècniques	2

Taula 5 - Tècniques amb més impacte durant el conflicte de l'Orient Mitjà

3.8.2. Sectors més atacats

	SECTOR	NOMBRE D'ATACS
1	Govern / militar / forces de seguretat	486
2	Finances / assegurances	101
3	Mitjans de comunicació / notícies / multimèdia	82
4	Transport / emmagatzematge / logística	68
5	Organitzacions (ONG, fundacions, etc.)	62

Taula 6 – Sectors industrials més impactats durant el conflicte de l'Orient Mitjà

3.8.3. Actors d'amenaça més actius

	ACTOR D'AMENAÇA	MÈTODE	CATEGORIA	NRE. D'ATACS
1	313 Team	**DDoS**	**Hacktivisme**	48
2	NoName057(16)	**DDoS**	**Hacktivisme**	35
3	Conquerors Electronic Army	**DDoS**	**Hacktivisme**	25
4	DieNet	**DDoS**	**Hacktivisme**	8

Taula 7 - Actors d'amenaça més actius durant el conflicte de l'Orient Mitjà

3.8.4. Països més atacats

	PAÍS	NRE. D'ATACS	% TOTAL
1	Israel	486	45,8%
2	Kuwait	113	10,7%
3	Bahrain	76	7,2%
4	Unió dels Emirats Àrabs	71	6,7%
5	Aràbia Saudita	70	6,6%

Taula 8 - Països més afectats per ciberatacs durant el conflicte de l'Orient Mitjà

4. PANORAMA DE CIBERAMENACES D'ESPANYA

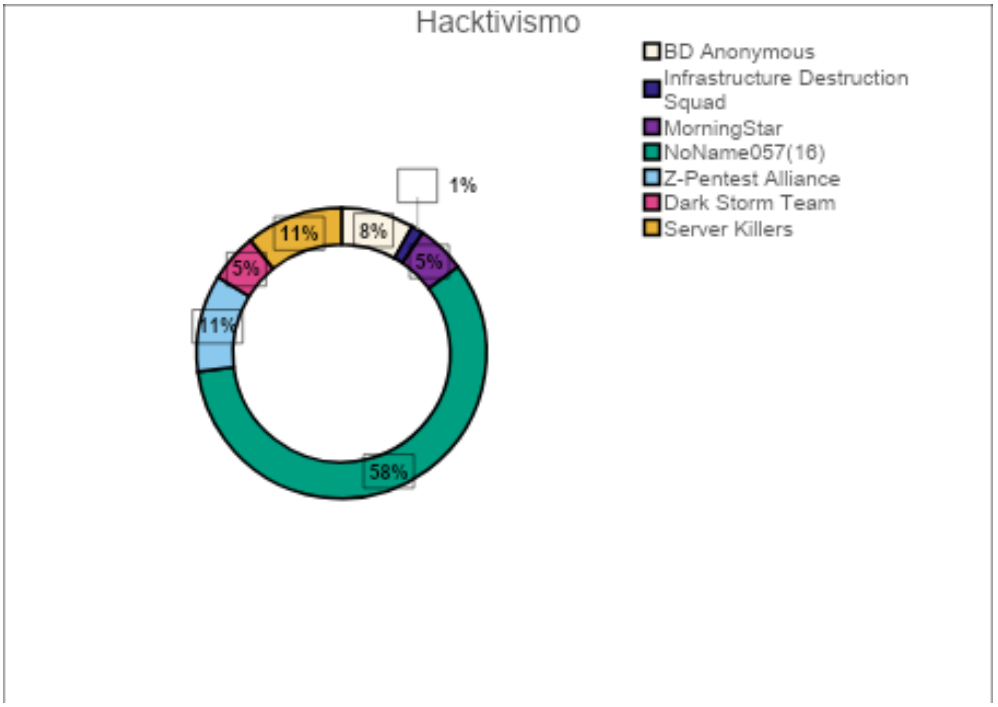
El següent apartat de l'informe ofereix una anàlisi completa del panorama de les ciberamenaces a Espanya del primer trimestre del 2026. Atesa la proximitat geogràfica i les estretes relacions entre Espanya i Andorra, es considera rellevant incloure aquestes dades com a referència del context regional. En aquest sentit, s'analitzarà l'activitat del hacktivisme i el cibercrim, incloent-hi incidents de programari de segrest (*ransomware*) i venda d'accessos il·lícits.

4.1. Hacktivisme

El següent apartat de l'informe ofereix una anàlisi completa del panorama de les ciberamenaces a Espanya del primer trimestre del 2026. Atesa la proximitat geogràfica i les estretes relacions entre Espanya i Andorra, es considera rellevant incloure aquestes dades com a referència del context regional. En aquest sentit, s'analitzarà l'activitat del hacktivisme i el cibercrim, incloent-hi incidents de programari de segrest (*ransomware*) i venda d'accessos il·lícits.

4.1.1. Ciberatacs hacktivistes

A partir de les dades recopilades, durant el primer trimestre del 2026 s'han detectat els grups següents que van realitzar atacs amb motivació hacktivista. El grup més actiu durant aquest període va ser NoName057(16), amb un 58 % dels atacs registrats, seguit pels grups Z-Pentest Alliance i Server Killers amb un 11 % tots dos.



Gràfic 2 - Grups hacktivistes més actius a Espanya durant el primer trimestre del 2026

4.1.1.1. Gener

Al gener, es van detectar 3 grups involucrats en atacs hacktivistes. Durant aquest període es pot detectar que l'activitat maliciosa va estar liderada per l'actor BD Anonymous, i va representar el 62,5 %.

	ACTOR D'AMENAÇA	NRE. D'ATACS	% TOTAL
1	BD Anonymous	5	62,50%
2	MorningStar	2	25,00%
3	Infraestructure Destruction Squad	1	12,50%

Taula 9 - Grups hacktivistes actius a Espanya durant gener de 2026

4.1.1.2. Febrer

Al febrer, NoName057(16) es proclama com el principal actor, amb 43 atacs. Grups com Z-Pentest Alliance i Server Killers tots dos amb 8 atacs cadascun, acaparen el 24,24 % del total.

	ACTOR D'AMENAÇA	NRE. D'ATACS	% TOTAL
1	NoName057(16)	43	65,15%
2	Z-Pentest Alliance	8	12,12%
2	Server Killers	8	12,12%
3	Dark Storm Team	4	6,06%
4	MorningStar	2	3,03%
5	BD Anonymous	1	1,52%

Taula 10 - Grups hacktivistes actius a Espanya durant el febrer del 2026

4.1.1.3. Març

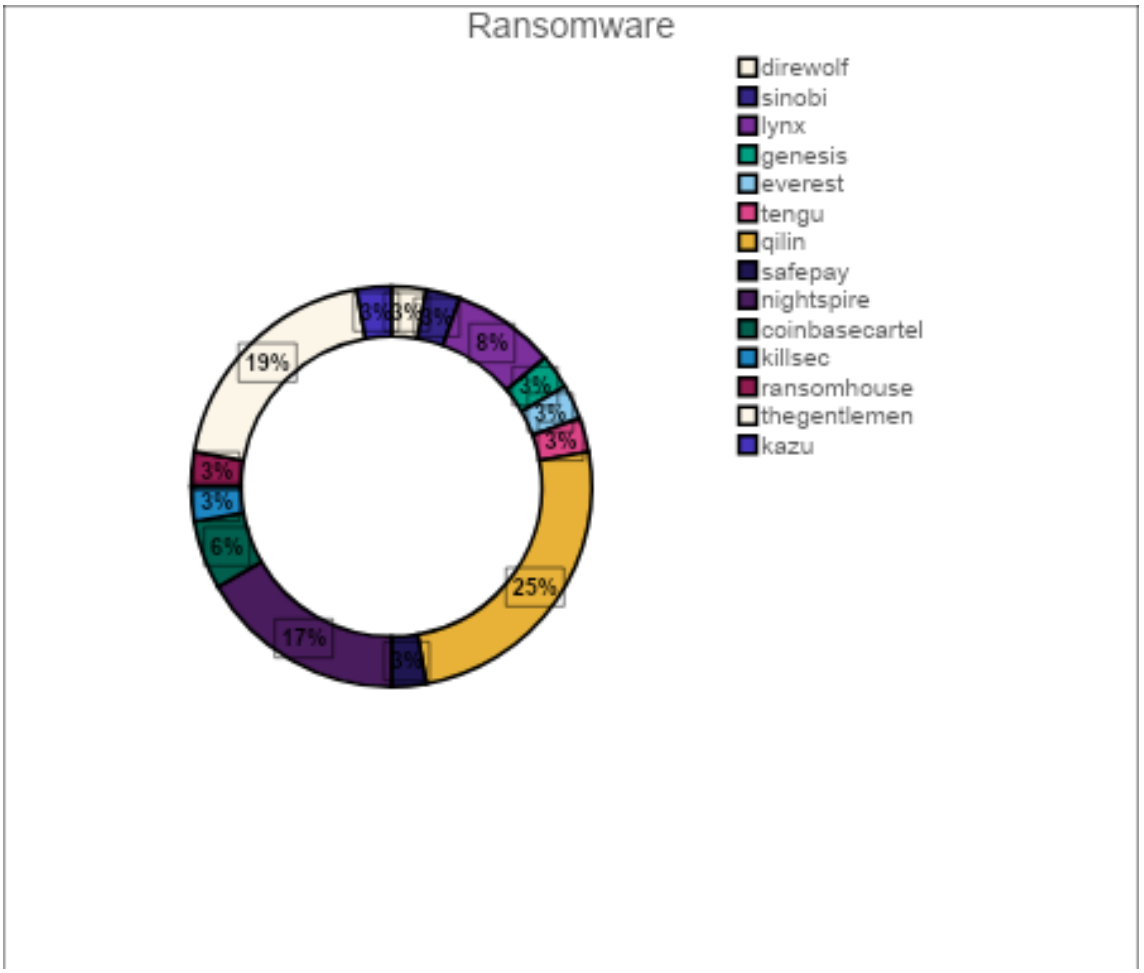
Al març, no es va detectar cap activitat d'atacs perpetrats per grups hacktivistes.

4.2. Ciberdelinqüència

A continuació, analitzarem el panorama de la ciberdelinqüència durant el primer trimestre del 2026. Aquest trimestre en comparació al quart de l'any 2025 veiem que han reduït aquest tipus d'atacs, que passen de 48 el quart trimestre del 2025 a 40 el primer trimestre del 2026, fet que suposa una disminució del 16,7 %.

4.2.1. Incidents de programari de segrest

El grup més actiu durant aquest trimestre va ser novament Qilin, que passa de 16 ciberatacs el quart trimestre del 2025 a 9 ciberatacs el primer trimestre del 2026. A partir de les dades recopilades, durant el primer trimestre del 2026 s'han detectat els grups següents que van realitzar atacs de tipus programari de segrest (*ransomware*):



Gràfic 3 - Grups de ransomware més actius durant el primer trimestre del 2026

4.2.1.1. Gener

Al gener, el grup Qilin es posiciona com el grup amb més atacs, amb un 29,41 % del total. La resta d'activitat cibercriminal està molt distribuïda, amb 11 grups diferents que fan almenys un atac de tipus *ransomware*.

	ACTOR D'AMENAÇA	NRE. D'INCIDENTS	% TOTAL
1	Qilin	5	29,41%
2	Nigthspire	2	11,76%
3	Direwolf	1	5,88%
3	Sinobi	1	5,88%
3	Lynx	1	5,88%

3	Genesis	1	5,88%
3	Everest	1	5,88%
3	Tengu	1	5,88%
3	Safepay	1	5,88%
3	Thegentlemen	1	5,88%
3	Kazu	1	5,88%
3	Payoutsking	1	5,88%

Taula 11 - Activitat de grups de ransomware a Espanya el gener de 2026

4.2.1.2. Febrer

Al febrer, Qilin torna a liderar juntament amb Thegentlemen com els grups més actius, la resta dels actors presenten una participació similar amb un ciberatac cadascun.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Qilin	3	23,08%
1	Thegentlemen	3	23,08%
2	Lynx	2	15,38%
3	Nigthspire	1	7,69%
3	Coinbasecartel	1	7,69%
3	Killsec	1	7,69%
3	Ransomhouse	1	7,69%
3	Vect	1	7,69%

Taula 12 - Activitat de grups de programari de segrest a Espanya el febrer de 2026

4.2.1.3. Març

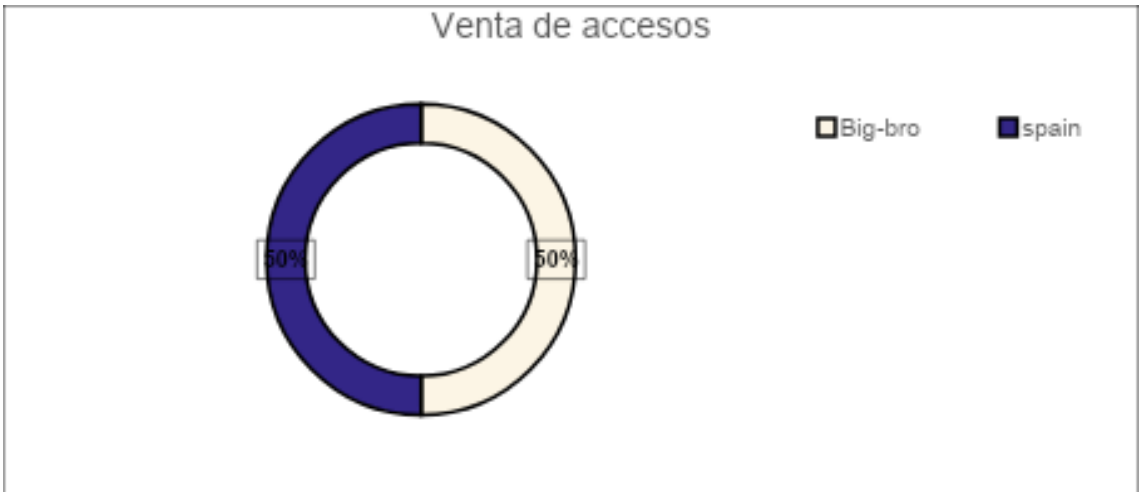
Al març, l'activitat es concentra principalment a Nightspire i Thegentleman amb un 60 % del total d'atacs. La resta dels grups representant el 40% tenen una participació menor.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Nightspire	3	30,00%
1	Thegentleman	3	30,00%
2	Qilin	1	10,00%
2	Coinbasecartel	1	10,00%
2	Akira	1	10,00%
2	Payload	1	10,00%

Taula 13 - Activitat de grups de ransomware a Espanya el març de 2025

4.2.2. Venda d'accessos

A partir de les dades recopilades, durant el primer trimestre del 2026 s'han detectat els grups Big-bro i Spain, que van fer vendes d'accés.



Gràfic 4 - Grups més actius en vendes d'accés durant el primer trimestre del 2026

4.2.2.1. Gener

Al gener és on es veurà reflectida tota l'activitat de casos cibercriminals.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	Big-bro	1	50,00%
1	Spain	1	50,00%

Taula 14 - Distribució de vendes d'accés per grup durant el gener del 2026

4.2.2.2. Febrer

Al febrer, no es va detectar cap activitat d'atacs perpetrats per grups ciberdelinqüents.

4.2.2.3. Març

Al març, no es va detectar cap activitat d'atacs perpetrats per grups ciberdelinqüents.

5. CONCLUSIONS

Després de l'anàlisi del primer trimestre de l'any 2026, veiem clarament un increment molt significatiu de l'activitat de les ciberamenaces a nivell global, amb una pujada del 54 % del volum de les ciberamenaces en comparació del quart trimestre de l'any 2025. Aquest gran augment es deu principalment a l'activitat cibernètica de conflictes geopolítics.

Com ja indiquem en el trimestre anterior, amb una geopolítica tan inestable com l'actual pensem que per al pròxim període de l'any (T2 2026) es pot esperar un nou increment o un volum similar de ciberatacs, principalment motivat per les guerres actuals d'Ucraïna/Rússia i Gaza/Israel, com també el conflicte de l'Orient Mitjà, que està actualment en pausa, però el conflicte regional a la zona continua molt actiu.

L'escenari actual apunta a la continuïtat de campanyes hacktivistes, operacions de desinformació, atacs dirigits contra infraestructures governamentals, com també una continuïtat de l'activitat de la ciberdelinqüència, amb campanyes de programari de segrest i robatori d'accessos.

Amb totes aquestes dades analitzades, l'informe dona per conclòs l'anàlisi corresponent al primer trimestre de l'any 2026, i deixa una base de referència per al trimestre següent, en què serà de vital importància continuar monitorant l'evolució dels actors d'amenaça, el context geopolític i les noves campanyes que podran afectar sectors crítics i estratègics.

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.