ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Panorama de les ciberamenaces en el tercer trimestre de 2025

TLP: WHITE

OCTUBRE 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	29/10/2025	31/10/2025

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 oferir una visió actualitzada del panorama de les ciberamenaces del tercer trimestre de l'any 2025, amb l'objectiu de conèixer quines són les amenaces emergents a les quals s'han d'enfrontar les organitzacions i els governs, comparar aquestes dades amb les del primer i segon trimestre per poder treure conclusions i veure l'evolució del panorama.

Per fer aquest informe s'han extret dades globals, continentals i fins i tot d'Espanya. Amb la recopilació d'aquestes dades, podrem entendre què està succeint allà fora, al ciberespai, i prestarem més atenció a les dades més rellevants per a Andorra a causa de factors com ara la proximitat geogràfica i el context geopolític.

El trimestre anterior es va caracteritzar per una gran activitat per part dels grups cibercriminals, que van enderrocar els grups hacktivistes després de la seva dominància el primer trimestre de l'any. En aquest trimestre tot continua igual, els ciberdelinqüents continuen dominant a nivell mundial, encara que a nivell europeu la cosa difereix, perquè diferents conflictes geopolítics que es tractaran més endavant en aquest informe fan que la balança es decanti pels atacs moguts per raons ideològiques.

Al llarg d'aquest informe, analitzarem els sectors més atacades, els països més afectats, els actors d'amenaça més actius, les motivacions darrere dels ciberatacs i les diferents campanyes executades per actors d'amenaça.

Per acabar, s'exposarà de manera detallada i especificada l'activitat cibernètica que s'ha viscut a Espanya durant el tercer trimestre.

3. TENDÈNCIES I EVOLUCIÓ DE LES CIBERAMENACES AL 3T 2025

A l'apartat següent, s'analitzaran els ciberatacs registrats el tercer trimestre del 2025 a nivell global i regional, les tendències, l'evolució, les motivacions, els actors d'amenaça més actius i els patrons d'amenaces.

3.1. Ciberatacs registrats durant el tercer trimestre del 2025

Durant el tercer trimestre del 2025 es van registrar 3.985 ciberatacs a nivell mundial, cosa que ha suposat una baixada del 4 % respecte als registrats durant el segon trimestre i una reducció acumulada del 17,7 % en comparació del primer trimestre de l'any.

Tot i això, i malgrat aquest descens, el volum d'atacs continua sent elevat i no difereix del nombre d'atacs del segon trimestre, amb una mitjana superior als 40 ciberatacs diaris.

3.2. Europa continua dominant el nombre d'atacs rebuts

Europa, igual que els trimestres anteriors de l'any 2025, veiem que segueix dominant pel que fa als ciberatacs rebuts, s'han registrat un 4,1 % més de ciberatacs durant aquest trimestre en comparació a l'anterior. Europa continua mantenint-se com el continent més atacat, amb una concentració fins al 37,7 % dels ciberatacs que es registren a nivell mundial.

A la taula següent es mostren les dades relatives als ciberatacs registrats a cada continent i la seva comparativa en els diferents trimestres:

	CIBERATACS 1T	CIBERATACS 2T	CIBERATACS 3T
Europa	38,6 %	33,6 %	37,7 %
Amèrica	36,9 %	31,2 %	32,2 %
Àsia	15,4 %	24,5 %	16,1 %
Àfrica	1,5 %	3,4 %	6,0 %
Oceania	1,4 %	1,5 %	1,6 %
N/D	6,2 %	5,8 %	6,5 %

Taula 1 - Comparativa trimestral de ciberatacs registrats per continent

Com es pot apreciar a la taula, Europa ha registrat un 5,5 % més d'atacs respecte a Amèrica durant aquest trimestre. També veiem com Europa cada cop es distancia més en comparació a altres regions del món.

Tot i que Europa sigui el continent més atacat, veiem com els Estats Units, una vegada més, es manté com el país més atacat del món. Torna a ocupar el lloc més alt del rànquing, dominant molt per sobre dels altres països, igual que el primer trimestre i el segon trimestre.

S'ha elaborat un top ten de països més afectats pels ciberatacs el tercer trimestre, i veiem com els Estats Units continuen mantenint una diferència força significativa respecte a altres països:

	PAÍS	Nombre d'atacs	% TOTAL
1	Estats Units	1024	26,2 %
2	Alemanya	335	8,6 %
3	França	208	5,3 %
4	Itàlia	194	5,0 %
5	Ucraïna	155	4,0 %
6	Marroc	137	3,5 %
7	Espanya	126	3,2 %
8	Japó	110	2,8 %
9	Gran Bretanya	90	2,3 %
10	Canadà	86	2,2 %

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

3.3. Actors d'amenaça més actius

L'actor d'amenaces més actiu durant aquest tercer trimestre, igual que el primer i el segon, ha estat el grup prorús NoName057(16), a qui se li atribueixen 786 ciberatacs, i ha provocat el 20,1 % dels registrats durant aquest període. L'operació Eastwood no ha estat un impediment per al grup prorús que torna a ser novament al TOP 1.

Qilin i Akira, com ja va succeir el primer i segon trimestre, tornen a formar part d'aquest rànquing i ho fan amb més números d'atacs que mai, i s'erigeixen en els grups de programari de segrest més actius el tercer trimestre de l'any.

Com es pot apreciar a la taula, la gran majoria d'atacs registrats provenen de grups vinculats al cibercrim, representen un 70 % del total, cosa que ja vam veure al segon trimestre, tot i que al primer la balança es decantava més pels grups hacktivistes.

	ACTOR D'AMENAÇA	MÈTODE	CATEGORIA	Nombre d'atacs	% TOTAL
1	NoName057(16)	DDoS	Hacktivisme	786	20,1 %
2	Keymous+	DDoS	Hacktivisme	348	8,9 %
3	Qilin	Ransomware	Cibercrim	216	5,5 %
4	Akira	Ransomware	Cibercrim	163	4,2 %
5	INC Ransom	Ransomware	Cibercrim	124	3,2 %
6	Play	Ransomware	Cibercrim	104	2,7 %
7	Safepay	Ransomware	Cibercrim	68	1,7 %
8	Red Wolf Cyber	DDoS	Hacktivisme	67	1,7 %
9	Lynx	Ransomware	Cibercrim	60	1,5 %
10	DragonForce	Ransomware	Cibercrim	60	1,5 %

Taula 3 - Top 10 d'actors més actius d'amenaça durant el tercer trimestre

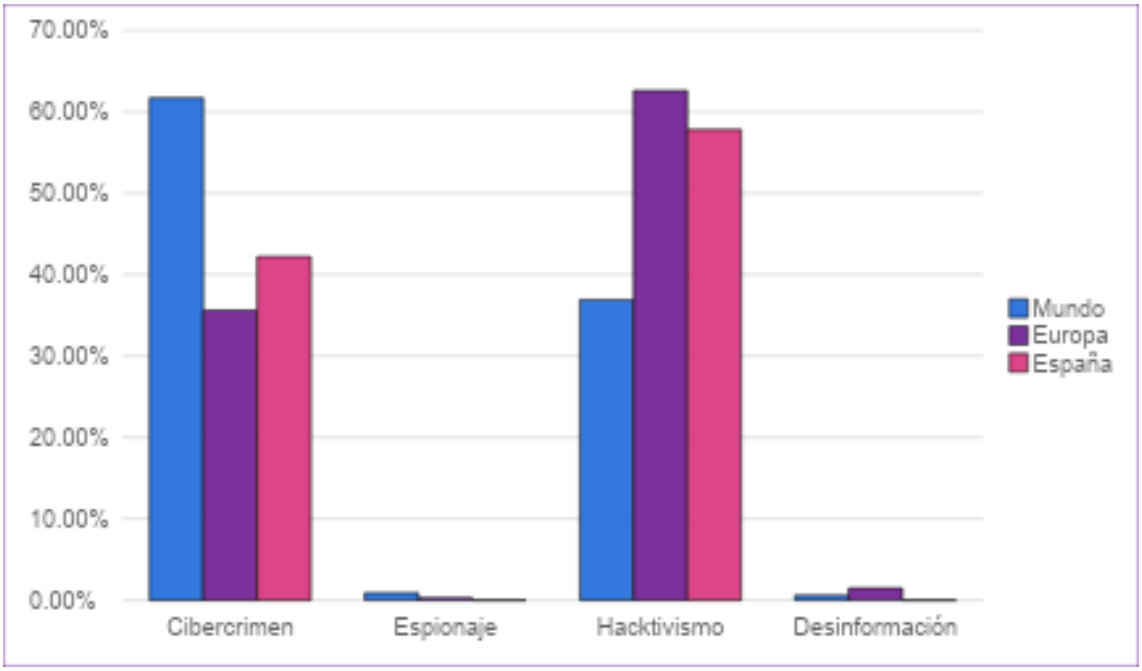
3.4. Motivacions després dels ciberatacs

A nivell europeu i espanyol, les campanyes de ciberatacs motivades pel rèdit polític han estat les més recurrents durant aquest tercer trimestre, al contrari que al segon trimestre en què el rèdit econòmic va ser més recurrent.

El tercer trimestre, el cibercrim és el problema més gran del món, i destaca per sobre de les dades d'Europa i Espanya.

El hacktivisme té una presència més significativa a Europa i Espanya aquest tercer trimestre, això és degut als atacs diaris del grup prorús NoName057(16), atès que la majoria de les seves víctimes són del continent europeu.

Es mostra un gràfic que recull les dades sobre la proporció de ciberatacs registrats en funció de les motivacions que les van impulsar.



Taula 4 - Distribució de ciberatacs per motivació al tercer trimestre

A continuació, es mostra una taula que recull les dades sobre la proporció de ciberatacs registrats en funció de les motivacions que les van impulsar el primer, segon i tercer trimestre. Aquesta taula permet veure com ha anat evolucionant tot al llarg de l'any.

El cibercrim és el problema principal al món, a Europa i a diferents regions la seva aparició no és tan consistent. El hacktivisme és més rellevant a Europa, cosa que indica un patró molt diferencial a la resta del món. L'espionatge i la desinformació són molt puntuals a diferents regions, els casos informats són molt pocs.

	MÓN						EUROPA						ESPANYA					
	primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre	
	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%
Cibercrim	2935	60,6%	2360	56,9%	2457	61,7%	559	29,9%	535	39,7%	534	35,6%	47	22,9%	69	88,5%	54	42,2%
Espionatge	39	0,8%	44	1,1%	35	0,9%	9	0,5%	9	0,7%	5	0,3%	0	0,0%	0	0,0%	0	0,0%
Hacktivisme	1852	38,3%	1723	41,5%	1469	36,9%	1288	69,0%	796	59,1%	940	62,6%	158	77,1%	9	11,5%	74	57,8%
Desinformació	14	0,3%	20	0,5%	24	0,6%	12	0,6%	7	0,5%	23	1,5%	0	0,0%	0	0,0%	0	0,0%
TOTAL	**4840**	**100,0%**	**4147**	**100,0%**	**3985**	**100,0%**	**1868**	**100,0%**	**1347**	**100,0%**	**1502**	**100,0%**	**205**	**100,0%**	**78**	**100,0%**	**128**	**100,0%**

Taula 5 - Evolució trimestral de ciberatacs segons les motivacions

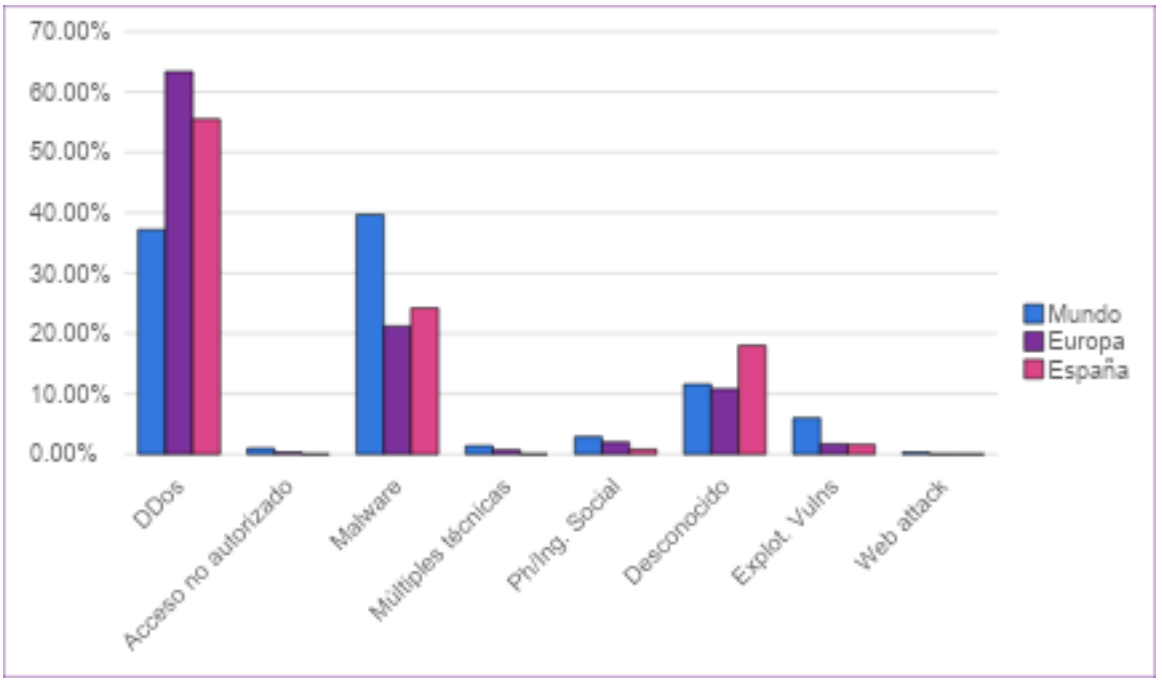
3.5. Tipologia de ciberatacs més recurrents

Basat en les dades, a nivell mundial, europeu i espanyol, els atacs DDoS, novament, han estat els més prevalents.

L'ús del codi maliciós novament torna a tenir molta rellevància com ja la va tenir en el primer i segon trimestre.

Encara que el cibercrim amb codi maliciós abasta més actors, els atacs DDoS són molt més nombrosos en el total.

Espanya s'ha caracteritzat durant aquest trimestre perquè els atacs dels quals ha estat víctima amb més recurrència han estat els atacs DDoS, al contrari del trimestre anterior on l'ús de codi maliciós va ser més gran.



Taula 6 - Distribució dels ciberatacs més freqüents al tercer trimestre

A continuació, es mostra una taula que recull les dades sobre la proporció de les tipologies de ciberatacs registrades el primer, segon i tercer trimestre. Aquesta taula permet veure com ha anat evolucionant tot al llarg de l'any.

Els atacs DDoS i programari maliciós (programari de segrest) són els més freqüents globalment. A Europa els atacs DDoS són els que fan més soroll, aquestes dades estan molt correlacionades amb el nivell d'hacktivisme que pateix el Vell Continent.

	MÓN						EUROPA						ESPANYA					
	primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre	
	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%
DDos	1855	38,3%	1721	41,5%	1483	37,2%	1297	69,4%	807	59,9%	952	63,4%	158	77,1%	9	11,5%	71	55,5%
Accés no autoritzat	34	0,7%	35	0,8%	38	1,0%	5	0,3%	6	0,4%	4	0,3%	0	0,0%	1	1,3%	0	0,0%
programari maliciós	1760	36,4%	1553	37,4%	1581	39,7%	343	18,4%	372	27,6%	319	21,2%	29	14,1%	43	55,1%	31	24,2%
Múltiples tècniques	57	1,2%	27	0,7%	55	1,4%	12	0,6%	7	0,5%	10	0,7%	0	0,0%	0	0,0%	0	0,0%
Doctorat/Ing. Social	104	2,1%	121	2,9%	114	2,9%	17	0,9%	20	1,5%	30	2,0%	0	0,0%	1	1,3%	1	0,8%
Desconegut	476	9,8%	491	11,8%	463	11,6%	135	7,2%	108	8,0%	162	10,8%	11	5,4%	22	28,2%	23	18,0%
Explot. Vulns	517	10,7%	177	4,3%	240	6,0%	53	2,8%	24	1,8%	25	1,7%	5	2,4%	1	1,3%	2	1,6%
Atac web	37	0,8%	22	0,5%	11	0,3%	6	0,3%	3	0,2%	0	0,0%	2	1,0%	1	1,3%	0	0,0%
TOTAL	4840	100,0%	4147	100,0%	3985	100,0%	1868	100,0%	1347	100,0%	1502	100,0%	205	100,0%	78	100,0%	128	100,0%

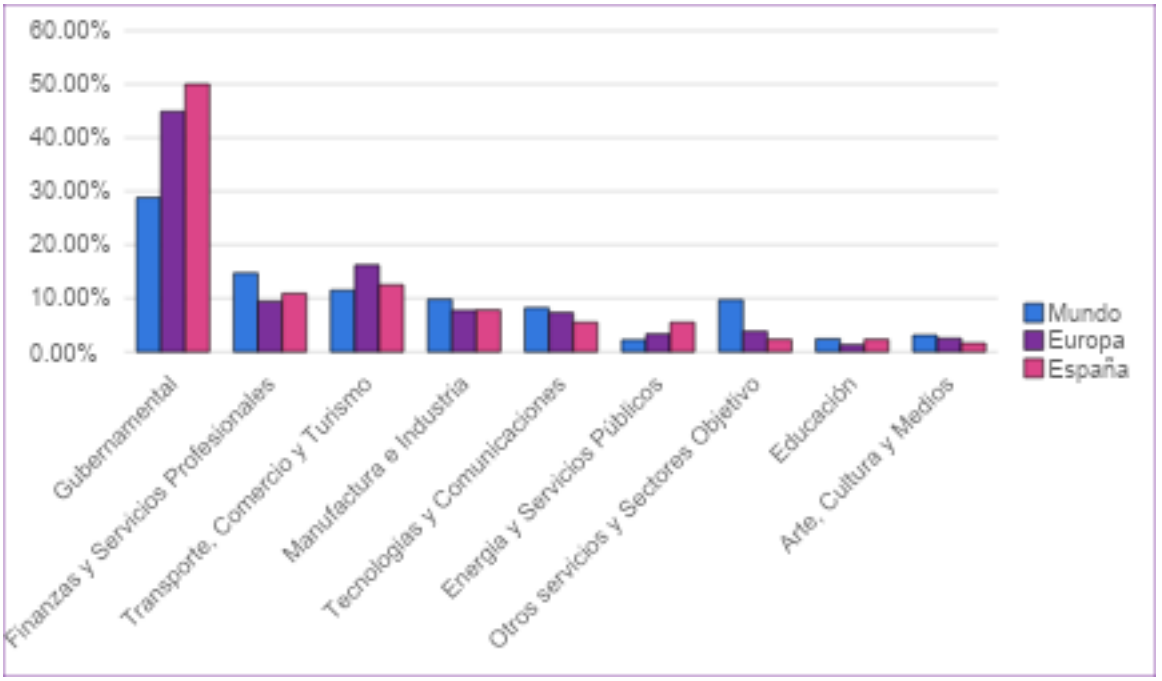
Taula 7 - Distribució i evolució dels tipus de ciberatacs per trimestre

3.6. Els sectors més afectats

Si s'analitzen les dades veiem que hi ha una tendència que es manté com al primer i al segon trimestre i és que, a les regions a nivell mundial i europeu, el sector governamental ha estat l'objectiu principal dels ciberatacs; Espanya, aquest trimestre s'uneix a aquesta tendència, amb un 50 % dels atacs a nivell governamental.

El sector de finances i serveis professionals és el segon més atacat a tot el món, aquest sector representa un focus molt important per als atacs, ja que la informació del sector és sensible i molt lucrativa per als actors d'amenaça.

La indústria de transport, comerç i turisme ha tornat a ser rellevant a l'època de vacances a l'estiu, com ja ho va ser el primer trimestre amb l'època nadalenca.



Taula 8 - Sectors més impactats per ciberatacs al tercer trimestre

A continuació, s'exposa la taula amb les dades detallades relatives al primer, segon i tercer trimestre. Aquesta taula permet veure com ha anat evolucionant tot al llarg de l'any.

El sector governamental és el més atacat al continent europeu. Els sectors estratègics (finances, manufactura, tecnologies…) són objectius molt recurrents a nivell mundial, europeu i en diferents regions.

SECTORS	EUROPA						ESPANYA						MÓN					
	primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre		primer trimestre		segon trimestre		tercer trimestre	
	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%	Total	%
Agricultura i Recursos Naturals	8	0,4%	3	0,2%	4	0,3%	2	1,0%	0	0,0%	0	0,0%	26	0,5%	17	0,4%	19	0,5%
Art, Cultura i Mitjans	43	2,3%	35	2,6%	37	2,5%	3	1,5%	2	2,6%	2	1,6%	127	2,6%	142	3,4%	123	3,1%
Construcció i infraestructura	19	1,0%	23	1,7%	23	1,5%	0	0,0%	0	0,0%	0	0,0%	153	3,2%	111	2,7%	114	2,9%
Educació	29	1,6%	17	1,3%	19	1,3%	0	0,0%	3	3,8%	3	2,3%	121	2,5%	104	2,5%	95	2,4%
Energia i Serveis Públics	108	5,8%	55	4,1%	50	3,3%	2	1,0%	6	7,7%	7	5,5%	159	3,3%	123	3,0%	88	2,2%
Finances i serveis professionals	197	10,5%	149	11,1%	141	9,4%	13	6,3%	17	21,8%	14	10,9%	633	13,1%	611	14,7%	587	14,7%
Governamental	783	41,9%	519	38,5%	675	44,9%	138	67,3%	12	15,4%	64	50,0%	1204	24,9%	1122	27,1%	1148	28,8%
Assistència sanitària	37	2,0%	26	1,9%	19	1,3%	5	2,4%	6	7,7%	1	0,8%	255	5,3%	232	5,6%	195	4,9%
Tecnologies i comunicacions	191	10,2%	131	9,7%	110	7,3%	6	2,9%	2	2,6%	7	5,5%	460	9,5%	342	8,2%	326	8,2%
Manufactura i Indústria	122	6,5%	130	9,7%	116	7,7%	8	3,9%	13	16,7%	10	7,8%	548	11,3%	407	9,8%	392	9,8%
Altres serveis i sectors objectiu	37	2,0%	53	3,9%	57	3,8%	1	0,5%	5	6,4%	3	2,3%	397	8,2%	400	9,6%	386	9,7%
Organitzacions benèfiques (ONG, Fundacions…)	20	1,1%	31	2,3%	8	0,5%	5	2,4%	2	2,6%	1	0,8%	72	1,5%	81	2,0%	52	1,3%
Transport, Comerç i Turisme	274	14,7%	175	13,0%	243	16,2%	22	10,7%	10	12,8%	16	12,5%	685	14,2%	455	11,0%	460	11,5%
TOTAL	1868	100,0%	1347	100,0%	1502	100,0%	205	100,0%	78	100,0%	128	100,0%	4840	100,0%	4147	100,0%	3985	100,0%

Taula 9 - Comparativa trimestral dels sectors més impactats per ciberatacs

4. PANORAMA DE CIBERAMENACES D'ESPANYA

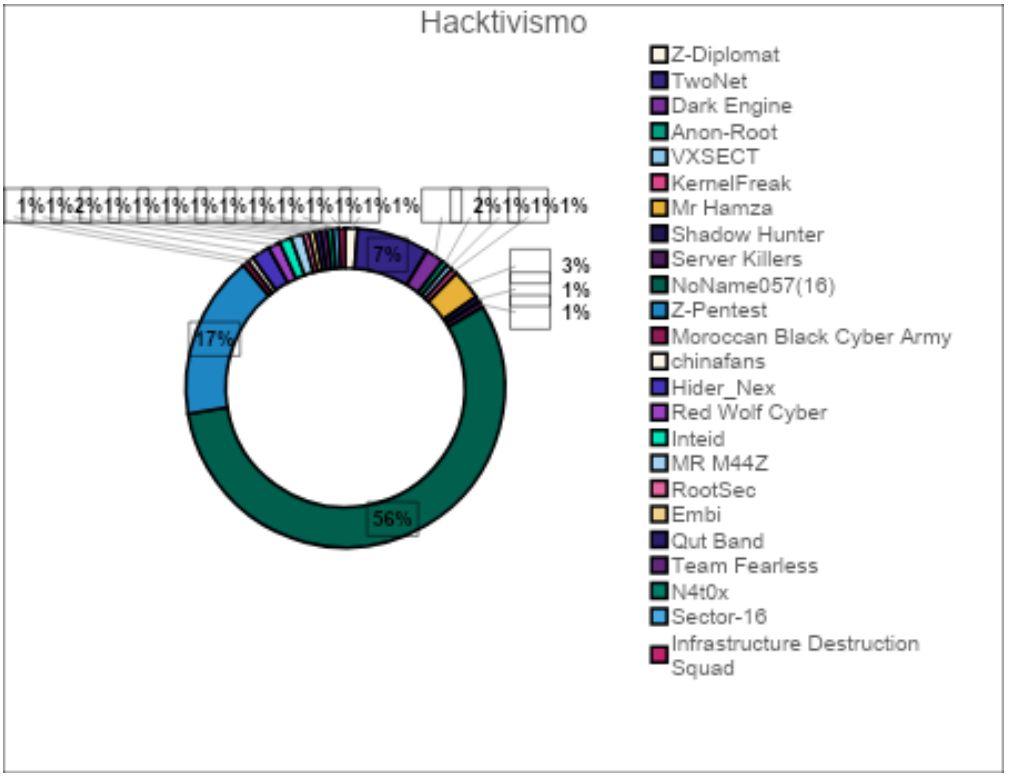
L'apartat següent de l'informe ofereix una anàlisi completa del panorama de ciberamenaces a Espanya del tercer trimestre del 2025, on s'analitzarà l'activitat del hacktivisme i el cibercrim, incloent-hi les campanyes més rellevants, incidents de programari de segrest i venda d'accessos.

4.1. Hacktivisme

A continuació, analitzarem el panorama del hacktivisme durant el tercer trimestre del 2025. Aquest trimestre en comparació del segon veiem que la balança s'ha inclinat en aquest tipus d'atacs, passant d'un 11,5 % al 57,8 %. S'han detectat múltiples causes polítiques i socials que han fet que aquest trimestre tingui més pes els atacs hacktivistes en comparació del cibercrim.

4.1.1. Activitats destacades

A partir de les dades recopilades, durant el tercer trimestre del 2025 s'han detectat els grups següents que van realitzar atacs amb motivació hacktivista. El grup més actiu durant aquest període va ser NoName057(16).



Taula 10 - Grups més actius en hacktivisme a Espanya durant el tercer trimestre del 2025

4.1.1.1. Juliol

El juliol es van detectar 9 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	Z-Diplomat	2	16,67 %
1	TwoNet	2	16,67 %
1	Dark Engine	2	16,67 %
2	Anon-Root	1	8,33 %
2	VXSECT	1	8,33 %
2	KernelFreak	1	8,33 %
2	Mr.Hamza	1	8,33 %
2	Shadow Hunter	1	8,33 %
2	Server Killers	1	8,33 %

Taula 11 - Grups hacktivistes actius a Espanya durant el juliol del 2025

4.1.1.2. Agost

L'agost, NoName057(16) es proclama com a principal actor. Z-Pentest, aliat i soci de NoName057(16), té també força protagonisme durant aquest mes. Aquests dos grups a l'agost van protagonitzar una campanya força rellevant que es detalla més endavant en aquest document.

	ACTOR D'AMENAÇA	Nre. d'atacs	% TOTAL
1	NoName057(16)	85	72,65 %
2	Z-Pentest	24	20,51 %
3	Mr Hamza	3	2,56 %
4	TwoNet	2	1,71 %
5	Moroccan Black Cyber Army	1	0,85 %
5	chinafans	1	0,85 %
5	Dark Engine	1	0,85 %

Taula 12 - Grups hacktivistes actius a Espanya durant l'agost del 2025

4.1.1.3. Setembre

El setembre, el grup NoName057(16) cau al 18,18 %, i cedeix el lideratge al TwoNet que passa de l'1,71 % al 24,24 %. Z-Pentest, col·laborador de NoName057(16), també cau més d'un 10 % després de la campanya desplegada al juliol.

	ACTOR D'AMENAÇA	Nre. d'atacs	% TOTAL
1	TwoNet	8	24,24 %
2	NoName057(16)	6	18,18 %
3	Z-Pentest	3	9,09 %
3	Hider_Nex	3	9,09 %
4	Red Wolf Cyber	2	6,06 %
4	Inteid	2	6,06 %
4	MR M44Z	2	6,06 %
5	RootSec	1	3,03 %
5	Embi	1	3,03 %
5	Mr Hamza	1	3,03 %
5	Qut Band	1	3,03 %
5	Team Fearless	1	3,03 %
5	N4t0x	1	3,03 %
5	Sector-16	1	3,03 %
5	Infrastructure Destruction Squad	1	3,03 %

Taula 13 - Grups hacktivistes actius a Espanya durant el setembre del 2025

4.1.2. Campanyes

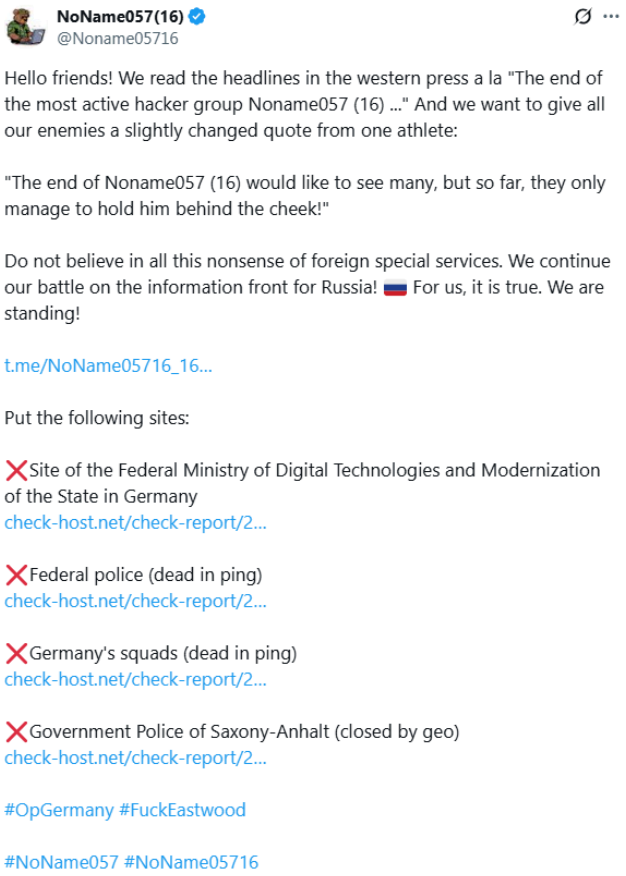
Tot seguit, es detallaran les campanyes més rellevants de l'hacktivisme a Espanya del tercer trimestre de l'any 2025.

4.1.2.1. #OpSpain #FuckEastwood #TempsDeRetribució

La campanya amb els hashtags #OpSpain #FuckEastwood #TimeOfRetribution, va ser executada pels grups NoName057(16) i Z-Pentest, com a venjança després dels esdeveniments ocorreguts a l'Operació Eastwood.

L'Operació Eastwood, que va iniciar entre el 14 i 17 de juliol de 2025, va permetre desmantellar gran part de les infraestructures del grup hacktivista NoName057(16). L'operació va ser coordinada per l'Europol i l'Eurojust, en què van participar 19 països, entre ells membres de la Unió Europea, com ara França, Alemanya i Espanya, i altres aliats com els Estats Units i el Canadà.

NoName057(16) es va pronunciar després d'aquest dur esdeveniment amb el següent post a X, indicant que tot el que havia exposat Europol era mentida i mostrava nous atacs dirigits a Alemanya.

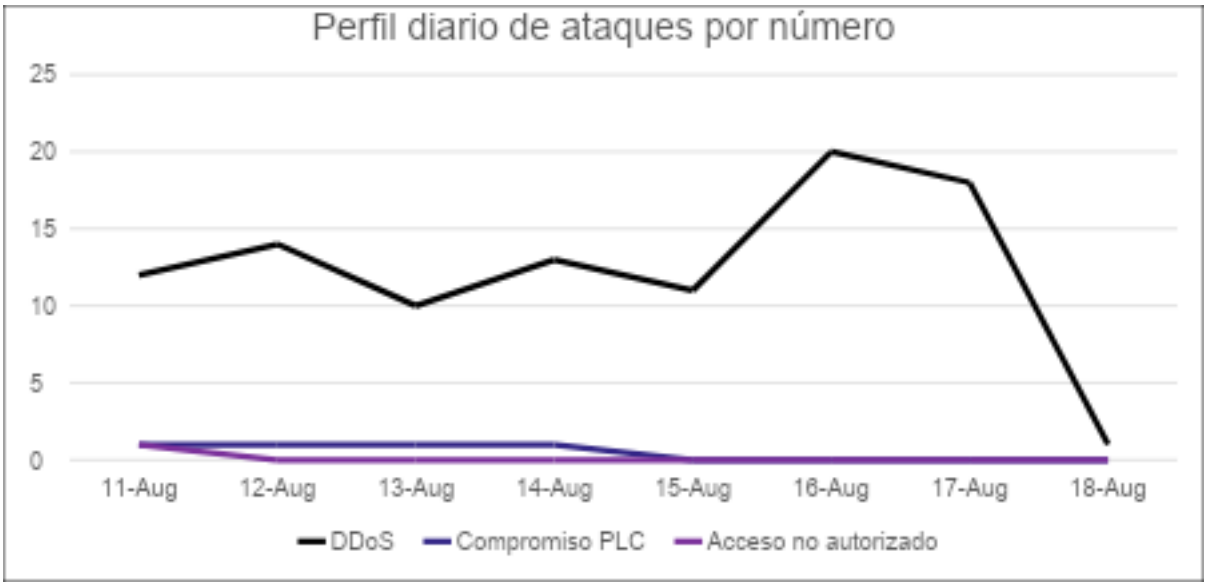


Taula 14 - Publicació de NoName057(16) a X després de l'operació Eastwood

Tot i aquest post a X, gran part de la infraestructura de NoName057(16) es va intervenir, d'això no en queda cap dubte. Això va ser un cop dur per al grup prorús, tot i que va saber recompondre's i va començar la seva campanya contra diferents països membres de l'OTAN.

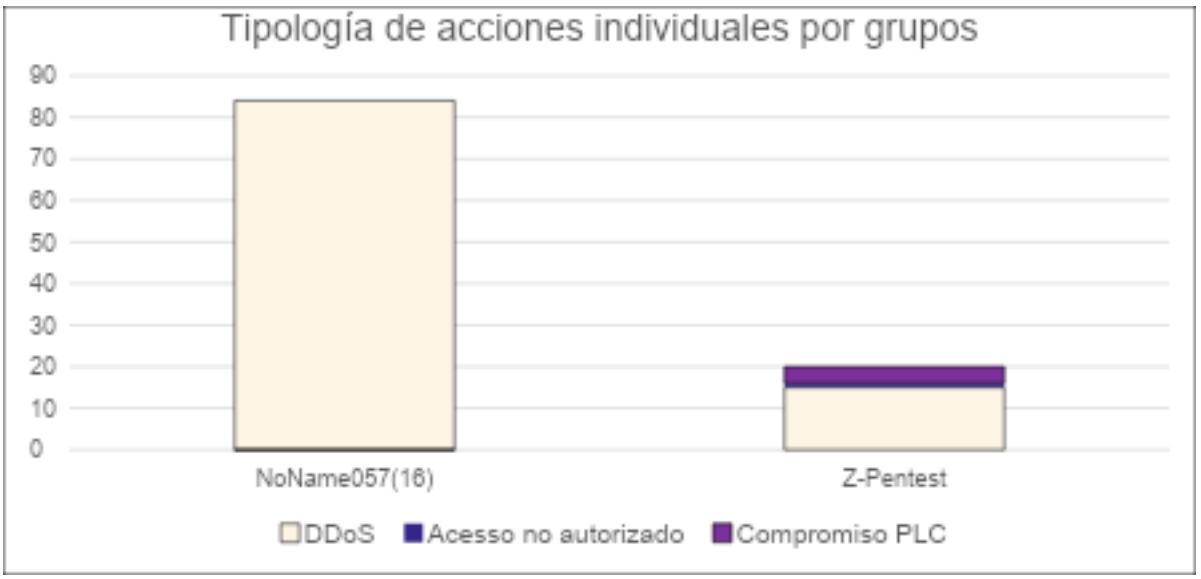
La campanya #OpSpain #FuckEastwood #TimeOfRetribution es va desenvolupar entre els dies 11 i 18 d'agost, on es van fer 104 atacs (99 DDoS, 4 compromisos PLC i 1 accés forçat).

A continuació mostrarem el perfil diari dels atacs per nombre que van protagonitzar els grups NoName057(16) i Z-Pentest. Veiem que els atacs DDoS van tenir més protagonisme. Els compromisos PLC van ser puntuals, tot i que van tenir un gran impacte per a les entitats afectades.



Taula 15 - Perfil diari d'atacs per número

En la tipologia d'accions individuals per grups, veiem que NoName057(16) es va enfocar completament en la seva especialitat, els atacs DDoS. Z-Pentest veiem que es va repartir diverses accions on destaquen els compromisos PLC que van tenir un gran impacte.



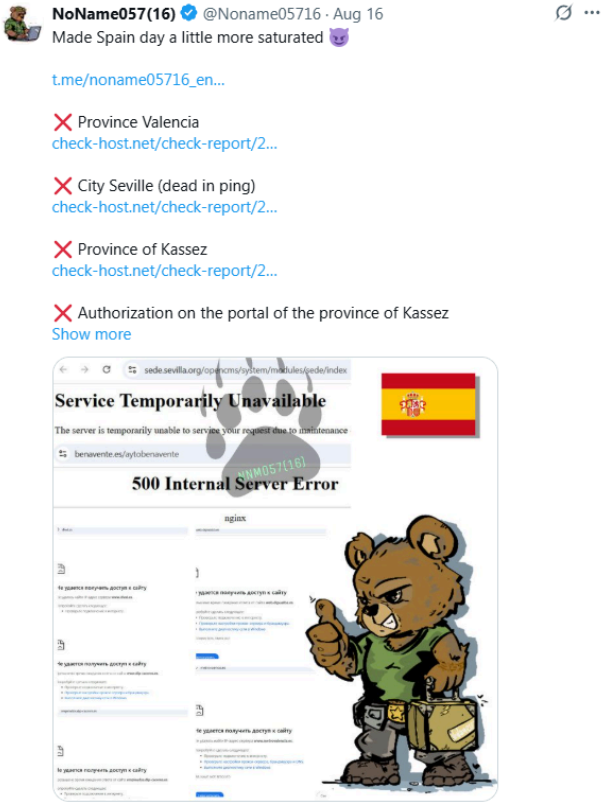
Taula 16 - Tipologia d'accions individuals per grups

Z-Pentest es va pronunciar amb el missatge següent al seu canal de Telegram, on mostra proves clares d'un compromís PLC:

Taula 17 - Proves de compromís PLC publicades per Z-Pentest al seu canal de Telegram

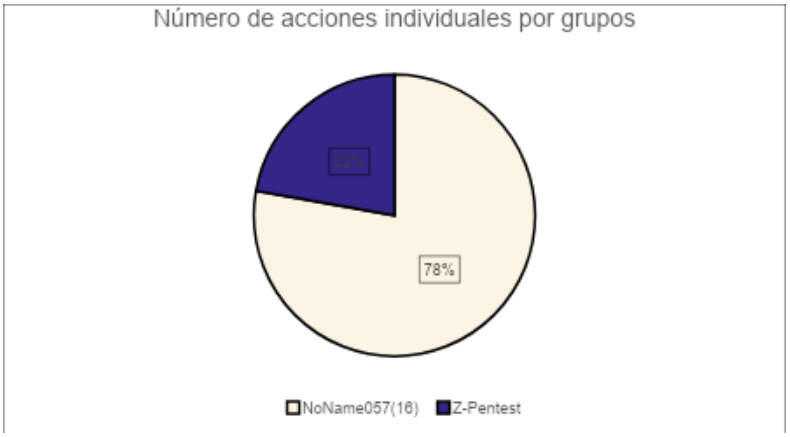
Treball de l'alumne. Espanya. ✔️ Ens introduïm dins del sistema de gestió de filtració d'aigua —la seguretat és feble, tot sota control.

NoName057(16) també es va pronunciar respecte als seus atacs DDoS.



Taula 18 - Publicació de NoName057(16) sobre els seus atacs DDoS

Amb el gràfic següent podem observar el nombre d'accions individuals pels grups en aquesta operació. Veiem clarament com NoName057(16) es consolida com a líder d'aquesta campanya i Z-Pentest actua com un col·laborador tàctic.



Taula 19 - Nombre d'accions individuals per grups

4.1.2.2. #OpMortadelos

La campanya amb el hashtag #OpMortadelos, va ser executada pels grups NoName057(16), Z-Pentest, TwoNet, Mr Hamza, Inteid com a venjança després de l'ordre d'arrest posada per l'Audiència Nacional contra Enrique Arias Gil, àlies «Desinformador Rus» per «delictes de sabotatge amb finalitat terrorista.»

Després de l'ordre d'arrest posada per l'Audiència Nacional, NoName057(16) es va pronunciar amb el missatge següent al seu canal de Telegram:

Taula 20 - Publicació de NoName057(16) després de l'ordre d'arrest d'Enrique Arias Gil (Desinformador Rus)

«Portem a terme un atac en senyal de solidaritat amb el nostre simpatitzant injustament condemnat (https://t[.]me/c/2634086323/1425), autor del canal Desinformador rus (https://t[.]me/musicarusaesp) 😈»

A continuació, desglossarem els atacs executats per cadascun dels grups implicats a la campanya #OpMortadelos:

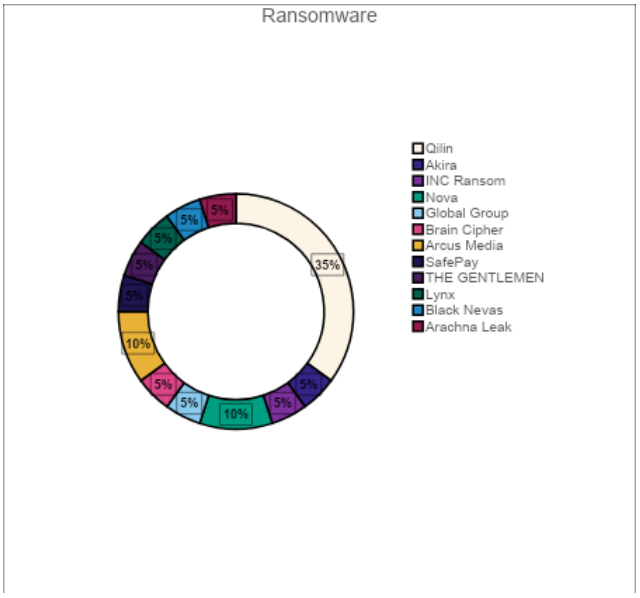
- NoName057(16) realitza 6 atacs DDoS.
- TwoNet realitzo 4 filtracions de dades.
- Inteid realitzo un compromís PLC.
- Z-Pentest realitzo dos compromisos PLC.
- N4t0x realitzo una filtració de dades.
- Mr Hamza va realitzar 7 atacs DDoS contra webs de govern.

4.2. Cibercrim

A continuació, analitzarem el panorama del cibercrim durant el tercer trimestre del 2025. Aquest trimestre en comparació del segon veiem que s'han reduït aquest tipus d'atacs, passant del 88,5 % al 42,2 %. Com hem comentat anteriorment, s'han detectat múltiples causes polítiques i socials que han fet que el tercer trimestre tinguin més pes els atacs hacktivistes en comparació amb el cibercrim, és per això la baixada tan agressiva que han patit aquest tipus d'atacs.

4.2.1. Incidents de ransomware

A partir de les dades recopilades, durant el tercer trimestre del 2025 s'han detectat els grups següents que van realitzar atacs de tipus programari de segrest. El grup més actiu durant aquest trimestre va ser Qilin.



Taula 21 - Grups més actius en ransomware durant el tercer trimestre del 2025

4.2.1.1. Juliol

El juliol, el grup Qilin domina el panorama amb un terç dels atacs registrats, un 33 %. 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	3	33,33 %
2	Akira	1	11,11 %
2	INC Ransom	1	11,11 %
2	Nova	1	11,11 %
2	Global Group	1	11,11 %
2	Brain Cipher	1	11,11 %
2	Arcus Media	1	11,11 %

Taula 22 - Activitat de grups de ransomware a Espanya el juliol de 2025

4.2.1.2. Agost

L'agost, Qilin repeteix la seva dominància respecte del mes anterior. Es pot apreciar una reducció dels atacs del 55% en comparació del juliol.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	Qin	3	75,00 %
2	SafePay	1	25,00 %

Taula 23 - Activitat de grups de ransomware a Espanya l'agost de 2025

4.2.1.3. Setembre

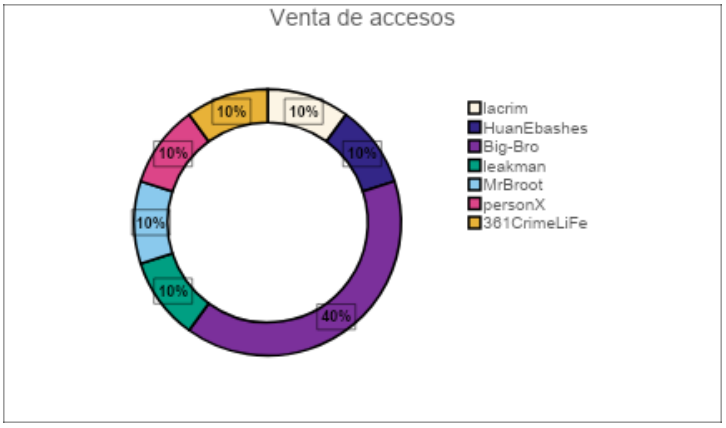
El setembre, l'escenari està completament equilibrat i sense cap líder dominant.

	ACTOR D'AMENAÇA	NOMBRE D'INCIDENTS	% TOTAL
1	THE GENTLEMEN	1	14,29 %
1	Qilin	1	14,29 %
1	Nova	1	14,29 %
1	Lynx	1	14,29 %
1	Arcus Media	1	14,29 %
1	Black Nevas	1	14,29 %
1	Arachna Leak	1	14,29 %

Taula 24 - Activitat de grups de ransomware a Espanya el setembre de 2025

4.2.2. Venda d'accessos

A partir de les dades recopilades, durant el tercer 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.



Taula 25 - Grups més actius en vendes d'accés durant el tercer trimestre del 2025

4.2.2.1. Juliol

Al juliol, l'activitat és limitada. No s'observen patrons de gran volum; això pot indicar que les vendes d'aquestes dades han estat dirigides i molt selectives.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	lacrim	1	50,00 %
1	HuanEbashes	1	50,00 %

Taula 26 - Distribució de vendes d'accés per grup durant el juliol del 2025

4.2.2.2. Agost

L'agost, el grup Big-Bro apareix per primer cop i aconseguirà mantenir l'activitat al setembre.

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

Taula 27 - Distribució de vendes d'accés per grup durant l'agost del 2025

4.2.2.3. Setembre

El setembre, Big-Bro es consolida com a venedor dominant d'aquest mes i del trimestre en general, la meitat del mercat es reparteix entre diversos actors no gaire recurrents.

	ACTOR D'AMENAÇA	NÚM. ACCESSOS COMPROMESOS	% TOTAL
1	Big-Bro	3	50,00 %
2	MrBroot	1	16,67 %
2	personX	1	16,67 %
2	361CrimeLiFe	1	16,67 %

Taula 28 - Distribució de vendes d'accés per grup durant el setembre del 2025

5. CONCLUSIÓ

Després d'haver analitzat el panorama de ciberamenaces del tercer trimestre del 2025 a nivell mundial, tot sembla indicar que les ciberamenaces s'han reduït, perquè han passat de 4840 atacs el primer trimestre a 3985 atacs al tercer.

A nivell europeu s'esperen més atacs, pel fet que la tendència d'aquests està en augment, i passen de 1347 atacs el segon trimestre a 1502 atacs el tercer. La guerra de Rússia i Ucraïna continuarà sent clau, ja que aquest conflicte continua alimentant la inestabilitat geopolítica al continent europeu.

Els atacs hacktivistes i el cibercrim continuaran tenint força protagonisme, probablement a l'últim trimestre de l'any la balança s'inclinarà pel cibercrim, perquè l'època nadalenca és a tocar i això suposa un període molt interessant per als ciberdelinqüents.

Els atacs als governs continuaran en augment a causa de les guerres d'Ucraïna-Rússia i Gaza-Israel, com ja hem comentat anteriorment a causa de la inestabilitat geopolítica.

Aquest escenari ens convida a mantenir-nos atents a les diferents mètriques i dades del panorama de les ciberamenaces, i reflexionar sobre la seguretat de les organitzacions i els governs que cada cop pateixen més ciberatacs, atès que els cibercriminals estan més professionalitzats que mai.

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.