ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Panorama de les ciberamenaces en el primer trimestres del 2025

TLP: WHITE

ABRIL 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	30/04/2025	30/04/2025

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA **4**
2. INTRODUCCIÓ **5**
3. TENDÈNCIES I EVOLUCIÓ DE LES AMENACES A NIVELL MUNDIAL **6**
3.1. Ciberatacs registrats durant el primer trimestre del 2025 6
3.2. Indústries més afectades 6
3.3. Països més atacats 7
3.4. Actors d'amenaça més actius 8
3.4.1 Tipologia d'atacs amb més predominança 9
3.4.2 Tècniques i tàctiques d'atac més rellevants 10
3.5. Cibertacats motivats pels conflictes actuals 11
3.5.1 Campanya de NoName057(16) contra l'Administració espanyola 11
3.5.2 Campanya de NoName057(16) contra l'Administració de França 12
4. AMENACES EMERGENTS **13**
4.1. ASM: riscos associats a la gestió de la superfície d'atac 13
4.2. L'auge de les campanyes d'infecció mitjançant infostealers 13
4.2.1. Auge del LummaC2 13
5. CONCLUSIONS I RECOMANACIONS **15**
6. CLÀUSULA DE CONFIDENCIALITAT **16**

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 clara i actualitzada del context d'amenaces al qual s'enfronten actualment les organitzacions, com també anticipar possibles riscos i proposar recomanacions per enfortir la ciberseguretat aquest 2025.

Les dades recopilades i analitzades durant el primer trimestre d'enguany ens han permès establir quines són les tendències principals en el panorama de les ciberamenaces, com també aquelles amenaces emergents que cal tenir en compte perquè les organitzacions estiguin preparades davant de qualsevol ciberatac.

Això és rellevant perquè Andorra està ubicada estratègicament entre dos països que són un blanc important de ciberatacs a causa del context polític en el qual ens trobem.

Al llarg del document, s'examinen les indústries més atacades, els països més afectats i els actors d'amenaça més actius (amb focus a l'actor d'amenaça NoName057(16) i les amenaces emergents. Al final del document trobareu les conclusions i recomanacions.

Aquest primer trimestre del 2025 ha posat en evidència que les ciberamenaces continuen evolucionant a gran velocitat i afectant tota mena d'organitzacions, des d'institucions públiques fins a empreses privades. Específicament, els atacs de denegació de servei distribuït (DDoS) s'han consolidat com una de les principals tècniques emprades pels ciberdelinqüents.

Tot i que molts d'aquests atacs no han causat danys permanents, han posat a prova la capacitat de resposta de les entitats afectades i fan una crida a la necessitat de reforçar les mesures de seguretat per afrontar aquest escenari que canvia constantment.

3. TENDÈNCIES I EVOLUCIÓ DE LES AMENACES A NIVELL MUNDIAL

Pel que fa al panorama de ciberamenaces globals, observem que les tècniques emprades pels actors d'amenaça s'han tornat més sofisticades i estan orientades principalment als atacs DDoS i a l'exfiltració de dades crítiques. Igualment, hem identificat tendències importants com el desenvolupament i la comercialització de codi maliciós com ara el LummaC2.

Per entendre millor l'evolució d'aquestes amenaces, hem analitzat les indústries més afectades, els països més atacats i els actors d'amenaça més actius. Aquesta anàlisi no només permet identificar els riscos actuals, sinó que també facilita la previsió de possibles escenaris futurs.

3.1. Ciberatacs registrats durant el primer trimestre del 2025

Si se segueix la dinàmica que s'està produint durant els últims mesos, la xifra de ciberatacs registrats el primer trimestre del 2025 a nivell mundial torna a batre tots els rècords, amb un total de **6373 ciberatacs**, cosa que ha suposat un **augment del 127,3 % respecte dels registrats durant el trimestre anterior.** D'aquests, **654 van tenir un impacte crític, el 10,3 % del total**, xifra que també ha suposat un increment del **62,7 %** respecte als tres mesos previs.

3.2. Indústries més afectades

Si s'analitza la tipologia d'entitats que s'han vist afectades pels atacs i es classifiquen en funció de l'àmbit industrial al qual pertanyen, es pot apreciar que **aquelles que pertanyen a l'àmbit governamental s'han erigit en l'objectiu principal dels actors d'amenaça** aquest primer trimestre.

A la taula següent es poden apreciar els sectors industrials més afectats durant aquest primer trimestre.

	Indústria	Nombre d'atacs rebuts
1	Governamental (AP / Seguretat)	1.357
2	Manufacturera	731
3	Telecomunicacions (ICT)	456
4	Sector científic	453
5	Logística (Transport / emmagatzematge)	411

Com es pot apreciar, les organitzacions i les entitats governamentals, que abasten les administracions públiques, organismes militars i de seguretat, ocupen de manera destacada aquest rànquing, i pràcticament dupliquen el nombre d'atacs rebuts per part de la segona indústria més atacada, la manufacturera.

El context polític complex que es continua vivint, a causa dels conflictes entre Rússia i Ucraïna i entre Israel i Palestina, han provocat que **grups de hacktivistes i actors patrocinats per Estats hagin centrat els seus esforços a impactar contra la infraestructura crítica del que consideren països enemics**.

D'altra banda, el **sector de les telecomunicacions** és un altre dels més afectats, i ocupa el tercer lloc del rànquing, a nivell mundial. En relació amb aquest sector, el març del 2025 **Andorra Telecom** va detectar un atac de pesca a través de correu electrònic. Els usuaris van rebre un missatge fals que indicava que si els usuaris no clicaven a l'enllaç adjunt, el seu usuari a la companyia telefònica seria eliminat en les pròximes 72 hores.

La companyia va activar ràpidament els protocols necessaris per desactivar l'amenaça i va alertar els usuaris sobre l'intent de frau, tal com es pot apreciar a la imatge següent.

3.3. Països més atacats

Alguns països han esdevingut objectius prioritaris de ciberatacs a causa del seu pes econòmic, polític i tecnològic. Els **Estats Units, Ucraïna, Itàlia, Israel, França, Índia** i **Espanya** es troben entre els països més afectats. Continuant amb el que hem comentat a l'apartat anterior, els conflictes polítics han estat determinants també per entendre quins països han rebut el nombre més gran d'atacs.

A la taula següent s'exposa el top 10 dels països més atacats durant aquest primer trimestre de l'any.

	PAÍS	NRE. D'ATACS	% TOTAL
1	**Estats Units**	1.236	24,8 %
2	**Ucraïna**	361	5,7 %
3	**Itàlia**	324	5,1 %
4	**Israel**	296	4,6 %
5	**França**	292	4,6 %
6	**Índia**	272	4,3 %
7	**Espanya**	266	4,2 %
8	**Polònia**	208	3,3 %
9	**Canadà**	182	2,9 %
10	**Alemanya**	179	2,8 %

Si bé Andorra no es troba al llistat dels top 10 més atacats, prenem França i Espanya com a referència a causa de la proximitat geogràfica.

França ocupa el **cinquè lloc** de la llista, i ha rebut un total de 292 atacs el primer trimestre del 2025. Durant aquest trimestre, França ha estat blanc de diversos ciberatacs que han afectat, principalment, organismes governamentals i infraestructures municipals.

Espanya, per l'altra banda, **ocupa el setè lloc** d'aquesta llista, i ha rebut un total de 266 atacs fins al març. Aquest fet s'explica majoritàriament per les diferents **campanyes d'atacs DDoS que ha impulsat el grup NoName057(16) contra diferents organismes de l'Administració pública**, com a resposta als diferents pronunciaments públics del Govern contra Rússia. Aprofundirem sobre aquest tema més endavant.

3.4. Actors d'amenaça més actius

Segons les dades mundials, l'actor d'amenaces més actiu durant el primer trimestre de l'any va ser **NoName057(16)**, que té atribuïts 1.201 ciberatacs, i ha provocat gairebé el 20 % dels atacs registrats en aquest període.

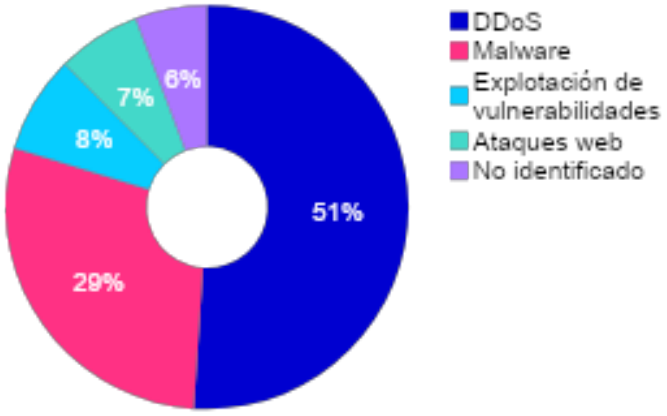
A la taula següent s'indica un rànquing dels actors més rellevants.

	ACTOR D'AMENAÇA	MÈTODE	ATACS	% TOTAL
1	**NoName057(16)**	DDoS	1.201	18,8 %
2	**Cl0p**	Programari segrest	401	6,3 %
3	**RipperSec**	DDoS	269	4,2 %
4	**Akira**	Programari segrest	229	3,6 %
5	**RamsomHub**	Programari segrest	229	3,6 %
6	**Keymous+**	DDoS	184	2,9 %
7	**Mr Hanza**	DDoS	129	2,0 %
8	**Dark Storm Team**	DDoS	126	2,0 %
9	**Qilin**	Programari segrest	113	1,8 %
10	**Red Wolf ceyber**	Ciberespionatge	103	1,6 %

És rellevant assenyalar que, dels 10 actors més actius, sis s'especialitzen en atacs DDoS. Aquesta dada és clau per contextualitzar l'apartat següent, on s'analitzaran les tipologies d'atac principals registrades durant el primer trimestre del 2025.

3.4.1 Tipologia d'atacs amb més predominança

En relació amb l'apartat anterior, tot seguit es mostra una representació de les tipologies d'atacs que s'han registrat més.



Com es pot observar, **predominen els atacs de Denegació de Servei Distribuït (DDoS), que representen més de la meitat del total d'atacs**. Aquest tipus d'atac continua sent una tàctica àmpliament utilitzada per la seva efectivitat per interrompre serveis, saturar infraestructures i causar danys reputacionals a les organitzacions afectades.

	TIPOLOGIES D'ATAC	ATACS
1	**DDos**	3161
2	**Programari maliciós**	1776
3	**Explotació de vulnerabilitats**	483
4	**No identificat**	416
5	**Atacs web**	357

3.4.2 Tècniques i tàctiques d'atac més rellevants

Si es parteix de la matriu desenvolupada per MITRE ATT&CK, hem analitzat les tàctiques i tècniques (TTPs) més utilitzades pels actors d'amenaça durant els seus atacs.

D'aquesta manera, i coneixent quins són els procediments que fan servir més, l'objectiu és ajudar l'organització a posar el focus en aquells elements que, per la seva tendència d'ús, mereixen una atenció especial per identificar en una etapa primerenca qualsevol indici d'un possible atac.

Accés inicial	Execució	Persistència	Escalada de privilegis
Phishing (T1566)	Intèrpret d'ordres i scripts (T1059)	Execució d'inici automàtic d'arrencada o sessió (T1547)	Execució d'inici automàtic d'arrencada o sessió (T1547)
Adjunt de spearphishing (T1566.001)	Tasca programada (T1053.005)	Execució activada per esdeveniment (T1546)	Manipulació del testimoni d'accés (T1134)
Enllaç de spearphishing (T1566.002)	Execució d'usuari (T1204)	Execució d'inici automàtic d'arrencada o sessió (T1547)	Mecanisme de control d'elevació abús (T1548)
Serveis remots externs (T1133)	Explotació per a l'execució del client (T1203)	Evasió del depurador (T1622)	
Replicació mitjançant suports extraïbles (T1091)			

Evasió de defensa	Descobriment	Moviment Lateral	Col·lecció
Virtualització/Sandbox Evasion (T1497)	Descobriment de la finestra de l'aplicació (T1010)	Transferència d'eines laterals (T1570)	Arxiu les dades recollides (T1560)
Execució del servidor intermediari binari del sistema (T1218)	Evasió del depurador (T1622)	Serveis a distància (T1021)	Captura d'entrada (T1056)
Deteriorament de les defenses (T1562)	Virtualització/Sandbox Evasion (T1497)	Replicació mitjançant suports extraïbles (T1091)	Captura de pantalla (T1113)
	Detecció de grups de permisos (T1069)		Recollida automatitzada (T1119)
			Segrest de sessió del navegador (T1185)

Comandament i control	Exfiltració	Impacte

Protocols web (T1071.001)	Exfiltració automatitzada (T1020)	Dades xifrades per impacte (T1486)
Protocols de correu (T1071.003)	Exfiltració a través del servei web (T1567)	Desfiguració (T1491)
Resolució dinàmica (T1568)	Exfiltració per protocol alternatiu (T1048)	Denegació de servei de punt final (T1499)

3.5. Ciberatacs motivats pels conflictes actuals

Tal com hem esmentat prèviament, el context polític influeix en els ciberatacs que succeeixen a diferents països, sobretot en el marc dels conflictes entre Ucraïna i Rússia, com també entre Israel i Palestina. En aquest sentit, s'està fent una onada d'atacs a institucions europees.

És important que les organitzacions estiguin pendents de qualsevol pronunciament polític que es pugui produir des del govern d'Andorra, perquè es podrien desencadenar respostes similars a les experimentades quan els governs d'Espanya o França han condemnat les accions de Rússia.

Tot seguit comentarem la campanya de l'actor d'amenaça NoName057(16) contra les administracions d'Espanya i França.

3.5.1 Campanya de NoName057(16) contra l'Administració espanyola

Des de finals de febrer del 2025, Espanya ha estat objectiu d'una sèrie de ciberatacs en resposta al suport del president Pedro Sánchez a Ucraïna. L'ofensiva OpSpain, llançada contra infraestructures espanyoles en represàlia pel suport militar del Govern espanyol a Ucraïna, s'ha dut a terme després de la reunió a Kíev del president del Govern, Pedro Sánchez, amb el seu homòleg ucraïnès, el 24 de febrer. En aquesta reunió va anunciar ajuts per valor de 1.000 milions d'euros en ajuda militar a Ucraïna.

Atacs de denegació de servei distribuïda (DDoS) coordinats pel grup NoName 057(16), entre altres actors d'amenaces, van afectar institucions governamentals, empreses privades i serveis locals, i van generar interrupcions temporals als seus sistemes informàtics. Per exemple, van causar interrupcions temporals a llocs web estratègics com els de la Moncloa, Hisenda i ports clau com Vigo, Castelló i Huelva.

Encara que aquests atacs no van implicar robatori directe d'informació, sí que van generar disrupcions operatives importants i van danyar la reputació dels organismes afectats, cosa que va reflectir clarament les implicacions polítiques i estratègiques darrere d'aquesta onada de ciberdelinqüència recent.

2.5.1.1 Organismes afectats

Alguns dels serveis que es van veure afectats per les accions de NoName057(16) van ser:

- **Diputacions provincials:** Càceres, Badajoz, València, Guipúscoa, Girona, Ciudad Real i Toledo.

- **Ajuntaments:** Sant Sebastià, Irun, Hondarribia, Saragossa, Mèrida, València, Barcelona, La Corunya, Santiago de Compostel·la, Vigo, Palma de Mallorca i Valladolid.

- **Altres organismes:** Tramvia de Saragossa, pàgines de la Província d'Osca i la comunitat autònoma de Castella-la Manxa.

3.5.2 Campanya de NoName057(16) contra l'Administració de França

Senat, com a part de la seva campanya contra països pro-OTAN i pro-Ucraïna. Tot i això, els atacs a França no semblen ser tan freqüents ni intensos com els dirigits a Espanya, Ucraïna o els països bàltics.

Cal destacar que els incidents a França han causat interrupcions temporals, però no danys significatius, i les autoritats franceses estan activament investigant possibles connexions amb actors estrangers en casos més recents, com ara els atacs a les presons.

4. AMENACES EMERGENTS

4.1. ASM: riscos associats a la gestió de la superfície d'atac

Hi ha una màxima que explica que **allò que no es coneix, no es pot protegir**. I a això és al que fa referència quan es parla dels riscos associats a l'ASM, és a dir, a l'**exposició no controlada de la infraestructura d'una organització**.

Moltes entitats no tenen visibilitat sobre la totalitat de la seva infraestructura IT, cosa que comporta un gran risc, perquè deixa una part **fora de l'abast dels diferents sistemes de seguretat i protecció**.

És imprescindible conèixer i fer el mapatge de tots els *endpoints* relatius a una entitat perquè cada un pot ser utilitzat per un atacant com a punt d'entrada: **cal informació detallada de tots els dispositius per determinar-ne la finalitat, el propietari i l'estat de seguretat**.

L'any 2024 es va tancar amb dades molt reveladores: fins al 79 % dels **accessos autoritzats** detectats no es va fer ús de codi maliciós, cosa que indica que l'explotació de **vulnerabilitats sense pedaços o les fallades en els controls d'accessos van ser les dues causes principals**. I aquesta tendència s'ha continuat mantenint aquest primer trimestre a nivell general.

Per garantir la protecció de l'ASM és imprescindible enumerar i protegir cada ordinador, servidor o dispositiu mòbil que permeti accedir a tota o una part de la xarxa corporativa.

4.2. L'auge de les campanyes d'infecció mitjançant *infostealers*

Els *infostealers* han estat els altres grans protagonistes pel que fa a amenaces emergents. L'ús de codis maliciosos dissenyats per robar informació dels equips que infecten s'ha disparat. I si n'hi ha hagut un que ha destacat sobre els altres, aquest ha estat el **LummaC2, del qual, des de l'equip de Ciberintel·ligència, n'identifiquem una campanya activa de distribució des de principis del 2025**.

El **LummaC2** es caracteritza per l'alta capacitat de recopilació de dades d'autenticació (credencials, mecanismes MFA) i financers (bitlleteres de criptomonedes), i permet, fins i tot, manipular transaccions. Concretament, se centra en informació emmagatzemada a navegadors web basats en Chromium i Mozilla.

4.2.1. Auge del LummaC2

LummaC2 és un codi maliciós que es va crear per ser comercialitzat, és a dir, sustentat en el **model de negoci Malware-as-a-Service (MaaS)**, i des que va aparèixer s'ha venut en fòrums clandestins com XSS, Exploit.in o RAMP, a més de mercats del web fosc o canals de Telegram.

Com passa amb el **MaaS** en general, aquest tipus de codi maliciós s'adreça al gran públic, i **pot ser explotat fins i tot per usuaris sense altes capacitats o coneixements tècnics**. A més, s'ofereix mitjançant subscripció, facilita versions millorades i amb capacitats més bones als usuaris que optin per aquesta opció.

Aquest fet, juntament amb un preu assumible per a molts cibercriminals, que oscil·la entre els 250 $ al mes (amb la possibilitat de fer un pagament únic de 20.000 $), explica que LummaC2 acapari el 85 % del mercat del codi maliciós.

5. CONCLUSIONS I RECOMANACIONS

Després d'haver analitzat el panorama de ciberamenaces del primer trimestre del 2025 a nivell mundial, tot apunta que la tendència d'augment i la sofisticació de ciberatacs continuarà augmentant.

Durant el primer trimestre del 2025, els atacs de Denegació de Servei Distribuït (DDoS) van representar una quantitat significativa respecte als ciberatacs registrats a nivell global. Aquest increment subratlla la preferència creixent dels actors d'amenaça per aquestes tàctiques a causa de la seva efectivitat en la interrupció d'operacions i generació d'impacte econòmic.

També es va observar un augment significatiu de ciberatacs contra sectors crítics com ara l'administració pública de països com Espanya o França. Aquest increment reforça la necessitat d'enfortir les capacitats de detecció i de resposta a nivell sectorial. Es preveu que els atacs DDoS continuaran augmentant, específicament per grups de hacktivistes vinculats a la situació geopolítica. Andorra no pot ser aliena a aquest context atès que és un país que per proximitat geogràfica es pot veure impactat per aquests ciberatacs.

És important tenir en compte que LummaC2 s'ha posicionat com una de les eines més utilitzades per robar informació, cosa que obliga a prestar una atenció especial als *infostealers*, que s'erigeixen en una de les principals amenaces a causa de la seva capacitat per robar grans volums d'informació delicada de manera ràpida i eficient.

Aquest escenari ens convida a reflexionar sobre la seguretat de les organitzacions. És imperatiu reforçar-ne la vigilància, actualitzar periòdicament les mesures de protecció i fomentar una cultura de ciberseguretat que els permeti anticipar-se a les amenaces i prevenir futurs incidents que puguin posar-les en perill.

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.