Resum de tendències de ciberseguretat

MAIG 2025

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

ÍNDEX

1 Catalunya reforça l'ecosistema de ciberseguretat: creixement empresarial, innovació i demanda de talent

Tendència

Durant el mes de maig, Catalunya ha reafirmat el seu **compromís estratègic amb la ciberseguretat**, i s'ha convertit en un punt de trobada clau per a la innovació i el talent digital.

El Barcelona Cybersecurity Congress (BCC) ha deixat palesa la importància que té la ciberseguretat al territori, on s'han posat de manifest tant **els avenços tecnològics** com els reptes estructurals d'un sector en **plena expansió**. Més de 10.000 professionals d'empreses, administracions i centres de recerca, així com visitants d'arreu del món, han mostrat un entusiasme creixent envers la necessitat de protegir sistemes crítics i combatre les amenaces digitals aplicant noves tecnologies i regulacions.

En paral·lel, durant aquest mes de maig, **l'Agència de Ciberseguretat de Catalunya** ha publicat la seva memòria de 2024, en què destaca la importància d'estar envoltat d'un **ecosistema sòlid** davant d'un augment dels incidents del **26%,** els quals han afectat especialment **l'àmbit universitari.**

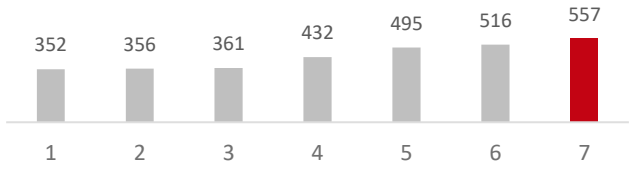
Malgrat aquest dinamisme, el sector afronta un repte persistent: **la necessitat de talent que té el país**. Les empreses presenten necessitats no cobertes de perfils i rols especialitzats. Tot i els esforços formatius, la **demanda supera àmpliament l'oferta**. Per això, esdeveniments com la HackUPC i el mateix BCC d'aquest mes s'estan convertint en espais essencials per captar, mostrar i connectar talent jove amb les necessitats reals del mercat.

Indicadors

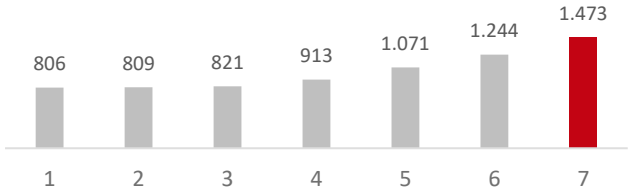
Consolidació de la ciberseguretat com un àmbit estratègic a Catalunya

Impulsada per una demanda creixent de serveis i solucions, tant en el terreny empresarial com en l'institucional, amb un increment del **58,2 %** en el nombre d'empreses i del **82,8 %** en la facturació entre 2018 i 2024.

Evolució nombre d'empreses en el sector de la ciberseguretat a Catalunya, 2018-2024



Evolució de la facturació de les empreses en el sector de la ciberseguretat a Catalunya (M€), 2018-2024

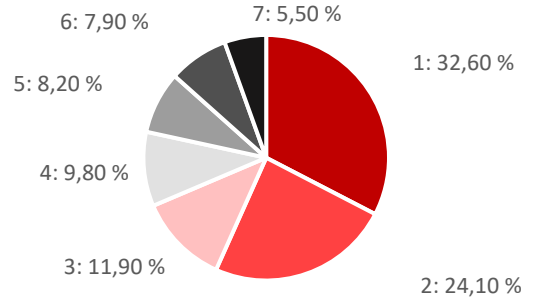


[Acció]

Mercat de la ciberseguretat a Catalunya

Els serveis financers, l'administració pública i l'àmbit de la salut són els sectors que més sol·liciten serveis de ciberseguretat.

Distribució de la quota de mercat de la ciberseguretat, per sector sol·licitador (en %, 2023)



[Statista]

La necessitat no coberta de professionals de la ciberseguretat segueix creixent

La necessitat de professionals no coberta va pujar un **19 %** a escala global i un **12,8 %** a Catalunya.

	Professionals de la ciberseguretat existents		Necessitat de professionals no coberta	
	vs. 2023	2024	*vs.* 2023	2024
MÓN	+0,1 %	**5,45 M**	+19 %	**4,76 M**
EUROPA	-0,7 %	**1,3 M**	+12,8 %	**392 K**
CATALUNYA*	-0,7 %	**28 K**	+12,8 %	**13,5 K**

[ISC2]

*Estimació

1 Catalunya reforça l'ecosistema de ciberseguretat: creixement empresarial, innovació i demanda de talent

Fets rellevants

El BCC impulsa la ciberseguretat amb intel·ligència artificial, la NIS2 i la criptografia quàntica

El BCC va celebrar la seva sisena edició amb la participació de més de 10.000 professionals. Aquest esdeveniment va subratllar la importància d'integrar la ciberseguretat com a prioritat en empreses i indústries, amb un enfocament especial cap a la Directiva NIS2, la intel·ligència artificial i la criptografia quàntica.

Entre les innovacions destacades, es va presentar l'ús de la IA per detectar amenaces i la criptografia quàntica per protegir dades delicades davant futurs ciberatacs. A més, activitats pràctiques com un *escape room* van permetre als assistents experimentar de manera immersiva els reptes de la ciberseguretat.

L'Agència de Ciberseguretat de Catalunya gestiona 3.372 ciberincidents durant el 2024

L'Agència de Ciberseguretat de Catalunya va presentar la seva memòria anual, on anuncia que va registrar un repunt notable d'incidents digitals: 3.372 ciberatacs gestionats el 2024, un 26 % més que l'any anterior. L'increment s'explica per l'allau de 6.900 milions d'atacs registrats i la millora en sistemes de detecció i prevenció. L'àmbit universitari ha patit més de la meitat dels incidents, seguit pel sector sanitari i l'administració. L'Agència destaca l'impacte de noves mesures com simulacres, bloqueig proactiu de correus i el reconeixement com a òrgan auditor de l'Esquema Nacional de Seguretat.

La comunitat DCA Ciberseguretat celebra la seva primera trobada anual dins el BCC

El 15 de maig, la comunitat DCA Ciberseguretat (de la Digital Catalonia Alliance) va celebrar la seva primera trobada anual en el marc del Barcelona Cybersecurity Congress.

Va ser un esdeveniment pensat per connectar l'ecosistema català de ciberseguretat; per reforçar la col·laboració entre les empreses, les institucions i els professionals del sector, i per compartir avenços i estratègies comuns, en un moment clau, marcat per l'adaptació a noves normatives europees, com la Directiva NIS2.

Catalunya registra un augment de la facturació en ciberseguretat del 18,4 %

Segons l'informe anual de ciberseguretat a Catalunya, elaborat per ACCIÓ i l'Agència de Ciberseguretat de Catalunya, el sector ha experimentat un augment del 18,4 % en el volum de negoci, i ha assolit els 1.473 M€. Actualment, 557 empreses es dediquen a la ciberseguretat, amb 10.672 professionals, de les quals el 82,6 % són pimes i el 10,6 %, *start-ups*.

L'ecosistema català disposa d'empreses que es dediquen a totes les branques de la ciberseguretat. La immensa majoria de les companyies treballen per millorar la protecció, seguida de la identificació i de la detecció.

La manca de talent en ciberseguretat a Catalunya s'estima en 13.500 professionals

Segons l'informe publicat per ACCIÓ a partir de les dades de l'ISC2, un dels principals reptes del sector de la ciberseguretat a Catalunya és la creixent manca de talent. La diferència entre les necessitats del sector i els professionals disponibles ha augmentat un 12,8 % en el darrer any, amb una demanda de 13.500 nous professionals.

A Catalunya, es disposa de 14 graus, màsters i postgraus en ciberseguretat, amb 45 centres d'estudis que ofereixen 62 cursos de formació professional.

Aquest fenomen també és global, amb una necessitat estimada de 4 milions de treballadors al món.

700 joves talents internacionals exploren solucions innovadores al HackUPC

Del 2 al 4 de maig, 700 estudiants de tot el món van participar en la HackUPC 2025, organitzada a la UPC de Barcelona. Durant 36 hores van desenvolupar projectes tecnològics vinculats a àmbits com la ciberseguretat, el desenvolupament de *software* i tecnologies emergents.

També hi van participar empreses tecnològiques, com Siemens, Revolut o JetBrains, que hi van aportar experts i recursos. A més de la competició, es busca potenciar el talent jove en enginyeria i ciberseguretat i enfortir una comunitat internacional de futurs professionals del sector.

2 Telegram evoluciona cap a una aplicació més lícita i responsable

Tendència

L'aplicació de missatgeria **Telegram** ha estat objecte de controvèrsia entre la **defensa de la privacitat digital** i l'ús **il·lícit** de la plataforma per part d'actors maliciosos.

Tot i que Telegram fins fa poc mantenia una posició de **neutralitat estricta**, recentment ha iniciat un **canvi estratègic important**: només en tres mesos ha col·laborat amb les autoritats entregant dades de 22.777 usuaris, cosa que mostra una evolució cap a una **aplicació més lícita.**

Aquest **gir** respon a la pressió creixent d'institucions i governs, que durant el mes de maig han posat Telegram sota el focus pel seu paper en la **propagació de continguts il·legals** i per la dificultat d'**intervenció judicial** derivada del seu sistema de xifratge.

El Vietnam, per exemple, ha bloquejat l'aplicació per la seva aparent tolerància amb canals vinculats a **fraus i narcotràfic**, mentre que França ha exigit **canvis en l'encriptació,** cosa que va portar Telegram a plantejar-se **abandonar el país** per no vulnerar la **privacitat** dels seus usuaris.

Tot i aquest nou escenari, la plataforma encara és utilitzada per a **activitats delictives**. Casos com el del grup Haowang Guarantee —que gestionava el **mercat il·legal** més gran detectat dins de Telegram—, l'ús de ***malware*** per **filtrar dades** o la distribució de continguts com **imatges de menors** i ***deepfakes*** evidencien la complexitat del repte.

Indicadors

L'activitat cibercriminal a Telegram va augmentar durant el 2024

Una anàlisi dels canals que operen de manera oculta en la plataforma revela que els ciberdelinqüents utilitzen cada cop més aquesta aplicació per a activitats del mercat clandestí.

Tipus de missatges delictius que han incrementat de volum respecte de l'any anterior

Falsificació de documents
Atacs DDoS com a servei
Cobrament en efectiu
Distribució de bases de dades filtrades
Esquemes de frau

↑ **53 %**

Segon trimestre de 2024 *vs.* any anterior

[Kaspersky]

Telegram, una font de fraus

Estafes més comunes de Telegram percebudes durant el primer trimestre de 2025

Esquemes d'inversió fraudulents
Estafes en criptomonedes
Estafes romàntiques
Estafes laborals
Atacs de *phishing*
Estafes de suplantació d'identitat
Regals falsos

[Comparitech]

Telegram: detecció i bloqueig de continguts il·legals

Entre el 17 de febrer de 2024 i el 17 de febrer de 2025, Telegram va restringir globalment un total de 3.869.935 continguts per incomplir els seus termes de servei.

Top 5 de categories restringides per contingut il·legal a Telegram

Spam	**67,4 %**
Frau, estafa i extorsió	**10,9 %**
Substàncies controlades	**5,5 %**
Hackeig i ciberdelinqüència	**4,8 %**
Diners falsos, documents falsos	**0,9 %**

Metodologies de detecció del contingut restringit aplicades per Telegram

Detecció algorítmica i de senyals	**70,6 %**
Informes d'usuaris	**11,9 %**
Intel·ligència artificial	**8,3 %**
Moderadors humans (proactius)	**5,3 %**
Hashes (firmes digitals ja conegudes)	**3,9 %**

[Telegram]

Telegram ja no és tan privat com asseguraven en un principi

Telegram ha multiplicat per quatre la seva col·laboració amb les autoritats durant el primer trimestre de 2025, com a part del seu compromís amb la transparència.

Nombre d'usuaris de qui Telegram ha facilitat dades a les autoritats, T1 2024 *vs.* T1 2025

5.826 → **22.777**

[Github] T1 2024 T1 2025

Fets rellevants

El Vietnam bloqueja Telegram per no cooperar en la lluita contra el cibercrim

El Ministeri de Tecnologia del Vietnam va ordenar als proveïdors de serveis de telecomunicacions bloquejar l'aplicació de missatgeria Telegram per la seva manca de cooperació en la lluita contra delictes com fraus, tràfic de drogues i terrorisme.

Segons un document filtrat, el 68 % dels 9.600 canals i grups de Telegram al país vulneren la llei, la qual cosa ha portat a bloquejar l'aplicació.

Les autoritats vietnamites han alertat contínuament sobre els riscos de frau i vulneracions de seguretat associats a l'aplicació.

Telegram es planteja abandonar el mercat francès per la pressió sobre el xifratge

Telegram, conegut per la seva forta posició en defensa de la privacitat dels usuaris a través del xifratge de punta a punta, es veu ara al centre d'una controvèrsia amb el Govern francès.

França demana que es modifiquin els estàndards de xifratge per raons de seguretat nacional, com la lluita contra el terrorisme i el crim organitzat. Telegram ha advertit que, si s'ha de comprometre en aquest aspecte, consideraria abandonar el mercat francès. Aquesta situació posa en relleu la tensió entre la privacitat personal i la seguretat estatal.

França rebutja les acusacions sobre interferència en les eleccions de Romania

El fundador de Telegram, Pàvel Dúrov, va acusar França de demanar-li que bloquegés veus conservadores a Romania abans de les eleccions presidencials. França va desmentir categòricament les acusacions i va cridar al respecte per la democràcia romanesa.

El Ministeri d'Afers Exteriors francès va destacar que Dúrov, nadiu rus, intentava desviar l'atenció dels veritables intents d'interferència, com la involucració russa en les eleccions. A més, les acusacions van provocar una allau de desinformació a internet, amb falses acusacions de França intervenint a Romania.

Telegram tanca el canal del mercat il·legal més gran de la plataforma

Telegram va aconseguir tancar el mercat il·legal més gran creat a la seva plataforma, Haowang Guarantee, que va facilitar 27.000 M$ en transaccions il·legals relacionades amb activitats com el blanqueig de diner, estafes amb criptomonedes i robatori d'identitats. Aquesta mesura arriba després de pressions internacionals que van assenyalar Telegram com a plataforma per al blanqueig de diner. Tot i aquest avenç, Telegram s'enfronta al dilema de preservar la privadesa de les seves comunicacions mentre lluita contra la cibercriminalitat. Paral·lelament, ha sorgit un nou mercat il·legal, Xinbi Guarantee, que ja ha transaccionat 7.230.000 milions d'euros.

PupkinStealer utilitza Telegram per filtrar dades robades

S'ha detectat que l'*infostealer* PupkinStealer utilitza Telegram com a eina clau per filtrar dades robades de PCs. A diferència de la majoria, que empra Telegram per facilitar la distribució del *malware*, en aquest cas, un cop PupkinStealer s'instal·la al dispositiu de la víctima, recull dades delicades, com contrasenyes de navegadors web, arxius personals i fins i tot captures de pantalla del dispositiu infectat. Aquestes dades es recullen de manera ràpida i es preparen en un arxiu ZIP que posteriorment és enviat utilitzant l'API de Telegram a la conversa d'un bot privat controlat per ciberdelinqüents. Aquesta tècnica permet als ciberatacants mantenir-se en l'anonimat.

Una criminòloga alerta sobre la distribució d'imatges de menors a Telegram

La criminòloga espanyola María Aperador va alertar sobre els perills de compartir imatges de menors a les xarxes socials. Aconsella als pares no pujar les seves fotografies a plataformes com Instagram, ja que aquestes imatges poden acabar en canals d'internet amb fins obscurs, com grups de Telegram que difonen contingut de menors. A més, adverteix que l'ús de la intel·ligència artificial facilita la creació de muntatges amb fotos de menors, traient-los la roba digitalment. Per la seva part, Telegram ha reforçat les seves eines de moderació per combatre aquesta pràctica.

3 L'ús recurrent d'*infostealers* combinats amb la intel·ligència artificial potencia els fraus d'identitat

Tendència

Els *infostealers* són programes maliciosos dissenyats específicament per **capturar** credencials, contrasenyes, claus de criptomonedes, dades bancàries i informació personal emmagatzemada en **dispositius infectats**. Aquest 2025, la seva difusió ha estat notable gràcies principalment a la distribució mitjançant **xarxes socials** o a la integració en **plataformes aparentment legítimes**.

Durant aquest mes de maig, les operacions internacionals han aconseguit **desmantellar** grans xarxes criminals vinculades als *infostealers* Lumma Stealer i Danabot, que acumulaven dades de **centenars de milers** de dispositius compromesos.

Aquest robatori massiu d'informació no es queda només en els mercats negres digitals, sinó que **actua com a combustible** per a nous esquemes de **frau d'identitat** molt més sofisticats. La combinació de les dades sostretes amb eines **d'IA** permet als cibercriminals generar suplantacions altament personalitzades, adaptades a cada víctima i amb una major taxa d'èxit.

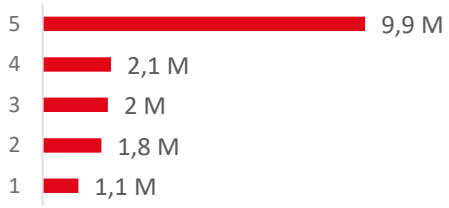
A Espanya, la tendència ja s'ha traduït en diferents incidents de suplantació d'identitat, que cada vegada es **denuncien més**. Aquesta tendència també es veu reflectida **globalment**: l'FBI ha alertat de múltiples campanyes de fraus generats amb IA que suplanten la identitat d'alts càrrecs del Govern dels EUA amb l'objectiu d'establir una relació de confiança prèvia a cometre el frau.

Indicadors

Els *infostealers*, al capdavant del robatori de credencials

Durant el 2024 es van detectar 3.200 milions de credencials robades, de les quals un **75 %** van ser sostretes a través d'*infostealers*.

TOP 5 d'*infostealers* més actius de 2024 segons el nombre de dispositius o *hosts* infectats (milions)



[Flashpoint]

URLs d'on s'han extret més credencials fent ús d'*infostealers*

Els ciberdelinqüents estan emprant el robatori de comptes en plataformes amb l'objectiu de cometre frau d'identitat, entre d'altres.

TOP 5 d'URLs d'on s'han extret més credencials (2024)

1	accounts.google.com
2	facebook.com
3	roblox.com
4	login.live.com
5	Instagram.com

[Checkpoint]

L'amenaça creixent del frau d'identitat en l'era digital

12 % L'augment anual registrat de frau d'identitat des de 2020.

70 % De tots els fraus d'identitat es produeixen a través de canals en línia.

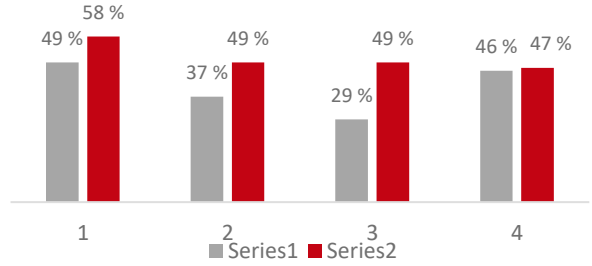
30 % Dels casos de frau d'identitat impliquen l'ús d'identitats sintètiques, creades parcialment amb dades reals i falses.

[Javelin]

La irrupció dels *deepfakes* i la IA generativa intensifiquen el frau d'identitat

Els *deepfakes* i la IA generativa es consoliden com una amenaça que afavoreix el frau d'identitat i la vulneració dels sistemes d'autenticació.

Ús de tècniques en incidents de frau d'identitat, 2022 *vs.* 2024



[Regula]

3 L'ús recurrent d'*infostealers* combinats amb la intel·ligència artificial potencia els fraus d'identitat

Fets rellevants

Una campanya utilitza vídeos generats per IA a TikTok per distribuir programari *infostealer*

S'ha detectat una nova campanya que emprava TikTok per distribuir programari *infostealer*, com Vidar i StealC, mitjançant vídeos curts generats per IA.

A diferència de les tècniques tradicionals, aquesta campanya no depèn de webs maliciosos ni d'injeccions de JavaScript, sinó que usa vídeos amb instruccions verbals i visuals per convèncer els usuaris que executin comandes de PowerShell, cosa que infecta els seus dispositius.

Alguns d'aquests vídeos han aconseguit una gran interacció, amb més de 500.000 visualitzacions.

L'Europol i Microsoft desmantellen la infraestructura tècnica de Lumma Stealer

Microsoft, juntament amb associats internacionals, ha liderat una operació per desmantellar Lumma Stealer, un *infostealer* emprat per ciberdelinqüents per robar contrasenyes, dades bancàries i personals, i informació confidencial. Mitjançant una ordre judicial als EUA, es van bloquejar 2.300 dominis i es va interrompre la infraestructura de Lumma, que comptava amb més de 394.000 dispositius infectats.

Lumma es ven a través de fòrums clandestins i permet als cibercriminals fer atacs com el *phishing* i robar dades per extorsionar o vendre-les al mercat negre.

Desmantellament global de Danabot, l'*infostealer* que robava dades delicades

Danabot, un *malware* de tipus *infostealer* utilitzat en atacs globals, va ser desmantellat gràcies a una operació internacional liderada pel Departament de Justícia dels EUA, amb el suport d'empreses de ciberseguretat. Aquest *malware*, ofert com a servei (MaaS), robava informació privada, com contrasenyes, dades bancàries i carteres de criptomonedes, i permetia als ciberdelinqüents controlar sistemes de manera remota. Propagat mitjançant enginyeria social i anuncis falsos, Danabot es va distribuir a països com l'Argentina i el Perú, i també a Europa. L'operació va tenir el suport d'agències com l'FBI i l'Europol, i d'empreses com ESET i Amazon.

Suplantació d'identitat en la declaració de la renda, amb milers de contribuents afectats per suposats guanys falsos en jocs en línia

Milers de contribuents han denunciat suplantació d'identitat a l'hora de preparar la declaració de la renda. Han rebut notificacions de l'Agència Tributària informant sobre guanys ficticis vinculats a jocs en línia i apostes en què mai havien participat.

Aquesta suplantació sembla una tècnica per amagar guanys i evitar impostos. La Direcció General d'Ordenació del Joc (DGOJ) ha activat el Protocol de Suport a Contribuents Suplantats (PACS).

El 2024, es van registrar més de 7.700 denúncies relacionades amb aquest frau.

La Policia Nacional alerta sobre una estafa de suplantació d'identitat per WhatsApp

La Policia Nacional adverteix d'una estafa creixent a WhatsApp basada en enginyeria social.

Els ciberdelinqüents accedeixen primer al compte d'un conegut (familiar o amic) i, fent-se passar per ell, contacten amb noves víctimes. Amb una excusa creïble (com recuperar un compte perdut), demanen un codi de verificació SMS, que en realitat és la clau per robar el perfil de WhatsApp.

Un cop obtenen l'accés, sol·liciten diners als contactes de la víctima aprofitant la confiança i la informació de les converses prèvies.

L'FBI alerta d'una campanya de suplantació de personalitats amb SMS i veus generades amb IA

Des de l'abril de 2025, l'FBI ha detectat una campanya activa a gran escala en què ciberactors usen missatges de text (*smishing*) i missatges de veu generats per intel·ligència artificial (*vishing*) per suplantar alts càrrecs del Govern dels EUA. L'objectiu és establir una falsa relació de confiança amb les víctimes per accedir a comptes personals o institucionals, robar dades delicades o fins i tot diners. Els atacants contacten tant amb funcionaris en actiu com retirats, i també amb persones del seu entorn, i es fan passar per figures d'autoritat conegudes. Una vegada han guanyat una certa confiança, els enganyen perquè accedeixin a enllaços maliciosos o els proporcionin dades.

Indicadors

Augment dels ciberincidents en el sector de l'aigua

Durant el 2024, el sector de l'aigua va experimentar un lleu increment en el nombre d'incidents de ciberseguretat registrats a Espanya, amb set casos més respecte a l'any anterior.

[INCIBE]

% d'incidents detectats a operadors de serveis vinculats al sector de l'aigua a Espanya

4,58 % (2023) → **5 %** (2024)

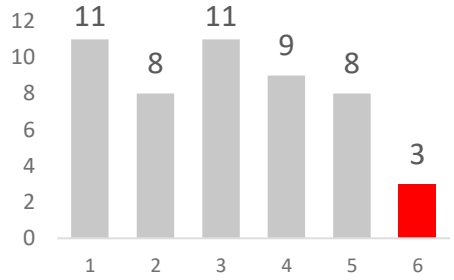
Any rere any es repeteixen les campanyes de *smishing* que suplanten l'AEAT

Segons dades de l'AEAT (Agència Estatal d'Administració Tributària), des de 2020 és recurrent la suplantació de l'AEAT en campanyes fraudulentes de *phishing* per SMS.

Fins al mes de maig de 2025, ja s'ha alertat de tres campanyes.

[AEAT]

Nombre de campanyes de *phishing* suplantant l'AEAT

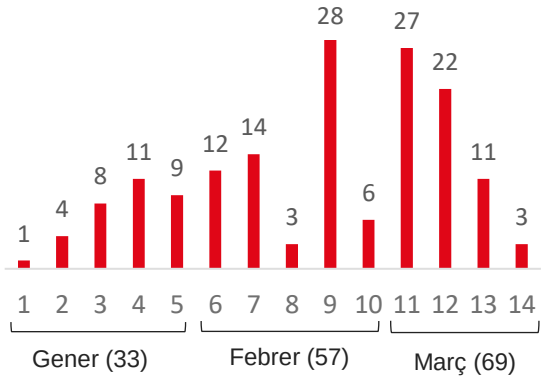


Cada setmana s'exploten una mitjana d'aproximadament 11 vulnerabilitats per primera vegada

Durant el primer trimestre de 2025, es van identificar 159 vulnerabilitats (CVE) com a explotades activament per primera vegada. Aquestes vulnerabilitats s'exploten a un ritme molt ràpid, amb un 28,3 % que presenten evidències d'explotació el primer dia després de la seva publicació com a CVE.

[Vulncheck]

Evolució setmanal de les vulnerabilitats explotades per primera vegada durant el 1r trimestre de 2025



Pèrdues rècord en criptomonedes el primer trimestre de 2025

Durant el primer trimestre de 2025, es van perdre més de 1.536 M€ en criptomonedes a causa de 197 incidents de robatoris i estafes. Només el 0,4 % dels fons robats han estat recuperats.

[CertiK]

Evolució interanual de les pèrdues en criptomonedes per ciberdelinqüència (T1 de 2024 *vs.* T1 de 2025)

303 %

T1 2024 → T1 2025

Fets rellevants

Catalunya acull el primer congrés estatal sobre ciberseguretat hídrica

El 14 de maig es va celebrar el Primer Congrés Nacional "La Ciberseguretat de les Entitats Crítiques Vinculades al Sector de l'Aigua", organitzat per la Càtedra INCIBE en Digitalització i Ciberseguretat Hídrica de la Universitat de Girona. L'esdeveniment va reunir 60 professionals i va abordar reptes clau, com la protecció de sistemes industrials IT/OT, la detecció d'atacs, la privacitat i l'ètica en infraestructures crítiques. Addicionalment, es van compartir experiències reals (Agbar/Veolia i Depuradores d'Osona), que van permetre conèixer de primera mà com s'està gestionant la ciberseguretat en la infraestructura.

Demanen 30 anys de presó per al gironí acusat de l'estafa més gran en criptomonedes

Un inversor gironí, responsable de la plataforma Arbistar 2.0, s'enfronta a una pena de presó de 30 anys, acusat d'una presumpta estafa a través d'una estafa piramidal de criptomonedes.

L'empresa Arbistar 2.0 comercialitzava un *software* d'intel·ligència artificial que generava algoritmes i que "mai va existir".

L'Audiència Nacional està jutjant aquests dies Fuentes, a qui s'atribueix haver comès l'estafa més gran de la història amb criptomonedes, que va afectar 32.000 inversors, que haurien perdut més de 1.900 M€.

Avís de l'Agència Tributària sobre fraus durant la campanya de la renda 2024

Durant la campanya de la renda 2024, l'Agència Tributària adverteix d'un augment de fraus digitals per correu electrònic (*phishing*) i SMS (*smishing*), en què els ciberdelinqüents suplanten la identitat per obtenir dades personals o econòmiques.

L'Agència recorda que no demana informació confidencial ni fa devolucions via targeta o Bizum, ni cobra per cap servei. Davant qualsevol correu o SMS sospitós, es recomana no obrir enllaços ni fitxers adjunts, i es pot denunciar a través dels canals oficials per combatre el frau digital.

Kaspersky vincula el grup d'espionatge Careto al Govern espanyol

Careto, un grup de ciberespionatge descobert per Kaspersky el 2014, hauria estat operat pel Govern espanyol, segons fonts internes de Kaspersky.

El *malware*, altament sofisticat, capaç d'interceptar dades crítiques i d'accedir a governs i empreses, va començar a ser investigat a partir d'una infecció a Cuba. Internament, Kaspersky va concloure que Espanya n'era responsable, però mai ho va fer públic per política de no atribució.

El cas situa Espanya al costat de potències com els EUA o França en operacions cibernètiques estatals secretes.

L'ex número dos d'Interior, a presó per vincles amb el ciberdelinqüent espanyol Alcasec

La jutgessa de l'Audiència Nacional va decretar presó preventiva per a Francisco Martínez, ex secretari d'estat de Seguretat amb Rajoy, i el conegut ciberdelinqüent Alcasec, per presumpta participació en una xarxa criminal de ciberatacs i blanqueig de capitals. La policia nacional investiga una infraestructura clandestina que accedia il·legalment a dades crítiques de milions de ciutadans, elaborava perfils i els venia al mercat negre. Martínez hauria donat accés al sistema amb el pretext de proves legals. La xarxa operava amb servidors al núvol, criptomonedes i estructures opaques.

La UE crea una base de dades europea de vulnerabilitats per reforçar la ciberseguretat

La Comissió Europea ha anunciat el llançament de l'EU Vulnerability Database (EUVD), una nova base de dades gestionada per l'Agència de la UE per a la Ciberseguretat (ENISA) (https://euvd.enisa.europa.eu/).

Aquesta eina centralitzarà informació de vulnerabilitats digitals rellevants per al mercat europeu, cosa que facilitarà el compliment de la Directiva NIS2 i del Reglament de resiliència cibernètica (CRA). L'EUVD ajudarà tant entitats públiques com privades a gestionar millor els riscos en la cadena de subministrament i en productes amb elements digitals, la qual cosa reforçarà l'autonomia i la sobirania tecnològica de la Unió Europea.

Resum executiu

El nombre d'incidents ***ransomware*** amb afectació a Espanya arriba a les **15 víctimes**, i es manté en un **nivell baix** d'amenaça. Aquests incidents suposen un increment del **86 % respecte al mes d'abril**. Els grups més actius a Espanya durant aquest mes han estat **Arcus Media i Akira**, seguits de **Brain Cipher i NighSpire**. Al seu torn, el sector més afectat a Espanya ha estat el de la **indústria manufacturera**, seguit dels **serveis professionals**.

El nombre de vendes d'accessos compromesos en fòrums i mercats de cibercrim amb afectació a Espanya es manté en un **nivell baix d'amenaça**, amb **cinc casos**. Els actors actius durant el mes de maig han estat **krasnyylotos, BenjaminFr, jamalunga i LongNight**. Al seu torn, els sectors afectats han estat el del **govern / sector públic**, **la indústria manufacturera i el turisme**.

El nombre de publicacions de **venda de bases de dades i informació robada es manté estable**, amb un **nivell d'amenaça mitjà**, amb afectacions a institucions públiques i empreses privades.

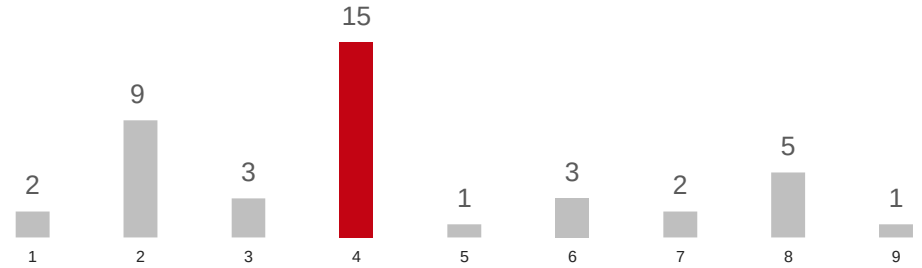
Activitats destacades

La sobtada desaparició del fòrum de cibercrim **BreachForums** podria provocar que les activitats il·lícites es traslladin a altres fòrums de característiques similars, com ara **DarkForums**, o a fòrums de parla russa, com **XSS i Exploit**. A més, és probable que fins que no s'aclareixi el que ha passat, continuïn apareixent suposats clons de **BreachForums**, que semblen respondre a intents d'estafa per part de diferents usuaris.

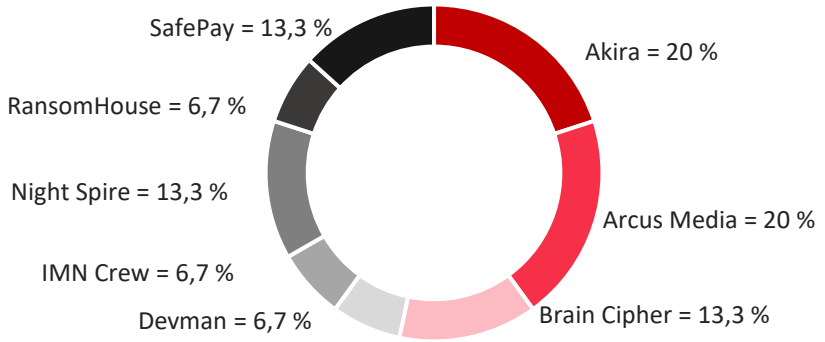
El grup **SafePay** ha anunciat durant aquest període, al seu web de víctimes a la **xarxa Tor**, el suposat compromís de l'entitat manufacturera **Azpiaran**, amb uns ingressos anuals estimats de 13,2 milions d'euros, al web **azpiaran.com**. El grup va publicar-ne una mostra amb evidències i ha indicat haver compromès un conjunt de dades d'aquesta entitat.

El grup **Devman** ha anunciat durant aquest període, al seu web de víctimes a la **xarxa Tor**, el suposat compromís de l'entitat del sector **governamental / públic Ajuntament de Níjar**, al web **nijar.es**. El grup va aportar-ne evidències i ha indicat haver compromès un conjunt de dades d'aquesta entitat que contenien aproximadament **120 GB**.

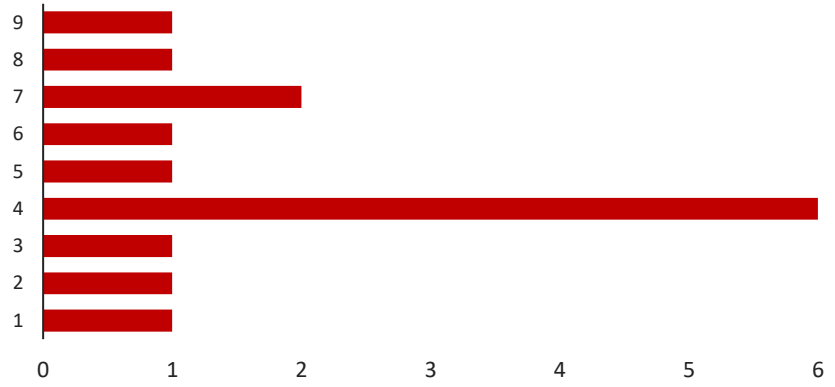
Incidents per països: Amèrica llatina, Portugal i Espanya



Grups de *ransomware*



Sectors afectats en l'àmbit iberoamericà



Referències

Catalunya reforça l'ecosistema de ciberseguretat: creixement empresarial, innovació i demanda de talent

https://www.redestelecom.es/seguridad/novedades-de-la-sexta-edicion-del-barcelona-cybersecurity-congress/
https://ciberseguretat.gencat.cat/ca/detalls/noticia/agencia-ciberseguretat-catalunya-gestiona-3372-ciberincidents-2024
https://dca.cat/ca/2025/05/la-comunitat-dca-ciberseguretat-celebra-amb-exit-la-seva-primera-trobada-anual/
https://ciberseguretat.gencat.cat/ca/detalls/noticia/sector-ciberseguretat-catalunya-factura-1400-milions-euros
https://ciberseguretat.gencat.cat/ca/detalls/noticia/sector-ciberseguretat-catalunya-factura-1400-milions-euros
https://www.upc.edu/es/sala-de-prensa/noticias/700-hackers-se-reunen-para-la-hackupc-2025

Telegram evoluciona cap a una aplicació més lícita i responsable

https://cybernews.com/tech/vietnam-telegram-nationwide-block-leaked-document-reveals/
https://cyberexperts.com/telegram-faces-french-showdown-over-encryption-will-they-exit/
https://therecord.media/france-rejects-durov-telegram-accusations-romania-election
https://www.cointribune.com/es/telegram-anuncia-la-eliminacion-masiva-de-cuentas-relacionadas-con-un-mercado-ilicito-chino/
https://www.picussecurity.com/resource/blog/pupkinstealer-net-infostealer-using-telegram-for-data-theft
https://www.20minutos.es/tecnologia/ciberseguridad/alerta-maria-aperador-criminologa-padres-no-suban-redes-sociales-nada-ninos-telegram-5707768/

L'ús recurrent d'*infostealers* combinats amb la intel·ligència artificial potencia els fraus d'identitat

https://www.infosecurity-magazine.com/news/ai-tiktok-videos-infostealer/
https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/
https://tn.com.ar/tecno/novedades/2025/05/24/otro-golpe-al-cibercrimen-desmantelaron-danabot-una-peligrosa-estructura-de-malware-que-robaba-datos/
https://andaluciainforma.eldiario.es/tramites/sorpresa-al-presentar-la-renta-miles-de-contribuyentes-denuncian-suplantacion-de-identidad/
https://www.20minutos.es/tecnologia/ciberseguridad/policia-alerta-sobre-ultima-estafa-whatsapp-te-puedes-quedar-sin-dinero-datos-5708311/
https://www.ic3.gov/PSA/2025/PSA250515

Encara no és tendència…

https://cyberh2o.es/exito-en-el-i-congreso-nacional-la-ciberseguridad-de-las-entidades-criticas-vinculadas-al-sector-del-agua/
https://www.diaridegirona.cat/comarques/2025/05/10/30-anys-preso-gironi-estafa-criptomonedes-117228775.html
https://sede.agenciatributaria.gob.es/Sede/todas-noticias/2025/mayo/6/aviso-seguridad-campana-renta-2024.html
https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/
https://www.rtve.es/noticias/20250529/prision-francisco-martinez-exsecretario-estado-interior-gobierno-rajoy/16601668.shtml
https://digital-strategy.ec.europa.eu/en/news/eu-launches-european-vulnerability-database-boost-its-digital-security

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

ciberseguretat.gencat.cat

@ciberseguracat

linkedin.com/company/ciberseguracat