Informe Mensual de Hacktivisme

Ideològic, oportunista o simulat

07/2026

Edició Andorra i entorn europeu

Resum executiu

Nivell actual de l'amenaça: ALT

Les dades d'aquesta quinzena reflecteixen que, als països de l'entorn d'Andorra, s'han produït 93 atacs dins l'espectre de l'hacktivisme (enfront dels 23 de la quinzena anterior), amb 71 víctimes identificades (enfront de 23). Les reivindicacions han estat efectuades pels actors de amenaça NoName057(16), Desinformador Rus, Z-Pentest Alliance, BD Anonymous Team, Odessa: Still Loading, SUB-ZER0, ksx403, order403, dulce403, Antonkill, misere, Panataran i DBHunter.

L'operació de Legió Meta Yadro contra la UE, l'OTAN i els aliats d'Ucraïna, que va romandre activa la quinzena passada, s'ha paralitzat sobtadament. En canvi, els actors prorussos més actius (NoName057(16), Z-Pentest Alliance i Desinformador Rus), fins ara centrats en els conflictes internacionals vigents, han llançat una campanya ofensiva contra països de l'entorn d'Andorra arran de la detenció d'un periodista italià presumptament vinculat a Z-Pentest Alliance, i dels paquets d'ajuda militar i econòmica que aquests països envien a Ucraïna.

Actors i volum d'atacs

Actors destacats	Nº d'atacs
NoName057(16)	46
Desinformador Rus	26
Z-Pentest Alliance	8
BD Anonymous Team	6
SUB-ZER0	1
Altres actors (ksx403, order403, dulce403, Antonkill, misere, Panataran, DBHunter, Odessa: Still Loading)	6
Total	**93**

Sectors i tipologia d'atac

Sectors més afectats: governamental, defensa i serveis públics.

Dels 93 atacs registrats, 49 (52,69 %) han estat DDoS, 30 bretxes d'informació (32,26 %), 12 accessos OT (12,90 %) i els 2 (2,15 %) restants, defacements.

Esdeveniments destacats — entorn

Z-Pentest Alliance ha amenaçat i, de fet, ha atacat països de l'entorn d'Andorra com a conseqüència de la detenció d'un periodista italià, acusat de pertànyer al seu entramat — cosa que el col·lectiu nega, afirmant que es tracta només d'un aliat que va lluitar contra la pederàstia en un govern europeu. L'ofensiva ha estat secundada per NoName057(16) i Desinformador Rus a causa del suport militar i econòmic que aquests països presten a Ucraïna.

Per la seva banda, BD Anonymous Team opera de manera independent contra països de la regió en protesta per la seva postura davant el conflicte palestí.

Atacs de Z-Pentest Alliance

Víctimes: Càmeres de videovigilància en ubicacions aleatòries, sistemes domòtics en complexos residencials, i diverses empreses dels sectors tecnològic i elèctric de la regió.

Actor: Z-Pentest Alliance

Tipus d'atac: Accés OT

Atacs de Desinformador Rus

Víctimes: Membres de cossos de seguretat de l'estat de països veïns.

Actor: Desinformador Rus

Tipus d'atac: Filtració de fotografies pixelades i dades identificatives dels afectats

Atacs de NoName057(16)

Víctimes: Administracions de l'estat, defensa, transport i altres serveis públics.

Actor: NoName057(16)

Tipus d'atac: 42 DDoS i 4 accessos OT

Atacs de BD Anonymous Team

Víctimes: Diversos ajuntaments i autoritats portuàries de la regió.

Actor: BD Anonymous Team

Tipus d'atac: DDoS

Rellevància per al Principat d'Andorra

Durant el període analitzat no s'ha identificat cap reivindicació hacktivista dirigida específicament contra Andorra. No obstant això, el CSIRT-AD constata que la intensitat de l'activitat hacktivista als països veïns comporta un risc de contagi indirecte, atès el grau d'interconnexió d'Andorra amb les infraestructures digitals, financeres i de telecomunicacions de la regió.

- Sector financer: exposició reputacional per associació geogràfica i possibles campanyes de DDoS oportunistes contra entitats amb presència transfronterera.
- Administració pública i serveis essencials: risc d'escombratges (scanning) i intents d'accés oportunista a sistemes OT, per efecte d'arrossegament de campanyes regionals.
- Sector turístic: a les portes de l'època de màxima afluència, especial atenció a plataformes de reserva i pagament connectades a proveïdors regionals.
- Proveïdors compartits: cal revisar la cadena de subministrament TIC comuna amb operadors dels països veïns, atès que diversos incidents d'aquesta quinzena han afectat OT i domòtica de tercers.

El CSIRT-AD recomana a les entitats públiques i privades del Principat mantenir un nivell de vigilància reforçat, revisar l'exposició d'actius OT i IoT accessibles des d'internet, i notificar qualsevol indicador de compromís a csirt.anc@govern.ad.

Calendari geopolític global

Cimera de l'OTAN — 07/07/2026 – 08/07/2026 · Turquia

L'Aliança Atlàntica ha escenificat el traspàs progressiu de la càrrega defensiva cap a un pilar europeu obligat a assumir més autonomia estratègica davant el repliegament dels Estats Units. La cimera ha conclòs amb compromisos rellevants de despesa militar, suport a Ucraïna i inversió industrial per reforçar la dissuasió davant Rússia.

Conferències d'Adhesió amb Ucraïna, Moldàvia i Montenegro — 14/07/2026 · Bèlgica

La Unió Europea ha impulsat la seva agenda d'ampliació en obrir les negociacions amb Moldàvia i Ucraïna i tancar provisionalment, amb Montenegro, els capítols clau de política de competència i unió duanera.

Final de la Copa del Món de la FIFA 2026 — 19/07/2026 · EUA, Mèxic i Canadà

Esdeveniment esportiu global que ha reunit per primer cop 48 seleccions sota la coorganització d'Estats Units, Mèxic i Canadà. El torneig s'ha desenvolupat amb total normalitat i sense reivindicacions per part de col·lectius hacktivistes, malgrat l'elevada notorietat mediàtica i política de l'esdeveniment.

Eleccions a São Tomé i Príncipe — 19/07/2026

Eleccions presidencials que han conclòs amb la reelecció, en primera volta, de Carlos Vila Nova amb el 55,94 % dels vots, en uns comicis marcats per la baixa participació. Els resultats resten pendents de validació definitiva.

L'actor hacktivista més actiu del moment, NoName057(16), no ha dirigit les seves operacions contra els estats coorganitzadors del Mundial de la FIFA, la final del qual s'ha mantingut exempta d'atenció hacktivista. Per contra, l'ofensiva s'ha concentrat gairebé en exclusiva a Alemanya, França i altres països de l'entorn d'Andorra, impulsada en el primer cas per l'obertura a la cooperació nuclear entre dues nacions amb finalitats de defensa davant Rússia, i en el segon tant per la detenció del periodista italià esmentat com pels anuncis de nous paquets d'ajuda militar i econòmica dirigits al front ucraïnès.

Tendències globals

Bloc 1 · Rússia – Ucraïna

- Durant aquest període, NoName057(16) ha mantingut la seva activitat centrada en Alemanya, Ucraïna i altres països de l'entorn d'Andorra.
- L'ofensiva es deu, en el cas d'Ucraïna, a la intensificació del conflicte bèl·lic amb Rússia, mentre que a Alemanya la diplomàcia es debilita per les acusacions sobre el desenvolupament de programes nuclears secrets destinats a enfortir l'OTAN i les fronteres europees amb Rússia. En altres països de la regió, el focus és la detenció del periodista italià esmentat i els enviaments d'armes i paquets d'ajuda econòmica a Ucraïna per contenir l'amenaça russa.

En plena escalada militar amb drons ucraïnesos i míssils balístics russos, Zelenski ha destituït el comandant Oleksandr Syrskyi per frenar les protestes desencadenades arran del cessament de M. Fedorov, ministre de Defensa.

Bloc 2 · Israel – Palestina

- Les autoritats de Gaza xifren en més de 1.170 els morts per atacs israelians des de l'entrada en vigor de l'alto el foc del 10 d'octubre de 2025.

- El pla de reconstrucció de Trump s'ha reduït a un projecte pilot a Rafah, paralitzat per les violacions de l'alto el foc. No es preveuen avenços abans de les eleccions israelianes del 27/10, que podrien provocar la caiguda de Netanyahu o incitar-lo a una nova ofensiva total.

Hamàs ha triat com a nou líder Jalil Al Hayya, el seu principal negociador i un perfil proper a l'Iran, en substitució de Yahia Sinwar. De moment, el grup rebutja el desarmament i el traspàs del control de Gaza a un govern tecnòcrata.

Bloc 3 · Eleccions

- Malàisia ha celebrat comicis regionals a Johor l'11/07 i São Tomé i Príncipe eleccions presidencials el 19/07. A causa del període estival, no s'han celebrat processos electorals de gran transcendència, i els que han tingut lloc s'han caracteritzat per l'absència d'activitat hacktivista.
- Pròxims comicis: Pakistan (regionals a l'Azad Caixmir), 27/07; Regne Unit (Greater Manchester Mayoral By-Election i locals a Rumworth), 30/07; Malàisia (regionals a Negeri Sembilan), 01/08.

Els processos electorals de la darrera quinzena no han tingut una rellevància significativa i s'han desenvolupat amb normalitat; els col·lectius hacktivistes han orientat la seva atenció cap a altres assumptes.

Bloc 4 · Estats Units – Amèrica Llatina

Els Estats Units han publicat un informe, impulsat per Marco Rubio, que acusa Cuba de ser la «capital del terrorisme del segle XXI» per haver desplegat dècades de subversió i infiltració al seu territori, la qual cosa intensifica les tensions geopolítiques i debilita encara més els fràgils canals diplomàtics entre ambdues nacions; tot això en un context paradoxal en què Trump acaba d'enviar un primer carregament d'ajuda humanitària a l'illa mentre manté el bloqueig petrolier.

- A Bolívia, les autoritats han desarticulat una xarxa de tràfic de persones que reclutava ciutadans amb falses ofertes laborals per enviar-los forçosament al front rus a Ucraïna.

Marco Rubio ha confirmat la implicació dels Estats Units en la transició cap a la democràcia a Veneçuela, i ha celebrat l'acord entre el chavisme i l'oposició per iniciar a l'agost un diàleg de reconciliació politicoinstitucional.

Bloc 5 · Groenlàndia – Estats Units

- Onze aliats europeus i transatlàntics (Noruega, Dinamarca, Canadà, Finlàndia, França, Alemanya, Islàndia, Països Baixos, Portugal, Suècia i Regne Unit) han signat a la cimera d'Ankara un acord per reforçar la presència militar i la vigilància a l'Àrtic davant Rússia i la Xina. Amb aquesta mesura, Europa busca demostrar la seva capacitat defensiva a l'Atlàntic Nord per calmar les exigències dels Estats Units, alhora que tanca files amb Dinamarca en defensa de la sobirania de l'illa.

Per protegir les seves dades i els seus científics, l'Institut de Recursos Naturals de Groenlàndia ha suspès la col·laboració amb els Estats Units davant la pressió mediambiental i els intents de control de Trump.

Bloc 6 · Iran – Estats Units

- Els Estats Units han llançat una nova onada d'atacs contra l'Iran a l'estret d'Ormuz, cosa que ha paralitzat els esforços diplomàtics al Pakistan per salvar l'alto el foc i ha desencadenat un repunt dels preus de l'energia. Malgrat la contínua mediació internacional per assolir la pau, Trump ha descartat reunir-se amb Teheran i ha insinuat la possibilitat d'intensificar les ofensives militars prop d'instal·lacions nuclears iranianes.
- Davant el risc d'una operació terrestre dels Estats Units, l'Iran amenaça amb bombardejar el seu propi territori per evitar una ocupació, i adverteix sobre possibles captures de soldats i atacs a països veïns.

L'Iran ha congelat les negociacions formals amb els Estats Units i ha limitat el contacte a intercanvis indirectes, condicionant la fi de la guerra a la preservació de la seva seguretat, independència i identitat nacional.

Previsió d'atacs

Categoria d'atac	Probabilitat	Impacte	Risc
Atacs de DDoS	Molt alta	Baix	Mitjà
Atacs contra OT	Alta	Mitjà	Mitjà
Bretxa de dades	Alta	Alt	Alt
Atacs de defacement	Alta	Mitjà	Alt
Atacs de ransomware hacktivista	Baixa	Alt	Mitjà

Esdeveniments a monitorar

- Conflicte bèl·lic entre Rússia i Ucraïna — abast global
- Crisi a Cuba i inestabilitat regional — abast global

Font: CCN-CERT