ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

Informe de Ciberintel·ligència

El panorama de les ciberamenaces 2T 2026

TLP: WHITE

JULIOL 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	30/07/2026	03/08/2026

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 clara i actualitzada sobre el panorama de ciberamenaces corresponent al segon trimestre de l'any 2026, amb una atenció especial a aquelles que puguin tenir un impacte significatiu en el context d'Andorra. Si bé la disponibilitat de les dades específiques sobre el país andorrà continua sent limitada, en aquest trimestre s'inclou per primera vegada una anàlisi dels incidents identificats amb afectació directa a Andorra, complementada amb una anàlisi més completa del país veí, Espanya, a causa de la proximitat geogràfica, els llaços i l'operativa propera.

A partir d'aquest trimestre, l'informe s'elaborarà sobre fonts d'intel·ligència pròpies, basades en el monitoratge continu d'alertes, les reivindicacions d'actors d'amenaça i l'activitat en fòrums i canals ciberdelinqüents. Aquest canvi de fonts també implica un canvi sobre les dades, per la qual cosa les xifres d'aquest trimestre no són comparables amb les de trimestres anteriors i constitueixen una nova línia base de referència per als trimestres vinents.

Durant el segon trimestre de l'any, l'activitat maliciosa global ha mostrat un creixement sostingut, amb un volum mensual d'alertes que gairebé es triplica entre l'abril i el juny. La tipologia més dominant ha estat l'exposició de credencials i dades compromeses, que concentren més de la meitat de tota l'activitat registrada, molt per davant dels atacs directes com els *defacements* o els atacs de DDoS.

En el cas específic d'Espanya, el trimestre ha estat marcat per un canvi de patró: l'activitat de programari de segrest (*ransomware*) retrocedeix clarament al juny, la venda d'accessos i dades compromeses escala fins a màxims del període. D'altra banda, el hacktivisme ha mostrat un comportament volàtil i oportunista, amb un repunt significatiu al juny.

Per a l'elaboració d'aquest informe s'han recopilat i analitzat les principals tendències en l'àmbit global, incloent-hi l'evolució de tota l'activitat, la severitat i la tipologia, els actors d'amenaça més actius, els països i sectors més afectats i l'ecosistema criminal en què es publica tota aquesta activitat.

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

3. TENDÈNCIES I EVOLUCIÓ DE LES CIBERAMENACES EN L'ÀMBIT GLOBAL

A l'apartat següent, s'exposaran i analitzaran les tendències principals i l'evolució de les ciberamenaces en l'àmbit global del segon trimestre de l'any 2026. I es prestarà atenció al volum d'alertes registrades i la seva evolució al llarg del trimestre, la distribució per severitat i tipologia, els actors d'amenaça més actius, els països i sectors més afectats i l'ecosistema delinqüent on els ciberdelinqüents publiquen i monetitzen l'activitat.

3.1. Activitat global registrada durant el 2T del 2026

Durant el segon trimestre de l'any 2026 es van registrar en total 57.101 alertes a escala mundial, fet que suposa una mitjana aproximada de 634 alertes diàries al llarg dels mesos d'abril, març i juny.

L'activitat ha mostrat un creixement sostingut durant tot el trimestre: el volum mensual gairebé es triplica entre l'abril amb 9.531 alertes i el juny amb 27.924 alertes, passant per les 19.422 registrades al maig.

Alertes totals	Mitjana diària	Severitat alta	Pic – 24 juny
57.101	634	10,2%	1.236

*Setmanes parcials.

Gràfic 1 - Evolució setmanal d'alertes registrades en l'àmbit mundial durant el segon trimestre

3.2. Distribució per severitat

La distribució per severitat de les alertes s'ha mantingut estable durant tot el trimestre. La severitat baixa és la més dominant, amb un 72,9 % del total, mentre que la severitat alta se situa al voltant del 10 % de tot el volum.

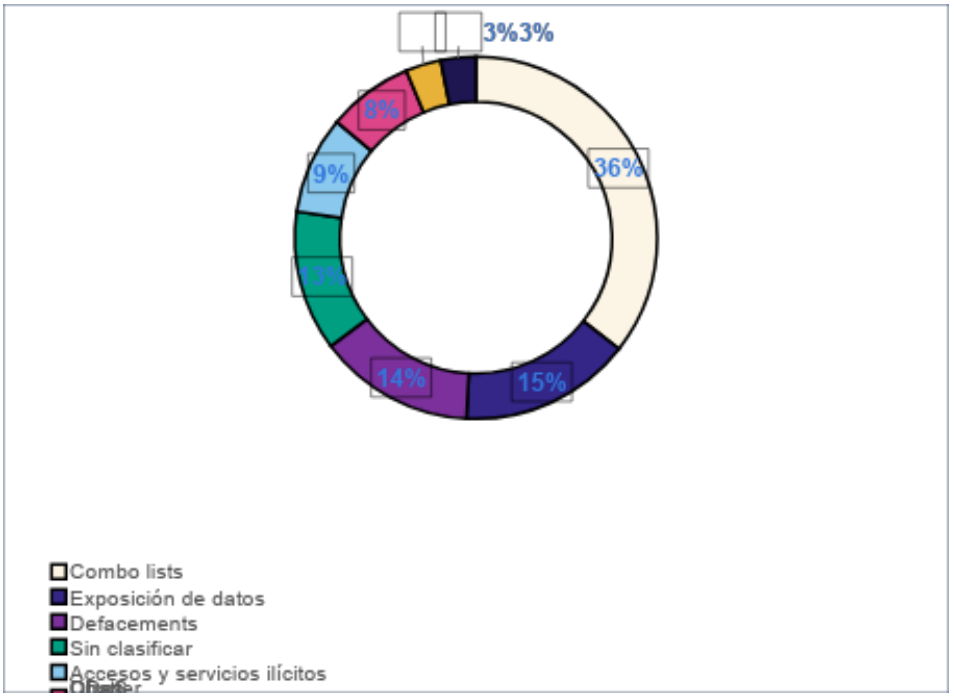
	SEVERITAT	NOMBRE D'ALERTES	% TOTAL
1	Baixa	41.622	72,9%
2	Mitjana	9.642	16,9%
3	Alta	5.837	10,2%

Taula 1 - Distribució d'alertes per severitat durant el segon trimestre.

3.3. Tipologia de les alertes

Les *combolists* suposen per si soles el 35,5 % de totes les alertes del trimestre, i es consoliden com la tipologia dominant. Si a les *combolists* s'hi sumen les bretxes, filtracions i *logs* de *stealers*, l'exposició de dades i credencials, concentren més de la meitat de l'activitat del trimestre amb un 50,8 %, molt per sobre dels atacs directes com els *defacements* amb un 13,9 % o els atacs de denegació de servei amb un 3,2 %.

Aquesta distribució mostra un ecosistema orientat principalment a la comercialització de la informació compromesa més que a l'atac directe, un patró que més endavant tornarem a veure a l'apartat dedicat exclusivament a Espanya.



Gràfic 2 - Tipologia d'alertes registrades durant el segon trimestre

	SEVERITAT	CATEGORIES INCLOSES	NRE. D'ALERTES	% TOTAL
1	Llistes combinades	Llista combinada	20.285	35,5%
2	Exposició de dades	Violació de dades + Fuga de dades + Registres	8.744	15,3%
3	Desfiguració	Desfiguració	7.964	13,9%
4	Sense classificar	-	7.164	12,5%
5	Accessos i serveis il·lícits	Accés inicial + Serveis + Comptes + Targetes	4.978	8,7%
6	Xerrada	Mencions en fòrums/canals	4.379	7,7%
7	DDoS	Atac DDoS	1.801	3,2%
8	Altres	Ciberatac, programari maliciós, pesca, vulnerabilitat…	1.786	3,1%

Taula 2 - Tipologia d'alertes registrades durant el segon trimestre (amb les categories incloses)

3.4. Actors d'amenaça més actius

El rànquing d'actors del trimestre l'encapçalen DimasHxR amb 1.336 alertes atribuïdes i el duo de *defacement* massiu chinafans/0xteam amb 1.226 alertes atribuïdes. La resta del rànquing el protagonitzen grups distribuïdors de *combolists* i credencials compromeses, un perfil coherent una vegada analitzades prèviament les més de 20.000 alertes de *combolists*.

	ACTOR D'AMENAÇA	MÈTODE	NRE. ALERTES
1	DimasHxR	Distribució de credencials	1.336
2	chinafans / 0xteam	*Defacement*	1.226
3	CODER	Distribució de credencials	861
4	Nicotine / Umbra Community	Distribució de credencials	728
5	Cloudredhat	Distribució de credencials	642
6	Capsen	Distribució de credencials	441
7	thejackal101	Exposició de dades	419
8	MetaCloud3	Distribució de credencials	408
9	HQcomboSpace	Distribució de credencials	399
10	UniqueCombo	Distribució de credencials	394

Taula 3 - Top 10 d'actors d'amenaça més actius durant el segon trimestre (exclosa activitat DDoS)

Cal assenyalar que aquest rànquing exclou l'activitat d'actors de DDoS, per la qual cosa els col·lectius hacktivistes com NoName057(16) no hi figuren malgrat mantenir-se plenament actius durant el trimestre, tal com es detalla a l'apartat dedicat a Espanya.

Després d'haver analitzat els actors d'amenaça més actius, a continuació, analitzarem els grups de programari de segrest:

En aquest àmbit, Qilin es manté com el grup amb més víctimes publicades del trimestre, amb 295 i segueix en línia amb el que s'ha observat en trimestres anteriors, en què ja es posicionava com el grup de programari de segrest amb més impacte. El segueix The Gentlemen emergent amb 252 víctimes publicades, que consolida el creixement que ja apuntava al començament d'any.

A continuació, mostrem la taula amb el top 10 de grups de ransomware més prolífics:

	Grups de *ransomware*	Nombre de víctimes publicades
1	Qilin	295
2	TheGentlemen	252
3	DragonForce	144
4	Akira	119
5	LockBit 5	108
6	INC Ransom	99
7	APT73	72
8	NightSpire	63
9	CoinbaseCartel	63
10	Nova	61

Taula 4 - Top 10 de grups de ransomware per víctimes publicades durant el segon trimestre

3.5. Països més afectats

S'ha elaborat un top 10 de països més afectats per les alertes registrades durant el segon trimestre de l'any 2026. Els Estats Units concentra el volum més gran del trimestre amb 2.172 alertes registrades, seguit d'Indonèsia amb 1.419 alertes i França amb 900 alertes.

Andorra no ocupa el top 10 de països, però a causa de la proximitat amb països com ara Espanya i França podria patir un efecte de danys col·laterals, per la qual cosa és important analitzar els països veïns:

- França se situa al lloc 3r del rànquing mundial, amb 900 alertes registrades, sent el país europeu més afectat del trimestre.
- Espanya ocupa el lloc 14è, amb 232 alertes, i queda fora del top 10 mundial. El detall de l'activitat contra Espanya es desenvoluparà més endavant en aquest informe.

	PAÍS	NOMBRE D'ALERTES	% TOTAL
1	Estats Units	2.172	3,8%
2	Indonèsia	1.419	2,5%
3	**França**	**900**	**1,6%**
4	Índia	790	1,4%
5	Alemanya	645	1,1%
6	Brasil	547	1,0%
7	Regne Unit	520	0,9%
8	Israel	418	0,7%
9	Xina	415	0,7%
10	Mèxic	325	0,6%
…	…	…	…
14	**Espanya**	**232**	**0,4%**

Taula 5 - Top 10 de països més afectats durant el segon trimestre

Nota: els percentatges es calculen sobre el total d'alertes del trimestre (57.101). Els valors són reduïts perquè la major part de les alertes no tenen atribució geogràfica o es distribueixen en una llarga cua de països amb volums menors, per la qual cosa el rànquing s'ha d'interpretar en termes relatius entre països i no com a quota del total.

3.6. Sectors més afectats

Entre les alertes amb sector identificat, tecnologia amb 32,4 %, administració pública amb 22,4 % i educació amb 17,1 % concentren més de dos terços de l'activitat. El sector financer i assegurador ocupa la quarta posició amb un 15,2 %, mentre que la sanitat registra el volum relatiu més baix amb un 4,7 %.

La posició elevada de l'administració pública és especialment rellevant des de la perspectiva d'aquest informe, atès que, com es veurà a l'apartat dedicat a Espanya, el sector públic és també el més afectat per la venda de dades compromeses a escala nacional.

	PAÍS	NOMBRE D'ALERTES	% TOTAL
1	Tecnologia	2.443	32,4%
2	Administració pública	1.690	22,4%
3	Educació	1.294	17,1%
4	Financer i assegurances	1.147	15,2%
5	Comerç	618	8,2%
6	Sanitat	355	4,7%

Taula 6 - Sectors més afectats durant el segon trimestre

Nota: només el 13 % de les alertes del trimestre tenen sector atribuït (7.547 de 57.101). Els percentatges es calculen sobre aquest subconjunt, per la qual cosa s'han d'interpretar com a distribució relativa entre sectors identificats.

3.7. Ecosistema delinqüent

Els *claims* delinqüents del segon trimestre de l'any es concentren majoritàriament en fòrums de la clear net: cracked.st amb 7.001, crackingx.com amb 5.328 i patched.to amb 4.772 encapçalen el rànquing de plataformes, amb Telegram com a quart canal amb 5.255.

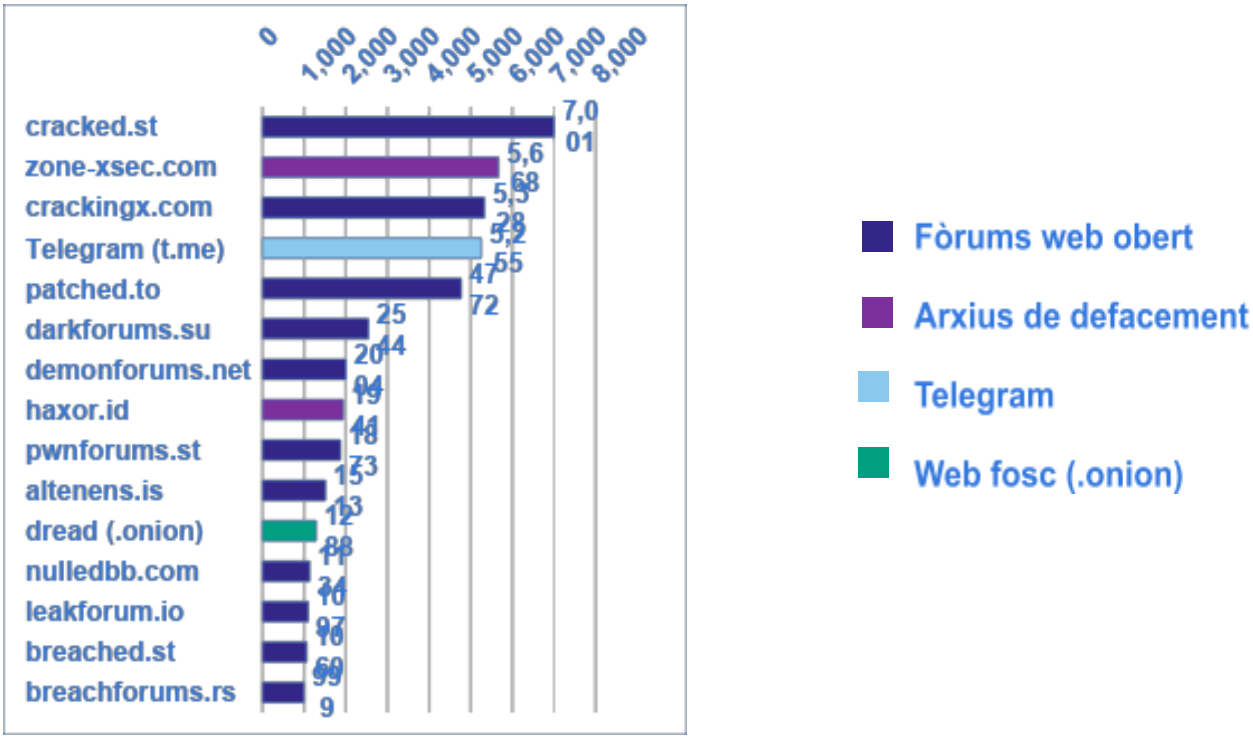
Els *claims* del web fosc (.onion) són minoritaris en volum, amb una sola plataforma al top i un 3 % dels *claims*, així i tot, el web fosc manté la seva rellevància en la compravenda de dades més valuoses.

Aquest repartiment de *claims* confirma una tendència ja consolidada a l'ecosistema criminal, perquè l'activitat de publicació i comercialització s'ha desplaçat cap a plataformes més accessibles públicament, on els actors obtenen més visibilitat i abast.

A continuació, es mostren els *claims* per tipus de plataforma durant el segon trimestre:

	TIPUS DE PLATAFORMA	NRE. ALERTES	% TOTAL
1	Fòrums de web obert (10 plataformes)	28.997	66,7%
2	Fitxers de *defacement* (zone-xsec, haxor.id)	7.609	17,5%
3	Telegram	5.255	12,1%
4	Web fosc (.onion)	1.288	3,0%

Taula 7 - Distribució de claims *per tipus de plataforma durant el segon trimestre*



Gràfic 3 - Claims *per plataforma durant el segon trimestre*

4. PANORAMA DE LES CIBERAMENACES D'ANDORRA

Durant el segon trimestre del 2026 es van identificar tres incidents amb menció o afectació al país, dels quals un correspon a una víctima andorrana identificada i els dos restants a distribucions massives de credencials en les quals Andorra figura entre múltiples països afectats.

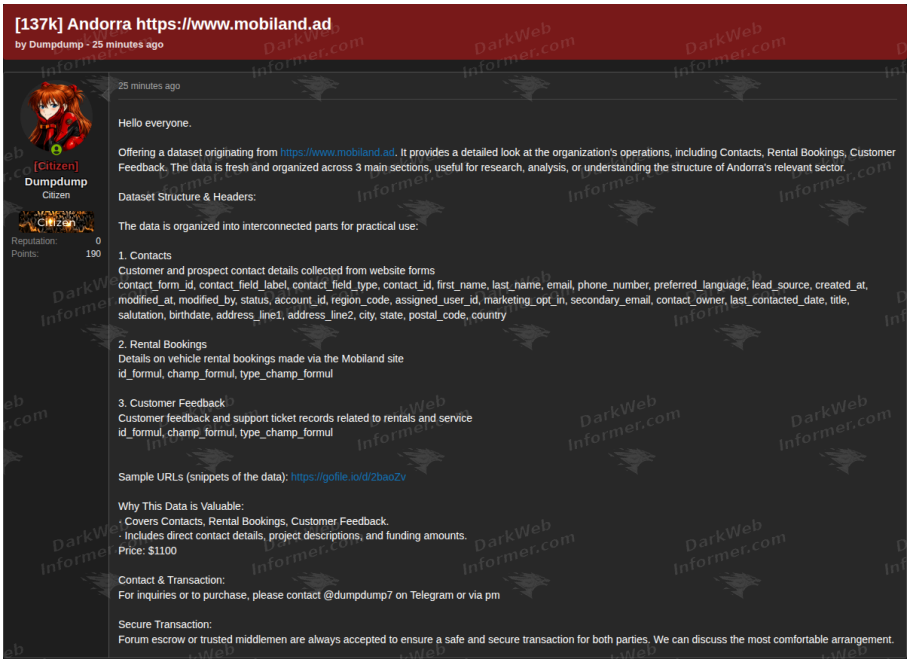
El volum és reduït i no permet establir tendències ni comparacions estadístiques, però sí que permet caracteritzar el perfil d'exposició del país.

	DATA	CATEGORIA	ACCIDENT	ACTOR	PLATAFORMA
1	01/04	*Combolist*	Distribució d'11 milions de credencials de múltiples països, incloent-hi Andorra	CODER	CrackingX
2	04/06	*Combolist*	Distribució de credencials adreçada a Andorra, Algèria, Albània i Samoa Americana	CODER	CrackingX
3	05/06	Bretxa de dades	Venda de més de 137.000 registres de clients de Mobiland (mobiland.ad)	Dumpdump	Breached

Taula 8 - Incidents amb afectació a Andorra durant el segon trimestre

4.1. Bretxa de dades a Mobiland

El 5 de juny es va publicar al fòrum Breached la venda d'un conjunt de dades atribuït a Mobiland, empresa andorrana de lloguer de vehicles, per un preu de 1.100 dòlars. L'anunci descrivia aproximadament 137.000 registres distribuïts en tres blocs: dades de contacte de clients (noms, correus electrònics, telèfons, adreces i dates de naixement), formularis de reserva i registres d'atenció al client.



Imatge 1 - Bretxa de dades a Mobiland

4.2. Inclusió d'Andorra a les distribucions massives de credencials

Els dos incidents restants corresponen a distribucions de *combolists* publicades a la plataforma CrackingX i difoses a través de canals de Telegram, en què Andorra apareix enumerada al costat d'altres països sense que hi hagi una selecció deliberada del país com a objectiu. Les dues publicacions s'atribueixen a l'actor CODER, que ocupa la tercera posició al rànquing global d'actors més actius del trimestre, amb 861 alertes atribuïdes.

Imatge 2 - Inclusió d'Andorra a distribucions massives de credencials 1

Imatge 3 - Inclusió d'Andorra a distribucions massives de credencials 1

4.3. Perfil d'exposició i senyals primerencs del tercer trimestre

De l'anàlisi conjunta es desprèn que Andorra no ha estat objecte de campanyes dirigides, ni hacktivistes ni de programari de segrest, durant el segon trimestre del 2026. La seva exposició es concentra en l'àmbit de la comercialització de dades, tant de manera col·lateral, a través de les recopilacions massives de credencials, com directa, mitjançant la venda de dades d'entitats andorranes concretes.

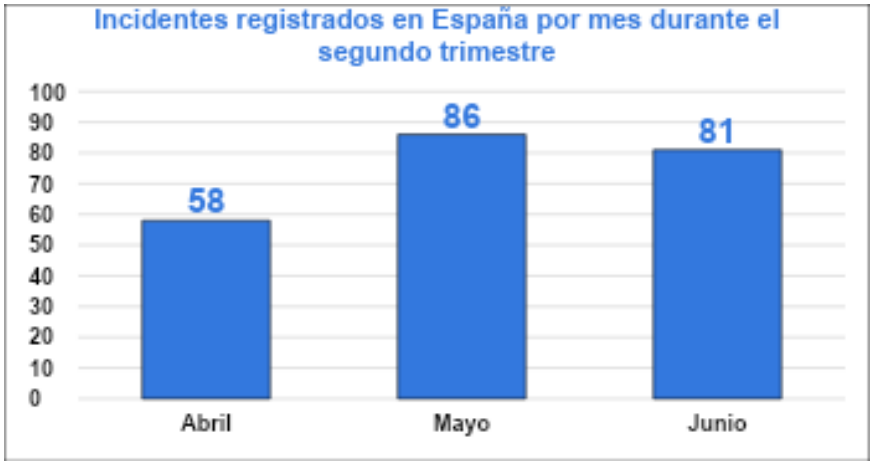
5. PANORAMA DE LES CIBERAMENACES A ESPANYA

L'apartat següent de l'informe ofereix una anàlisi completa del panorama de les ciberamenaces a Espanya durant el segon trimestre de l'any 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 per completar l'anàlisi específica recollida a l'apartat anterior.

S'analitzarà l'activitat registrada pel *feed* nacional d'incidents, la ciberdelinqüència, l'activitat hacktivista, els incidents més destacats del període i les amenaces latents de cara al trimestre vinent.

5.1. Visió general

Es van registrar 225 incidents en total amb afectació a Espanya durant el segon trimestre de l'any 2026, amb una tendència creixent: amb 58 incidents a l'abril, 86 al maig i 81 al juny.



Gràfic 4 - Incidents registrats a Espanya per mes durant el segon trimestre

Per categories, dominen els *defacements* amb 72 incidents i les bretxes de dades amb 71, seguits per les filtracions de dades amb 31. En conjunt, les categories vinculades a l'exposició de dades i la venda sumen més de la meitat dels incidents de trimestre, cosa que es replica en l'àmbit global com hem vist anteriorment.

	CATEGORIA	NOMBRE D'INCIDENTS
1	*Defacement*	72
2	*Data breach*	71
3	*Data leak*	31
4	*Carding*	16
5	*Combo list*	14
6	*Initial access*	8
7	Altres	13

Taula 9 - Incidents registrats a Espanya per categoria durant el segon trimestre

*Nota: Només es recullen els incidents publicats i reivindicats en fòrums i canals criminals (*defacements*, bretxes, vendes de dades i accessos), per la qual cosa l'activitat de denegació de servei s'analitza de manera específica a l'apartat de hacktivisme.*

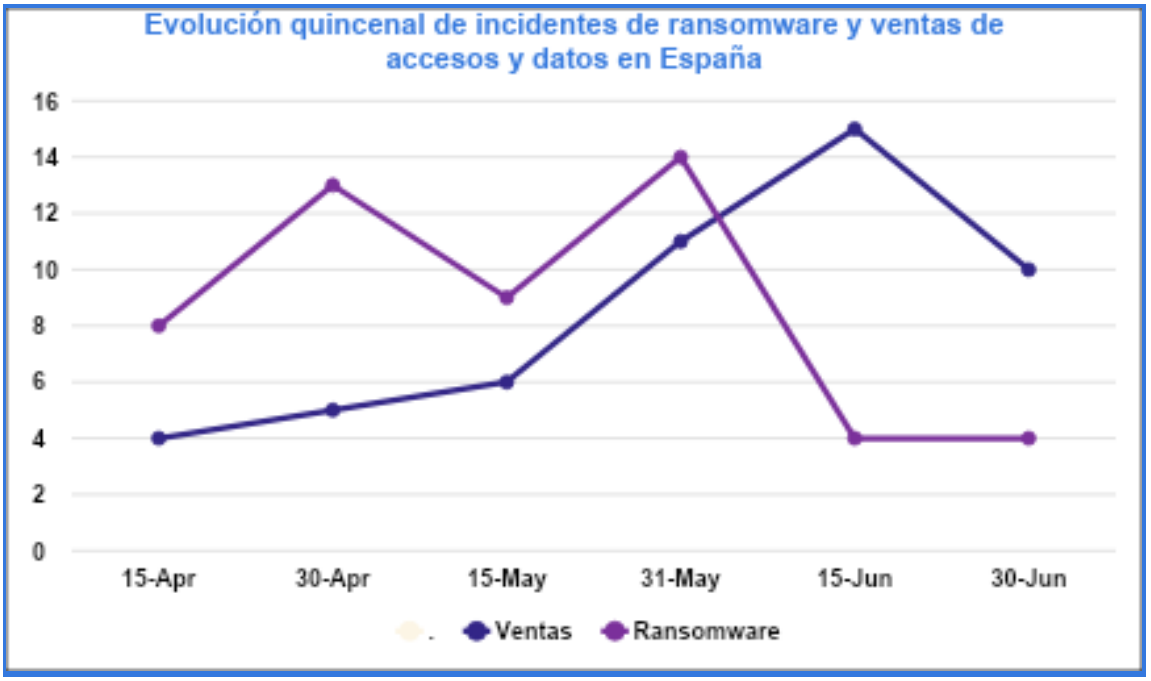
5.2. Ciberdelinqüència

A continuació, s'analitzarà el panorama de la ciberdelinqüència a Espanya durant el segon trimestre de l'any 2026. El nivell d'amenaça es va mantenir baix durant tot el trimestre, tret de la quinzena del 15 de juny, en la qual es va observar una pujada del nivell d'amenaça mitjanament, en coincidir amb el màxim de vendes d'accessos i dades.

La dada més important del trimestre és la cruïlla de trajectòries entre les dues sèries analitzades: mentre les víctimes de programari de segrest cauen des dels pics de 13-14 per quinzena registrats entre finals d'abril i maig fins a 4 per quinzena al juny, les vendes d'accessos i dades escalen des de 4 casos a l'inici del període fins a un màxim de 15 a mitjan juny. La monetització de la ciberdelinqüència es desplaça així des del xifratge i l'extorsió cap a la comercialització directa d'informació compromesa.

	QUINZENA	NIVELL	PROG. SEGREST	VENDA DE DADES	FAMÍLIES DESTACADES
1	15/04	SOTA	8	4	Krybit, Qilin
2	30/04	SOTA	13	5	Qilin, Lamashtu, Lapsus$ Group
3	15/05	SOTA	9	6	LockBit, Qilin
4	31/05	SOTA	14	11	INC Ransom, Nova, Qilin
5	15/06	MITJÀ	4	15	Dire Wolf, Qilin, Safepay, TheGentlemen
6	30/06	SOTA	4	10	Projecte Booba, Safepay, TheGentlemen
TOTAL			52	51	

Taula 10 - Resum quinzenal de l'activitat de la ciberdelinqüència a Espanya durant el segon trimestre



Gràfic 5 - Evolució quinzenal d'incidents de ransomware i vendes d'accessos i dades a Espanya

5.2.1. Incidents de programari de segrest

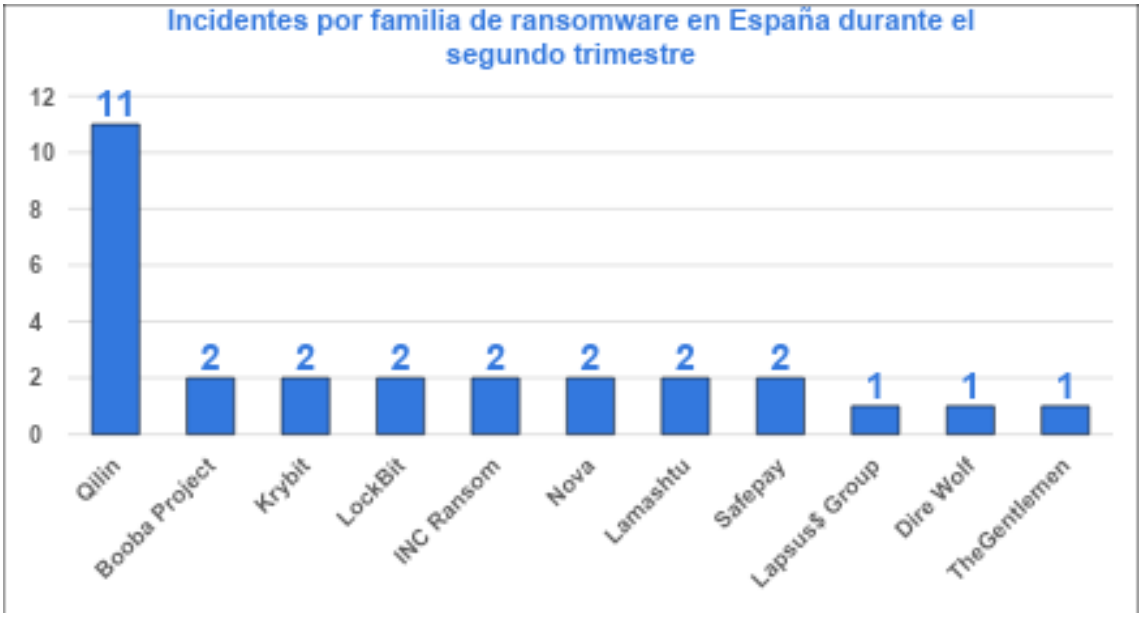
Durant el segon trimestre del 2026, es van detectar 52 víctimes de programari de segrest (*ransomware*) amb afectació a Espanya. El grup de programari de segrest més actiu del període va ser novament Qilin amb 11 incidents atribuïts, apareix com a família destacada a cinc de les sis quinzenes del trimestre, molt per davant de la resta de famílies.

Després de Qilin, l'activitat està molt repartida entre la família amb dos incidents atribuïts com Booba Project, Krybit, LockBit, INC Ransom, Nova, Lamashtu i Safepay, i famílies amb Lapsus$ Group, Dire Wolf i The Gentlemen.

Cal destacar la irrupció de The Gentlemen en les dues últimes quinzenes del trimestre; tot i que el seu volum a Espanya encara és reduït, es tracta del segon grup més prolífic en l'àmbit global, per la qual cosa la seva activitat contra objectius espanyols s'haurà de vigilar durant el trimestre que ve.

Pel que fa a l'evolució temporal, l'activitat es va concentrar entre finals d'abril i maig, amb pics de 13 i 14 víctimes per quinzena, per caure de forma abrupta a quatre víctimes per quinzena durant tot el juny.

Els sectors més recurrents entre les víctimes de programari de segrest van ser manufactura, tecnologia, consum, logística i serveis professionals.



Gràfic 6 - Incidents per família de ransomware a Espanya durant el segon trimestre

Nota: les xifres per família provenen de les taules d'actors destacats; els incidents englobats en altres actors no estan desglossats, per la qual cosa la suma per famílies no arriba al total de 52 víctimes del trimestre.

5.2.2. Venda d'accessos i dades

Durant el segon trimestre del 2026, es van detectar 51 casos de venda d'accessos i dades amb afectació a Espanya, amb una evolució ascendent passant de 4 casos a la quinzena del 15 d'abril al màxim de 15 a mitjan juny, moment en què el nivell d'amenaça es va elevar a mitjà.

El sector públic/governamental és el més atacat per la venda de dades, i apareix com a sector destacat durant el trimestre, juntament amb energia, telecomunicacions i serveis financers. Entre les víctimes espanyoles del trimestre hi ha la Junta d'Andalusia, Naturgy, Zara, Mapfre, Endesa, l'Ajuntament de Valdemoro, Mupol, Ahorramas, Irestal Group i TRIQUIM.

Pel que fa a l'ecosistema de comercialització, PwnForums es consolida com el fòrum dominant per a la venda de dades espanyoles, amb presència a totes les quinzenes del període, seguit de DarkForums, Breached/BreachForums i SpearCX. Entre els actors recurrents destaquen spain, kr0x6 i catwoman, a més de KikoRivera, Skull1172, GFX666, Aquahack, Saturn, CocoMelon, Leads, NightBroker, Jenk, gang i s1ethx7z.

Cal assenyalar que, mentre a escala global els *claims* es concentren en fòrums generalistes de credencials, la comercialització de dades específicament espanyoles es canalitza de manera preferent a través de PwnForums, plataforma que al rànquing global ocupa una posició intermèdia. Aquesta especialització convé tenir-la en compte a efectes de monitoratge.

5.3. Hacktivisme

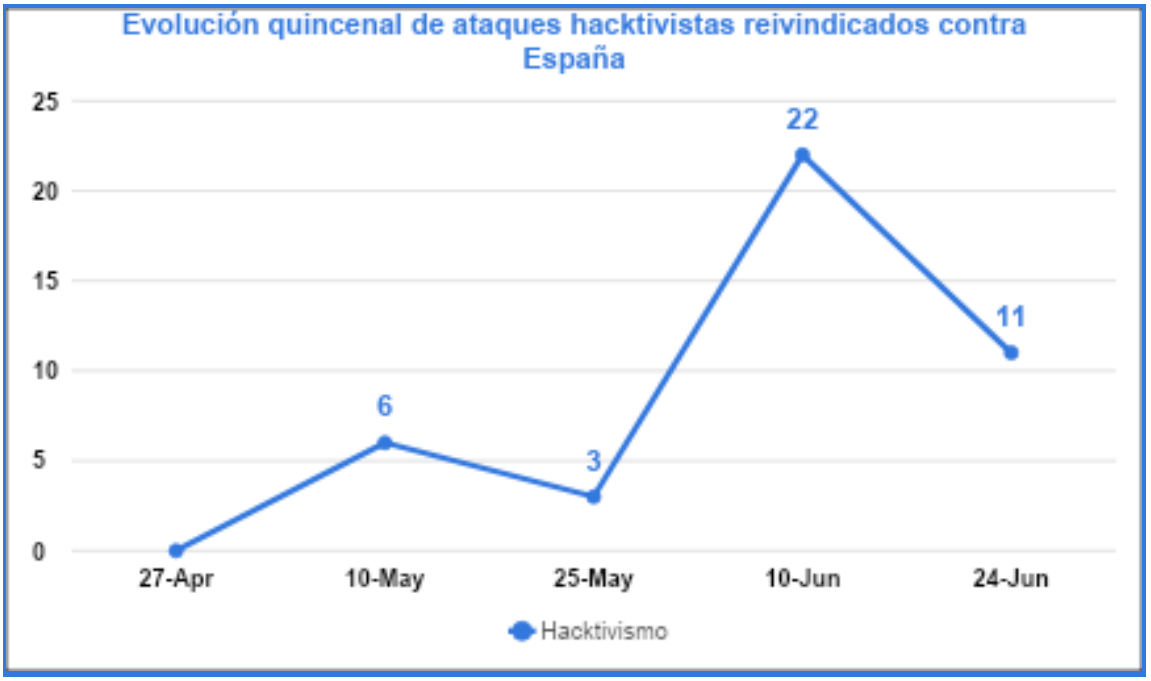
Tot seguit, s'analitzarà el panorama del hacktivisme a Espanya durant el segon trimestre del 2026. El nivell d'amenaça va passar de baixa a finals d'abril a mitjana durant la resta del trimestre.

Durant el trimestre s'han registrat 42 atacs hacktivistes reivindicats contra objectius espanyols. L'activitat va ser molt volàtil: partint de l'absència total d'atacs a finals d'abril, es va assolir el màxim del trimestre el 10 de juny, amb 22 atacs reivindicats en una quinzena, per baixar a 11 al tancament.

Cal recalcar que no s'ha identificat una campanya sostinguda contra Espanya. La majoria de les accions registrades responen a un patró oportunista, amb els grans actors del panorama hacktivista centrats prioritàriament en els conflictes internacionals i Espanya com a objectiu secundari o circumstancial.

	QUINZENA	NIVELL	ATACS	TIPOLOGIA	ACTORS DESTACATS
1	27/04	SOTA	0	Només amenaça (insiders en defensa/UAV)	Desinformador Rus
2	10/05	MITJÀ	6	4 *defacements*, 1 intrusió, 1 accés OT	404 Crew Cyber Team
3	25/05	MITJÀ	3	2 accessos OT, 1 bretxa	Z-Pentest Alliance, Desinformador Rus / Perun de Swarog
4	10/06	MITJÀ	22	13 DDoS, 8 bretxes, 1 accés OT	NoName057(16), catwoman, Bambi, IDS, EsqueleSquad
5	24/06	MITJÀ	11	6 bretxes, 5 accessos OT	NoName057(16), Keishell, AvangardSec, Z-Pentest
TOTAL			42		

Taula 11 - Resum quinzenal de l'activitat hacktivista a Espanya durant el segon trimestre



Gràfic 7 - Evolució quinzenal dels atacs hacktivistes reivindicats contra Espanya

5.3.1. Actors hacktivistes més actius

L'actor més actiu del trimestre va ser NoName057(16), amb 17 atacs, concentrats en dues onades de DDoS al juny amb 13 i 4 atacs respectivament. El seu lideratge manté la tendència observada en trimestres anteriors, en la qual ja figurava com a actor hacktivista més actiu tant en l'àmbit global com contra objectius espanyols.

El segueix 404 Crew Cyber Team, amb 6 atacs al començament de maig, i un grup d'actors amb 3 atacs cadascun: catwoman, Keishell i Z-Pentest Alliance.

	ACTOR D'AMENAÇA	NRE. ALERTES
1	NoName057(16)	17
2	404 Crew Cyber Team	6
3	catwoman	3
3	Keishell	3
3	Z-Pentest Alliance	3
4	Bambi	2

Taula 12 - Actors hacktivistes més actius contra Espanya durant el segon trimestre

5.3.2. Evolució de les tipologies d'atac

L'activitat d'aquest trimestre va evolucionar des dels *defacements* oportunistes del maig, de baix impacte operatiu i finalitat principalment reivindicativa, cap a un predomini de les bretxes d'informació i els accessos a sistemes de control industrial (OT) al juny.

Al conjunt del trimestre, la distribució de tipologies va ser la següent: 15 bretxes d'informació, 13 atacs de denegació de servei, 9 accessos a sistemes OT, 4 *defacements* i 1 intrusió.

	TIPOLOGIA	Núm. d'alerta	% TOTAL
1	Bretxes d'informació	15	35,7%
2	DDoS	13	31,0%
3	Accessos a sistemes OT	9	21,4%
4	*Defacements*	4	9,5%
5	Intrusions	1	2,4%

Taula 13 - Tipologia dels atacs hacktivistes contra Espanya durant el segon trimestre

5.4. Incidents destacats en el període

A continuació, es detallaran els incidents de més rellevància registrats contra objectius espanyols durant el segon trimestre del 2026.

5.4.1. Filtració atribuïda a la Direcció General de la Policia

El 30 de maig, l'actor Skull1172, vinculat al col·lectiu EsqueleSquad, va anunciar una suposada filtració de més de 19 milions de registres de ciutadans espanyols, incloent-hi fotografies biomètriques i documents d'identitat, presumptament extrets de la Direcció General de la Policia. La publicació es va dur a terme al fòrum Breached.

Es tracta de l'incident de més abast potencial del trimestre pel volum i la naturalesa especialment delicada de les dades afectades. Tot i això, la base de dades no va arribar a divulgar-se durant el període analitzat, per la qual cosa l'anunci no ha pogut ser verificat i podria respondre tant a una filtració real no consumada com a una acció de notorietat sense suport material.

Imatge 4 - Filtració atribuïda a la Direcció General de la Policia

5.4.2. Venda de documents espanyols

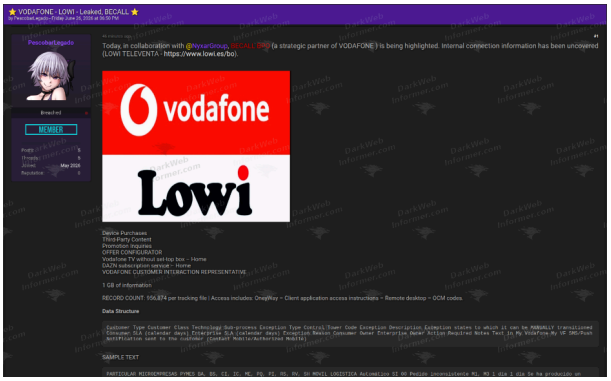
L'actor catwoman va anunciar al juny la venda 11,4 milions de documents d'identitat espanyols, atribuïts a la publicació a l'Agència Estatal d'Administració Digital. L'anunci es va registrar dues vegades durant el mes, el 6 i el 25 de juny, a les plataformes SpearCX i PwnForums respectivament.

Aquest cas resulta especialment il·lustratiu de la convergència entre ciberdelinqüència i hacktivisme assenyalada més endavant a les conclusions, atès que catwoman figura simultàniament entre els actors recurrents en la venda de dades espanyoles i entre els actors que van reivindicar atacs hacktivistes durant el trimestre.

Imatge 5 - Venda de documents d'identitat espanyols

5.4.3. Bretxa a BECALL BPO amb afectació a Vodafone/Lowi

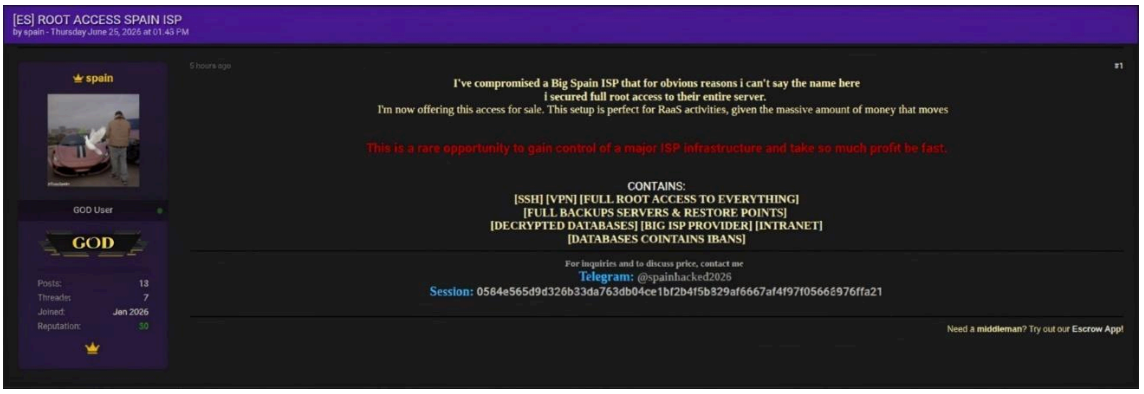
El 26 de juny es va publicar a PwnForums una suposada bretxa de dades contra el proveïdor de serveis BECALL BPO, que va exposar sistemes interns i dades de clients de Vodafone i Lowi, amb un volum estimat al voltant de 957.000 registres.



Imatge 5 - Bretxa a BECALL BPO amb afectació a Vodafone/Lowi

5.4.4. Venda d'accés inicial a un proveïdor de serveis d'Internet

El 25 de juny, l'actor spain va publicar a PwnForums la venda d'un accés inicial amb privilegis de *root* sobre la infraestructura d'un proveïdor de serveis d'internet espanyol no identificat.



Imatge 7 - Venda d'accés inicial a un proveïdor de serveis d'Internet

5.4.5. Incidents al sector energètic

El sector energètic va concentrar diversos dels anuncis de més volum del trimestre. Es van publicar dues ofertes de dades atribuïdes a Endesa que al·ludien a més de 20 milions de registres de clients amb informació personal i dades bancàries (IBAN), la primera el 7 de maig a DarkForums i la segona el 10 de juny a SpearCX, atribuïdes a actors diferents. Addicionalment, es van registrar dues publicacions relatives a Naturgy, el 30 d'abril i el 30 de maig.

Atès que els volums anunciats superen amb comoditat la base de clients de les companyies afectades, aquestes xifres s'han de prendre amb una cautela especial i considerar-les reivindicacions no verificades.

Imatge 8 - Incidents al sector energètic

Imatge 9 - Incidents al sector energètic

5.4.6. Accessos a sistemes de control industrial (OT)

Durant el trimestre es van reivindicar nou accessos a sistemes de control industrial a Espanya, sent aquest el vector de més criticitat potencial del període. Entre els casos identificats destaquen:

- Accés a infraestructura hídrica el dia 2 de juny: compromís d'un sistema de control industrial responsable de l'operació de dues estacions de bombament d'aigua, reivindicat per Infrastructure Destruction Squad.
- Sistemes de reg agrícola al juny: compromís de sistemes de control de reg en explotacions agrícoles espanyoles, inclòs el sistema SCADA de l'empresa Margal Agronomía. L'atribució d'aquests incidents no resulta concloent, atès que apareixen reivindicats a través de canals i per actors diferents segons la font consultada.
- Accés OT a Telefónica de España a finals d'abril: inclòs a l'onada del col·lectiu 404 Crew Cyber Team, que va combinar aquest accés amb *defacements* contra entitats educatives i sanitàries i amb la intrusió a deu càmeres de videovigilància, sense reivindicació ideològica associada.
- Panell de control industrial el dia 12 de juny: accés no autoritzat a un panell HMI d'una instal·lació de rentada de vehicles, reivindicat mitjançant canals vinculats al Projecte DDoSia.

Tot i que en cap dels casos identificats no s'ha documentat una afectació operativa real ni conseqüències físiques, la reiteració d'aquest tipus d'accessos sobre infraestructures d'aigua, agricultura i telecomunicacions evidencia un interès sostingut dels actors hacktivistes per entorns OT espanyols amb nivells d'exposició insuficients.

5.5. Previsió i amenaces latents

Al tancament del segon trimestre de l'any 2026, s'identifiquen dues operacions anunciades i no materialitzades que mantenen el nivell de vigilància elevat sobre objectius espanyols.

5.5.1. Operacions anunciades

Operació anunciada

Operació Bloodborne

Anunciada por AvangardSec (UAC-0252/APK) contra Alemanya, Ucraïna i Espanya, liderada por Eye of Sauron, amb possible ús del programari de segrest AVANWARE. Sense objectius espanyols afectados en tancar el període.

Campanya hacktivista

Possible reactivació de #OpSpain

Interès creixent de Z-Pentest Alliance i NoName057(16) en la regió eleva la probabilitat d'una nova onada coordinada contra objectius espanyols.

5.5.2. Escenaris de més risc

Escenaris de més risc

Bretxa de dades - DDoS - OT

Bretxa de dades amb probabilitat molt alta; DDoS contra entitats governamentals i atacs a sistemas de control industrial (OT) com a escenaris secundaris.

5.5.3. Esdeveniments catalitzadors

Catalitzadors que s'han celebrat

Visita del Papa - Mundial FIFA 2026

Identificats en tancar el trimestre com a catalitzadors potencials d'activitat hacktivista. Tots dos esdeveniments han tingut lloc al juliol, l'anàlisi de l'activitat materialitzada es recollirà a l'informe del 3T.

6. CONCLUSIONS

Després de l'anàlisi del segon trimestre de l'any 2026, el panorama global de les ciberamenaces es caracteritza per un creixement sostingut de l'activitat maliciosa al llarg de tot el període, amb un volum mensual d'alertes que es triplica gairebé entre abril i juny i sense reculades significatives entre setmanes consecutives.

La conclusió més consistent del trimestre ha estat el predomini de l'exposició de credencials i dades compromeses, que concentra més de la meitat de les alertes registrades, molt per davant dels atacs directes.

Aquest mateix patró es reprodueix a escala nacional i constitueix la principal troballa de l'anàlisi d'Espanya: mentre l'activitat de programari de segrest retrocedeix amb claredat al juny, la venda d'accessos i dades compromeses escala fins als màxims del període.

El hacktivisme contra Espanya s'ha mostrat volàtil i oportunista, sense una campanya sostinguda contra el país, però amb una evolució tipològica que eleva el risc real associat: des dels *defacements* de baix impacte del maig fins a les bretxes d'informació i, especialment, els accessos a sistemes de control industrial.

De cara al pròxim període 3T 2026, l'escenari més probable és la continuïtat i la intensificació de les bretxes i filtracions de dades, seguida de noves onades de denegació de servei contra entitats governamentals i d'atacs contra sistemes OT. A això cal sumar-hi dues operacions anunciades i no materialitzades, Bloodborne i la possible reactivació de #OpSpain. La celebració durant el mes de juliol de dos esdeveniments de gran visibilitat internacional, la visita oficial del Papa a Espanya i la Copa Mundial de la FIFA 2026 també han estat identificats com a catalitzadors potencials d'activitat hacktivista, l'efecte real dels quals serà objecte d'anàlisi.

Pel que fa a Andorra, no s'ha identificat cap campanya dirigida, ni hacktivista ni de programari de segrest, i l'activitat detectada es concentra íntegrament en l'àmbit de la comercialització de dades: de forma directa, amb la venda d'un conjunt d'aproximadament 137.000 registres d'una empresa andorrana, i de manera col·lateral, amb la inclusió de credencials andorranes en recopilacions massives distribuïdes per actors situats entre els més actius del panorama global.

Amb totes aquestes dades analitzades, l'informe dona per conclòs l'anàlisi corresponent al segon trimestre de l'any 2026. Deixant una base de referència per al trimestre següent, en què serà de vital importància continuar monitorant l'evolució dels actors d'amenaça, el desplaçament de la monetització de la ciberdelinqüència cap a la venda de dades i l'exposició dels entorns OT.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat d'Andorra Digital. 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 d'Andorra Digital.