ANDORRA DIGITAL

ANDORRA DIGITAL CIBERSEGURETAT

Informe de Ciberintel·ligència

Exposició de credencials en el web fosc: del *leak* a la intrusió

TLP: WHITE

AGOST 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	31/08/2026	02/09/2026

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 l'exposició de credencials al web fosc i a l'ecosistema criminal associat, amb afectació a Espanya i Andorra, durant el període de gener a agost de 2026. L'informe parteix d'una premissa que condiciona tota l'anàlisi i és que una credencial exposada no és un incident tancat sinó l'inici d'una cadena d'atac. És per això que, més enllà de quantificar l'activitat de credencials detectades, l'informe segueix el recorregut complet d'una credencial robada, des de la captura a l'equip de la víctima, passant per la comercialització en fòrums i mercats criminals, fins a l'explotació com a vector d'intrusió.

L'informe s'elabora sobre fonts d'intel·ligència pròpies, basades en el monitoratge continu de fòrums de compravenda del web obert, canals de Telegram i llocs de la xarxa Tor (.onion) on els actors d'amenaça publiquen i comercialitzen la seva activitat.

El monitoratge comprèn una quarantena de fòrums de compravenda, amb seguiment de més de 150 seccions i dels canals de missatgeria ràpida (*shoutboxes*). Es comptabilitzen les publicacions on l'actor identifica Espanya o Andorra com a país de l'organització o de les dades afectades. Aquestes xifres reflecteixen deteccions, no una mesura de l'exposició total real, i els volums de registres esmentats als anuncis corresponen a afirmacions dels mateixos actors, llevat que se n'indiqui de manera expressa la verificació. Durant els vuit mesos analitzats es van registrar 386 publicacions úniques vinculades a Espanya i Andorra, amb mitjana aproximada de 48 publicacions mensuals, sense cap altra per sota de 30. La tipologia dominant és la comercialització d'informació compromesa: les bretxes i les filtracions de dades concentren prop de tres quartes parts de les publicacions, i les llistes combinades de *cred* parells usuari-contrasenya. És important prestar atenció als 75 anuncis de venda d'accés inicial a sistemes d'organitzacions espanyoles, perquè es tracta de la categoria que connecta de manera més directa la credencial exposada amb la intrusió i, en última instància, amb el programari de segrest (*ransomware*).

En el cas d'Andorra, l'única detecció directa de tot el període correspon a la venda de dades d'una organització andorrana, anunciada el juny. Encara que només hi hagi una detecció no s'ha d'interpretar com a absència d'exposició, perquè els actors poques vegades segmenten les seves publicacions per països més petits, per la qual cosa el material andorrà pot circular sense identificar dins de recopilacions etiquetades com a espanyoles o europees.

Per a l'elaboració d'aquest informe es descriu, en primer lloc, el cicle de vida d'una credencial robada, des de la captura fins a l'explotació; tot seguit, s'analitza el paper específic dels *infostealers* i la diferència operativa entre un *log* recent i una llista de credencials reciclada; es presenta l'anàlisi detallada del període per a Espanya i Andorra, i s'examina la connexió entre la credencial exposada i l'activitat de mercat.

Per acabar l'informe, es recullen les conclusions de l'anàlisi, un annex amb l'origen de les dades, la cobertura de fonts i les famílies d'*infostealer* observades en el període.

3. CICLE DE VIDA D'UNA CREDENCIAL ROBADA

És important comprendre l'exposició de credencials com un procés, perquè entre el moment que una contrasenya queda compromesa i el moment en què es pot utilitzar per a finalitats malicioses, poden transcórrer des d'uns minuts fins a diversos mesos, i al llarg d'aquest temps la credencial haurà passat per diferents mans, preu o propòsit. Aquest cicle de vida s'estructura en tres fases: captura, comercialització i explotació. Aquestes tres fases són importants per a un equip de ciberseguretat, atès que són tres oportunitats per trencar la cadena d'atac abans d'un incident.

Figura 1 - Cicle de vida de la credencial compromesa

3.1. Captura

La primera fase és obtenir la credencial. Hi ha diferents vies, però a efectes d'aquest informe és important diferenciar-ne dues per les seves implicacions defensives totalment diferents.

El primer és la **bretxa d'un servei**, el compromís de la base de dades d'una organització exposa les credencials dels usuaris. L'impacte només afecta, en principi, aquest servei, i la seva reutilització només depèn que les víctimes hagin fet servir la mateixa contrasenya en altres llocs. Un cas particular és l'elaboració de *combolists*, recopilacions de parells d'usuari-contrasenya fusionades a partir de bretxes antigues, filtracions prèvies i credencials reciclades, que es redistribueixen de manera massiva.

El segon origen és el ***malware infostealer*** (programari maliciós de robatori d'informació), un programa maliciós que s'executa a l'equip de la víctima i de forma automatitzada extreu totes les credencials guardades al navegador, juntament amb les galetes de sessió, les dades d'autoremplenament i també moneders de criptomonedes juntament amb dades de targetes bancàries. La diferència amb la bretxa és qualitativa, perquè l'*infostealer* no compromet un compte, sinó l'equip complet i tota la identitat digital que s'ha emmagatzemat a l'equip.

La diferència és determinant perquè condiciona tot el que segueix, una credencial procedent d'una *combolist* reciclada pot haver caducat fa temps, mentre que un *log* d'*infostealer* extret recentment arriba acompanyat de galetes de sessió que permeten eludir autenticació.

3.2. Comercialització

Un cop exfiltrada la credencial, aquesta entra en un mercat que avui dia ja té un grau notable d'especialització i liquiditat. Aquesta fase és la més visible per al monitoratge i la que concentra la pràctica total de les publicacions analitzades en aquest informe.

El contingut es distribueix i es ven a través dels fòrums de compravenda, canals de missatgeria i mercats automatitzats, amb models que van des de la venda directa d'un conjunt concret de dades fins a la distribució gratuïta de llistes de credencials com a reclam reputacional entre els actors maliciosos. En aquest mercat operen diferents perfils i qui captura la informació no sol ser qui l'explota. Les credencials passen per intermediaris com a distribuïdors de *combolists*, venedors de *logs* d'*infostealer* i, els de més valor, els Initial Access Brokers que comercialitzen accessos ja validats a les xarxes corporatives, abans d'arribar a l'actor que finalment els utilitza.

Una mateixa dada es pot revendre i redistribuir repetides vegades, per actors diferents i en dates diferents. A les dades obtingudes del període s'observa precisament això de manera directa en la reaparició de lots de credencials amb un volum idèntic anunciats en moments separats, indici de revenda o refregit del mateix contingut. La conseqüència defensiva és que l'exposició no s'esgota amb la primera publicació: una credencial no invalidada continua tenint valor de mercat mentre continuï sent vàlida.

Tota aquesta comercialització es concentra, en plataformes de la web oberta accessible mitjançant un registre, molt més que en infraestructures ocultes. Aquest desplaçament cap a canals molt més accessibles amplia la visibilitat i l'abast de l'oferta, encara que això també en facilita el monitoratge.

3.3. Explotació

La fase final és l'ús de la credencial per obtenir accés i tractar de causar un impacte. Aquí és on la credencial deixa de ser una dada en un mercat per convertir-se en clau d'intrusió.

Els vectors d'explotació són variats. El més directe és el *credential stuffing*, que és l'assaig automatitzat de parells d'usuari-contrasenya, procedents de *combolists*, contra múltiples serveis, que aprofiten la reutilització de contrasenyes, per això no és aconsellable tenir dues contrasenyes similars per a diferents serveis. Quan el material inclou galetes de sessió vàlides, l'atacant pot segrestar una sessió ja autenticada sense necessitat de conèixer la contrasenya ni superar un segon factor d'autenticació. I en el cas més greu, la credencial vàlida sobre un servei d'accés remot, un panell d'administració o la xarxa d'una organització es converteix en un accés inicial: el punt d'entrada que un broker ven i que un altre actor fa servir per desplegar l'atac, generalment solen ser operadors de programari de segrest o afiliats.

4. ORIGEN *INFOSTEALER*: PER QUÈ ÉS IMPORTANT LA DISTINCIÓ

No totes les credencials exposades representen el mateix risc. Dues publicacions diferents poden mostrar, en aparença el mateix, per exemple, parells d'usuari-contrasenya d'Espanya o d'Andorra, i, no obstant això, poden representar amenaces molt diferents segons l'origen. Distingir entre una llista de credencials reciclada i un *log* d'*infostealer* recent és el més important a l'hora de prioritzar la resposta davant d'una exfiltració.

4.1. Dos orígens, dos nivells de risc

Una **llista combinada** és una recopilació de credencials acoblada a partir de bretxes antigues, filtracions prèvies i altre tipus de llistes. El seu valor per al ciberdelinqüent és de probabilitat, perquè realment no sap quins d'aquests parells continuen sent vàlids, i la seva explotació depèn de l'intent massiu de *login* contra múltiples serveis (*credential stuffing)* i que les víctimes reutilitzin contrasenyes. Una gran part d'aquests *combolists* està caducat, revocat o duplicat al moment en què es distribueix.

Un **registre de lladre d'informació** (*log* d'*infostealer*) és completament diferent. Procedeix d'un equip infectat i conté una captura de tot allò que el programari maliciós va poder extreure del navegador i del sistema en el moment de l'execució, com ja hem comentat: credencials desades, galetes de sessió actives, tokens d'autenticació, dades d'autoremplenament, historial, etc. La diferència més gran amb el *combolist* és que un *log* recent és vàlid en el moment de la captura, i descriu no un compte, sinó la identitat digital completa associada a un dispositiu compromès.

DIMENSIÓ	LLISTA COMBINADA RECICLADA	*LOG INFOSTEALER* RECENT
Origen	Agregació de bretxes i filtracions prèvies	Equip concret infectat per codi maliciós *infostealer*.
Validesa	Agregació de bretxes i filtracions prèvies	En el moment de la captura.
Contingut	Parells usuari-contrasenya	Credencials, galetes de sessió, tokens, autoremplenament, moneders cripto.
Elusió de MFA	No	Sí, mitjançant reproducció de galetes de sessió.
Abast	El compte afectat	El dispositiu i tota la identitat de què disposa.
Resposta adequada	Restabliment de contrasenya i MFA	Forense de l'equip concret infectat, invalidació de sessions i rotació àmplia.

Taula 1 - Diferències operatives entre una llista combinada reciclada i un log d'infostealer recent

4.2. Implicacions per a la resposta

Davant d'una credencial procedent d'una *combolist*, el restabliment de la contrasenya afectada, unit a un MFA, resol en gran manera el risc. En canvi, davant d'un *log* d'*infostealer*, aquesta mateixa resposta no és suficient, perquè restablir la contrasenya no invalida les sessions ja segrestades mitjançant galetes, no aborda la resta de les credencials exfiltrades al mateix *log*, i no resol la infecció del dispositiu, que pot continuar capturant les noves credencials que es vagin canviant o introduint. Un *log* d'*infostealer* exigeix tractar l'incident com a compromís del dispositiu.

4.3. Els *infoestealers* a les dades del període

En les dades del període analitzat, les publicacions explícitament com a distribució de *stealerlogs* són escasses, amb quatre publicacions davant de les 366 del total. Aquestes publicacions són, explícites quant a la seva naturalesa, anuncien lots de *logs* atribuïts a les famílies META Stealer, Mystic Stealer i WhiteSnake Stealer, amb víctimes a Espanya identificades pel sistema operatiu i el navegador compromesos, i descriuen, bàsicament, continguts que inclouen credencials, galetes de sessió i dades de moneders de criptos.

Aquesta xifra tan baixa no s'ha d'interpretar com una presència menor d'*infostealer*, atès que la comercialització de *logs* es produeix majoritàriament en mercats automatitzats i en serveis de subscripció *clouds of logs* que operen al marge de la publicació individual en fòrums; i a part, avaluem amb confiança mitjana que una proporció significativa de les 22 *combolistes* del període, anunciades com a fresques i de qualitat alta es nodreix de credencials extretes per *infostealers*, atès que, avui, aquest és el mecanisme principal d'obtenció de credencials recents i vàlides.

4.4. Context de l'ecosistema (fonts obertes)

Segons el *2026 Global Threat Intelligence Report* de Flashpoint, els *infostealers* van comprometre 7,4 milions de dispositius durant el primer semestre del 2026, un increment del 27 % respecte al semestre anterior i van extreure al voltant de 1.700 milions de credencials. La mateixa font situa Vidar, StealC i Lumma entre les variants més actives durant aquest període.

L'ecosistema es troba en un moment de reconfiguració, atès que les operacions contra la infraestructura de Lumma i Rhadamanthys el 2025 van alterar el repartiment del mercat i van afavorir l'ascens d'altres famílies d'*infostealers* com ara Vidar.

5. ANÀLISI DEL PERÍODE: ESPANYA I ANDORRA

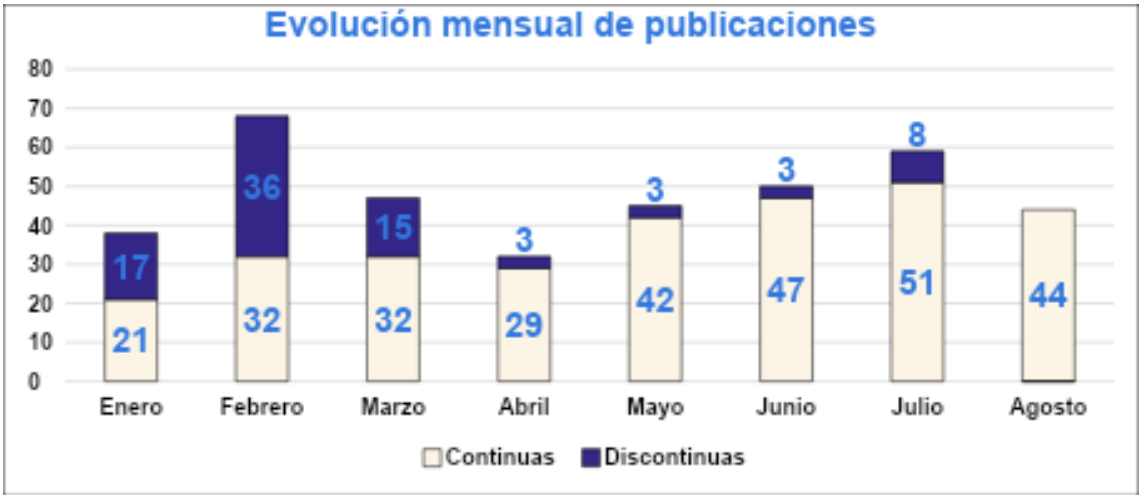
En l'apartat següent analitzarem l'activitat registrada entre gener i agost de 2026 amb afectació a Espanya i Andorra. Tot seguit s'exposaran els punts següents: el volum de publicacions i la seva evolució mensual, el desglossament per categoria, els sectors més afectats i l'ecosistema de plataformes en què es comercialitza el material. Andorra es tracta de manera diferenciada al tancament de la secció.

5.1. Volum i tendència mensual

Durant el període es van registrar 386 publicacions úniques, amb una mitjana de 48 publicacions mensuals i cap mes per sota de 30.

MES (2026)	PUBLICACIONS	FONTS CONTÍNUES	FONTS DISCONTINUADES
Gener	38	21	17
Febrer	68	32	36
març	47	32	15
Abril	32	29	3
Maig	45	42	3
Juny	50	47	3
Juliol	59	51	8
Agost	44	44	0

Taula 2 - Evolució mensual de publicacions vinculades a Espanya i Andorra, amb desglossament entre fonts presents durant tot el període i fonts l'aportació de les quals s'interromp a partir d'abril. Tres publicacions sense data normalitzada s'exclouen de la sèrie, no del total.



Gràfic 1 - Evolució mensual de publicacions

El pic del febrer amb 68 publicacions s'explica en gran manera per la concentració d'anuncis d'accés inicial: 28 aquest mes, el màxim del període. El repunt del juliol amb 59 respon, en canvi, a bretxes i filtracions de dades.

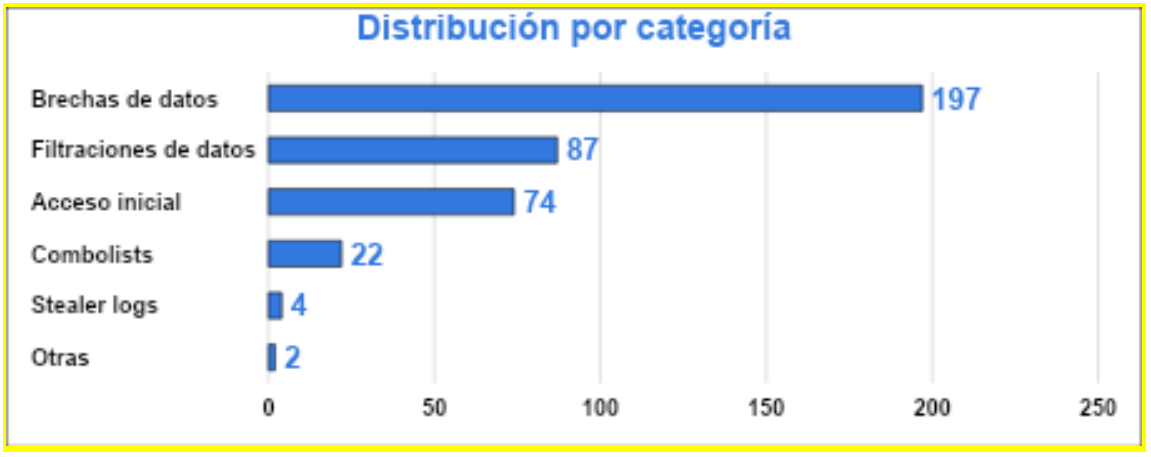
La sèrie mensual mostra una tendència creixent sostinguda al llarg del període, de 21 publicacions el gener a 51 el juliol.

5.2. Desglossament per categoria

La tipologia dominant és la comercialització d'informació compromesa: les bretxes i les filtracions de dades concentren en conjunt prop de tres quartes parts de les publicacions del període.

CATEGORIA	PUBLICACIONS	% DEL TOTAL
Bretxes de dades (*Data Breach*)	197	51,0%
Filtracions de dades (*Data Leak*)	87	22,5%
Accés inicial (*Initial Access*)	74	19,2%
Combolists	22	5,7%
Logs of infostealers	4	1,0%
Altres	2	0,5%

Taula 3 – Distribució per categoria de les publicacions del període. «Altres» comprèn una sol·licitud de compra de credencials corporatives i una amenaça declarada contra objectius espanyols.



Gràfic 2 - Distribució per categoria

Tres observacions qualitatives sobre aquest desglossament:

- ***Combolists***: volum reclamat i reciclatge. De les 22 *combolists*, 19 declaren volum, amb un agregat d'uns 5,4 milions de parells de credencials. La repetició de xifres idèntiques en dates diferents amb lots de 491.000, 436.000 i 362.000 parells anunciats dues vegades cadascun, això indica revenda o redistribució del mateix material, per la qual

cosa l'agregat s'ha de llegir com a cota superior del que s'ha anunciat, no com a credencials úniques.

- **Accés inicial**: la categoria de més severitat. Els 74 anuncis d'accés inicial inclouen accessos RDP, panells d'administració amb *webshell*, accés *root* a un proveïdor de serveis d'Internet no identificat, un proveïdor de serveis gestionats el compromís dels quals afectaria una vintena de clients corporatius, una plataforma municipal de gestió documental que l'actor afirma que dona servei a més de trenta ajuntaments, i portals d'administració de nòmines del sector públic.
- ***Logs* d'*infostealers***: presència baixa en fòrums, rellevància alta. Les publicacions directes de *logs* són escasses, però explícites: lots de 500 *logs* de META Stealer i 1.000 de Mystic Stealer descrits com de víctimes a Espanya, i 2.500 de WhiteSnake Stealer amb mostres que inclouen sistemes espanyols.

5.3. Desglossament sectorial (Espanya)

En el 74 % de les publicacions en relació amb Espanya s'hi troba un sector identificable. L'administració pública encapçala el desglossament, seguida de prop per finances, comerç al detall i energia.

CATEGORIA	PUBLICACIONS
Administració pública i organismes governamentals	46
Finances, banca i assegurances	42
Comerç minorista	32
Energia i *utilities*	31
Comerç electrònic	16
Educació	16
Telecomunicacions	12
Sanitat	12

Taula 4 - Sectors més afectats per les publicacions relatives a Espanya (vuit primers, que agrupen variants d'etiquetatge). En el 26 % de les publicacions (101) el sector no hi consta i s'exclou del recompte.

Gràfic 3 - Sectors més afectats (Espanya)

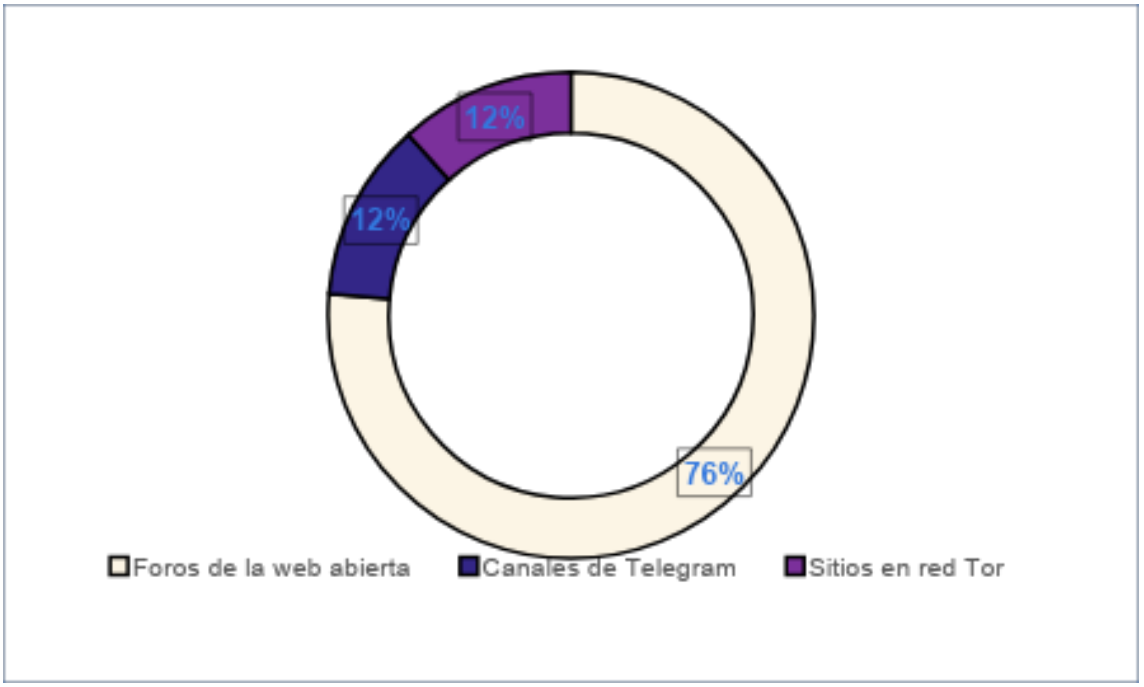
L'administració pública destaca tant en bretxes de dades com en anuncis d'accés inicial, combinació que avaluem amb confiança mitjana com l'escenari de risc afegit més gran del període: la superfície de credencials exposades i l'oferta d'accés a sistemes conviuen per al mateix sector.

5.4. Ecosistema de comercialització

El web obert concentra tres quartes parts de les publicacions del període, cosa que confirma que el mercat de credencials opera majoritàriament en fòrums accessibles mitjançant registre, no en infraestructura oculta.

CATEGORIA	PUBLICACIONS	% DEL TOTAL
Fòrums del web obert	295	76,4%
Canals de Telegram	46	11,9%
Llocs en xarxa Tor	45	11,7%

Taula 5 – Distribució de les publicacions del període per tipus de plataforma. El detall per plataforma concreta es recull a l'annex



Gràfic 4 - Distribució de les publicacions del període per tipus de plataforma.

Entre els fòrums, Breached/BreachForums, DarkForums i PwnForums concentren el nombre més gran de publicacions amb afectació a Espanya i Andorra durant el període, seguits d'Exploit, Darknet Army, Spear, NulledBB i Demonforums.

5.5. Andorra

En el període es va registrar una única publicació vinculada a Andorra, la presumpta bretxa d'una organització del sector de lloguer de vehicles, anunciada el juny amb un volum reclamat d'uns 137.000 registres amb dades de contacte de clients, reserves i tiquets de suport i un preu de 1.100 dòlars. Cap publicació del període no anuncia *combolists*, *stealer logs* ni accessos inicials específics d'Andorra.

6. DE LA CREDENCIAL AL PROGRAMARI DE SEGREST (*RANSOMWARE)*

Les seccions anteriors descriuen l'exposició de credencials com un cicle que culmina a l'explotació. La secció següent desenvolupa el tram final d'aquest cicle perquè és on l'exposició de credencials deixa de ser un problema de dades per convertir-se en un problema operatiu. La baula que connecta els dos mons és l'Initial Access Broker.

6.1. L'Initial Acces Broker com a baula

L'Initial Access Broker és un actor especialitzat a comprometre organitzacions i revendre aquest accés a tercers, entre ells operadors de programari de segrest i els seus afiliats. La seva existència introdueix una divisió del treball que ha professionalitzat la ciberdelinqüència: un actor obté les credencials (per *infostealer*, força bruta, pesca o explotació d'un servei exposat), un segon les converteix en accés a la xarxa i el posa a la venda, i un tercer executa el xifratge i l'extorsió. La credencial exposada és la primera matèria d'aquesta cadena i l'accés inicial és el producte intermedi de més valor.

6.2. Els accessos inicials a la telemetria del període

Com es detalla a la secció 5, durant el període es van registrar 74 anuncis de venda d'accés inicial amb afectació a organitzacions espanyoles, la tercera categoria per volum amb un 19,2 % de les publicacions i la de més severitat potencial, per situar-se un pas abans de la intrusió.

6.3. La connexió amb el *ransomware* de segrest contra les organitzacions espanyoles

El context en què s'inscriu aquesta oferta d'accessos és el d'una activitat de programari de segrest en clara expansió a Espanya. Fonts del sector, recollides per mitjans que citen l'INCIBE i el CCN-CERT, situen la duplicació dels atacs de *ransomware* a Espanya el 2026 respecte a l'any anterior, amb les credencials robades i els accessos remots sense doble factor entre els vectors d'entrada més freqüents. Les anàlisis de vectors d'accés inicial per al 2026 coincideixen a assenyalar els *infostealers* i els Initial Access Broker com a dues de les vies per les quals els operadors de programari de segrest obtenen l'entrada, i adquireixen sovint accessos validats en lloc de comprometre ells mateixos la víctima.

7. CONCLUSIONS

L'anàlisi del període entre gener i agost del 2026 confirma que l'exposició de credencials vinculades a Espanya i Andorra és sostinguda, amb 386 publicacions detectades i una tendència creixent. L'activitat no respon a episodis puntuals sinó a un mercat en funcionament continu.

La troballa principal és orientar aquest mercat cap a la comercialització d'informació compromesa més que cap a l'atac directe. Gairebé tres quartes parts de les publicacions corresponen a bretxes i filtracions de dades, i la categoria que segueix en volum, els 74 anuncis de venda d'accés inicial, és també la de més severitat potencial, per situar-se immediatament abans de la intrusió.

La distinció entre l'origen de les credencials exposades és la conclusió de més valor operatiu. Una *combolist* reciclada i un *log* d'*infostealer* recent poden anunciar-se de manera indistingible i exigeixen, però, respostes completament diferents: la primera es resol en gran manera amb el restabliment de la contrasenya i una autenticació robusta i el segon constitueix un compromís de dispositiu que requereix una anàlisi forense de l'equip compromès, invalidació de totes les sessions actives i rotació. Tractar un *log* com si fos una *combolist* és l'error de resposta més costós que es pot cometre davant d'aquesta mena d'alertes, perquè deixa obertes les vies que l'atacant utilitza realment.

En el pla sectorial, l'administració pública concentra simultàniament el volum més gran de bretxes de dades i una presència destacada al mercat d'accessos, combinació que avaluem amb confiança mitjana com l'escenari de més risc agregat del període. El segueixen en exposició els sectors financer, de comerç detallista i energètic.

Pel que fa a Andorra, l'única detecció directa del període no permet establir tendències ni sostenir que hi hagi una campanya dirigida contra el país. L'absència de deteccions en un país de mida reduïda reflecteix en bona part les pràctiques d'etiquetatge dels actors i no s'ha de confondre amb absència d'exposició.

8. 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.