



Generalitat
de Catalunya

**Centre de Seguretat
de la Informació
de Catalunya**

**Informe de tendències de
ciberseguretat**

T2 2019

“El renaixement del ransomware”



Generalitat de Catalunya
**Centre de Seguretat de la Informació
de Catalunya**

El contingut d'aquesta guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND.
L'autoria de l'obra es reconeixerà a través de la inclusió de la menció següent:



Generalitat de Catalunya
**Centre de Seguretat de la Informació
de Catalunya**

Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.

Llicenciada sota la llicència CC BY-NC-ND.

Aquesta guia es publica sense cap garantia específica sobre el contingut.

Aquesta llicència té les particularitats següents:

Vostè és lliure de:

 Copiar, distribuir i comunicar públicament l'obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de l'obra de la manera especificada per l'autor o el llicenciador (en tot cas, no de manera que suggereixi que gaudeix del suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

***Avís:** En reutilitzar o distribuir l'obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.*

El text complet de la llicència es pot consultar a <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.ca>

L'informe inclou recursos gràfics, com imatges i icones, subministrades des de plataformes de continguts gratuïts de lliure difusió. Agraïments i menció específica a: <https://www.iconfinder.com>, <https://pixabay.com>.

The background of the entire page is a close-up of a hand holding a smartphone. Overlaid on this is a complex digital graphic. A large, semi-circular arc of white lines radiates from the center of the phone's screen area. This arc is surrounded by several thick, blue, pill-shaped segments. The entire scene is set against a background of blurred, glowing blue and white circles and lines, suggesting a data or network environment.

Aquest document és fruit del seguiment i de l'anàlisi de les tendències en relació amb les amenaces de ciberseguretat detectades per part del CESICAT durant el període indicat.

Per a la realització d'aquest informe s'han tingut en compte l'activitat i la documentació pròpies generades pel CESICAT, així com diversos informes de referència i fonts qualificades d'entitats, fabricants, organismes i professionals del món de la ciberseguretat, tant de l'àmbit nacional com internacional.

Índex

Resum	2
Ha estat notícia	4
<i>Ransomware</i> dirigit a organismes públics	10
Fuites de dades	18
<i>Business Email Compromise (BEC)</i>	24
Ciberseguretat en clau geopolítica	30
Baròmetre d'amenaçes	38

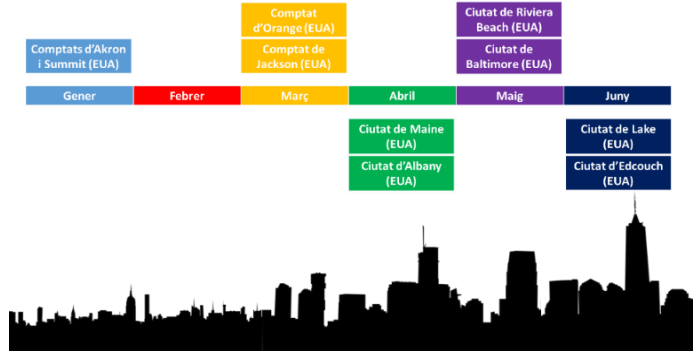


Resum

Resum

Ransomware dirigit a organismes públics. Els atacs de *ransomware* d'aquest trimestre s'han **duplicat** respecte del trimestre anterior i evolucionen cap a un **model d'atac més dirigit**, basat en centrar els esforços contra entitats que disposin d'una important **capacitat financera**, factor que ha provocat que els **rescats esdevinguin cada cop més elevats**. En especial, es prioritzen organitzacions al càrrec de **serveis essencials** i que no puguin fer front a una aturada dels seus sistemes, fet que incrementa la probabilitat que **optin pel pagament del rescat**.

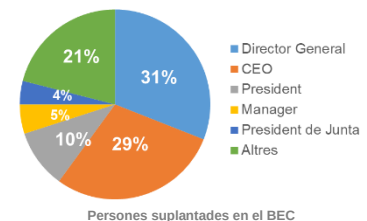
Mentre que inicialment les víctimes preferides eren empreses, actualment es constata un creixement dels atacs contra **organitzacions públiques, com centres de salut i institucions**. La ciberdelinqüència, habitualment centrada en maximitzar beneficis al menor esforç, pot haver descobert que és un àmbit amb **mancances de ciberseguretat** i amb una alta **predisposició al pagament del rescat**, especialment quan disposa d'assegurança, ja que qualsevol aturada de servei pot tenir un impacte directe sobre la ciutadania. Dos exemples de l'abast d'aquesta ciberamença són els casos de les ciutats de **Baltimore** i de **Lake City** (EUA). La primera va decidir **no pagar el rescat i tres mesos després continuava sense haver recuperat la normalitat de les seves operacions**. En canvi, la segona va **pagar el rescat i va poder recuperar ràpidament alguns sistemes** com la telefonia fixa i el correu electrònic, tot i que la realitat és que tampoc va aconseguir assolir la normalitat de forma immediata. En qualsevol cas, **la recomanació és no pagar**, atès que no hi ha cap garantia de recuperar la informació, i **posar-se en contacte amb els serveis de gestió d'incidents** corresponents per determinar la millor acció a prendre.



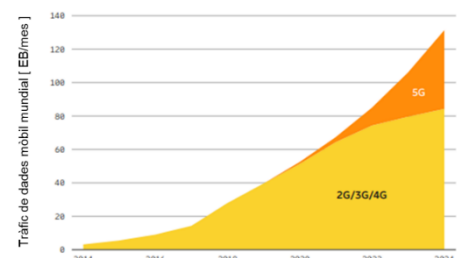
Fuites de dades. En el segon trimestre de 2019, el volum d'informació exposada en les fuites de dades manté la mateixa **tendència creixent** dels mesos previs. És especialment rellevant el cas de les **fuites derivades d'errors de configuració**: el primer trimestre el nombre de registres exposats va doblar tot el 2018, però **aquest trimestre novament s'ha doblat** fins a arribar a més de **5.300 milions de registres**. Els incidents amb bases de dades **MongoDB** han estat protagonistes.



Enginyeria social. En aquest segon trimestre de 2019 s'ha observat un creixement especial dels atacs anomenats **Business Email Compromise (BEC)** contra entitats, en els quals **el hacker suplanta un correu electrònic de confiança d'un treballador o un proveïdor** per aconseguir una **transferència econòmica**. Aquesta tècnica és cada cop més **sofisticada** i mostra elevades possibilitats d'**èxit**. Als EUA, **el 2018** aquesta tècnica **va doblar** la quantitat de diners defraudats el 2017, arribant a **superar els 1.200 milions de dòlars**.



Ciberseguretat en clau geopolítica. Les capacitats de la **tecnologia 5G** donaran l'oportunitat d'oferir tecnologies i serveis impensables a dia d'avui, però també **incrementarà el risc de ciberamenaces**. Els estats han reconegut la tecnologia 5G com un **assumpte estratègic** i han començat a prendre mesures pel seu control que, a més, representen una mostra de la lluita pels **interessos comercials** i el **posicionament geopolític** de les principals economies del món. El **conflicte dels EUA amb Huawei** n'és una mostra, el qual ha acabat amb la inclusió del gegant xinès en la llista de companyies perilloses i amb tota la indústria a l'expectativa de què pugui passar els propers mesos. L'interès geopolític també es fa evident en l'àmbit d'Internet. Estats com **Rússia** i **Iran** treballen per la creació d'una **Xarxa pròpia** que respongui als seus interessos de control, supervisió i censura.



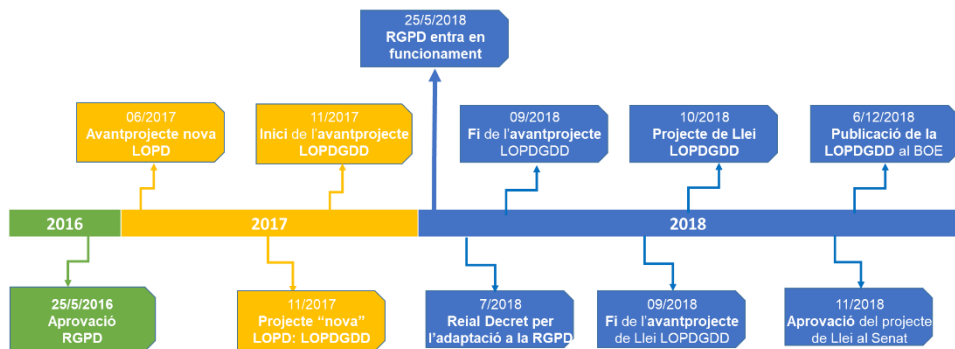


Ha estat notícia

Ha estat notícia

L'RGPD compleix un any

El 25 de maig de 2019 va ser el **primer aniversari de l'entrada en vigor del Reglament General de Protecció de Dades (RGPD)** per als països membres de la Unió Europea (UE). A l'Estat espanyol, el RGPD s'ha complementat a nivell estatal a través de la **Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**.



Il·lustració 1. Cronograma fins a l'aprovació de la LOPDGDD

El nou paradigma que acompanya l'aparició del Reglament tot just acaba de començar però, després d'un any de vigència, és possible valorar les seves primeres implicacions, el grau de compliment i la problemàtica associada.

L'**RGPD** (Reglament General de Protecció de Dades) és el nou reglament europeu d'obligat compliment a partir del 25 de maig de 2018 que, a Espanya, s'ha ampliat amb la nova Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals (LOPDGDD). Estableix canvis importants amb relació a la normativa precedent: la responsabilitat proactiva de l'encarregat de tractar les dades i l'enfocament de la ciberseguretat orientada al risc.

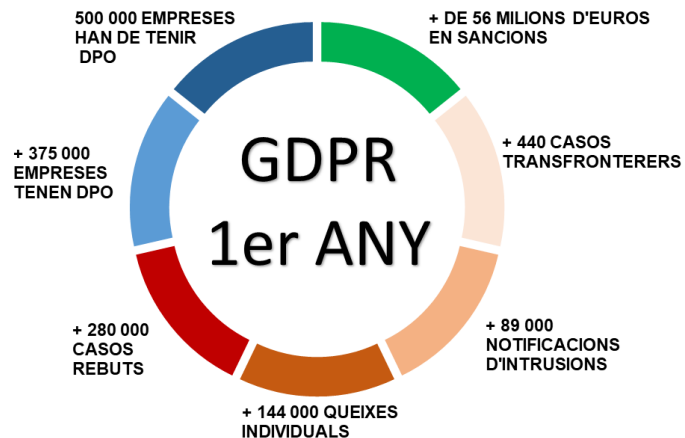
Augment de la consciència

Una de les primeres conclusions que l'Eurobaròmetre del 2019 del Parlament Europeu mostra és l'augment de la consciència dels ciutadans europeus amb relació als seus drets i les seves dades personals: **el 67 % ha sentit a parlar del Reglament i el 36 % és conscient de què comporta**. A més, **el 57 % sap que existeix una autoritat pública al seu país responsable de la protecció de les dades personals dels ciutadans**, la qual cosa significa un augment de 20 punts percentuals en comparació amb els resultats de l'Eurobaròmetre del 2015¹.

Augment de la consciència dels ciutadans europeus amb relació als seus drets i les seves dades personals.

¹ https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_bg

Aquesta nova consciència també es reflecteix en el nombre de reclamacions presentades davant de les agències europees de protecció de dades, **les quals són informades d'una mitjana de 767 casos** amb afectació a la seguretat de les dades personals al dia².



Il·lustració 2. Evolució de la implantació del RGPD a la UE³

L'RGPD a Catalunya en xifres

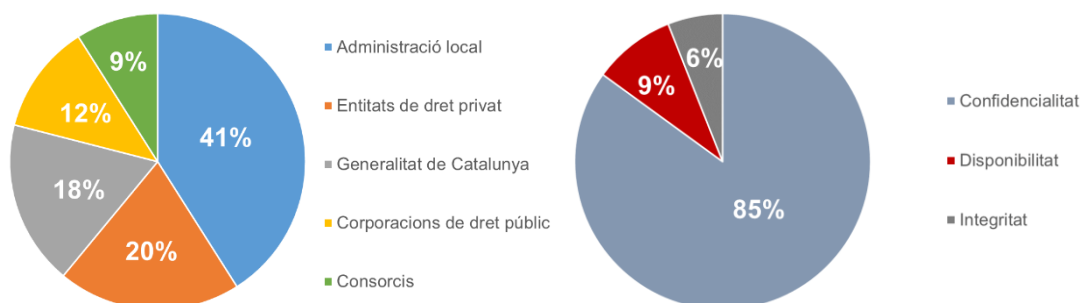
A Espanya, l'Agència Espanyola de Protecció de Dades (AEPD) és l'autoritat pública independent encarregada de vetllar per la privacitat i la protecció de les dades dels ciutadans. Tanmateix, existeixen altres autoritats de control amb àmbits competencials propis, com l'Agència Basca de Protecció de Dades i l'Autoritat Catalana de Protecció de Dades (APDCAT). En concret, l'APDCAT⁴ té com a àmbit d'actuació les administracions públiques de Catalunya i informa dels drets en matèria de protecció de dades i accés a la informació vinculada, com s'exerceixen i què s'ha de fer si no es respecten, a més d'informar, assessorar sobre les obligacions que preveu la legislació i controlar que les entitats la compleixin.

En qualsevol cas, el primer any de vida de l'RGPD a Catalunya ha permès identificar que **el 85% de les notificacions tenen a veure amb incidents de ciberseguretat relacionats amb la confidencialitat**, fet que es corrobora amb el creixent nombre de fuites de dades personals detectat (veure [Fuites de dades](#)), i que **el 41% afecten l'Administració local**.

² http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

³ <https://iapp.org/resources/article/gdpr-one-year-anniversary-infographic/>

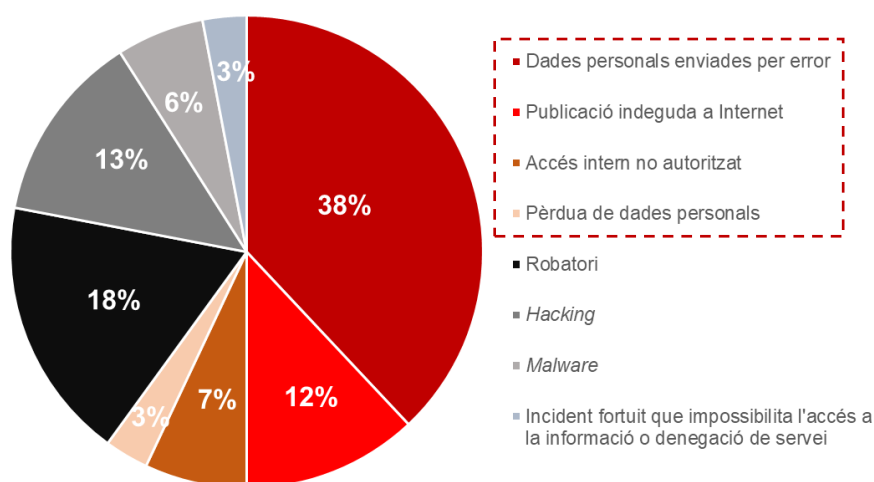
⁴ https://apdcat.gencat.cat/ca/autoritat/estructura/autoritat_catalana_de_proteccio_de_dades/



Il·lustració 3. Notificacions de violacions de seguretat segons el tipus d'entitat afectada (esquerra) i la tipologia d'incident (dreta) ⁵

Adicionalment, es pot constatar que la suma dels incidents causats per **errors, publicacions indegudes, accessos no autoritzats i pèrdues d'informació són el 60%**. Aquests són incidents que tenen **origen directe en el factor humà** i, per tant, cal destacar la importància de la formació, sensibilització i conscienciació dels empleats i ciutadans en general per evitar la major part dels incidents.

Importància de la formació, sensibilització i conscienciació dels empleats i ciutadans en general per evitar la major part dels incidents.



Il·lustració 4. Notificacions segons tipus d'incident ⁶

Palanca per a un canvi global

No hi ha cap mena de dubte que el nou Reglament ha tingut un fort impacte en l'àmbit internacional. En aquest sentit, com ja avançava el CESICAT en el seu article *RGPD: bona notícia per a la ciberseguretat*⁷, cal destacar la seva capacitat per impulsar un **canvi global: les empreses de fora de la UE que ofereixen**

⁵ http://www.isacabcn.org/images/18juny2019/prezi_compressed-1-comprimido-1.pdf

⁶ http://www.isacabcn.org/images/18juny2019/prezi_compressed-1-comprimido-1.pdf

⁷ https://ciberseguretat.gencat.cat/web/.content/PDF/22062018_Article-RGPD.pdf



productes a ciutadans europeus o en monitoritzen la conducta han optat per acceptar el compliment del Reglament i nomenar un representant a la UE, de manera que **són residuals els casos d'empreses que han cessat la seva activitat**. Així, la majoria de companyies s'han adaptat a l'RGPD, una norma restrictiva i exigent respecte d'altres legislacions i ja estan en condicions d'estendre als usuaris d'arreu del món el mateix tractament que ofereixen als ciutadans de la UE.

A més, diversos països de fora de la UE han establert **regulacions similars a l'RGPD** i, segons la Comissió Europea, proveeixen un nivell de protecció suficient per permetre **transferències internacionals de dades personals sense necessitat d'una autorització de l'AEPD**. És el cas, entre d'altres, de països com **Suïssa, Canadà, Andorra, Argentina, Japó, Uruguai, Nova Zelanda i Israel**⁸. En aquesta línia, tot indica que el col·lectiu creixerà i evolucionarà per constituir un marc comú internacional conformat per països amb garanties comunes pel que fa al tractament de les dades dels ciutadans.

Evolucionarà per constituir una autèntica comunitat mundial de països amb garanties comunes pel que fa al tractament de les dades dels ciutadans..

Estats com Califòrnia han fet ús de la seves competències per aprovar la California Consumer Privacy Act (CCPA), i altres com Arizona i Vermont han endurit la seva legislació.

Als Estats Units d'Amèrica (EUA), la norma és més laxa que l'europea, però **es permeten les transferències internacionals de dades personals amb entitats certificades dels EUA** en el marc de l'acord **Privacy Shield**⁹. Tanmateix, la **discussió entre els ciutadans nord-americans sobre la necessitat de fer un**

canvi de rumb i adoptar una norma similar a l'europea en matèria de dades personals és més viva que mai. Estats com Califòrnia han fet ús de les seves competències per aprovar la **California Consumer Privacy Act (CCPA)**¹⁰, i altres com **Arizona i Vermont** han endurit la legislació. Fins i tot companyies com **Microsoft** s'hi han posicionat a favor¹¹.

Sancions exemplars

Tot i que l'RGPD només té un any de vida, s'han aplicat **sancions per un import total de 56,6 milions d'euros**, si bé un 90% de l'import correspon a la sanció de **50 milions d'euros a Google** dictada per la *Commission Nationale de l'Informatique et des Libertés*, l'organisme regulador de la privacitat i les dades personals a França, al·legant "manca de transparència, informació incorrecta i absència de consentiment vàlid en la publicitat

⁸ <https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html>

⁹ <https://www.privacyshield.gov/list>

¹⁰ <https://www.caprivacy.org/>

¹¹ <https://www.zdnet.com/article/gdpr-usa-microsoft-says-us-should-match-the-eus-digital-privacy-law/>

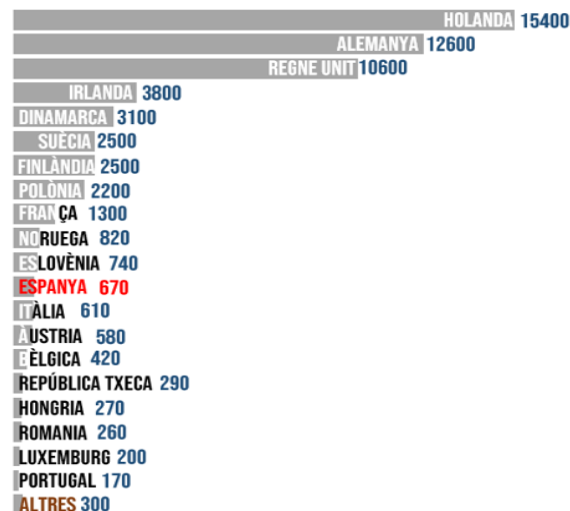
personalitzada"¹². Aquesta sanció queda molt lluny de la de **250.000 euros** que l'AEPD va imposar a **La Liga de Futbol** per una app que espiava els usuaris amb l'objectiu de detectar emissions de futbol il·legals en bars¹³.

S'han aplicat sancions per un import total de 56,6 milions d'euros, si bé un 90% de l'import correspon a la sanció de 50 milions d'euros a Google.

El marc sancionador de l'RGPD s'ha plantejat com un aspecte clau per promoure el seu compliment. Per aquest motiu, les **quantitats són severes i exemplificadores**: poden arribar a **20 milions d'euros o al 4% de la facturació anual**¹⁴. No obstant això, el desplegament de les sancions està essent adequat a la realitat de cada país de la UE amb l'objectiu d'adaptar i impulsar de forma progressiva **la millora de la ciberseguretat i la creació d'un marc europeu uniforme** en matèria de tractament de dades personals.

El nivell d'implantació efectiva del Reglament a cada Estat de la UE és força diferent.

A dia d'avui, el nivell d'implantació efectiva del Reglament a cada Estat de la UE és força diferent. Mentre s'obliga a informar **del nombre d'incidents amb afectació sobre dades personals** en un termini de 72 hores, no succeeix així a tots els països de la UE i el **nombre de fuites d'informació notificades és molt desigual**. El 28 de gener, Espanya havia rebut 670 notificacions, gairebé tres vegades més que les 260 de Romania, però fins a 23 vegades menys que les 15.400 dels Països Baixos¹⁵.



Il·lustració 5. Nombre de fuites de dades personals notificades (fins el 28/01/2019)¹⁶

¹² <https://www.xataka.com/legislacion-y-derechos/google-tendra-que-pagar-50-millones-euros-francia-violar-gdpr>

¹³ <https://www.expansion.com/juridico/actualidad-tendencias/2019/06/11/5c994e5468aeb331b8b45a8.html>

¹⁴ <https://gdpr.eu/fines/>

¹⁵ <https://www.dlapiper.com/~media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf>

¹⁶ <https://www.dlapiper.com/es/spain/insights/publications/2019/01/gdpr-data-breach-survey/>



CYBER CRIME

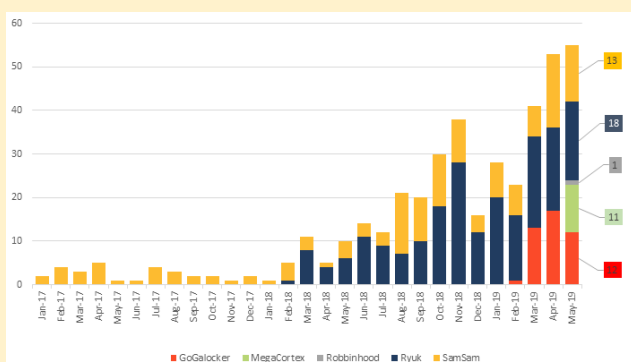
*Ransomware dirigit a
organismes públics*

Baròmetre

Els atacs de *ransomware* són notícia per causar catastròfiques conseqüències en organismes i empreses. Respecte el segon trimestre de 2018, aquests atacs dirigits han crescut un 365%, mentre que els atacs massius han decrescut un 12%¹⁷.

Increment del *ransomware* dirigit

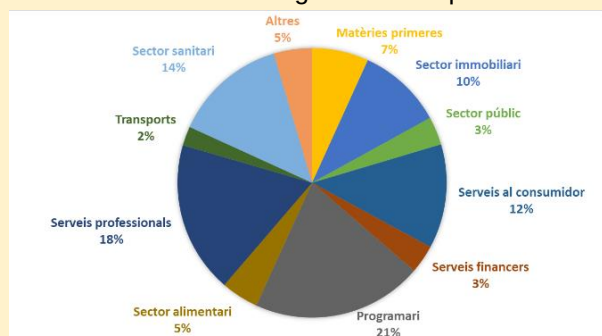
S'observa una tendència alcista del nombre de víctimes de *ransomware* dirigit: el nombre d'incidents s'ha doblat aquest trimestre. A darrere s'hi troben les principals famílies del *malware*: Ryuk, SamSam, GoGalocker, MegaCortex o Robinhood.



Il·lustració 6. Evolució del nombre d'incidents de ransomware dirigit¹⁸

Atacs dirigits a organitzacions públiques

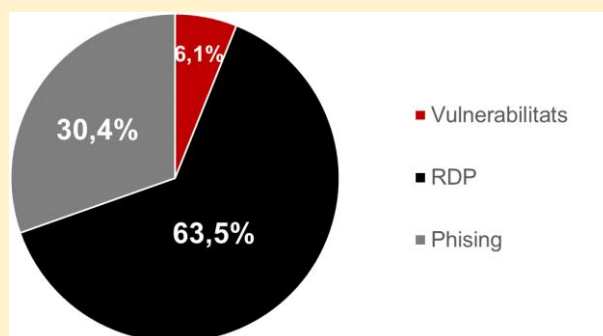
Els ciberatacants segueixen fent ús de *ransomware* contra el sector sanitari (14%) però recentment mostren interès per les organitzacions públiques (3%). A Catalunya, atès que l'àmbit sanitari pertany majoritàriament al sector públic, aproximadament un 17% dels atacs estan dirigits contra aquest darrer.



Il·lustració 7. Sectors atacats per ransomware durant el segon trimestre¹⁹

Vectors d'atac

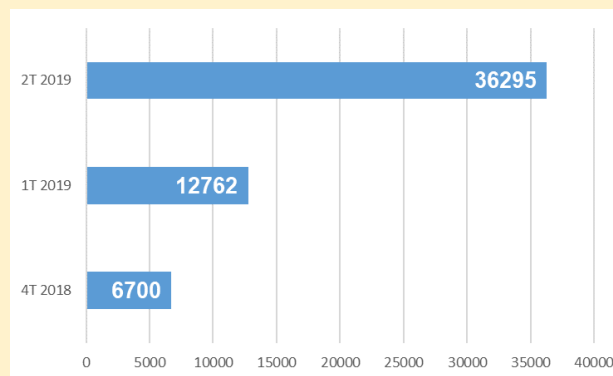
Els principals vectors d'atac són les connexions d'escriptori remot (RDP), el *phishing* (principalment per correu electrònic) i l'explotació de vulnerabilitats. La millor estratègia per tal de ser víctima d'un atac de *ransomware* rau en la prevenció: disposar de còpies de seguretat fresques, mantenir els sistemes protegits, actualitzats i formar els treballadors.



Il·lustració 8. Vectors d'atac més habituals²⁰

Rescats

L'import mitjà dels rescats segueix creixent a causa de l'increment dels atacs dirigits, en els quals es reclamen quanties superiors als atacs massius.



Il·lustració 9. Evolució econòmica del cost mitjà dels rescats²¹

Un estudi realitzat a més de 1.000 empreses destaca que el 39% de les petites i el 74% de les mitjanes pagarien un rescat per recuperar les seves dades, tot i que la recomanació de les autoritats i les forces de l'ordre és que no es pagui, ja que tampoc no hi ha cap garantia d'èxit.

¹⁷ <https://blog.malwarebytes.com/reports/2019/08/labs-quarterly-report-finds-ransoms-gone-rampant-against-businesses/>

¹⁸ <https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat>

¹⁹ <https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases>

²⁰ <https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases>

²¹ <https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread>

Ransomware dirigit a organismes públics

El **ransomware** o programari de segrest és un programari maliciós que restringeix de manera total o parcial l'accés als fitxers d'un dispositiu fins que no es paga una determinada quantitat de diners.

Habitualment, el ciberatacant xifra els sistemes d'informació de la víctima, la qual rep una clau per a desxifrar i recuperar la seva informació si realitza el pagament d'un rescat en criptomoneda.

Els organismes públics són objectiu

Tal i com es pronosticava en l'Informe de Prospectives de Ciberseguretat 2019, el **ransomware** evoluciona com un atac cada vegada més dirigit²². Els ciberatacants escullen l'empresa o organisme que serà la víctima de l'atac i estableixen com a objectiu els sistemes d'informació que sostenen la seva operativa. Així, els afectats sovint es veuen empesos a pagar el rescat si volen recuperar la normalitat i aquest pot tenir un import més elevat. Aquesta tendència es constata en l'increment del valor mitjà dels rescats que, durant la primera meitat de 2019, s'ha multiplicat per més de 5 i arriba als 36.295 dòlars (veure il·lustració 8).

A final de 2018 es començava a visualitzar com creixien els atacs de ransomware dirigit a empreses (veure il·lustració 6), però el segon trimestre de 2019 ha evidenciat com els ciberdelinqüents han desplaçat el seu punt de mira cap als organismes públics, com governs locals i entitats de serveis per a la ciutadania. El motiu és que aquests organismes públics es poden veure empesos a pagar un rescat a causa de la **urgència i pressió per evitar una aturada d'activitat que pugui afectar milers (o fins i tot milions) de ciutadans**, la qual cosa causaria un important ressò en mitjans d'informació i podria malmetre seriosament la reputació de l'acció governamental.

Els ciberdelinqüents han dirigit el seu punt de mira cap als organismes públics, com governs locals i entitats de serveis per a la ciutadania.



Il·lustració 10. Principals institucions públiques afectades per ransomware durant el 2019

Aquesta tendència té un precedent clar en els fets del **març de 2018** a la ciutat d'Atlanta (EUA). **Atlanta va resultar afectada pel ransomware SamSam i se li demanava un rescat de 51.000 dòlars**, els quals no se sap del cert si van ser pagats. Però moltes bases de dades van quedar corrompudes, les quals no es van poder recuperar, i diversos serveis es

²² <https://ciberseguretat.gencat.cat/web/.content/PDF/Prospectives-de-seguretat-2019.pdf>



van veure afectats, incloent-hi el pagament d'impostos, de serveis municipals i de taxes judicials. **Restaurar la normalitat dels serveis va suposar a la ciutat una despesa de 17 milions de dòlars**²³. El greu impacte d'aquest incident i les severes crítiques de què va ser víctima el govern, a causa del programari desfasat i la manca de mesures de protecció, ha estat una **font inspiradora pels cibercriminals, els quals preveuen que les noves víctimes optaran per fer el pagament del rescat per tal de no viure una experiència similar**.

Per ara, els atacs coneguts es concentren principalment als EUA. S'estima que els motius són els limitats recursos públics que es dediquen a protegir la infraestructura IT de les administracions locals, la qual cosa les fa més vulnerables que l'administració estatal o l'empresa privada, així com pel volum de població que pot resultar impactada en un país amb 327 milions d'habitants²⁴. No obstant això, de ben segur que **les administracions locals d'arreu del món que no gaudeixin d'una bona salut en quant a ciberseguretat, incloses les catalanes, més tard o més d'hora resultaran seriosament amenaçades**.

Moltes bases de dades van quedar corrompudes, les quals no es van poder recuperar, i diversos serveis es van veure afectats.

Bandes organitzades

S'identifiquen clarament dos tipus d'actors principals quan es tracta de *ransomware*: grups criminals organitzats i actors estatals²⁵.

Els **grups criminals organitzats** han convertit l'atac per *ransomware* en un autèntic negoci lucratiu. Sovint estan formats per diferents equips criminals que actuen de forma coordinada, talment com una organització empresarial: hi ha equips programadors especialistes en escriure el codi del *malware*, altres s'ocupen de la distribució i infecció de les víctimes, de la gestió del pagament del rescat i el seu cobrament, etc. Aquest model resulta ser exitós, com ho demostra el cas dels creadors del *ransomware* de distribució massiva **Gandcrab**, els quals fa ben poc han cessat la seva activitat fent ostentació dels més de **2.000 milions de dòlars recaptats** per tota la xarxa criminal²⁶. A més, cal dir que **un entorn tan diversificat dificulta molt la tasca policial**.

Sovint estan formats per diferents equips criminals que actuen de forma coordinada, talment com una organització empresarial.

Els **actors estatals** són **grups de hackers subvencionats per Estats**. Aquests no tant sols operen per a robar fons, sinó també amb interès geopolític o la voluntat de sembrar el caos. Alguns casos són el del *ransomware* **Wannacry**, presumptament vinculat al grup Lazarus de Corea del Nord²⁷, o el *ransomware* **NotPetya**, que es relaciona amb l'agència d'intel·ligència russa GRU²⁸.

²³ <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/atlanta-recovery-17-million-dollars/>

²⁴ <https://www.zdnet.com/article/ransomware-why-cities-have-become-such-a-big-target-for-cyberattacks-and-why-itll-get-worse-before-it-gets-better/>

²⁵ <https://blog.chainalysis.com/reports/decoding-ransomware-attacks>

²⁶ <https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/>

²⁷ <https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group>

²⁸ <https://www.wired.com/story/white-house-russia-notpetya-attribution/>

Les conseqüències d'un atac de ransomware

Quan hom és víctima d'un *ransomware*, rep un missatge amb l'import del rescat, juntament amb les instruccions per fer-ne el pagament. Però, més enllà del pagament del rescat en el cas que s'opti per fer-lo, **el cost econòmic total d'un incident de ransomware es divideix en: el cost de recuperació i el cost d'oportunitat.**



Il·lustració 11. Missatge de rescat del conegut ransomware Wannacry

El cost de recuperació inclou totes les despeses que es faran per restablir la normalitat de les operacions: restauració d'ordinadors i servidors, l'anàlisi forense per trobar l'origen de l'atac, l'assessorament legal en cas que s'hagin compromès dades especialment de caràcter personal, la gestió de la crisi (en cas que es faci públic l'incident) i el pagament del rescat (en cas que es realitzi). La ciutat de **Baltimore** (veure Fets rellevants) ha estimat que el cost de recuperació serà d'uns **10 milions de dòlars**.

El cost econòmic total d'un incident de ransomware es divideix en: el cost de recuperació i el cost d'oportunitat.

El cost d'oportunitat, sovint més important en magnitud, **quantifica el que suposa per a la víctima la pèrdua de les funcions afectades fins que es recupera la normalitat de les operacions.** La ciutat de **Baltimore** (veure Fets rellevants), des del 7 de maig de 2019 fins encara al final del segon trimestre, no ha pogut operar amb normalitat com a conseqüència dels més de 10 000 ordinadors i servidors afectats pel *ransomware*. Algunes operacions han començat a realitzar-se amb un procediment alternatiu i d'altres, com el Registre de la Propietat, han passat a fer-se de manera completament manual. Baltimore estima que el seu cost d'oportunitat total serà de **8 milions de dòlars**²⁹.

²⁹ <https://www.vipre.com/blog/baltimore-ransomware-recovery-18-million/>

La còpia de seguretat o backup és la còpia d'un fitxer o un conjunt de fitxers, generalment actualitzada periòdicament, que permet restaurar les dades originals en cas de pèrdua.

Un pla de continuïtat de negoci o business continuity plan (BCP) és un pla logístic per a la pràctica de com una organització ha de recuperar i restaurar les seves funcions crítiques, parcial o totalment interrompudes, en un temps predeterminat després d'una interrupció no desitjada o desastre.

Un pla de recuperació de desastres o disaster recovery plan (DRP) és un procés de recuperació que cobreix les dades, el maquinari i el programari crític, perquè un negoci pugui començar de nou les seves operacions en cas d'un desastre.

La prevenció és la clau

De mitjana, les empreses triguen 6 dies a recuperar l'operativa habitual des que experimenten un atac de **ransomware**, però arriba als 9 dies quan es tracta de **malwares** com Bitpaymer o Ryuk. Aquesta diferència depèn de l'habilitat del grup de **hackers** que hi ha al darrere l'atac per dirigir-lo allà on causi més dany i de la capacitat del mateix **malware** per propagar-se sobre els sistemes d'informació de la víctima³⁰. Alguns **ransomware** aconseguixen paraitzar l'operativa de la víctima durant setmanes.

La millor manera d'evitar un incident de ransomware o minimitzar el seu impacte passa per establir mesures preventives.

Una llarga aturada no és assumible per a un organisme públic del qual depenen els tràmits administratius o els serveis a la ciutadania. En aquest sentit, la millor manera d'evitar un incident de **ransomware** o minimitzar el seu impacte passa per establir mesures preventives:



1. Sistemes protegits, actualitzats i treballadors formats.

Cal protegir-se preventivament davant dels principals vectors d'atac dels ciberatacants: escriptori remot (RDP), *phishing* i l'explotació de vulnerabilitats (veure il·lustració 8). Per evitar atacs d'RDP o l'aprofitament de vulnerabilitats és imprescindible disposar d'uns **sistemes d'informació actualitzats, protegits i posats a prova per professionals de la ciberseguretat**. Davant del *phishing*, al marge d'eines informàtiques de filtratge de correu electrònic, cal **dotar els treballadors de la formació adequada** per evitar conductes de risc, com obrir fitxers enviats des d'adreces de correu desconegudes o escrits amb un text especialment sospitos.



2. Planificació: BCP i DRP

En funció de com una organització hagi preparat el seu pla de continuïtat de negoci (BCP) i el seu pla de recuperació de desastres (DRP) podrà valorar ràpidament quin és l'impacte d'un incident de **ransomware** i establir els procediments que ha de seguir per restaurar la normalitat de les seves operacions, quant temps trigarà a fer-ho i com ho farà per tal que durant l'incident no es vegin totalment interromputs. Un **aspecte bàsic és la disponibilitat de còpies de seguretat fresques per recuperar la informació xifrada**. En canvi, una organització que no disposi de plans preventius l'única alternativa que té és el pagament d'un rescat a canvi de les claus de desxifratge, sense cap garantia que pugui ser una solució.

³⁰ <https://www.coveware.com/dharma-ransomware-payment>

Transferir el risc és el pagament d'una prima, per part d'algú que no és capaç de suportar una pèrdua, a una empresa que es compromet, segons uns termes acordats, a cobrir aquesta pèrdua. Un exemple d'una transferència del risc és una pòlissa d'assegurança.



3. Assegurança contra ciberatacs

Els costos associats a un atac de *ransomware* poden ser molt elevats, així que **transferir** aquest risc a un tercer pot ser una bona manera de mitigar-lo. Disposar d'una **assegurança que faci front als costos d'operació i oportunitat** pot ser una bona manera de fer-ho. Val a dir que, en molts casos, l'experiència demostra que l'assegurança opta per fer el pagament del rescat, en contra de qualsevol recomanació de les forces de l'ordre i malgrat no tenir cap garantia d'èxit³¹.

³¹ <https://gizmodo.com/ransomware-attackers-and-insurance-companies-are-formin-1837665669>



Fets rellevants

- ▶ El 2019 va començar amb els **comtats d'Akron i Summit** (EUA) víctimes d'un atac a partir d'una infecció per *phishing* i un desplegament manual de *ransomware*. El ràpid aïllament dels equips infectats i la intensa feina de recuperació, amb jornades de 20 hores diàries, van evitar **cap pèrdua de dades** i permetre el retorn al **correcte funcionament en menys de 10 dies**³².
- ▶ Encara al primer trimestre, el **comtat de Jackson** (EUA) va ser víctima d'un atac de *ransomware*. El sistema de correu electrònic del govern del comtat va resultar afectat i alguns departaments, inclosos els cossos de seguretat, van haver de **recórrer al paper per continuar la seva activitat**. El comtat va **pagar 400.000 dòlars** per obtenir la clau de desxifratge i recuperar l'accés als sistemes³³.
- ▶ També al primer trimestre, el **comtat d'Orange** (EUA) va rebre un atac de *ransomware* que va causar problemes de servei a oficines públiques clau, com ara el registre d'actes, el departament d'impostos, l'oficina del xèrif i les biblioteques, durant **diversos dies**. Destaca que fou el **tercer atac en 6 anys**³⁴.
- ▶ Just iniciat el segon trimestre es va donar a conèixer un atac de *ransomware* contra la **ciutat d'Albany**, la capital de New York (EUA). Sistemes com el correu electrònic i la programació horària del departament de policia van quedar afectats, però **en un cap de setmana es van poder restituir**. No ha transcendit si es va fer el pagament del rescat³⁵.
- ▶ El 18 d'abril de 2019 un *ransomware* va infectar 12 ordinadors i 10 servidors de la **ciutat de Maine** (EUA). Es van demanar 100.000 dòlars de rescat, però no es van pagar. Per evitar que no torni a succeir **es duu a terme formació**, tant formal com basada en atacs de *phishing* simulats, en ciberseguretat³⁶.
- ▶ A la fi del segon trimestre de 2019, la **ciutat de Baltimore** encara lluita per restaurar la normalitat de les seves operacions després que el 7 de maig de 2019 fos víctima per **segon cop en 15 mesos** d'un atac de *ransomware*. Es calcula que l'atac costarà a la ciutat uns **18 milions de dòlars**³⁷.
- ▶ La **ciutat de Riviera Beach** (EUA) va decidir **pagar un rescat de 600.000 dòlars** com a única opció per recuperar els seus arxius després de rebre les claus de desxifrat i, a més, va adoptar el compromís d'invertir un **milió de dòlars en renovar tots els seus equips**. Sembla ser que tot va començar amb un empleat obrint un correu infectat amb un *malware* que va permetre la introducció del *ransomware*³⁸.
- ▶ El 10 de juny, la **ciutat de Lake City** (EUA) va patir un atac de *ransomware* que va infectar ordinadors i telèfons, els mecanismes de pagament amb targeta de crèdit i els sistemes de correu electrònic de la ciutat. Com és habitual en aquests casos, **les tasques de l'administració van passar a fer-se amb paper i llapis** fins que la ciutat va decidir-se a **pagar un rescat de 460.000 dòlars**. Com a conseqüència, el Director de Tecnologies de la Informació fou acomiadat³⁹ i 40.
- ▶ L'11 de juny de 2019, la **ciutat d'Edcouch** (EUA) fou atacada amb un *ransomware* amb el qual es **demanava el pagament de 40.000 dòlars**. Es van inhabilitar els telèfons i els ordinadors de l'administració local, però també els sistemes del departament de subministrament d'aigua. El fet que aquest departament estigués sota investigació per un possible frau en la facturació **fa sospitar que l'atac tenia l'objectiu d'eliminar proves**⁴¹.

³² <https://www.craigslist.com/technology/three-pronged-defense-defeated-akrons-virus-attack>

³³ <https://statescoop.com/rural-jackson-county-ga-recovering-from-ransomware-attack/>

³⁴ <https://securityboulevard.com/2019/03/north-carolinas-orange-county-hit-by-third-ransomware-attack-in-six-years/>

³⁵ <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware-albany-ny-malware/>

³⁶ <https://www.msspalert.com/cybersecurity-news/augusta-maine-malware-attack/>

³⁷ <https://securityboulevard.com/2019/05/baltimore-struggles-to-rebuild-systems-after-refusing-to-pay-bitcoin-ransom/>

³⁸ <https://www.cbsnews.com/news/riviera-beach-florida-ransomware-attack-city-council-pays-600000-to-hackers-who-seized-its-computer-system/>

³⁹ <https://hotforsecurity.bitdefender.com/blog/ransomware-attack-paralyses-lake-city-email-landlines-and-credit-card-services-21329.html>

⁴⁰ <https://www.wcjb.com/content/news/City-of-Lake-City-moves-Forward-after-Cyber-Attack-511802711.html>

⁴¹ <https://hotforsecurity.bitdefender.com/blog/ransomware-attack-paralyses-lake-city-email-landlines-and-credit-card-services-21329.html>

[illegible]

Baròmetre

El segon trimestre de 2019 ha mantingut la tendència que les bases de dades de tipus MongoDB són protagonistes d'una part molt rellevant dels incidents causats per errors de configuració.

Principals fuites de dades personals

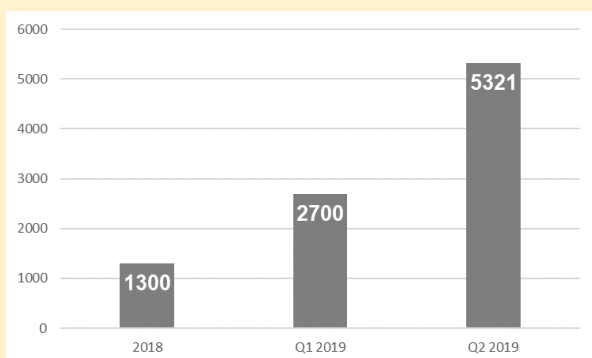
En aquest segon trimestre de l'any, les tres principals fuites de dades personals tenen en comú que deriven d'errors de configuració i que dues d'elles afecten bases de dades MongoDB. La immobiliària First American Financial ha estat l'entitat més afectada i ha protagonitzat la fuga de més de 885 milions de registres que contenen informació de préstecs hipotecaris, inversions i noms de clients.



Il·lustració 12. Fuites de dades més grans del trimestre

En segon lloc s'hi troba una exposició de dades personals que va afectar 275 milions de ciutadans indis. En tercera posició hi ha l'exposició de dades de la companyia índia de serveis de cerca local JustDial, la qual incloïa noms, correus electrònics, gènere i data de naixement.

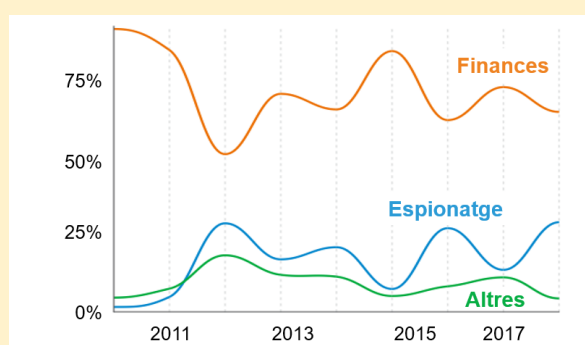
Registres exposats per mala configuració



Il·lustració 13. Evolució de les fuites de dades (en milions de registres)

Aquest segon trimestre de 2019 ha continuat la tendència a l'alça de fuites d'informació causades per una mala configuració. Si en el primer trimestre el nombre de registres exposats per mala configuració es va doblar, aquest trimestre ho ha tornat a fer i s'ha arribat als 5.321 milions de registres de dades personals.

La motivació financera de les fuites



Il·lustració 14. Motivacions del robatori de dades⁴²

Segons l'informe de Verizon sobre les filtracions de dades, la motivació econòmica està al darrere de prop del 75% de les filtracions de dades (tenint en compte que un error no tindria motivació). L'espionatge manté una tendència a l'alça.

Atacs a la cadena de subministrament

Continua el creixement dels atacs a través de proveïdors o, el que és el mateix, a través de la cadena de subministrament. Aquests tipus d'atacs van créixer un 78% el 2018 amb un cost mitjà de 7,5 milions de dòlars⁴³. En aquest àmbit, els grups de hackers més actius són anomenats Magecart i una de les seves víctimes més famoses d'aquest trimestre ha estat el grup de comunicació Forbes.



Il·lustració 15. Xifres dels atacs a la cadena de subministrament el 2018⁴⁴

⁴² <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

⁴³ <https://www.cybergx.com/ponemon-third-party-cyber-risk-management-report>

⁴⁴ <https://www.symantec.com/blogs/expert-perspectives/istr-2019-cyber-criminals-ramp-attacks-trusted-software-and-supply-chains>

Fuites de dades

Un registre és un conjunt de camps que contenen informació relativa a una persona o entitat.

Error de configuració

Des de 2018 s'ha evidenciat una tendència a l'alça en el nombre de registres de dades personals que queden exposats per **errors de configuració**. El **primer trimestre** de 2019 va marcar una autèntica fita al doblar el nombre de registres exposats en tot el 2018 i arribar als més de **2700 milions**, però aquest **segon trimestre** ha sobrepassat aquesta xifra i s'ha arribat als **5321 milions de registres** (veure il·lustració 13).

Al primer trimestre ja es va detectar un increment dels incidents causats per la **configuració incorrecta de sistemes amb bases de dades MongoDB**. Aquesta tendència es manté i les bases de dades MongoDB han estat protagonistes dels principals incidents del trimestre (veure il·lustració 12).

Les bases de dades MongoDB han estat protagonistes dels principals incidents del trimestre

També s'identifiquen nombrosos i importants incidents de seguretat vinculats a les **bases de dades Elasticsearch**. Destaquen casos com una base de dades sense autor que contenia dades personals de ciutadans nord-americans obtingudes a partir d'enquestes, o l'empresa de telefonia canadense Freedom Mobile, amb dades personals i de facturació dels seus clients.



Il·lustració 16. Alguns incidents importants amb bases de dades ElasticSearch

Tanmateix, no es pot oblidar com continuen els casos de **servidors d'Amazon S3** que segueixen oberts per error. Destaquen els casos de la base dades d'una empresa de màrqueting de la Índia que contenia 49 milions de registres, obtinguts a partir de 350.000 *influencers* d'Instagram, i d'una base de dades de l'empresa de selecció de personal Ladders, la qual disposava del currículum vitae de més de 13 milions de persones, entre d'altres dades.



Il·lustració 17. Alguns incidents importants a servidors Amazon S3

*El xifratge de dades **extrem a extrem** és un sistema de comunicació on només els usuaris que es comuniquen poden llegir els missatges. En principi, impedeix que tercers (inclosos els proveïdors de telecomunicacions, els proveïdors d'Internet i fins i tot el proveïdor del servei de comunicació) puguin accedir a les claus criptogràfiques necessàries per desxifrar la informació.*

Accions correctives

Cal recordar que durant el 2018 les exposicions de dades relacionades amb sistemes **Amazon S3** eren **protagonistes de la majoria d'incidents**. Avui, la situació ha canviat radicalment i els incidents d'Amazon S3 ja no ocupen els principals titulars. El motiu d'aquest canvi és la posada en pràctica de **mesures de seguretat addicionals que alerten als usuaris de les configuracions errònies**⁴⁵, aspecte que evidencia l'eficàcia d'implementar mesures de seguretat preventiva.

En efecte, els següents a moure fitxa són els responsables de les bases de dades MongoDB i així ho han fet: **la nova versió de MongoDB ja inclou el xifratge de dades **extrem a extrem****⁴⁶. Així, a mitjà-llarg termini, cal esperar conseqüències positives atès que, d'ara endavant, **les dades que es puguin arribar a filtrar des d'una base de dades MongoDB estaran xifrades**.

D'altra banda, cal destacar que importants fuites d'informació tenen lloc en països on les lleis de protecció per a les dades personals són més laxes, com ara els EUA (veure apartat Fets rellevants). Aquest tipus de legislacions faciliten la **proliferació de bases de dades que recopilen informacions personals de ciutadans de manera no consentida i, sovint, no en consta ni el seu administrador o autor**. Tot indica que aquestes situacions seguiran repetint-se fins que s'estenguin i es consolidin regulacions similars a l'RGPD de la UE.

Importants fuites d'informació tenen lloc en països on les lleis de protecció per a les dades personals són més laxes.

Magecart i els atacs a la cadena de subministrament

Aquest ha estat el trimestre de ressorgiment de Magecart, uns grups de *hackers* que ataquen proveïdors de serveis que ofereixen una plataforma de pagament a organitzacions o empreses⁴⁷. L'objectiu final és obtenir **dades i números de targetes de crèdit dels compradors**.

Magecart ja va ser responsable d'alguns dels atacs més importants dels últims anys, com els que van patir **British Airways** i **TicketMaster**. Durant 15 dies, del 21 d'agost al 5 de setembre de 2018, les dades dels **380 000 clients** de British Airways, els quals havien realitzat pagaments a través de la pàgina web i l'aplicació mòbil de la companyia, van ser robades⁴⁸. El juny de 2018, TicketMaster també en va ser víctima, com a conseqüència del fet que Magecart va afectar a Inbenta, un dels seus proveïdors, i es van filtrar les dades de **40.000 clients**. TicketMaster es troba davant d'una reclamació per danys i perjudicis de **6,5 milions de dòlars**⁴⁹.

⁴⁵ <https://www.helpnetsecurity.com/2018/11/19/prevent-amazon-s3-bucket-misconfiguration/>

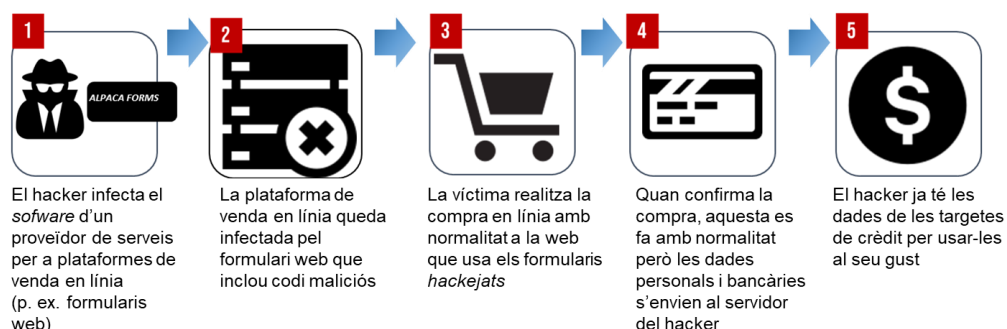
⁴⁶ <https://undercode.org/foro/noticias-informaticas-120/mongodb-4-2-presenta-el-cifrado-de-nivel-de-campo-de-extremo-a-extremo/>

⁴⁷ <https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf>

⁴⁸ <https://www.riskiq.com/blog/labs/magecart-british-airways-breach/>

⁴⁹ <https://www.iq-mag.net/2019/04/ticketmaster-lawsuit-uk-data-breach/>

Durant aquests últims mesos els *hackers* de Magecart han aconseguit afectar més de **17.000 dominis**⁵⁰. Entre les víctimes hi figuren proveïdors de serveis web com **Alpaca Forms**, **Picreel** i destaquen els casos de **Forbes** i **201 universitats** dels EUA i el Canadà a partir de l'atac a la plataforma **PrismWeb** utilitzada per dissenyar botigues universitàries⁵¹. El mes de maig també es va descobrir que **100 plataformes** de comerç electrònic havien estat infectades durant **més de 6 mesos**⁵².



Il·lustració 18. Mètode d'atac a la cadena de subministrament

Els atacs a la cadena de subministrament com els de Magecart són **difícilment detectables**, atès que els clients **deleguen completament la seguretat al proveïdor i no estan dotats de mitjans per supervisar-la**. A més de passar desapercebuts, els *hackers* poden obtenir un botí important: milers de dades personals i targetes de crèdit fresques.



⁵⁰ <https://www.wired.com/story/magecart-amazon-cloud-hacks/>

⁵¹ <https://www.databreaches.net/hackers-steal-card-data-from-201-online-campus-stores-from-canada-and-the-us/>

⁵² <https://www.bankinfosecurity.com/new-skimmer-attack-stealing-data-from-over-100-retail-sites-a-12465>

Fets rellevants

- ▶ El gegant immobiliari **First American** (EUA) va exposar **885 milions de registres**, amb dades financeres privades de clients acumulades des del 2003 al seu lloc web, de manera que qualsevol hi podia accedir⁵³.
- ▶ A la Índia es va descobrir una base de dades **MongoDB** amb **275 milions de registres** de ciutadans que contenia el nom, el gènere, la data de naixement, el correu electrònic, el número de telèfon mòbil, els detalls de l'educació, la informació professional (patró, historial laboral, habilitats, àrea funcional) i el salari actual. La base de dades **no tenia autor conegut** i va estar **sense protecció a Internet** durant més de dues setmanes⁵⁴.
- ▶ **3,5 milions de registres** que contien **dades personals i mèdiques** de ciutadans del **Panamà** van quedar **exposades** a Internet a causa d'un **error de configuració**. És rellevant que la població del Panamà és de 4 milions d'habitants⁵⁵.
- ▶ Una base de dades pertanyent a **JustDial**, el servei de cerca local més gran de la Índia, mostrava informació de **100 milions d'usuaris**. Tot i que la companyia nega aquest extrem, confirma l'existència de **vulnerabilitats a la seva web i aplicació per a mòbils**⁵⁶.
- ▶ Una base de dades de **24 GB** amb **informació diversa sobre 80 milions de llars dels EUA**, com el número de persones, noms, cognoms i estat civil dels seus membres, entre d'altres, va quedar exposada. La filtració afectava aproximadament el **65% del total de llars del país**⁵⁷.
- ▶ Els administradors d'una operació d'*spam* via SMS van deixar una instància **MongoDB** oberta amb la qual cosa es van exposar més de **80 milions de registres**⁵⁸.
- ▶ La botiga en línia japonesa **Uniqlo** va anunciar que les dades de **460.000 clients** van estar accessibles per a *hackers* des del 23 d'abril fins al 10 de maig. La companyia assegura que no hi ha possibilitat de filtració dels codis de seguretat de les targetes de crèdit. No obstant això s'ha produït una **allau de trucades al servei d'atenció al client** de la companyia, amb el conseqüent malbaratament de recursos⁵⁹.
- ▶ La web de l'**Alhambra** de Granada va ser víctima d'un "atac informàtic professional i organitzat d'origen desconegut" i en el qual es van robar les dades de més de **4,5 milions de clients i agències** que operaven a través d'ella⁶⁰.
- ▶ Un expert en ciberseguretat va detectar **8,4 TB de metadades de correus electrònics** publicades per **error** en una base de dades **Elasticsearch** de la **Shang Jiao Tong University de Shanghai**, una de les més prestigioses del país⁶¹.

⁵³ <https://www.zonamovilidad.es/885-millones-de-registros-de-first-american-financial-corporation-expuestos-en-linea.html>

⁵⁴ <https://www.bleepingcomputer.com/news/security/over-275-million-records-exposed-by-unsecured-mongodb-database/>

⁵⁵ <https://securitydiscovery.com/panama-citizens-massive-data-breach/>

⁵⁶ <https://www.2-spyware.com/justdial-data-breach-personal-details-of-100-million-users-leaked>

⁵⁷ <https://www.databreaches.net/report-unknown-data-breach-exposes-80-million-us-households/>

⁵⁸ <https://www.infosecurity-magazine.com:443/news/sms-spammers-expose-80m-records/>

⁵⁹ <https://www.cnn.com/2019/05/14/japans-uniqlo-says-hackers-access-data-from-460000-online-accounts.html>

⁶⁰ https://elpais.com/cultura/2019/05/22/actualidad/1558543799_516409.html

⁶¹ http://europe.chinadaily.com.cn/china/2013-06/20/content_16640860.htm



Business Email Compromise (BEC)

Baròmetre

L'enginyeria social és l'acció d'obtenir accés a actius o sistemes d'informació a través de l'explotació de la psicologia humana, enlloc d'utilitzar tècniques informàtiques. Es basa en aprofitar el fet que les persones volen ajudar, el primer moviment respecte a l'altre és de confiança, s'evita dir "no" i a tothom li agrada ser lloiat.

Top 5 atacs d'enginyeria social

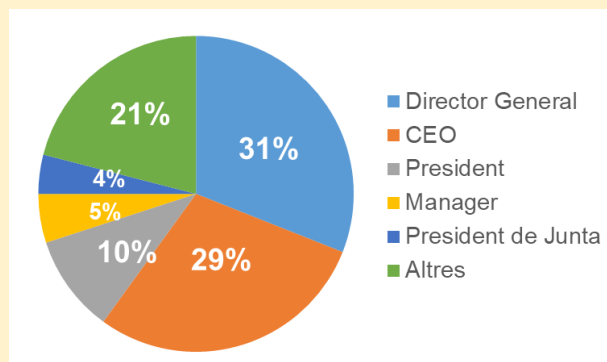
Segons dades dels EUA, l'atac d'enginyeria social que permet obtenir més diners és el BEC (*Business Email Compromise*). Pel que fa al nombre de víctimes afectades, es troba en segona posició, just darrere del frau vinculat al pagament i enviament de béns.

1	2	3	4	5
BEC	FRAU ROMÀNTIC	INVERSIONS	PAGAMENTS-ENVIAMENT	RENDA-ESTAT
\$1.300M	\$362M	\$253M	\$183M	\$150M
20.373	18.493	3.693	65.116	11.300
VÍCTIMES	VÍCTIMES	VÍCTIMES	VÍCTIMES	VÍCTIMES

Il·lustració 19. Principals atacs d'enginyeria social per import⁶²

Suplantació en el BEC

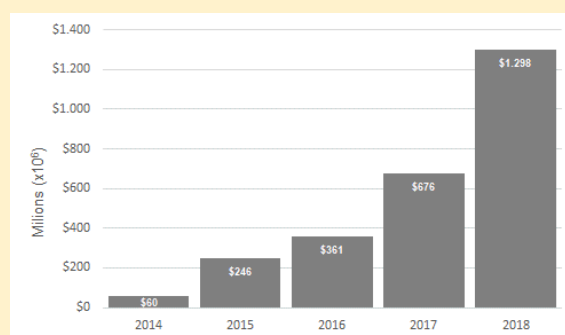
En els atacs de BEC, qualsevol membre del personal de l'empresa pot ser suplantat, tot depenent de la finalitat que tingui l'atacant: un comercial, una secretària, l'encarregat de comptabilitat, el cap del departament de compres, etc. Ningú està fora de perill. Ara bé, els principals candidats a ser suplantats són els càrrecs executius amb autoritat sobre l'operativa econòmica.



Il·lustració 20. Perfils suplantats en un atac de BEC⁶³

Quantitat de diners robats

El BEC manté una tendència creixent els últims anys. Tant sols als EUA, l'FBI ha detectat com la quantitat econòmica defraudada s'ha multiplicat més de 21 vegades en 4 anys, i ha arribat a gairebé als 1300 milions de dòlars el 2018⁶⁴.



Il·lustració 21. Quantitats defraudades per BEC als EUA

"Assumpte" en el BEC

Els atacs de BEC solen començar amb un correu electrònic amb un assumpte que crida l'atenció de la víctima. Symantec⁶⁵ ha identificat, per país, el contingut que figura en l'assumpte de les principals campanyes de BEC.

PAIS	ASSUMPTE	QUANTITAT
REGNE UNIT	IMPORTANT	\$ 20.234
EUA	IMPORTANT	\$ 11.930
AUSTRÀLIA	PAYMENT	\$ 4.292
JAPÓ	YOUR RECEIPT FROM APPLE	\$ 3.513
BÈLGICA	RE: U HEEFT RECHT OP EEN LAGERE ENERGIEREKENING IN 2018 ! (YOU ARE ENTITLED TO A LOWER ENERGY BILL IN 2018 !)	\$ 3.308
SINGAPUR	CONFIDENTIAL	\$ 2.520
ESPANYA	NOTIFICATION OF PAYMENT RECEIVED	\$ 1.765
CANADÀ	URGENT	\$ 1.758
FRANÇA	PAYMENT DUE 8 DEC	\$ 924
ALEMANYA	PAYMENT	\$ 921

Il·lustració 22. Assumpes de les campanyes de BEC per país

⁶² https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

⁶³ <https://www.trendmicro.com>

⁶⁴ https://pdf.ic3.gov/2018_IC3Report.pdf

⁶⁵ <https://www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019>

Business Email Compromise (BEC)

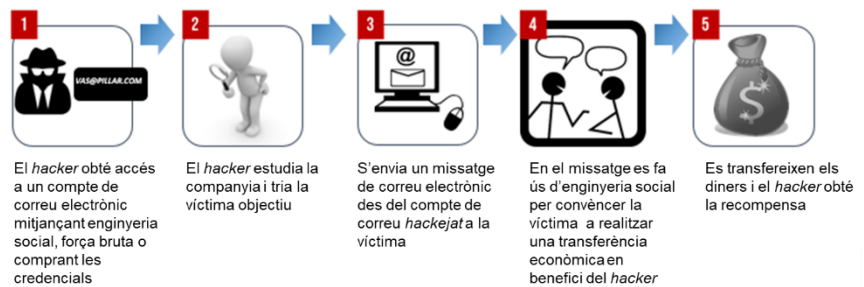
El **Business Email Compromise** (BEC) és un atac d'enginyeria social en què se suplanta el correu electrònic d'una persona, normalment amb poder de decisió dins d'una organització, per enviar missatges a un empleat, habitualment del departament de finances, instant-lo a transferir una gran quantitat de diners al compte de l'atacant sota una excusa com: el canvi de banc d'un proveïdor, una factura urgent, etc.

La **dark web** és la xarxa accessible mitjançant un programari específic i que, per les seves característiques d'anonimat i difícil traçabilitat, allotja multitud de mercats il·legals o continguts inadequats. Sovint el terme deep web s'utilitza com a sinònim, però, en realitat, es refereix a la part de la xarxa no visible per cercadors d'Internet (no indexada). La dark web és un subconjunt de la deep web.

Què és el BEC?

El **Business Email Compromise** (BEC) és una pràctica cada cop més estesa, sofisticada i que aporta més grans beneficis als ciberatacants. Només als **EUA, durant el 2018, la quantitat de diners defraudats es va doblar i va arribar pràcticament als 1300 milions de dòlars** (veure il·lustració 19). Així, l'**FBI destaca el BEC com el frau cibercriminal que ha aconseguit robar més diners durant el 2018**⁶⁶. Enguany, tot indica que la tendència continua.

L'FBI destaca el BEC com l'activitat cibercriminal que ha aconseguit robar més diners durant el 2018.



Il·lustració 23. Passos d'un atac de Business Email Compromise.

Per elaborar aquest atac es requereix obtenir el **control de la bústia de correu** de la persona a suplantar i un **profund coneixement de l'organització a atacar**: la seva operativa, la forma d'escriure correus electrònics, l'agenda i relacions professionals, etc.

Cal recordar que a la **dark web** es poden trobar **milions de credencials a la venda** que poden ser utilitzades per accedir al compte de correu electrònic de les víctimes potencials.

Tipus principals de BEC

Destaquen **dos tipus d'atac BEC** que són coneguts com el frau del proveïdor i el frau del CEO, **en funció de qui se suplanti** (aquest últim és el més emprat).

En el **frau del proveïdor**, l'atacant compromet el compte de correu electrònic d'un proveïdor de l'empresa objectiu i l'utilitza per informar que disposen d'un **nou número de compte bancari on hauran de dirigir els futurs pagaments**. El nou compte, òbviament, és propietat del hacker. Amb aquesta tècnica **Facebook** i **Google** van ser estafats amb més de **100 milions de dòlars**, tot i que en van poder recuperar una bona part (veure Fets rellevants).

⁶⁶ https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf



El **frau del CEO** consisteix en suplantar una persona de poder dins l'empresa objectiu i **es demana a un treballador amb funcions financeres que realitzi una transferència o pagament**, amb urgència i mitjançant qualsevol excusa convincent, a benefici del *hacker*.

Val a dir, però, que darrerament es donen casos d'una **nova varietat**. Aquesta consisteix en **suplantar un treballador** per, des del seu compte de correu compromès, sol·licitar al departament de recursos humans un **canvi en el número de compte on transferir la nòmina**.

Mesures de protecció

Esdevenir víctima del **BEC es pot evitar** seguint tres regles bàsiques:

1. Establir un **protocol de compres** a la companyia que els directius s'han de comprometre a seguir. Com a mínim, aquell qui rebí l'ordre de transferència hauria de validar-la amb el responsable que l'hagi ordenada per un mitjà alternatiu al correu electrònic, per exemple telèfon. Els directius ho haurien de respectar, en cas contrari un protocol es converteix en un suggeriment.
2. Fer ús de la **dobla autenticació** per connectar-se al banc i requerir **dobla signatura** per a poder fer una transferència. L'ús d'aquestes mesures combinades obliga el ciberdelinqüent a comprometre les credencials de dos usuaris i els seus telèfons mòbils, amb la qual cosa les possibilitats es redueixen dràsticament.
3. Establir una **operativa determinada amb la plataforma online del banc** segons els rols que estableixi clarament qui pot fer què, els quals només podran ser modificats pel CEO (Chief Executive Officer) o el CFO (Chief Financial Officer). Addicionalment, es podria arribar a limitar que la connexió amb la plataforma bancària només s'admeti des de determinades IP o ordinadors de la xarxa corporativa.

Altres atacs d'enginyeria social del Top 5

El BEC és l'atac d'enginyeria social que aconsegueix defraudar més diners i el segon en nombre d'afectats (veure il·lustració 19), però n'hi ha d'altres que cal destacar.



— Frau romàntic

El frau de confiança o frau romàntic és aquell en què **el criminal fa creure a la víctima que tenen una relació de confiança, sigui familiar, amistosa o romàntica**. Així, es persuadeix a la víctima per enviar **diners, informació personal i financerà o articles de valor al criminal**. No és pas un frau menor: només als EUA les víctimes d'aquest frau van perdre un total de 362 milions de dòlars l'any passat



— Fraus de pagament-enviament

Aquest frau es dona en situacions en les quals **la víctima realitza un pagament però mai rebrà cap bé o servei a canvi**. Darrerament destaca aquest frau sobre la plataforma Airbnb⁶⁷, però es pot donar en qualsevol plataforma de comerç electrònic o intercanvi de béns.



— Fraus d'inversions

En aquest tipus de frau **l'atacant s'aprofita tant la cobdícia de la víctima com el seu desconeixement dels mercats financers**. Molts usuaris que no entenen del tot el funcionament de les criptomonedes tenen l'afany d'obtenir beneficis ràpids, la qual cosa els fa perseguir falses promeses i a prendre decisions poc recomanables.



— Fraus de renda-Estat

L'atacant intenta suplantar una entitat recaptatòria per sol·licitar un pagament a la víctima. Els atacs se solen produir en època de pagament d'impostos i solen començar amb un correu brossa que intenta informar la víctima de la necessitat de realitzar un pagament pendent i que acaba amb la transferència econòmica de la víctima al compte dels criminals.



⁶⁷ <https://eu.usatoday.com/story/money/2019/05/19/airbnb-scam-hits-some-users-charges-them-fake-reservations/3732422002/>



Fets rellevants

- ▶ Al primer trimestre de l'any va destacar el cas d'un grup de *hackers* xinès que va robar **18,6 milions de dòlars** del braç indi de **Tecnimont SpA**, una empresa d'enginyeria italiana. L'estafa no només es va perpetrar per **BEC**, també es va suplantar el director general del grup italià, un advocat i altres alts directius en **reunions telefòniques**. L'objectiu era discutir una **adquisició "confidencial" a la Xina i convèncer el CEO indi perquè fos ell qui transferís els diners** ja que no es podia fer des d'Itàlia per problemes legals⁶⁸.
- ▶ També al primer trimestre de l'any, es va conèixer el cas d'una **dona de 61 anys** de Calgary (Canadà) que va ser víctima de **frau romàntic**. En una pàgina web de cites va conèixer un **home que suposadament treballava en una plataforma petrolífera a Kuwait**. Amb l'excusa que estava passant dificultats per rebre el seu sou, la dona li va començar a enviar diners. La relació va durar 22 mesos i la víctima **va acabar enviant-li 960.000 dòlars**⁶⁹.
- ▶ Un ciutadà de Lituània es va declarar culpable de frau de **BEC** després de ser acusat d'estafar més de **100 milions de dòlars** a companyies com **Facebook i Google**. Va falsificar una sèrie de documents legals, com ara **factures i contractes**, per obtenir pagaments d'aquests gegants tecnològics⁷⁰.
- ▶ Les **escoles del comtat de Scott** (EUA) van ser víctimes d'un important frau de **BEC** en el qual els atacants van suplantar un correu electrònic i falsificar factures. Va resultar en un frau de **3,7 milions de dòlars** que es podrien recuperar a través d'una l'assegurança contractada⁷¹.
- ▶ La parròquia **Saint Ambroise d'Ohio** (EUA) va ser víctima d'un **atac de BEC** en el qual van perdre **1,7 milions de dòlars**. La investigació de l'FBI va determinar que els atacants van fer-se passar per la constructora que estava reconstruint la parròquia per **informar d'un canvi en el compte bancari**⁷².

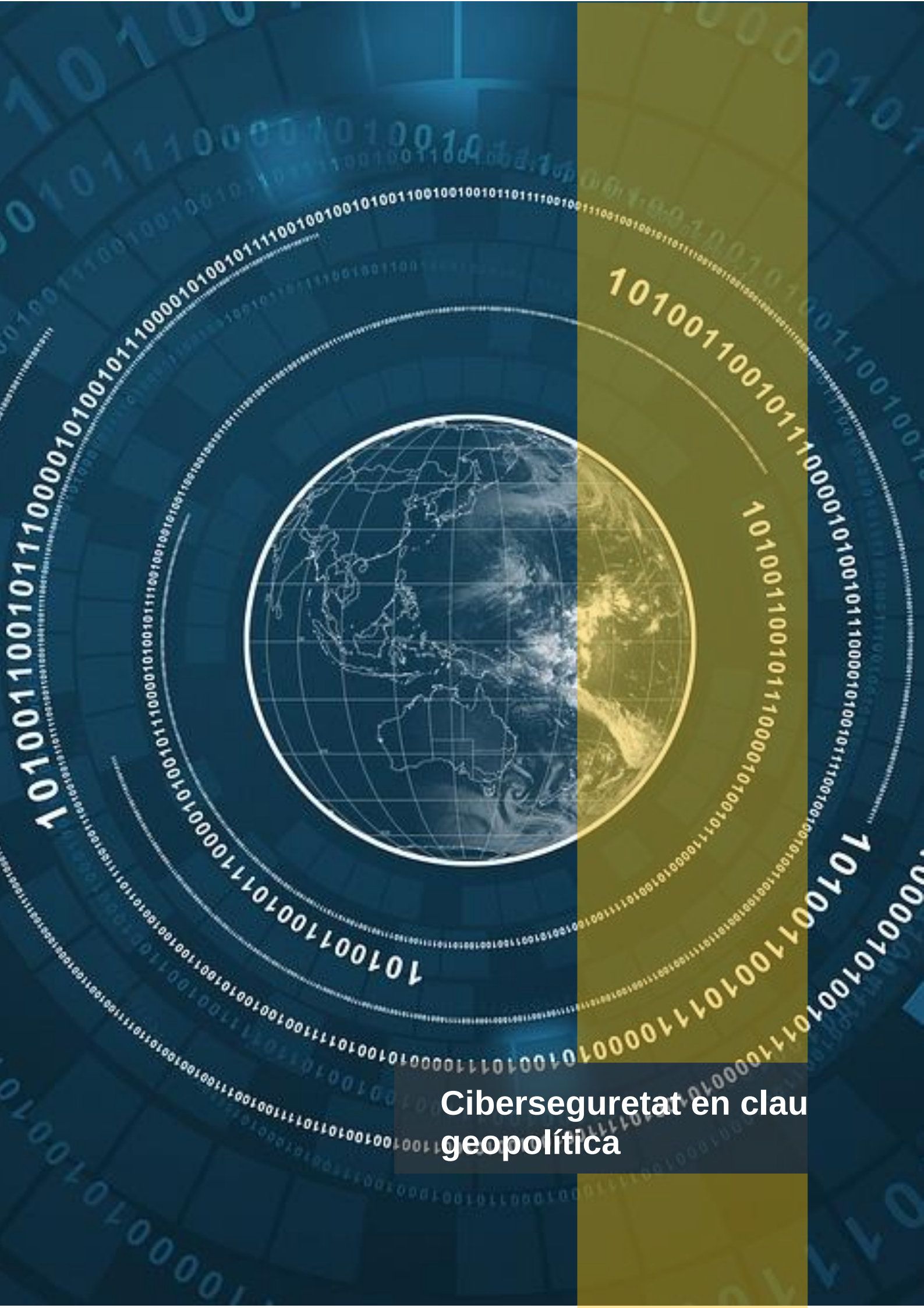
⁶⁸ <https://www.bankinfosecurity.com/bec-scam-leads-to-theft-186-million-fraud-a-11930>

⁶⁹ <https://globalnews.ca/news/5095659/romance-scam-money/>

⁷⁰ <https://www.secureworldexpo.com/industry-news/google-facebook-bec-business-email-compromise>

⁷¹ <https://www.wkyt.com/content/news/Scott-County-Schools-victim-of-37-million-scam-509017341.html>

⁷² <https://www.secureworldexpo.com/industry-news/business-email-compromise-example-2019>



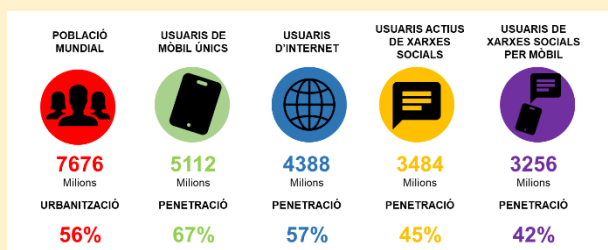
**Ciberseguretat en clau
geopolítica**

Baròmetre

Les característiques de les xarxes 5G ofereixen l'oportunitat de desenvolupar noves tecnologies i serveis encara impensables, però també és cert que el major grau d'interconnexió incrementarà el risc cibernètic. Tant el potencial com els riscos inherents al 5G han motivat que els estats considerin aquesta nova tecnologia un assumpte estratègic i hagin començat a prendre mesures per controlar-la.

Xifres d'un món digitalitzat i mòbil

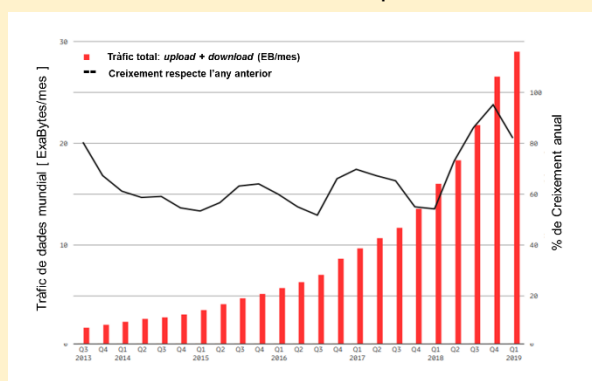
L'informe anual de *We Are Social* sobre l'evolució d'Internet apunta a un creixement de mil milions d'usuaris nous cada any.



Il·lustració 24. Dades de penetració d'Internet i la telefonia mòbil al món a data gener de 2019⁷³

El tràfic de dades mòbils creix

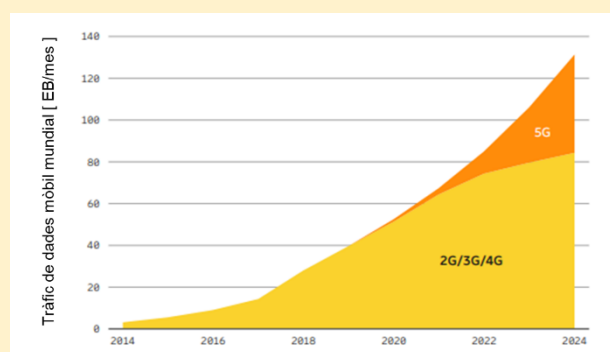
Cada cop s'utilitzen més dades a través de les tecnologies mòbils. Tan sols aquest últim any l'increment ha estat del 82% respecte del 2018.



Il·lustració 25. Tràfic mundial de dades des de dispositius mòbils⁷⁴

El tràfic 5G creix

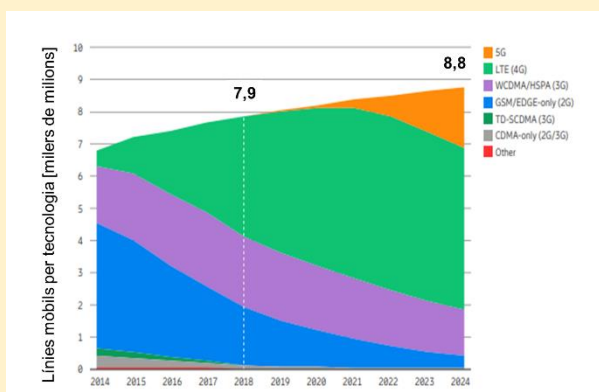
A partir del 2020 l'ús de la tecnologia 5G per a la transmissió de dades creixerà de forma exponencial i el 2024 arribarà al 35% del total. Les altres tecnologies mòbils, 2G/3G/4G, tendiran a poc a poc a l'estancament.



Il·lustració 26. Estimació del tràfic des de dispositius mòbils per tecnologia⁷⁵

El número de línies mòbils creix

S'estima que el 5G creixerà gradualment i assolirà el 20% del mercat mundial de línies de telèfon mòbil el 2024. El 2021 serà un punt d'inflexió per al 4G, el qual progressivament començarà a perdre quota de mercat.



Il·lustració 27. Estimació de la quota de mercat de les línies mòbils per tecnologia⁷⁶

⁷³ <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>

⁷⁴ <https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf>

⁷⁵ <https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf>

⁷⁶ <https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf>

Ciberseguretat en clau geopolítica

La **latència** és el temps que passa entre que s'envia una petició i es comença a rebre la resposta.

EUA: conflicte pel 5G

Des dels anys 90 l'economia de la Xina no ha parat de créixer fins a convertir-se en la potència mundial que és avui dia, superant ja en PIB tant els EUA com la UE. La Xina ja competeix en igualtat de condicions contra totes dues i totes tres tenen capacitat i voluntat de posicionar-se en tot allò que consideren estratègic, com la tecnologia 5G.

La tecnologia **5G** representarà una revolució en el model de comunicació actual: **velocitats de transmissió de dades molt superiors, comunicacions més fiables, una latència mínima i un augment del nombre màxim de dispositius connectables**. Així, nous serveis com la cirurgia remota, els vehicles autònoms o les ciutats intel·ligents podran ser realitat. Tot això suposarà un **volum d'informació molt superior i més crítica a l'actual circulant a través de les xarxes 5G** i, per tant, un **increment del risc en matèria de ciberseguretat**. Per aquest motiu, els Estats consideren estratègic que la xarxa 5G estigui sota el seu control, escenari que s'evidencia en el conflicte entre els EUA i Huawei.

Els Estats consideren estratègic que la xarxa 5G estigui sota el seu control, escenari que s'evidencia en el conflicte entre els EUA, la Xina i Huawei.



Cal remuntar-se al 2012, amb l'inici de la investigació de la tecnologia 5G, per constatar com els EUA van començar a imposar aranzels i prohibicions per evitar la penetració de la tecnologia xinesa rere acusacions d'espionatge. Però **el conflicte ha esclatat aquest 2019 a causa de la importància que estava adquirint Huawei en el desplegament de les xarxes 5G i les seves estretes relacions amb el govern de la Xina** (veure il·lustració 28).

Així, el mes de maig passat, **els EUA van incloure Huawei a l'entity list**⁷⁷, fet que prohibeix que pugui realitzar negocis amb empreses nord-americanes. No obstant això, el 29 de juny de 2019, els EUA van aixecar provisionalment el veto a Huawei per un període de 3 mesos, però mantenint-la dins la llista d'empreses perilloses⁷⁸. En cas que el veto esdevingui definitiu, les conseqüències immediates poden ser molt importants i immediates com, per exemple, **milions de terminals Huawei que podrien perdre les actualitzacions de seguretat d'Android i esdevenir dispositius vulnerables**.

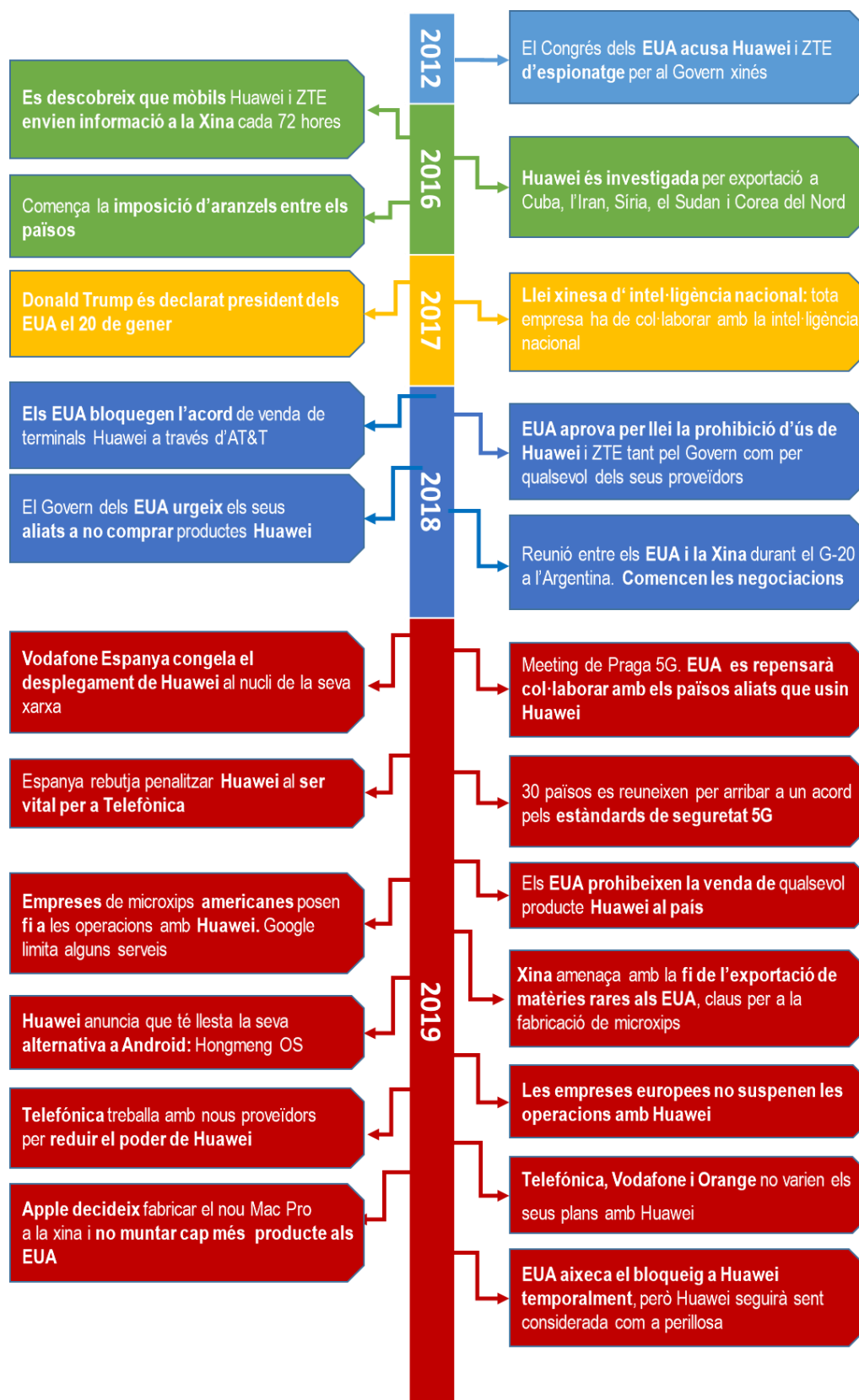
A la UE, països i operadors de telecomunicacions estan a l'expectativa del que succeeixi als EUA. Un estudi afirma que **el 5G europeu costaria 62.000 milions de dòlars més si es prescindeix de Huawei**⁷⁹. En canvi, a Rússia, la necessitat de tenir accés a la tecnologia 5G i la bona relació amb la Xina ha facilitat a un **acord entre ambdós països perquè Huawei implantí el 5G a Rússia**⁸⁰.

⁷⁷ <https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>

⁷⁸ <https://www.expansion.com/empresas/tecnologia/2019/05/21/5ce3799e22601d75648b4573.html>

⁷⁹ <https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-telcos-idUSKCN1T80Y3>

⁸⁰ <https://www.xataka.com/empresas-y-economia/huawei-sera-encargada-implementar-red-5g-rusia-nuevo-acuerdo-china-gobierno-putin>



Il·lustració 28. Histograma del conflicte EUA i Huawei pel 5G



Les **notícies falses**, fake news o desinformació són històries falses que semblen notícies, difoses a través de xarxes socials, portals de notícies o altres mitjans, creades amb l'objectiu d'enganyar o induir a un estat de desinformació deliberada a la ciutadania. La motivació pot ser econòmica, ja que la seva publicació esdevé un reclam de clics per als visitants d'una web. És més greu quan la motivació és obtenir un rendiment polític o un posicionament estratègic privilegiat, a través de la inducció a errors, la manipulació de decisions personals, el desprestigi o l'enaltiment de persones o entitats.

Un servidor de Domini de Noms o **DNS** (Domain Name System) permet l'accés a Internet perquè disposa d'una base de dades en què hi ha enregistrats els noms de domini, més fàcils d'utilitzar i recordar (p. ex. "exemple.com") vinculats amb les adreces IP dels seus servidors web (p. ex. "10.20.30.40"), les quals possibiliten dirigir les comunicacions a la xarxa. L'usuari li envia al DNS una consulta amb l'adreça web a la qual es vol dirigir i el DNS li retorna la IP del servidor corresponent.

Rússia: una Internet pròpia

Els interessos geopolítics de les potències econòmiques del món darrerament es concentren en el 5G, però **el control d'Internet** ha estat una prioritat des de fa temps. La Xina va ser pionera amb la supervisió de la Xarxa a través del Great Firewall, una combinació de lleis i tecnologies, des de l'entrada d'Internet al país. Les principals mesures aplicades són: el bloqueig de l'accés a determinats serveis web estrangers (Google, Facebook, Twitter, Wikipedia,...), el monitoratge tant del correu electrònic com de pàgines web nacionals a la recerca de llenguatge polític o continguts que fomentin la protesta, i el compliment d'una estricta normativa per a totes les companyies que es vulguin establir a la Xina⁸¹.

Recentment, però, **Rússia** ha esdevingut protagonista amb la seva pròpia iniciativa. L'1 de maig d'aquest 2019 el president del govern rus Vladimir Putin va aprovar una llei per a la creació d'una Internet local "sostenible, segura i completament funcional"

El president del govern rus Vladimir Putin va aprovar una llei per a la creació d'una Internet local "sostenible, segura i completament funcional" anomenada Runet.

anomenada **Runet**⁸² que **durant els estats d'emergència, el govern podrà desconnectar de la resta del món.**

Aquesta acció donarà a Rússia un mecanisme per ser **més efectiva davant de ciberatacs externs** i proporcionarà al govern un **control sobre Internet més gran**, però també suposarà una **limitació en l'accés dels ciutadans a informació no supervisada**. De fet, **aturar tant el contingut il·legal com la proliferació de notícies falses** va ser una de les raons esgrimides pel govern rus per a la creació de Runet.

Ara bé, el projecte té un abast colossal i suposa un autèntic repte. En primer lloc, **requereix la creació d'un sistema nacional de servidors de domini de noms (DNS)** per a la redirecció de les comunicacions com a suport del sistema global de noms de domini existent. La construcció d'aquest sistema de DNS rus serà gradual i es pretén que, **pel 2020, el trànsit de dades a través de servidors estrangers sigui únicament del 5%** i que el sistema estigui **100% funcional al 2021**⁸³.

Que Runet esdevingui realitat genera certs dubtes. La dependència de la xarxa russa de sistemes i tecnologia estrangers esdevindrà un factor clau, juntament amb el grau d'acceptació de la ciutadania russa de les mesures restrictives. És destacable com Rússia disposava d'una Internet

Rússia disposava d'una Internet 100% lliure fins que, a partir de 2012, s'ha anat transformant en un sistema cada cop més tancat i controlat.

100% lliure fins que, a partir de 2012, s'ha anat transformant en un sistema cada cop més tancat i controlat, a diferència dels xinesos que només han conegut la Internet filtrada que deixa passar el Great Firewall.

⁸¹ https://en.wikipedia.org/wiki/Great_Firewall

⁸² <https://futurism.com/russia-cut-off-internet-bill-law>

⁸³ <https://time.com/5578737/the-quick-read-about-russias-new-internet-law/>

Iran: una Internet pròpia i una intensa activitat fora

Iran és un altre país amb una intensa activitat al voltant d'Internet. També **s'hi pretén crear una Internet completament isolada de la resta del món i controlada pel govern**. La necessitat d'aquesta xarxa és cada cop més urgent pel govern iranià, ja que es calcula que més de **40 milions d'iranians tenen *smartphone* i usen aplicacions xifrades per comunicar-se**. Telegram és l'aplicació de missatgeria més usada a l'Iran⁸⁴.

Així, a principi del mes de juny, el govern iranià va anunciar que la seva **xarxa d'informació nacional (NIN)** està completa al 80%⁸⁵. A dia d'avui, Iran ja disposa de mecanismes de control i censura a Internet. Des de 2006, fa ús del **filtre de continguts SmartFilter⁸⁶**, el qual permet bloquejar pàgines com Facebook, Youtube, Twitter o la BBC.

A principi del mes de juny, el govern iranià va anunciar que la seva xarxa d'informació nacional (NIN) està completa al 80%.

A més, Iran ha estat notícia per ser l'**origen d'importantes campanyes de desinformació a través de comptes falsos que suplanten representants i polítics nord-americans amb l'objectiu d'influir en l'opinió pública⁸⁷**. El 28 de maig, **Twitter** va informar que havia tancat 5000 comptes⁸⁸ i **Facebook** va fer el mateix amb 51 comptes, 7 grups i 36 pàgines, algunes de les quals eren seguides per més de 21.000 persones⁸⁹.

Finalment, cal destacar l'existència de diversos **grups de *hackers*** que algunes fonts vinculen amb el propi Estat iranià. Així, l'Iran podria estar darrere de diversos grups de *hackers* com: **OilRig**, presumptament vinculat a atacs contra 97 organitzacions de 27 països i 18 indústries diferents⁹⁰; **Muddywater**, acusat d'estar darrere de diversos atacs contra organitzacions governamentals⁹¹; o els creadors del prolífic **ransomware SamSam**, detinguts i empresonats des de final de 2018⁹².

Existència de diversos grups de hackers que algunes fonts vinculen amb el propi Estat iranià.



⁸⁴ <https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-freedoms-citizens-access-social-media-telegram-a8182841.html>

⁸⁵ <https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/>

⁸⁶ https://en.wikipedia.org/wiki/Internet_censorship_in_Iran

⁸⁷ <https://www.securityweek.com/iran-based-social-media-scheme-impersonated-press>

⁸⁸ <https://threatpost.com/twitter-5000-accounts-disinformation-campaigns/145764/>

⁸⁹ <https://www.msn.com/en-xl/middleeast/top-stories/facebook-and-twitter-pull-down-more-fake-accounts-from-iran/ar-AAC4rYe?li=BBJGzsi&ocid=mailsignout&fbclid=IwAR1r5-ZXobESiXxPNw8Bx7PZtmu1DlcTHSI2itdnbMI1SMF-Oc6qhjbDeJU>

⁹⁰ <https://www.bankinfosecurity.com/despise-doxing-oilrig-apt-group-remains-threat-a-12449>

⁹¹ <https://www.bleepingcomputer.com/news/security/the-muddywater-apt-group-adds-new-tools-to-their-arsenal/>

⁹² <https://techcrunch.com/>



Fets rellevants

- ▶ Una fuga d'informació revela l'activitat del **grup de hackers iranià Rana**: detalls de les víctimes, estratègies d'atac, llistats d'empleats i captures de pantalla de les eines d'espionatge. També inclou informació de l'activitat dels grups de **hackers iranians OilRig i MuddyWater**. S'especula que els documents podrien tenir origen en el **hackeig** del Ministeri d'Intel·ligència iranià⁹³.
- ▶ Un informe relaciona amb l'**Iran** una **campanya de desinformació** que, a través de simular diaris en línia, tracten de **difamar contra els EUA, Israel i l'Àràbia Saudita**⁹⁴.
- ▶ **Facebook** va comunicar l'**eliminació de 97 comptes vinculats a Rússia**, dedicats a difondre desinformació sobre Ucraïna, i uns altres **21** per difamar contra diversos estats europeus. Així mateix, va eliminar **2.632 pàgines, grups i comptes vinculats a Iran, Macedònia i Kosovo**⁹⁵.
- ▶ Es descobreix que **agents d'agències d'intel·ligència occidentals** van atacar **Yandex**, el Google rus, el 2018. Sembla ser que van fer ús del **malware Reign**, vinculat a l'aliança Five Eyes (EUA, Regne Unit, Austràlia, Nova Zelanda i Canadà), amb l'objectiu de **conèixer la tecnologia d'autenticació dels usuaris per tal de poder obtenir-ne accés**⁹⁶.
- ▶ Un informe de la **UE** acusa **Rússia d'intentar interferir en les eleccions europees** per mitjà d'una "contínua i sostinguda" **campanya de desinformació**, similar a les realitzades contra els EUA i França. Apunta que caldran noves **accions per controlar aquest tipus d'atacs**⁹⁷.
- ▶ El **Regne Unit** presenta evidències de **activitat cibernètica maliciosa russa** contra 16 estats membres de l'OTAN⁹⁸.
- ▶ L'**armada russa** està en procés de substitució dels seus sistemes **Windows** per la distribució de **Linux Astra**, especialment certificat per tractar **informació classificada**⁹⁹.
- ▶ Els **codis font** de diverses eines de **hacking** utilitzada pel grup de hackers **OilRig**, vinculat a l'Iran, van ser deliberadament publicades a la **Xarxa i per Telegram**¹⁰⁰.
- ▶ En resposta a l'atac contra un dron nord-americà, els **EUA** van realitzar **ciberatacs contra els sistemes de míssils d'Iran** amb l'objectiu de desactivar-los. Segons el govern iranià, aquests no van tenir èxit¹⁰¹.
- ▶ El 21 d'abril, uns terribles **atemptats a Sri Lanka** van causar la mort a més de 200 persones. El govern va **tancar l'accés a xarxes socials** per evitar la difusió de desinformació, però al mateix temps va resultar **limitada la llibertat dels ciutadans**¹⁰².
- ▶ **Human Rights Watch** informa que la Xina utilitza **diverses tecnologies** com aplicacions mòbils, reconeixement facial i anàlisi de dades per **vigilar i realitzar detencions** entre la minoria musulmana de la regió de Xinjiang¹⁰³.
- ▶ El 6 de juny, i durant **2 hores**, es va detectar com una **gran quantitat de tràfic mòbil d'Europa era encaminat** a través de la infraestructura de l'empresa propietat de l'Estat **China Telecom**. Aquest fet genera dubtes sobre la seguretat del sistema global d'encaminament d'Internet, anomenat Border Gateway Protocol (BGP)¹⁰⁴.
- ▶ Diferents investigacions publiquen que **Xenotime**, el **grup de hackers rus** presumptament autor dels atacs amb el **malware Triton**, està intentant **atacar la xarxa elèctrica dels EUA**. Aquests, per la seva banda, **també haurien tingut èxit en atacs contra la infraestructura elèctrica russa**¹⁰⁵.

⁹³ <https://www.securityweek.com/leak-reveals-activity-iranian-hacking-group>

⁹⁴ <https://www.securityweek.com/report-links-vast-online-disinformation-campaign-iran>

⁹⁵ <https://www.reuters.com/article/us-facebook-fake-accounts/facebook-deletes-more-accounts-linked-to-russia-idUSKCN1SC1T4>

⁹⁶ <https://www.engadget.com/2019/06/28/western-intelligence-hackers-russia-yandex/>

⁹⁷ <https://www.engadget.com/2019/06/16/eu-accuses-russia-of-election-interference-campaign/>

⁹⁸ <https://securityaffairs.co/wordpress/86025/breaking-news/russia-hacking-campaigns.html>

⁹⁹ <https://securityaffairs.co/wordpress/86407/security/astra-linux-russia-army.html>

¹⁰⁰ <https://www.securityweek.com/source-code-new-iran-linked-hacking-tool-posted-online>

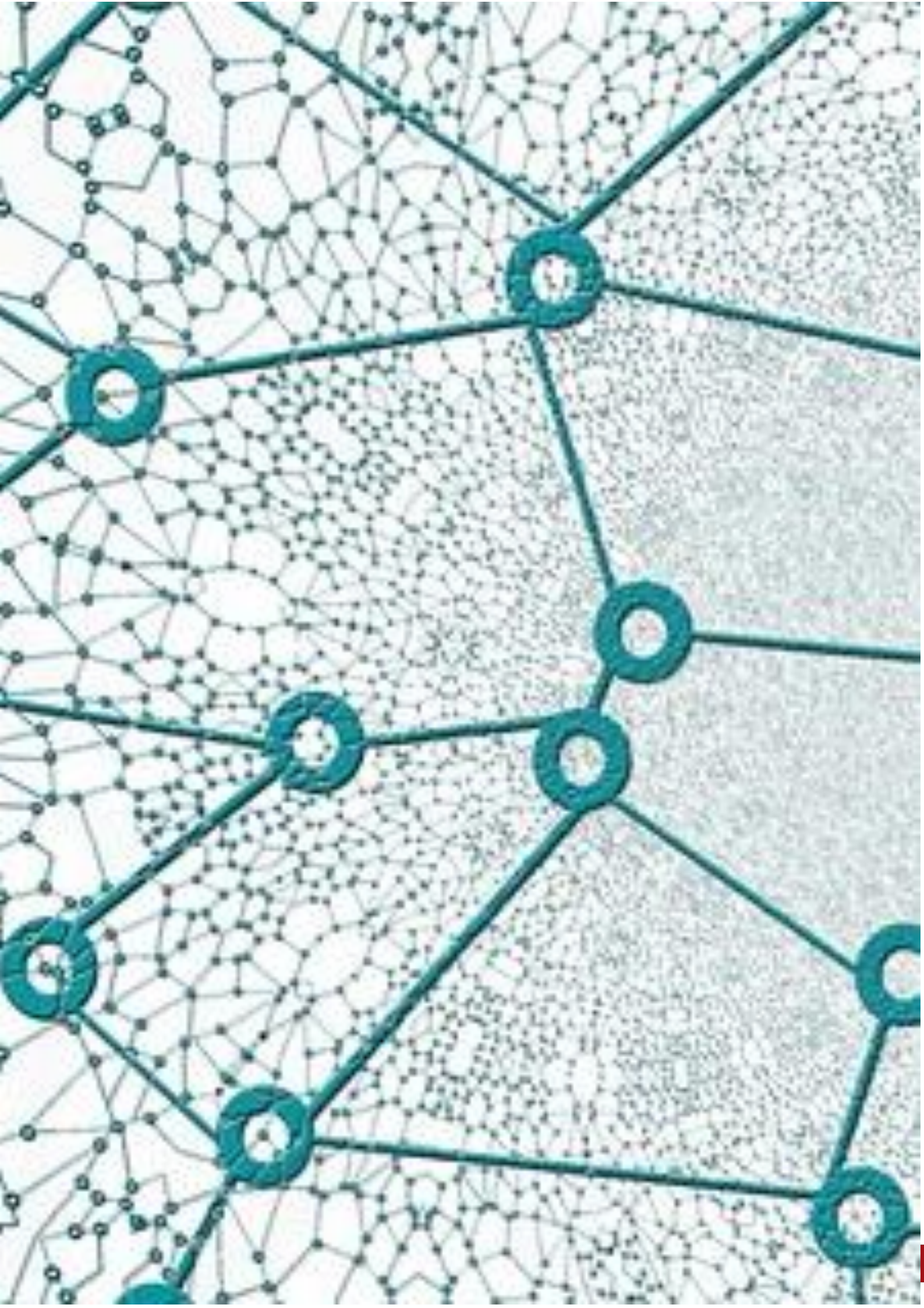
¹⁰¹ <https://lta.reuters.com/articulo/iran-eeuu-ciberataques-idLTAKCN1TP1BE-OUSLT>

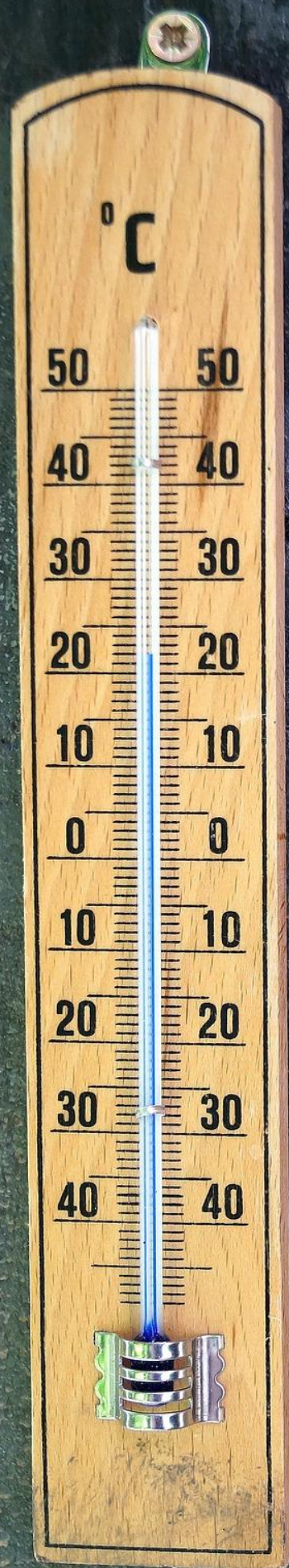
¹⁰² <https://www.elpuntavui.cat/politica/article/17-politica/1591740-una-cadena-d-explosions-provoca-mes-de-200-morts-a-sri-lanka.html>

¹⁰³ <https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang>

¹⁰⁴ <https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/>

¹⁰⁵ <https://siliconangle.com/2019/06/16/cyber-cold-war-heats-russia-us-attempt-hack-others-power-grids/>





Baròmetre
d'amenaces



Baròmetre

Top 5 ciberamenaces

Tenint en compte el nombre d'incidents que han tingut lloc durant el primer trimestre de 2019, a continuació es mostra l'evolució de les cinc ciberamenaces més rellevants i se'n destaquen els esdeveniments més significatius.

Una ciberamenaca és qualsevol circumstància o esdeveniment que tingui un impacte potencial negatiu en alguna de les dimensions d'un actiu d'informació: confidencialitat, integritat i/o disponibilitat.

T2 2019	vs	T1 2019	Ciberamenaces ¹⁰⁶
1		1	Compromís i/o pèrdua d'informació <i>Publicació d'informació o de credencials d'accés als sistemes d'informació de l'organització que la posen en compromís, així com informació de l'organització extraviada que no és recuperable de cap manera.</i>
2		2	Atacs deliberats <i>Difusió i/o execució de programari maliciós, accés lògic o físic no autoritzat, o abús de privilegis d'accés sobre els sistemes d'informació.</i>
3		3	Saturació i/o pèrdua de serveis essencials <i>Impossibilitat d'accedir als sistemes per inhabilitació o perquè han arribat a la màxima capacitat de processament, de manera que s'impedeix el correcte funcionament o es provoca l'aturada dels sistemes informàtics de l'organització.</i>
4		4	Frau econòmic <i>Atacs interns o externs contra l'organització mitjançant l'engany, en els quals es busca aconseguir un benefici econòmic.</i>
5		5	Coacció, extorsió o corrupció <i>Persuasió il·legítima, intimidació o suborn per obligar una víctima a cometre accions il·lícites o delictives contra els actius d'informació.</i>

▲ Puja ▼ Baixa || Es manté

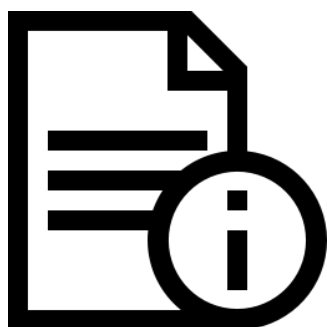
¹⁰⁶ Catàleg d'amenaces del CESICAT



1. Compromís i/o pèrdua d'informació

El compromís i/o pèrdua d'informació ha tornat a ser l'amenaça més habitual en el món de la ciberseguretat. Queda palès com en són d'importants per als cibercriminals les **dades personals** i, en especial, **les credencials i les dades de targetes de crèdit**. Així, destaquen els **atacs contra el comerç electrònic** i, en especial, l'activitat dels grups de *hackers* **Magercart**. S'ha fet menció de molts incidents rellevants com aquests (veure apartat [Fuites de dades](#)), però n'hi ha molts d'altres a destacar.

- ▶ **60 milions de registres de LinkedIn** van quedar exposats amb informació del perfil públic de l'usuari: noms, URL del perfil, historial laboral, educació, ubicació, habilitat, etc¹⁰⁷.
- ▶ **300.000 fitxers** que contenien informació financera del proveïdor de serveis informàtics alemany **CITICOMP** van ser **publicats** a Internet després que la companyia rebutgés pagar un **rescat de 5000 dòlars** per evitar-ho. Clients com **Airbus, Porsche, Toshiba** o **Volkswagen** en van resultar afectats¹⁰⁸.
- ▶ **1,3 milions de registres** que contenien dades personals de **professors i alumnes** de la universitat de **GeorgiaTech** (EUA) van quedar exposats per un accés no autoritzat que aprofitava una **vulnerabilitat** d'una aplicació web¹⁰⁹.
- ▶ A **Austràlia** uns *hackers* van accedir a les **dades mèdiques de 10 milions de ciutadans**. La xifra és esfereïdora si es compara amb la població d'Austràlia, poc més de 25 milions de persones¹¹⁰.
- ▶ El mes d'abril es va fer públic que els **treballadors d'Amazon**, ubicats a Boston, Costa Rica, Índia i Romania, **escolten els sons registrats per Alexa** amb l'objectiu de millorar els seus sistemes de reconeixement de veu. És preocupant pel fet que es podria filtrar **informació privada sense consentiment**¹¹¹.
- ▶ S'informa que el juny del 2018, un *hacker* va aconseguir penetrar la infraestructura de la **NASA** i robar **23 fitxers** mitjançant una placa **Raspberry Pi** de 35 dòlars que va connectar a la xarxa interna i va passar desapercebuda durant mesos¹¹².



¹⁰⁷ <https://securityaffairs.co/wordpress/84286/data-breach/scraped-linkedin-data-leaked.html>

¹⁰⁸ <https://www.2-spyware.com/it-giant-citycomp-blackmailed-to-pay-ransom-after-customer-data-breach>

¹⁰⁹ <https://www.zdnet.com/article/georgia-tech-reveals-data-breach-1-3-million-records-exposed/>

¹¹⁰ <https://www.cso.com.au/article/661702/least-10m-records-compromised-single-australian-data-breach-despite-drop-ndb-reports/>

¹¹¹ <https://www.lavanguardia.com/tecnologia/20190411/461590269818/trabajadores-amazon-escuchan-sonidos-registra-alexa-privacidad-dispositivos-altavoz-inteligente-tecnologia.html>

¹¹² <https://www.bbc.com/news/technology-48743043>

2. Atacs deliberats

Els atacs deliberats segueixen ocupant la segona posició en les amenaces del segon trimestre de 2019. El **ransomware és l'eina preferida pels ciberdelinqüents** a l'hora d'obtenir un rendiment econòmic i l'objectiu preferit són les **empreses o organitzacions** que poden permetre's pagar rescats elevats. Ara bé, als EUA es constata un important creixement dels **atacs dirigits a organismes públics** (veure apartat [Ransomware dirigit a organismes públics](#)).

El **phishing** és un atac d'enginyeria social en el qual l'atacant imita una organització de confiança simulant l'entorn habitual d'interacció que l'usuari tindria (pàgina web, correu electrònic, aplicació, etc.).

L'objectiu del phishing és enganyar l'usuari i obtenir-ne un benefici econòmic o una informació determinada.

Un **exploit** és una eina de programari dissenyada per aprofitar una vulnerabilitat o error i aconseguir el comportament no desitjat, per part del seu propietari, d'un dispositiu.



- ▶ El 3 de juny l'empresa de proves de laboratori **Eurofins Scientific**, amb 800 laboratoris a 47 països, va ser víctima d'un **ciberatac**. No s'han donat més dades però **les seves accions a borsa van baixar un 6%** el dia de la publicació de l'incident¹¹³.
- ▶ El mes d'abril, un grup de **hackers**, mitjançant una **botnet** formada per més de **152.000 dispositius** infectats, va atacar els **criptomoneders Electrum** i aconseguir robar més de **4,6 milions de dòlars**¹¹⁴.
- ▶ Els mesos d'abril i maig van ser intensos pel que fa al final de **sèries de televisió com Joc de Trons**. Kaspersky ha denunciat com aquest fet ha estat aprofitat pels cibercriminals per a la **difusió d'un malware** o per a motivar la **subscripció a webs d'streaming** amb l'objectiu d'obtenir dades valuoses dels usuaris^{115 i 116}.
- ▶ Un informe de ProofPoint apunta que els **ciberatacs** a aplicacions al **núvol**, com Microsoft Office 365 i Google G Suite, van **augmentar un 65%** durant el primer trimestre de 2019. El principal país de procedència d'aquests atacs és **Nigèria** i s'utilitzen tècniques de **força bruta** i **phishing** per obtenir-hi accés¹¹⁷.
- ▶ El 4 d'abril la **Polícia Nacional** va alertar de l'**estafa de phishing** que instava els usuaris a complimentar una **falsa enquesta** a canvi de 100 euros amb l'objectiu d'obtenir **dades personals**¹¹⁸.
- ▶ A mitjan juny, es va identificar com els servidors **Exim**, aproximadament el **57% dels servidors de correu del món**, van ser **massivament atacats** per dos grups de **hackers** utilitzant un **exploit** que aprofita la **vulnerabilitat** anomenada "Return of the WIZard". Els administradors han d'actualitzar el sistema a la versió 4.92 si volen protegir-lo¹¹⁹.
- ▶ El mes d'abril, els **Mossos d'Esquadra** van informar d'una estafa de **phishing** en la qual els ciberdelinqüents es feien passar per **Caixabank** i informaven d'un **moviment irregular** en el compte de l'usuari amb l'objectiu de robar les seves credencials¹²⁰.

¹¹³ <https://www.securityweek.com/lab-testing-firm-eurofins-scientific-hit-ransomware>

¹¹⁴ <https://thehackernews.com/2019/04/electrum-bitcoin-wallet-botnet.html>

¹¹⁵ <https://www.kaspersky.com/blog/tv-series-threats/26274/>

¹¹⁶ <https://www.kaspersky.com/blog/game-of-thrones-download-dangers/26961/>

¹¹⁷ <https://www.proofpoint.com/es/newsroom/press-releases/los-ataques-aplicaciones-cloud-aumentan-en-un-65-durante-el-primer-trimestre>

¹¹⁸ <https://www.elperiodico.com/es/sociedad/20190408/estafa-mercadona-7396790>

¹¹⁹ <https://www.zdnet.com/article/exim-email-servers-are-now-under-attack/>

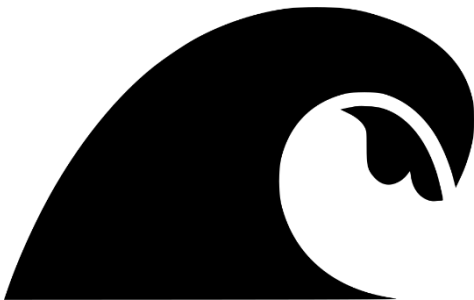
¹²⁰ https://www.economiadigital.es/finanzas-y-macro/caixabank-alerta-mossos-estafa-phishing_621092_102.html

3. Saturació i/o pèrdua de serveis essencials

Un **atac DDoS** (Distributed Denial of Service) és un atac originat per una xarxa de dispositius o botnet. L'objectiu és causar la indisponibilitat d'un servei i impedir-hi l'accés als usuaris legítims, amb la saturació del tràfic i el processat computacional que els servidors són capaços de suportar.

Els **atacs de ransomware**, actualment tant nombrosos, en molts casos acaben causant una **aturada en l'activitat** dels serveis essencials d'empreses o organismes públics (veure [Ransomware dirigit a organismes públics](#)). Sovint, l'objectiu rere d'un ciberatac no és obtenir un gran rescat, sinó simplement causar una interrupció dels serveis de la víctima per provocar pèrdues econòmiques o afectar la reputació, com succeeix en els **atacs DDoS**.

- ▶ L'**aeroport internacional de Cleveland Hopkins** (EUA) va ser objecte d'un atac de **ransomware** el 21 d'abril de 2019. L'atac va afectar els **sistemes de correu electrònic, nòmnes i registres** de l'aeroport, i va inhabilitar les **pantalles d'informació**¹²¹.
- ▶ **Asco Industries**, una companyia belga dedicada a la fabricació de components per **avions** tant civils com militars, va ser víctima d'un atac de **ransomware** el 7 de juny de 2019 que la va obligar a **paralitzar la producció a tot el món**¹²².
- ▶ **Norsk Hydro** (Noruega), una companyia dedicada a les energies renovables i a la indústria de l'alumini, a les acaballes del segon trimestre encara es recupera de l'atac del 12 de maig de 2019 amb **ransomware Lockergoga**. Després d'aproximadament un mes i mig, la companyia estimava que l'incident suposarà un **impacte de 52 milions de dòlars** a causa de la **interrupció** de les operacions i el cost de recuperació¹²³.
- ▶ La **clínica Estes Park Health** va patir un atac de **ransomware** el 2 de Juny de 2019 i, per **protegir els pacients** dels problemes derivats de l'aturada dels sistemes informàtics, va consultar la seva asseguradora i van optar per **pagar el rescat**.¹²⁴
- ▶ L'aplicació de missatgeria **Telegram** va patir, el 12 juny de 2019, un **atac de DDoS** que va provocar que els usuaris d'**arreu del món** patissin **problemes de disponibilitat**¹²⁵.



¹²¹ <https://www.cybersecurity-insiders.com/ransomware-attack-on-cleveland-hopkins-international-airport/>

¹²² <https://www.itdigitalsecurity.es/actualidad/2019/06/un-ataque-de-ransomware-paraliza-la-produccion-de-asco-industries>

¹²³ <https://www.computing.co.uk/ctg/news/3074971/norsk-hydro-cyber-attack-cost>

¹²⁴ <https://www.databreaches.net/co-hit-by-ransomware-estes-park-health-decides-to-pay-the-ransom-to-get-decryption-keys/>

¹²⁵ <https://gbhackers.com/telegram-ddos-attack/>

4. Frau econòmic

Una **hot wallet** o criptomoneder en línia és una eina informàtica mitjançant la qual els usuaris custodien el compte personal en què emmagatzemen criptomonedes i, a més, està permanentment connectat a les xarxes blockchain a través d'Internet per autoritzar les transaccions econòmiques. No són tan segures com les cold wallets, per la qual cosa són adequades per petites quantitats econòmiques que desencoratgin els atacants de fer qualsevol esforç.

Una **plataforma de canvi** plataforma web que actua com a borsa de valors i des d'on és possible comprar o vendre criptomonedes a canvi de contraprestacions econòmiques, en concepte de monedes de curs legal o altres criptomonedes, d'acord amb les tarifes de les operacions i el valor de les criptodivises



Aquest trimestre ha destacat l'estratègia del BEC per perpetrar frau econòmic (veure [Business Email Compromise \(BEC\)](#)), tot i que s'han desplegat moltes altres estratègies. També es constata que es manté l'interès dels ciberatacants pel robatori de criptomonedes, esperonats principalment per la pujada un altre cop del preu del bitcoin.

- ▶ Un grup de **hackers** va robar **40 milions de dòlars** en bitcoins d'un **hot wallet** allotjat a la **plataforma de canvi Binance**. Segons la companyia, per aconseguir-ho, els **hackers** van usar diverses tècniques, incloent-hi **phishing** i **malware**¹²⁶.
- ▶ S'ha donat a conèixer que **100 comptes de venedors d'Amazon** van ser compromesos durant més de **6 mesos** gràcies a obtenir les **credencials** d'administració per mitjà de correus de **phishing**. Els **hackers** periòdicament canviaven les dades bancàries legítimes dels venedors per les dels seus comptes per tal que els autèntics administradors no se n'adonessin¹²⁷.
- ▶ Als EUA s'han acusat **sis persones** que, amb l'objectiu de **robar criptomonedes**, van **suplantar les identitats** de les víctimes i saltar-se la doble autenticació mitjançant el **duplicat de la targeta SIM**. Tres empleats de la companyia de telefonia mòbil han estat acusats d'acceptar suborns per ajudar a robar les identitats dels subscriptors¹²⁸.
- ▶ En un esforç conjunt de diversos organismes de 6 països diferents han **desmantellat una xarxa de ciberdelinqüència** darrere del **malware GozNym**, responsable de robar gairebé **100 milions de dòlars** de més de **41.000 víctimes** a tot el món, principalment als EUA i Europa¹²⁹.
- ▶ L'**Europol** i la **polícia holandesa** han tancat **BestMixer.io**, que va començar el 2018 i havia assolit una **facturació de 200 milions de dòlars**. BestMixer.io era un servei que "mesclava **criptomonedes** potencialment identificables amb altres per tal d'**ocultar-ne el rastre**"¹³⁰.
- ▶ La plataforma de canvi de criptomonedes **Komodo** va descobrir una **vulnerabilitat** en els criptomoneders dels seus clients i, per evitar que fossin robats, **va avançar-se i va hackejar els usuaris** per retirar prop de **13 milions** de dòlars que posteriorment retornarien als seus propietaris¹³¹.

¹²⁶ <https://techcrunch.com/2019/05/07/binance-breach/>

¹²⁷ <https://www.engadget.com/2019/05/08/amazon-seller-hack/>

¹²⁸ <https://nakedsecurity.sophos.com/2019/05/17/hacking-gang-stole-millions-in-cryptocurrency-via-sim-swaps/>

¹²⁹ <https://www.europol.europa.eu/newsroom/news/gozonym-malware-cybercriminal-network-dismantled-in-international-operation>

¹³⁰ <https://es.cointelegraph.com/news/europol-shuts-down-200-million-crypto-mixing-service-bestmixer>

¹³¹ <https://gadgets.ndtv.com/internet/news/komodo-agama-wallet-hack-13-million-kmd-btc-2049567>

5. Coacció, extorsió o corrupció.

Novament, l'ús de **ransomware** i el corresponent pagament d'un **rescat** a canvi de recuperar els sistemes d'informació ha estat el **mètode predominant d'extorsió** aquest segon trimestre de 2019 (veure [Ransomware dirigit a organismes públics](#)).

- ▶ Una consulta mèdica de la **ciutat de Boardman** (EUA) va ser extorsionada amb la demanda d'un rescat de **75.000 dòlars** després d'un atac de **ransomware**. L'**aturada dels sistemes suposava uns 30.000 dòlars diaris** per a la companyia, així que va acabar **pagant el xantatge**, obtenir les claus de desxifrat i poder recuperar l'operativa normal¹³².
- ▶ El conegut grup de música **Radiohead** va patir un atac de **ransomware** que va xifrar les cançons que el grup pretenia treure en el seu nou àlbum. A més, li demanaven **150.000 dòlars sota l'amenaça de fer-les públiques**. El grup va optar per publicar-les igualment i no pagar el **hacker**¹³³.
- ▶ Un **banc d'aliments als EUA** va ser atacat per un **ransomware** i se li van demanar **9.500 dòlars** a canvi de desbloquejar el sistema informàtic. El banc d'aliments va decidir **no pagar els hackers** i iniciar una **campanya de recollida fons per reconstruir el sistema informàtic**¹³⁴.



¹³² <http://www.wfmj.com/story/40646778/boardman-medical-practice-hacked-told-to-pay-75000-in-bitcoin-to-unlock-system>

¹³³ <https://www.cnet.com/es/noticias/radiohead-18-horas-de-musica-inedita-tras-hackeo/>

¹³⁴ <https://www.bleepingcomputer.com/news/security/food-bank-hit-by-ransomware-needs-your-charity-to-rebuild/>

Conclusions

BARCELONA CYBERSECURITY CONGRESS



El delictes cibernètic existeix des de molt abans de l'existència d'Internet i les xarxes socials. Un dels primers *hackers* coneguts fou John Draper (EUA)¹³⁵, el qual el 1971 va descobrir com una joguina que es regalava amb una caixa de cereals permetia emetre un to d'una freqüència similar al que utilitzava l'operador telefònic AT&T per operar la xarxa. Així, va aconseguir enganyar la companyia telefònica per fer trucades a llarga distància gratuïtes.

Des d'aleshores l'activitat dels *hackers* ha evolucionat molt. En el present informe es tracta com el **ransomware** especialitzat i dirigit de forma manual vers organitzacions i empreses públiques és tendència, però tot just va ser el 2017 quan van aparèixer els primers **ransoms** que, difosos massivament, van agafar milers d'usuaris per sorpresa i van aconseguir un gran nombre de víctimes.

També es parla de la forta irrupció del **BEC**, un atac per correu electrònic molt dirigit i que requereix un elevat coneixement de la víctima, el qual permet assolir ingressos més elevats que la tècnica del **phishing** activa i que aconsegueix noves víctimes des de fa anys.

Les fuites de dades també són un tema destacat, ja siguin originades per error o per l'atac de hackers, ja que han originat un autèntic mercat negre en què l'actualitat de les dades i les possibilitats d'obtenir-ne un benefici econòmic determinen la seva cotització.

Aquestes amenaces són evidències de com l'àmbit de la ciberseguretat, que el 1971 contemplava com John Draper manipulava els tons de la xarxa telefònica amb una joguina, ha evolucionat ràpidament, al ritme de la imparable digitalització del món. Així, avui dia la ciberseguretat disposa d'interès geoestratègic i ha esdevingut un àmbit on els estats i les principals economies del món són actors principals.

Davant d'aquest escenari, el Govern de la Generalitat de Catalunya, a través del CESICAT, assumeix el repte de crear un país cibersegur i estimular el sector de la ciberseguretat des del Barcelona Cybersecurity Congress que enguany celebra la segona edició¹³⁶. El Congrés ofereix l'oportunitat perfecta als professionals de la ciberseguretat d'explicar, discutir i intercanviar coneixements i idees amb l'objectiu de contribuir a la construcció d'un sector preparat per fer front a les amenaces cibernètiques que tan ràpidament canvien.

La cita per seguir avançant és el 29, 30 i 31 d'octubre.

¹³⁵ https://es.wikipedia.org/wiki/John_Draper

¹³⁶ <https://barcelonacybersecuritycongress.com/en/>



Generalitat de Catalunya
**Centre de Seguretat de la Informació
de Catalunya**

ciberseguretat.gencat.cat

@ CESICAT a octubre de 2019