AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Informe de tendències de ciberseguretat

2n trimestre de 2021

La ciberamenaça impacta la societat

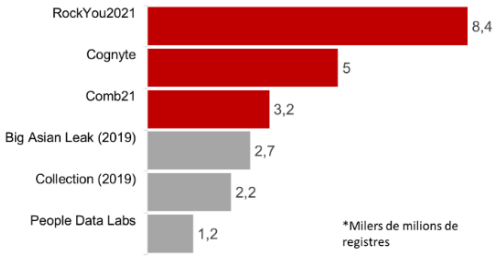
Índex

Aquest document és fruit del seguiment i de l'anàlisi de les tendències en relació a les amenaces de ciberseguretat detectades durant l'any 2021 per part de l'Agència de Ciberseguretat de Catalunya.

Per a la realització d'aquest informe, s'han tingut en compte l'activitat i la documentació pròpies generades per l'Agència de Ciberseguretat de Catalunya, 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.

Resum

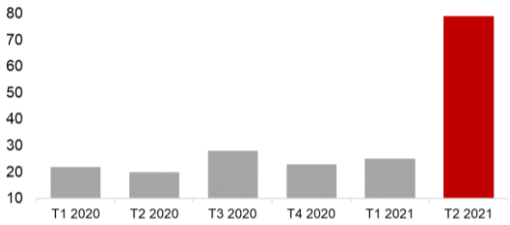
Ha estat notícia. Ha crescut l'ús de **tecnologies per al teletreball** i s'han convertit en el focus d'atenció de la ciberseguretat: uns busquen de millorar-la; altres intenten perpetrar ciberatacs. Així, durant el 2n trimestre, s'han identificat **nombroses vulnerabilitats** en **servidors de correu electrònic**, **VPN**, **tallafocs** i **plataformes de compartició de fitxers**. Les organitzacions han de ser conscients que, tan bon punt es publica una vulnerabilitat, comença el compte enrere per apedaçar-la abans que es pugui explotar.



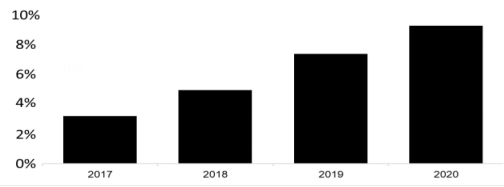
Les tres recopilacions de credencials més grans mai vistes s'han identificat la 1a meitat de 2021.

Les fuites massives de dades personals exposen la identitat digital de la ciutadania en un espai cibernètic que recopila i no oblida. Aquest trimestre, hi ha hagut **filtracions** amb dades personals de milions de catalans; si es tractés de dades úniques, haurien afectat més del **50% de la població**. Són dades que es podrien utilitzar en futurs **ciberatacs o fraus**. Des d'un punt de vista global, es manté la tendència de menys incidents, però de gran magnitud: les fuites de **més de 100 M de registres** han crescut un **33%** durant la 1a meitat de 2021 respecte de l'any anterior. Bona part es deuen a **errors de configuració**, **API vulnerables** o ***scrapping*** a les xarxes socials. Les fuites que acaben a la ***dark web*** creixen un **400%** respecte del trimestre passat, un fet que facilita l'aparició de **recopilacions massives**, com les **tres més grans de la història** identificades la 1a meitat de 2021. Els atacs de *ransomware* consoliden l'ús del **robatori d'informació com a mètode d'extorsió**, amb l'objectiu d'aprofitar la por de rebre una sanció milionària per incompliment de l'RGPD.

Les infraestructures crítiques són objectiu del *ransomware* i de grups APT que amenacen el subministrament de serveis essencials. S'estima que els ciberatacs dirigits a **infraestructures crítiques** creixeran un **80%** aquest any. Són objectiu d'atacs de ***ransomware*** o de **grups APT** que amenacen el subministrament de serveis essencials i posen en risc l'**estabilitat social i econòmica**. De fet, el **59%** de les infraestructures crítiques atacades han hagut d'aturar l'activitat. Després dels incidents de **Colonial Pipeline**, **JBS** i el **sistema sanitari d'Irlanda**, l'**OTAN** i el **G-7** han fixat la lluita contra el cibercrim com una prioritat. El cibercrim incrementa els recursos dels **atacs de DDoS**, que apunten també als serveis essencials i es consoliden com un **element d'extorsió addicional, potent i versàtil**. La col·laboració internacional s'ha constatat en les **operacions policials** que han permès detenir els responsables dels *ransomwares* **Egregor** i **Clop**. De la seva banda, la UE protegirà les cadenes de subministrament d'infraestructures crítiques amb la inclusió en la futura **Directiva NIS 2** del que s'anomenen serveis importants.



La presència d'incidents cibernètics amb afectació als subministraments públics creix un 300% el 2n trimestre de 2021.



L'increment anual dels sinistres de ciberassegurances causats per atacs de ransomware és més gran, any rere any. S'ha triplicat des del 2017.

El *ransomware* explota el pagament de rescats per part de les ciberasseguradores i el model de negoci se'n ressent. Les organitzacions han accelerat la transformació digital i han canviat les preocupacions: a l'Estat espanyol, un **58%** considera els **ciberincidents com la principal amenaça**. No és estrany, doncs, que proliferin les contractacions de pòlisses de ciberassegurança. En aquest context, el cibercrim ha atacat amb ***ransomware*** les **organitzacions ciberassegurades** per exigir rescats elevats. En aquesta situació, les asseguradores, per poder fer front als pagaments, s'han vist obligades a **apujar les primes entre un 25% i un 40%**, o a **deixar d'oferir suport** pel que fa a pagaments de rescats. Les **asseguradores** mateixes, atès que estan en possessió de les llistes d'empreses assegurades i tenen capacitat econòmica, també han estat **objectiu d'atacs**: la companyia **CNA Financial** va pagar **34 M€**, tot un **rècord** fins avui. Una dada interessant és la que prové del **sector educatiu**: els atacs amb *ransowmare* han augmentat un **200%** durant el 2n trimestre respecte de l'any passat. En conseqüència, les pòlisses de ciberassegurança han augmentat un **60%**.

Una VPN (Virtual Private Network), o xarxa privada virtual, és una xarxa privada que s'estén, mitjançant un procés d'encapsulació, i en algun cas de xifratge, dels paquets a diferents punts remots, i utilitza infraestructures públiques de transport.

(font: Termcat)

*RDP (*Remote Desktop Protocol*). Protocol que permet la comunicació en l'execució d'una aplicació entre un terminal i un servidor de qualsevol tecnologia.*

(font: Termcat)

Una vulnerabilitat és la feblesa d'un sistema informàtic davant de les amenaces a què està exposat.

(font: Termcat)

Una vulnerabilitat zero-day o de dia zero d'un dispositiu o sistema és desconeguda pel fabricant o es coneix des de fa poc temps i, per tant, encara no té protecció ni s'ha fet pública als usuaris.

(font: Termcat)

Un pedaç és un fitxer que conté una o diverses modificacions d'un programa destinades a corregir-ne un error, a incorporar-hi funcions noves o a actualitzar-lo.

(font: Termcat)

Ha estat notícia

Les tecnologies per al teletreball estan en el focus d'atenció de la ciberseguretat: uns busquen millorar-la i altres intenten perpetrar ciberatacs. Durant el 2n trimestre, s'han publicat nombroses vulnerabilitats en servidors de correu electrònic, VPN, tallafocs i plataformes de compartició de fitxers.

El teletreball es consolida

El **teletreball** ha esdevingut un element **essencial** per garantir la continuïtat de milers d'empreses a Catalunya i la resta del món durant la pandèmia. Es tracta d'un format laboral consolidat i ja és habitual sentir que "el teletreball ha arribat per quedar-s'hi". El 1r trimestre de 2021, el teletreball a l'Estat espanyol ha arribat a una xifra màxima, amb l'**11,2% dels ocupats teletreballant** més de la meitat dels dies (**2.146.000 teletreballadors**), un punt per sobre del darrer trimestre de l'any 2020 i més del doble dels registres de 2019[1].

La transició al teletreball no ha estat exempta de dificultats. Segons una enquesta a empleats del Regne Unit i els EUA, el **70% dels teletreballadors ha tingut dificultats tècniques durant la pandèmia**[2]. Precisament, la recerca d'un entorn de teletreball amb les condicions de ciberseguretat adequades ha estat un dels principals cavalls de batalla. Mentre que les tecnologies de treball remot s'han erigit com un element imprescindible, també s'han convertit en una porta d'entrada potencial de ciberatacs.

Durant el 2n trimestre de 2021, **les tecnologies relacionades amb el teletreball**, com ara les connexions VPN, RDP, els servidors de correu electrònic i les plataformes de compartició de fitxers, entre d'altres, han esdevingut el **focus d'atenció de la ciberseguretat**. Han estat **contínuament analitzades**: uns buscaven millorar-ne la seguretat; altres intentaven perpetrar ciberatacs. En conseqüència, ha estat notícia el **nombre extraordinari** de vulnerabilitats que s'han identificat i han pogut posar en risc les organitzacions del món.

Una allau de vulnerabilitats explotades

L'Informe de tendències del 1r trimestre de 2021 destacava el cas de les vulnerabilitats *zero day* als servidors de correu electrònic Microsoft Exchange. Tan bon punt les vulnerabilitats i els pedaços es van fer públiques, els ciberatacs que les explotaven es van disparar. De forma molt similar, la situació s'ha repetit durant el 2n trimestre, amb noves i alarmants vulnerabilitats en les tecnologies de teletreball[3].

[1] *https://elpais.com/economia/2021-06-08/teletrabajar-con-todos-los-recursos-tecnologicos-y-tecnicos-de-la-oficina.html*
[2] *https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home*
[3] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/Informe-de-Tendencies-1T-2021*

Una APT (Advanced Persistent Threat), o amenaça persistent avançada, és un atac a gran escala, subreptici, sofisticat, continu i dirigit a una entitat específica.

(font: Termcat)

El mes de maig, es van identificar **21 vulnerabilitats** a l'agent de transferència de correus electrònics **(MTA) Exim**, les quals afectaven **totes les versions** del programari des del 2004 permetent a un ciberatacant **prendre el control total del servidor afectat**[4]. Va ser un fet molt rellevant, ja que es calcula que un **60% dels servidors de correu** són Exim i una cerca a la web de Shodan permet comptabilitzar-ne **més de 4 milions**[5].

Cal destacar especialment les vulnerabilitats en tecnologies de **VPN**, utilitzades a bastament per a les connexions corporatives dels teletreballadors. En aquest sentit, ha plogut sobre mullat: a final de 2020, un **5% de les VPN no estaven actualitzades** i estaven afectades per diverses vulnerabilitats[6].

El mes d'abril, s'identificava una vulnerabilitat crítica a la **VPN Pulse Secure**, que permetia a un usuari sense autenticar **l'execució de codi remotament**. En aquest cas, la vulnerabilitat ha estat **explotada** per grups APT contra agències governamentals dels EUA[7]. Aquesta vulnerabilitat va permetre el ciberatac a la **Metropolitan Tranportation Authority** (MTA) de Nova York, en el qual van accedir als sistemes que supervisen la xarxa de metro, d'autobusos, el sistema ferroviari de Long Island i el Metro-North Railroad[8].

El mes de març, es van identificar unes vulnerabilitats crítiques en els productes de **correu electrònic i VPN de SonicWall** i, un mes més tard, es va detectar la primera campanya de ciberatacs en què era **explotada**[9]. El grup cibercriminal UNC2447 les utilitzava per infectar les víctimes amb la *backdoor* SOMBRAT i, posteriorment, desplegar el *ransomware* FiveHands[10].

Per últim, cal destacar diversos casos de vulnerabilitats en **plataformes per a l'intercanvi d'arxius** que han provocat que la informació dels usuaris quedés compromesa. En aquest aspecte, les vulnerabilitats a la plataforma **Accellion** encara són un element d'actualitat, tot i que van ser identificades el desembre de 2020. Els afectats inicials eren importants i nombrosos: la Universitat de Miami (EUA), el bufet Jones Day (que comptava amb Donald Trump com a client), la cadena de supermercats Kroger (número 1 als EUA), el gegant del petroli Shell (Països Baixos), el Banc de la Reserva de Nova Zelanda, etc. Però durant el 2n trimestre de 2021, s'han conegut **noves organitzacions impactades**: les **universitats de Stanford i Maryland** (EUA), el **Department of Health and Human Services** (EUA) i el gegant financer **Morgan Stanley** (EUA)[11]. Algunes de les víctimes han vist com es publicava la informació robada.

Una situació similar l'ha experimentada la popular plataforma de compartició d'arxius **FileZen**, de l'empresa japonesa **Solition**. Com en el cas d'Accellion, un grup de ciberatacants van explotar la vulnerabilitat i van robar informació sensible dels seus usuaris, entre els quals es trobava **govern del Japó**[12].

[4] *https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/21-nails-multiples-vulnerabilidades-exim-mail-server*
[5] *https://ciberseguretat.gencat.cat/web/.content/PDF/Avisos/Butlleti-de-seguretat-Noves-vulnerabilitats-dExim-Maig-2021.pdf*
[6] *https://betanews.com/2021/06/17/vpn-solutions-remain-unpatched/*
[7] *https://ciberseguretat.gencat.cat/web/.content/PDF/Avisos/202104_Bulleti-Amenaca-vulnerabilitat-0-day-Pulse-Secure-21-04.pdf*
[8] *https://www.scmagazine.com/home/security-news/data-breach/chinese-hackers-used-pulse-secure-zero-day-vulnerability-to-infiltrate-mta-systems/*
[9] *https://ciberseguretat.gencat.cat/web/.content/PDF/Avisos/Comunicat-de-ciberseguretat-Campanyes-Vulnerabilitats-SonicWall_04052021.pdf*
[10] *https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html*
[11] *https://www.msspalert.com/cybersecurity-breaches-and-attacks/accellion-vulnerabilities-victim-list/*
[12] *https://therecord.media/hacking-campaign-targets-filezen-file-sharing-network-appliances/*

Tan bon punt es publica una vulnerabilitat i comença el compte enrere per apedaçar-la

Algunes vulnerabilitats s'exploten amb facilitat i d'altres requereixen recursos i habilitats més difícils d'obtenir. Malauradament, les vulnerabilitats identificades durant el 2n trimestre de 2021 han estat especialment rellevants perquè han estat **explotades** d'una manera o d'una altra. Darrere dels ciberatacs hi ha **grups cibercriminals experts** que, ja sigui de forma **manual o automatitzada**, no han perdut l'oportunitat d'aprofitar les vulnerabilitats per obtenir accés als sistemes d'informació de les seves víctimes.

Cal considerar que, a partir del **moment en què s'informa de les vulnerabilitats** i es publiquen els pedaços, comença una **cursa contrarellotge** entre els responsables d'actualitzar els sistemes i els cibercriminals, que busquen explotar-les abans no s'apliquin els pegats de seguretat. Excepcionalment, pot passar que un actor maliciós exploti una vulnerabilitat **fins i tot abans de la publicació**.

En qualsevol cas, els responsables tecnològics han d'estar molt **alerta de les noves vulnerabilitats** que apareixen per tal de desplegar les actualitzacions pertinents de forma immediata.

Il·lustració 1. L'Agència de Ciberseguretat de Catalunya publica butlletins amb les vulnerabilitats més rellevants i comunicats amb les principals amenaces[13].

[13] *https://ciberseguretat.gencat.cat/ca/actualitat/avisos-i-butlletins/*

Les fuites massives de dades personals exposen la identitat digital de la ciutadania en un espai cibernètic que recopila i no oblida

Les fuites de dades personals han afectat milions de catalans que podrien ser objectiu de futurs ciberatacs o fraus. Des d'un punt de vista global, es manté la tendència de menys incidents però de gran magnitud. Tenen com a causes principals: els errors de configuració, les API vulnerables o l'*scrapping* a les xarxes socials. Les dades filtrades passen a engrossir recopilacions colossals de dades personals a la *dark web*. Els atacs de *ransomware* consoliden l'ús de la informació robada com a extorsió amb l'objectiu d'aprofitar la por a rebre una sanció milionària per incompliment de l'RGPD .

El 2n trimestre ha destacat per les grans fuites de dades personals que han afectat la ciutadania de Catalunya: Facebook, The Phone House, Glovo i LinkedIn. En cas es tractessin de dades úniques, no repetides, equivaldrien a més del 50% de la població. Des d'una perspectiva global, segueix la tendència de menys fuites i més massives: les fuites de més de 100 milions de registres de dades personals han crescut un 33% durant la 1a meitat de 2021 respecte del mateix període de 2020.

Els errors de configuració, les API vulnerables o l'*scrapping* a les xarxes socials són factors clau en les noves fuites de dades. Les dades filtrades que acaben compartides a la *dark web* creixen un 400% respecte del trimestre passat, un fet que facilita l'aparició de recopilacions massives. Durant la 1a meitat de l'any s'han identificat les majors recopilacions de la història que, conjuntament, recullen més de 15.000 milions de credencials.

El robatori de dades i l'amenaça de publicar-les, sovint en el context d'un atac *ransomware*, s'ha convertit en un mecanisme habitual d'extorsió. Els cibercriminals s'aprofiten del fet que les sancions d'incompliment de l'RGPD són cada com més milionàries com a mesura de pressió pel pagament del rescat.

Aspectes clau:

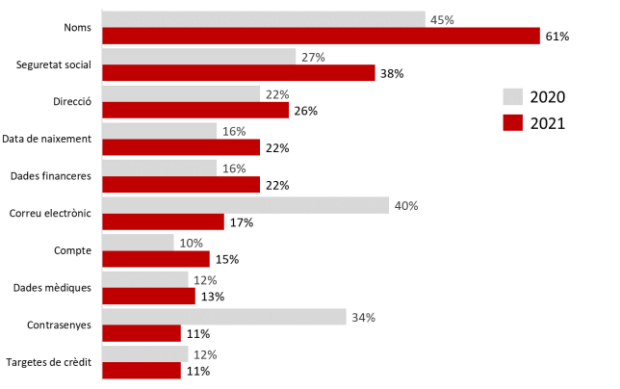
- **La identitat digital de més del 50% dels ciutadans de Catalunya es filtra en les fuites massives recents**
- **Els errors de configuració, les vulnerabilitats de les API i l'*scrapping* a les xarxes socials disparen el volum de les fuites dades**
- **El mercadeig amb dades personals creix i facilita l'aparició de noves i més grans recopilacions**
- **L'amenaça de publicar dades robades complementava el *ransomware* però ara es converteix en una pràctica d'extorsió principal**
- **Les multes per incompliment de l'RGPD són cada cop més elevades i el cibercrim ho utilitza com a element d'extorsió a canvi de no revelar les fuites**

Baròmetre

Les fuites de dades personals han experimentat un descens pel que fa al nombre d'incidents, però han crescut en magnitud. Permeten obtenir perfils complets i es comparteixen al mercat negre, en el qual s'aglutinen en forma de recopilacions massives preparades per a ser utilitzades en nou ciberatacs.

Les dades filtrades permeten crear perfils complets

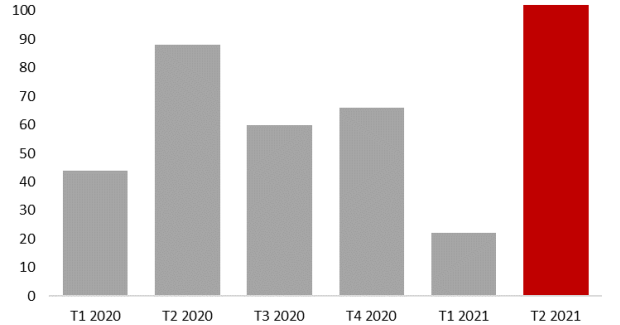
Les fuites de dades personals que han tingut lloc el 2021 contenen més noms, números de la seguretat social, adreces, dates de naixement... Són dades que afavoreixen la usurpació d'identitat a la xarxa. En canvi, han disminuït sensiblement els correus i contrasenyes, probablement arran de la progressiva millora de les mesures de protecció.



Il·lustració 2. Dades personals presents en les fuites de 2021 vs 2020[14].

Cada vegada es comparteixen més fuites de dades a la *dark web*

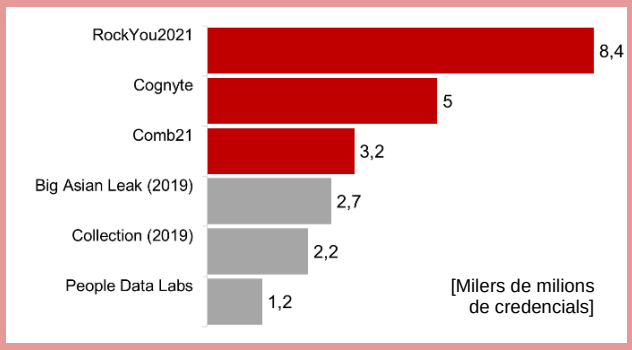
El 2n trimestre s'ha detectat un augment de les bases de dades personals compartides a la *dark web*. Sovint, l'origen de les publicacions són els robatoris de dades duts a terme en atacs de *ransomware* i la creació de recopilacions de dades.



Il·lustració 3. Presència als mitjans especialitzats de casos amb fuites de dades que acaben compartides a la dark web *(font: Agència).*

Recopilacions de credencials amb dimensions de rècord

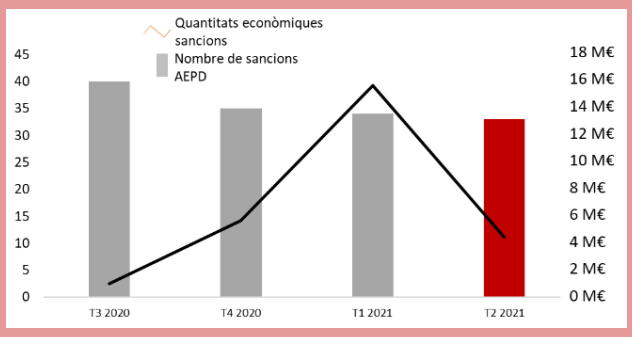
Durant la 1a meitat de 2021, s'han identificat les tres recopilacions de dades més importants de la història. Conjuntament, aquestes tres reuneixen un nombre de credencials que duplica els habitants del planeta. Són reculls de fuites de dades de diferents orígens: *scrapping*, errors de configuració, atacs de *phishing*, programaris maliciosos...



Il·lustració 4. Principals recopilacions de credencials identificades al mercat negre (font: Agència).

Segueix la tendència a l'alça de l'import de les multes per incompliment de l'RGPD

La quantitat de sancions per incompliment de l'RGPD imposades a l'Estat espanyol s'estabilitza entre les 30 i les 40 per trimestre. Pel que fa a l'import mitjà per sanció, ha baixat dels 460.000 € del 1r trimestre als 135.000 € del 2n trimestre. Cal recordar que, el 1r trimestre, l'AEPD va imposar sancions a Vodafone (8 M€) i Caixabank (6 M€). Ara bé, novament s'emeten sancions milionàries, com la d'EDP (3 M€) i Equifax (1 M€), molt per sobre dels valors habituals anteriors al canvi de tendència que va tenir lloc a final de 2020.



Il·lustració 5. Nombre de sancions i quantitats econòmiques totals. imposades per l'AEPD[15].

[14] *https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20Mid%20Year%20Data%20Breach%20QuickView%20Report.pdf*
[15] *https://www.enforcementtracker.com/*

Un registre és un camp que conté informació relativa a una persona o entitat.

*La informació d'identificació personal o PII (*Personally Identifiable Information*) és informació que, per ella mateixa o juntament amb algun altre tipus d'informació, pot identificar una persona en concret, en un entorn digital.*

(font: Termcat)

La identitat digital és un conjunt de dades i d'informació relatives a un individu, una empresa o un organisme que els representen a Internet, generades per aquests mateixos o per tercers.

(font: Termcat)

La dark web o web fosc és una part del web profund allotjat en xarxes xifrades, superposades a Internet, que utilitzen l'anonimat per a l'intercanvi d'informació.

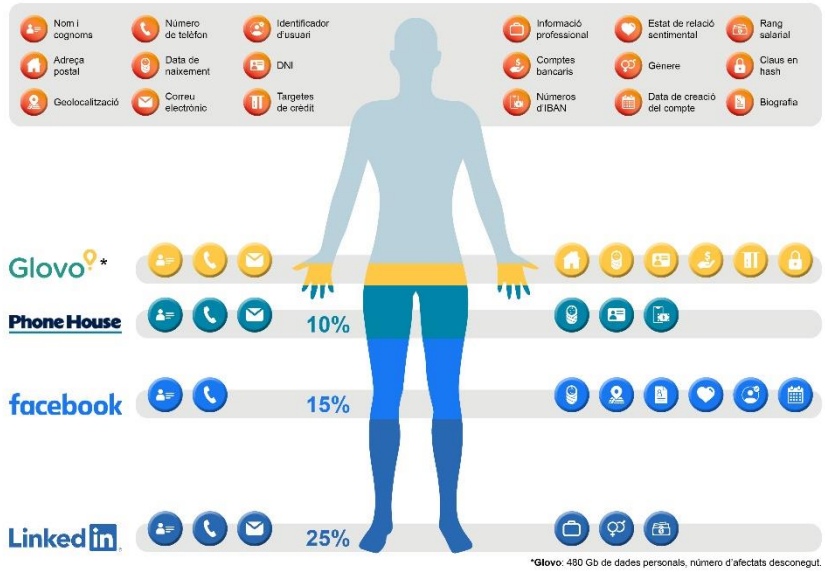
(font: Termcat)

La identitat digital de més del 50% dels ciutadans de Catalunya es filtra en les fuites massives recents

Com ja és una habitual, durant el 2n trimestre de 2021, s'han identificat diverses **fuites de dades massives** amb registres de dades personals. Incloïen informació d'identificació personal, així com altres informacions que permeten el perfilat dels afectats (veure il·lustració 2). Ara bé, aquesta vegada la particularitat és que han afectat milions de **ciutadans de Catalunya**.

En un escenari hipotètic en què les dades filtrades corresponguessin a **ciutadans únics no repetits**, més del **50% de la població de Catalunya tindria part de la seva identitat digital publicada**. En un altre escenari, en el qual les dades filtrades es concentressin en els **mateixos ciutadans**, gairebé un **10% de la població de Catalunya tindria un perfil digital molt complet i detallat publicat**: nom i cognoms, correus electrònic, telèfon, DNI, data de naixement, adreça, dades bancàries, dades professionals, salari, contactes propers, gustos culinaris, aficions...

En qualsevol cas, la situació derivada d'aquestes fuites serà procliu per tal que els cibercriminals puguin fer ús de les dades filtrades per perpetrar ciberatacs ben diversos, com l'enviament de missatges de ***phishing*** o ***smishing***, **usurpacions d'identitat** o **fraus econòmics**. Cal estar, doncs, ben alerta.



Il·lustració 6. Principals fuites de dades del 2n trimestre de 2021 que afecten la ciutadania de Catalunya.

Els incidents van començar l'abril del 2021, quan una base de dades de **Facebook**, amb la informació de més de **533 milions d'usuaris** de tot el món, es va filtrar a la *dark web*. No és la primera fuita que afecta els usuaris de Facebook, però aquesta vegada s'apunta que podria tenir l'origen en una **vulnerabilitat** de 2019, present en la funcionalitat utilitzada per importar contactes[16]. En total va afectar prop de **2 milions de catalans**, dels quals **1.298.284** circumscrits a un municipi o, fins i tot, a un barri. Les dades compromeses inclouen: **nom complet, dades de geolocalització, data de naixement, número de telèfon, identificador d'usuari de la xarxa, data de creació del compte, l'estat de relació sentimental i la biografia**[17].

[16] *https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/*
[17] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/La-fuga-de-datos-de-Facebook-afecta-a-casi-dos-millones-de-usuarios-en-Cataluna*

Un hash o funció resum és una funció matemàtica utilitzada amb finalitats de seguretat i verificació que s'aplica a un bloc de dades per a obtenir-ne un altre de longitud fixa, generalment més petita, que el representa.

(Font: Termcat)

L'scrapping és una tècnica que, mitjançant un programa de software*, consisteix en extreure informació de pàgines web de manera automatitzada, molts cops simulant la interacció d'un humà. La informació obtinguda sovint s'aglutina en una base de dades amb l'objectiu de realitzar anàlisis de màrqueting, controlar la imatge i visibilitat d'una marca a Internet, etc.*

*Una API (*Application Program Interface*) és una peça de codi que permet integrar un programa en aplicacions de tercers, de manera que s'expandeixen les seves funcionalitats.*

Una mica més tard, a mitjan abril, l'empresa espanyola de venda de serveis de telecomunicacions **The Phone House** va ser víctima d'un atac de ***ransomware***. Com que la companyia es va negar a pagar la quantitat econòmica que els ciberdelinqüents reclamaven, aquests van filtrar a la *dark web* les dades de **5,2 milions clients**, entre les quals hi havia més de **700.000 catalans**. Les comarques del Barcelonès, el Baix Llobregat i el Vallès Occidental van ser les més afectades, amb el 60% dels afectats. Entre les dades filtrades hi havia **noms, números de telèfon, dates de naixement, DNI, correus electrònics** i, en algun cas, els **números d'IBAN** dels clients que havien contractat alguna assegurança, un servei de finançament o de telefonia (aprox. un 3% del total)[18].

Però no és l'únic cas. El mes de maig, l'empresa de missatgeria i paqueteria **Glovo**, amb seu a Barcelona, va ser víctima d'un ciberatac. Els ciberatacants van poder accedir a la informació de clients i repartidors, i les dades robades es van posar a la venda a la *dark web*. En total eren **480 GB** de dades personals que incloïen: **nom i cognoms, adreça, correu electrònic, telèfon mòbil, data de naixement, DNI, comptes bancaris i dades de targetes de crèdit**, **contrasenyes en *hash***[19]...

I per si no n'hi havia prou, dues fuites més van afectar els usuaris de la xarxa social **LinkedIn**. Primer, es va identificar la venda de la informació de **500 milions d'usuaris** obtinguts utilitzant tècniques de *scrapping*. Les dades incloïen **nom**, **número de telèfon, gènere, correu electrònic, informació personal i professional**, entre d'altres[20]. Una mica més tard, es va detectar la venda de les dades de **700 milions d'usuaris**, és a dir, aproximadament el **92%** de la totalitat[21]. Per tenir una orientació de la magnitud de l'afectació a Catalunya, només cal tenir en compte que LinkedIn té gairebé **2 milions d'usuaris només a l'àrea metropolitana de Barcelona**[22]. En aquest cas, sembla que els cibercriminals van obtenir la informació a través d'un error a l'API de l'aplicació, la qual els va permetre realitzar descàrregues massives[23]. S'apunta que la filtració incloïa l'**estimació del rang salarial** de l'usuari fet per LinkedIn.

En els casos de **The Phone House** i **Glovo**, en el marc de la jurisdicció espanyola, les companyies van notificar a l'**AEPD** els incidents i l'entitat va obrir una **investigació**. L'AEPD també va confirmar la recepció de dues denúncies per la major filtració de dades de LinkedIn, tot i que la seu europea de la xarxa social està a Irlanda i li pertocarà a l'autoritat corresponent en aquest Estat estudiar el cas[24].

Els errors de configuració, les vulnerabilitats de les API i l'*scrapping* a xarxes socials disparen el volum de les fuites dades

El **nombre d'incidents** de fuites de dades registrats durant la 1a meitat de 2021 ha **baixat un 24%** respecte del mateix període de 2020, i el **nombre de registres** també ha baixat un **32%**. No obstant això, no tot són indicadors positius: el nombre de fuites de dades que superen els **100 milions de registres** ha **augmentat més d'un 30%** durant el 1r semestre del 2021 respecte del 1r semestre de 2020[25]. La tendència és clara: mentre que els incidents i el volum total de dades filtrades decreixen (de manera que evidencien una **millora de la**

[18] *https://internetsegura.cat/consells-fuita-dades-phone-house/*
[19] *https://computerhoy.com/noticias/tecnologia/datos-filtrados-usuarios-glovo-incluyen-tarjetas-credito-hackers-873771*
[20] *https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/*
[21] *https://blog.malwarebytes.com/awareness/2021/06/second-colossal-linkedin-breach-in-3-months-almost-all-users-affected/*
[22] *https://marketing4ecommerce.net/asi-son-los-usuarios-de-redes-sociales-en-espana-the-social-media-family/*
[23] *https://www.profesionalreview.com/2021/06/30/linkedin-datos/*
[24] *https://www.publico.es/actualidad/ciberderechos-privacidad-perfiles-linkedin-desnudo-brecha-seguridad-usuarios-imprudentes.html*
[25] *Agència de Ciberseguretat de Catalunya*

Les credencials són cada una de les dades de control que permeten identificar i autenticar un usuari i donar-li accés al sistema, d'acord amb els permisos que té assignats.

Les dades credencials més habituals són la combinació de nom d'usuari i contrasenya.

(font: Termcat)

Un infostealer és un troià dissenyat per a capturar informació d'un sistema.

(font: Termcat)

Un malware és un programari concebut específicament per a prendre el control d'un sistema informàtic, interferir en el seu funcionament normal, desestabilitzar-lo o danyar-lo.

(font: Termcat)

ciberseguretat), les fuites massives són més nombroses i permeten constatar el **creixement dels sistemes d'informació i les dades emmagatzemades**.

Els **errors de configuració** són un factor clau per entendre les fuites massives. Gairebé el **40%** dels registres exposats aquest trimestre han estat causats per errors de configuració, un percentatge que augmenta fins al **90%** en tot el semestre[26]. Així, es van descobrir **5.000 milions de** credencials emmagatzemades en un servidor ElasticSearch mal configurat. Eren una **recol·lecció** de diferents fuites i, irònicament, estaven custodiades per l'**empresa de ciberseguretat Cognyte** (EUA), que les utilitzava per alertar els seus clients[27]. El sector sanitari també s'ha vist impactat pels errors de configuració, un fet especialment greu a causa de la sensibilitat de les dades que s'hi tracten. El mes juny, es van detectar més de **1.000 milions de registres** de dades personals exposats sense protecció per part dels responsables de l'empresa **CVS Health** (EUA). Contenien informació relativa a la vacunació de la covid-19 i altres medicacions, així com el correu electrònic i altres dades personals dels pacients[28]. Val a dir, però, que aquests incidents van ser descoberts per investigadors i no hi ha constància que cap actor maliciós accedís a les dades.

Les **API** també són la causa de fuites massives. Si bé es tracta d'un mecanisme que permet l'intercanvi d'informació amb tercers, si presenta una vulnerabilitat pot permetre fer-ne un ús abusiu amb l'objectiu d'obtenir dades indiscriminadament. És el cas de les fuites de **Facebook** i **Linkedin**, comentades prèviament[29,30]. I també podria haver estat el cas de la companyia financera **Experian** (EUA), oferia amb una API que, per causa d'una vulnerabilitat, permetia que un atacant fes consultes massives sobre la situació creditícia dels ciutadans a partir del nom i adreça, una informació que és fàcil d'obtenir per a qualsevol ciutadà[31].

Un altre factor clau per entendre les fuites de dades massives són les bases de dades de dimensions colossals obtingudes amb tècniques de ***scrapping*** a partir de la **informació publicada a les xarxes socials**. Aquesta pràctica va ser l'origen d'una de les bases de dades de **Linkedin** posades a la venda[32], també comentada anteriorment, o la que aglutinava les dades d'**1,3 milions** d'usuaris de **ClubHouse**, compartida gratuïtament en un fòrum de la *dark web*[33]. La plataforma de botigues de comerç electrònic **Taobao**, propietat d'Alibaba, també va ser objecte de *scrapping* il·legal per part d'una empresa de màrqueting, la qual va capturar més de **1.000 milions de registres** de dades personals de clients. En aquest cas, els responsables van ser **detinguts i empresonats** per les autoritats xineses[34].

Val la pena destacar, també, com els ciberdelinqüents capturen les dades personals a través de l'ús de programaris maliciosos, com infostealers. En aquest sentit, uns investigadors van descobrir una base de dades exposada en un servidor obert al públic, que contenia dades robades per un *malware* indeterminat que s'havia propagat en **3,25 milions d'equips a través de còpies il·legals de programaris**. En total, incloïa **1,2 TB d'informació**, amb fitxers de text, *word* i *pdf*, així com dades de pagament, galetes de navegació, 1,1 milions de correus electrònics i 26 milions de credencials[35].

[26] *Agència de Ciberseguretat de Catalunya*
[27] *https://www.comparitech.com/blog/information-security/breach-database-leak/*
[28] *https://healthitsecurity.com/news/cvs-health-faces-data-breach1b-search-records-exposed*
[29] *https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/*
[30] *https://blog.malwarebytes.com/awareness/2021/06/second-colossal-linkedin-breach-in-3-months-almost-all-users-affected/*
[31] *https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/*
[32] *https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/*
[33] *https://cybernews.com/security/clubhouse-data-leak-1-3-million-user-records-leaked-for-free-online/*
[34] *https://www.cpomagazine.com/cyber-security/web-scraping-on-alibabas-taobao-resulted-in-data-leak-of-1-1-billion-records/*
[35] *https://vpnoverview.com/news/database-with-passwords-and-cookies-stolen-by-mystery-malware-discovered/*

L'atac de credential stuffing és un atac de força bruta en què l'accés al sistema es fa mitjançant la inserció automatitzada d'una gran quantitat de dades credencials obtingudes d'una manera fraudulenta.

(font: Termcat)

El password spraying és un mètode d'atac que consisteix a recollir el llistat d'usuaris de l'organització o empresa objectiu, i intentar entrar als comptes provant una mateixa contrasenya cada vegada amb un usuari diferent, per tal d'evitar que el compte en bloquegi l'accés i que l'administrador se n'assabenti.

El phishing és una pràctica fraudulenta que consisteix a simular una identitat falsa, sovint per suplantació de la identitat d'una persona o un organisme determinats, o bé per correu electrònic, o bé amb una trucada o bé per altres mitjans, amb l'objectiu d'incitar les possibles víctimes a fer una acció que permeti robar-los dades personals, habitualment dades credencials o números de targeta de crèdit.

(font: Termcat)

El mercadeig amb dades personals creix i facilita l'aparició de noves i més grans recopilacions

Els **cibercriminals**, quan obtenen **dades personals** a partir de l'explotació d'errors de configuració, *scrapping* o altres ciberatacs, les **posen a la venda o les comparteixen** en mercats i fòrums especialitzats en aquest tipus d'intercanvis, habitualment a la ***dark web***. Habitualment, abans de fer una venda, els ciberdelinqüents posen a disposició dels futurs compradors **mostres gratuïtes** de les dades ofertes, perquè puguin conèixer la "mercaderia".

Clarament, s'evidencia que **aquest mercadeig augmenta**. Les fuites de dades compartides a la *dark web* han crescut un **400%** durant el 2n trimestre respecte del 1r trimestre de 2021, i superen qualsevol registre previ (veure il·lustració 3)[36]. Alguns dels casos destacats han estat la venda de les dades dels **usuaris de 300 webs d'apostes** de Turquia per **800 dòlars**[37], o **13 milions** de registres dels clients del **banc mexicà Banorte**[38].

Aquestes bases de dades robades poden acabar **comprades o compartides gratuïtament** i, en alguns casos, acabar formant part de **grans recopilacions de dades de diferents fuites**. Aquestes recopilacions, a mesura que passa el temps i incorporen noves informacions, augmenten les seves dimensions. El 2019 s'identificava una recopilació anomenada **Collection**, que aglutinava uns **2.200 milions de credencials**[39]. Però, ara mateix, aquesta magnitud ha quedat àmpliament superada (veure il·lustració 4). El 1r trimestre de 2021 es va fer la troballa de la recopilació **COMB21**, amb **3.200 milions de credencials**[40]. I el 2n trimestre s'han superat els rècords: es van trobar **8.400 milions de credencials** en una recopilació anomenada **RockyYou2021**[41]. Paral·lelament, tot i que es tracta d'un cas diferent, també cal fer referència de nou a la recopilació de **5.000 milions de credencials** en mans de l'**empresa de ciberseguretat Cognyte**, oberta a Internet per error[42].

Aquestes bases de dades de credencials tan colossals constitueixen un autèntic problema, ja que permeten als posseïdors de realitzar **atacs massius** de *credential stuffing*, *password spraying* o *phishing*. I és que la relació entre **l'exposició de dades i els atacs posteriors pot ser força directa**. Per exemple, els clients de l'empresa **Ledger SAS** (França), desenvolupadora de solucions de programari i maquinari de criptomoneders, han experimentat intents de frau a través de ***phishing*** **després que l'empresa patís una fuita d'informació de 270.000 registres,** el desembre de 2020. Fins i tot, un client va rebre de regal un criptomoneder físic per emmagatzemar criptomonedes... Això sí, degudament manipulat per robar-les[43].

L'amenaça de publicar dades robades complementava el *ransomware*, però s'ha convertit en una pràctica d'extorsió principal

Els atacs de ***ransomware*** són protagonistes dels incidents de ciberseguretat més importants dels darrers temps. Inicialment, se centraven en el xifrat dels sistemes d'informació de la víctima i en sol·licitar un rescat per recuperar-los.

[36] *Agència de Ciberseguretat de Catalunya*
[37] *https://www.technadu.com/data-brokers-selling-user-details-300-turkish-betting-sites/277371/*
[38] *https://noticiasseguridad.com/hacking-incidentes/mas-de-13-millones-de-registros-pertenecientes-a-clientes-de-banorte-a-la-venta-en-dark-web-contacte-a-su-banco-para-prevenir-robo-y-fraude/*
[39] *https://www.genbeta.com/seguridad/siete-colecciones-3-500-millones-credenciales-filtradas-importante-que-nunca-aprender-a-proteger-tus-cuentas-online*
[40] *https://www.acfeinsights.com/acfe-insights/what-you-should-know-about-comb-data-leak*
[41] *https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/*
[42] *https://www.comparitech.com/blog/information-security/breach-database-leak/*
[43] *https://www.businessinsider.es/envian-falsos-dispositivos-ledger-otra-estafa-criptomonedas-886481*

La doble extosió és una modalitat de ransomware *que aplica una capa addicional a l'atac. Abans de xifrar les dades, descarrega la informació confidencial de la víctima i amenaça de publicar-la si no fa efectiu el rescat. Aquestes dues operacions (xifratge i amenaça) constitueixen la doble extorsió.*

L'RGPD és un reglament europeu de compliment obligatori a partir del 25 de maig de 2018 que, a Espanya, substitueix la Llei Orgànica de Protecció de Dades (LOPD).

Aquest reglament estableix canvis importants en relació a la normativa precedent: la responsabilitat proactiva de l'encarregat de tractar les dades i l'enfocament de la seguretat orientada al risc.

Però, darrerament, s'han especialitzat en la doble extorsió: el robatori de dades i l'amenaça de filtrar-les si no es realitza un pagament. Es practica en el **81% dels atacs de *ransomware***, un **5% de creixement** respecte del 1r trimestre[44].

Fixem-nos, de fet, que l'**extorsió** a través del **robatori de dades** s'ha convertit en una **pràctica efectiva per si sola**. Durant el 2n trimestre de l'any, s'han donat casos que evidencien que l'amenaça de publicació de dades confidencials robades té cada cop més importància. Així, un grup de ciberdelinqüents va robar dades de propietat intel·lectual a **Quanta**, un proveïdor d'Apple, el qual va desestimar fer cap pagament en concepte de rescat. Com a resposta, els ciberdelinqüents van decidir passar a extorsionar **Apple** directament, i exigir un pagament de **42 M€ per evitar la filtració de la informació robada**[45].

Anàlogament, després de la vulnerabilitat a la plataforma de compartició de fitxers **Accellion** de final de 2020[46], diverses organitzacions han rebut **missatges d'extorsió** que instaven a fer un pagament per evitar la publicació de les dades compromeses. La llista d'afectats és llarga: diverses **universitats dels EUA**[47], la cadena de benzineres nord-americana **RaceTrac Petroleum** (EUA), **Shell** (Països Baixos)[48]...

Ara bé, tot i que l'extorsió amb dades robades és una **pràctica cada vegada més estesa**, les xifres indiquen que l'**efectivitat decreix**. L'any 2020, el **65%** de les organitzacions extorsionades únicament amb el robatori d'informació van **optar per pagar**, una xifra que ha **baixat fins al 50%** durant el 2n trimestre de 2021[49]. En qualsevol cas, la capacitat d'extorquir les víctimes dependrà de la sensibilitat i el compromís de les dades robades: seran **objectiu** dels cibercriminals aquelles dades que puguin **impactar en la reputació de clients, proveïdors o socis**.

Les multes per incompliment de l'RGPD són cada cop més elevades i el cibercrim ho utilitza com a element d'extorsió a canvi de no revelar les fuites

L'**amenaça de filtrar dades personals robades** busca impactar les organitzacions des del punt de vista **reputacional**, però també des d'un punt de vista **econòmic**, a base d'exposar-les a les sancions de les agències de protecció de dades personals. Les fuites de dades personals poden tenir l'origen en un **incompliment de les mesures de seguretat** requerides per l'RGPD. Això és: pot comportar una **sanció** que, dit sigui de passada, és cada vegada més elevada.

D'una banda, cal destacar com el **segon motiu d'incompliments** de l'RGPD en l'àmbit europeu és la manca de **mesures tècniques** i d'organització per vetllar per la seguretat de la informació[50]. D'altra banda, el 2n trimestre s'han decretat unes quantes **sancions rècord** per incompliment de l'RGPD: **746 M€** a **Amazon** per incomplir els principis generals del reglament i **225 M€** a **WhatsApp** per incomplir les obligacions en matèria d'informació als afectats[51,52].

[44] *https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority*
[45] *https://www.wired.com/story/apple-ransomware-attack-quanta-computer/*
[46] *https://us-cert.cisa.gov/ncas/alerts/aa21-055a*
[47] *https://ucsdguardian.org/2021/04/11/accellion-cyber-attack-on-the-uc-network-prompts-new-personal-safety-measures/*
[48] *https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/*
[49] *https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority*
[50] *https://www.enforcementtracker.com/*
[51] *https://www.businessinsider.es/europa-condena-amazon-pagar-multa-746-millones-euros-907537*
[52] *https://www.euronews.com/next/2021/11/22/whatsapp-rewrites-its-europe-privacy-policy-after-a-record-225-million-gdpr-fine*

L'import ascendent de les sancions també es troba a l'Estat espanyol (veure il·lustració 5). A final de 2020, la sanció de **5 M€** al **BBVA** es va convertir en la multa més gran que s'havia imposat mai. Però, durant el 1r trimestre de 2021, aquesta xifra es va superar amb els **6 M€** a **CaixaBank** i els més de **8 M€** a **Vodafone**. Aquest ritme ascendent de sancions milionàries s'ha mantingut durant el 2n trimestre, amb els **3 M€** a **EDP Energia** i **1 M€** a **Equifax**.

Recomanacions

- **Els usuaris no han de revelar credencials a tercers, ni de forma escrita (en el cas del *phishing*) ni de forma oral (en el cas del *vishing*).**
- **Els usuaris han de compartir informació personal a les xarxes socials conscientment, ja que quedarà disponible públicament i podrà ser utilitzada per fer suplantacions, dirigir atacs de *phishing* o cometre fraus.**
- **Els administradors de sistemes, i si pot ser la resta d'usuaris, han de disposar d'accessos amb doble factor d'autenticació.**
- **Les organitzacions han d'emmagatzemar les dades personals amb xifratge segur per evitar que un intrús pugui robar la informació en text pla.**
- **Els responsables de sistemes han de realitzar auditories de seguretat periòdiques quan es realitzin canvis en els sistemes o en l'arquitectura. Així s'evitarà que la informació quedi exposada per errors de configuració.**
- **Les organitzacions han de realitzar anàlisis de riscos en matèria de privacitat (Avaluació d'Impacte de Dades Personals) per tal d'establir les mesures de protecció adequades a les dades personals.**
- **Les organitzacions, en cas de produir-se un incident que pugui afectar els drets i les llibertats de les persones, han d'informar l'autoritat competent en un termini màxim de 72 hores.**

Fets rellevants

- Les dades personals de més de 533 milions d'usuaris de Facebook a tot el món es van filtrar a la *dark web*. La fuita va afectar prop de 2 milions d'usuaris catalans, 1,3 dels quals podrien estar, a més, geolocalitzats. Les dades compromeses incloïen el número de telèfon, identificador d'usuari, nom, ubicació, etc. Tot indica que les dades es van extreure el 2019 amb *scrapping* explotant una vulnerabilitat[53].
- La companyia de productes i serveis de telefonia The Phone House va ser víctima d'un atac de *ransomware* amb robatori de dades. Com que es va negar a pagar el rescat, es van filtrar a la *dark web* les dades de 5,2 milions de clients, que incloïen 700.000 catalans. S'hi podien trobar noms, números de telèfon, dates de naixement, DNI, correus electrònics i, en algun cas, números d'IBAN, probablement d'aquelles persones que havien contractat assegurances o algun tipus de finançament[54].
- Un ciberdelinqüent va posar a la venda 500 milions de registres d'usuaris de LinkedIn, recopilats mitjançant tècniques de *scrapping*. Incloïen el nom, número de telèfon, gènere, correu electrònic i informació personal i professional, entre d'altres. La base de dades estava a la venda per diversos milers d'euros. Poc després, es posaven a la venda les dades de 700 milions d'usuaris, aproximadament el 92% de la totalitat de la xarxa social. En aquest cas, sembla que la informació es va obtenir a través d'un error a l'API de l'aplicació, la qual cosa va permetre realitzar descàrregues massives. La filtració incloïa l'estimació del rang salarial de l'usuari fet per LinkedIn[55,56,57].
- L'empresa de ciberseguretat Cognyte va exposar un servidor Elasticsearch amb més de 5.000 milions de registres d'usuaris amb noms, adreces electròniques i contrasenyes. Les dades eren un recull de les diverses fuites de dades (Tumblr, Rambler, Myspace, iMesh, Vk, MGM, Edmodo i Zoosk, entre d'altres) que utilitzaven, precisament, per alertar els seus clients[58].
- Es va detectar una col·lecció amb 8.400 milions de contrasenyes úniques, disponibles en un fòrum de ciberdelinqüents. La llista RockYou2021, un arxiu .txt de 100 GB, producte de la recopilació de múltiples fuites de dades dels darrers temps. L'origen rau en una fuita del 2009 de la xarxa social RockYou, que inicialment contenia 32 milions de comptes d'usuari i que, amb el temps, va créixer[59].
- Apple va ser extorsionada amb una quantitat de 42 M€ arran de la informació de propietat intel·lectual robada a un dels seus proveïdors: Quanta Computer (Taiwan). Un atac de *ransomware* per part del grup REvil (Sodinokibi) va suposar el robatori d'informació de productes que s'estaven desenvolupant. Quanta es va negar a negociar el rescat i els cibercriminals van dirigir-se directament a Apple[60].
- L'AEPD va multar amb 1 M€ l'empresa d'analítica de dades Equifax Ibérica. La sanció es va fixar després de 96 denúncies per incloure dades de persones vinculades a suposats deutes al Fitxer de Reclamacions Judicials i Organismes Públics, sense consentiment previ[61].
- L'AEPD va multar amb 3 M€ l'empresa EDP Energía S.A.U. (1,5 M€ per EDP Energía i 1,5 M€ per EDP Comercializadora). Es considera que no es prenien les mesures adients, ni tècniques ni organitzatives, per garantir que una persona que actua en nom d'una altra disposa de l'autorització adequada per contractar o per donar consentiment en l'ús de les dades personals. També es considera que la informació lliurada sobre el tractament de les dades i la seva justificació legal era insuficient[62].
- Noves sancions històriques del RGPD: a Luxemburg, es va sancionar Amazon amb 746 M€ per un mal ús de la recopilació de dades personals; a Irlanda, es va sancionar WhatsApp amb 225 M€ per falta de transparència en l'ús de les dades personals recollides[63,64].

[53] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/La-fuita-de-dades-de-Facebook-afecta-gairebe-dos-milions-dusuaris-catalans*
[54] *https://internetsegura.cat/consells-fuita-dades-phone-house/*
[55] *https://www.diaridegirona.cat/tecnologia/2021/04/08/dades-500-milions-dusuaris-linkedin/1098838.html*
[56] *https://blog.malwarebytes.com/awareness/2021/06/second-colossal-linkedin-breach-in-3-months-almost-all-users-affected/*
[57] *https://www.profesionalreview.com/2021/06/30/linkedin-datos/*
[58] *https://www.securityweek.com/cybersecurity-firm-exposes-breach-database-containing-5-billion-user-records*
[59] *https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/*
[60] *https://www.cultofmac.com/740367/ransomware-criminals-try-to-extort-apple-following-data-breach/*
[61] *https://www.dataguidance.com/news/spain-aepd-fines-equifax-%E2%82%AC1m-gdpr-lawfulness-accuracy*
[62] *https://edpb.europa.eu/news/news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-energia-sau-two-infractions-gdpr_en*
[63] *https://www.businessinsider.es/europa-condena-amazon-pagar-multa-746-millones-euros-907537*
[64] *https://www.euronews.com/next/2021/11/22/whatsapp-rewrites-its-europe-privacy-policy-after-a-record-225-million-gdpr-fine*

Les infraestructures crítiques són objectiu del *ransomware* i de grups APT que amenacen el subministrament de serveis essencials

Les infraestructures crítiques són objectiu d'atacs de *ransomware* o de grups APT, els quals amenacen el subministrament de serveis essencials i posen en risc l'estabilitat social i econòmica. Els atacs de DDoS, es consoliden com un mecanismes d'extorsió addicional i una amenaça pels serveis essencials. Després dels incidents paradigmàtics de Colonial Pipeline, JBS i el sistema sanitari d'Irlanda, l'OTAN i el G-7 fixen la lluita contra el cibercrim com una prioritat. Destaquen diverses operacions policials internacionals han acabat amb la detenció de grups cibercriminals i com la UE inclourà els serveis importants en la futura Directiva NIS 2.0 per protegir les cadenes de subministrament.

S'estima que els ciberatacs dirigits contra infraestructures crítiques hauran crescut un 80% durant el 2021, a causa de la proliferació d'atacs de *ransomware* i la intensa activitat de grups APT amb motivacions geopolítiques.

En el 2n trimestre, alguns ciberatacs han sobrepassat totes les línies vermelles: han impactat infraestructures crítiques i han posat en risc l'estabilitat social i econòmica. Són els incidents a l'oleoducte Colonial Pipeline, a la multinacional càrnica JBS i al sistema sanitari d'Irlanda. Els atacs de DDoS s'hi sumen, consolidant-se com una eina d'extorsió addicional per atacar serveis essencials de TI.

En resposta a aquests ciberatacs, l'OTAN els ha comparat amb els atacs armats, i el G-7 ha exigit accions de responsabilitat a Rússia. La UE inclourà altres entitats importants en la Directiva NIS 2.0, a més de les entitats essencials.

Les conseqüències es fan notar. Diverses operacions policials internacionals impacten el cibercrim, com ara les detencions dels responsables dels *ransomwares* Egregor i Clo. A l'Estat espanyol, s'han detingut grups criminals responsables de fraus cibernètics.

Aspectes clau:

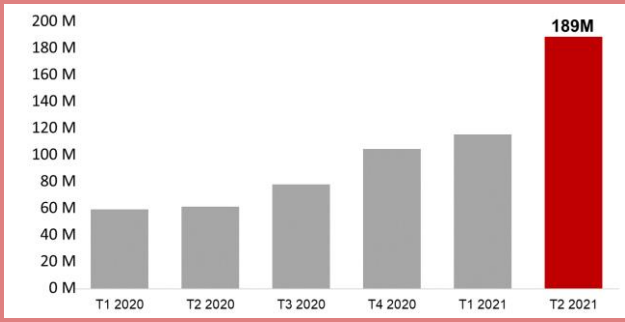
- **Els ciberatacs a infraestructures crítiques creixen motivats pel *ransomware* i el ciberespionatge**
- **Els atacs de *ransomware* traspassen línies vermelles amb els atacs a Colonial Pipeline, la productora de carn JBS i el sistema sanitari d'Irlanda**
- **Els atacs de DDoS segueixen els passos del *ransomware*: més recursos, objectius més ambiciosos i grans impactes en serveis essencials**
- **Arran de l'escalada en la gravetat dels ciberatacs, els governs fixen la ciberseguretat com a prioritat**
- **Els cibercrim ja no actua impunement: grans operacions policials persegueixen els ciberdelinqüents amb els operadors de *ransomware* en el punt de mira**

Baròmetre

Els ciberatacs a infraestructures crítiques han esdevingut cada com més habituals. Posen en risc els serveis essencials i amenacen l'estabilitat econòmica i social. Al darrere, hi ha els grups de *ransomware*, a la recerca de rescats milionaris, i els grups APT, amb motivacions geopolítiques.

Les temptatives d'atacs de *ransomware* augmenten un 60% en el 2n trimestre

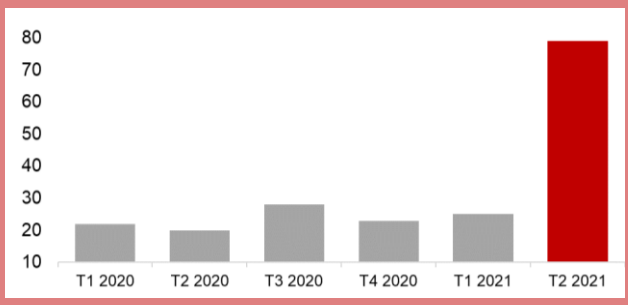
Els atacs de *ransomware* són la principal amenaça per a l'activitat de les infraestructures crítiques. Doncs bé, la 1a meitat de 2021, el nombre d'intents d'atac de *ransomware* ha superat un 150% la xifra de la 1a meitat de 2020. Només durant el 2n trimestre, s'han detectat 189 milions d'intents d'atacs de *ransomware*, un augment de més del 60% respecte del 1r trimestre.



Il·lustració 7. Intents d'atac de ransomware *en l'àmbit mundial*[65].

Els ciberatacs als subministraments públics es disparen

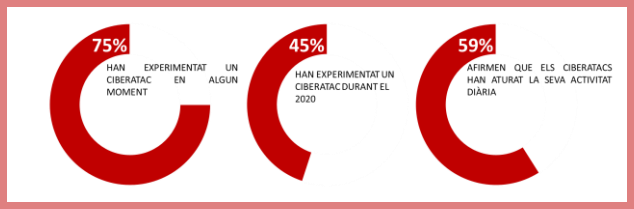
En el 2n trimestre de 2021, els incidents cibernètics que han impactat els subministraments públics (aigua, electricitat i gas), proveïts per operadors essencials d'infraestructures crítiques, han crescut un 300% respecte del trimestre anterior. L'incident a l'oleoducte Colonial Pipeline n'és un bon exemple.



Il·lustració 5. Presència als mitjans especialitzats d'incidents cibernètics amb afectació als subministraments públics (font: Agència).

La meitat dels operadors d'infraestructures crítiques van patir un ciberatac el 2020

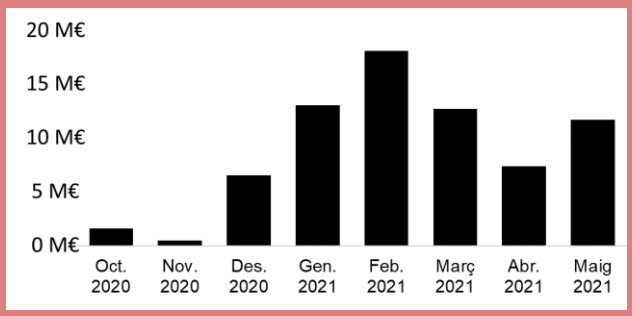
Una enquesta a empreses proveïdores de serveis essencials ha permès determinar que, durant el 2020, pràcticament una de cada dues va viure algun ciberatac. L'impacte d'aquests ciberatacs pot ser crític i, de fet, el 59% de les empreses atacades afirmen que els han provocat aturades d'activitat. Així, es calcula que el temps mitjà per recuperar la normalitat supera els set mesos.



Il·lustració 6. Enquesta sobre els ciberatacs que han patit les companyies que operen infraestructures critiques[66].

Els atacs de *ransomware* a infraestructures crítiques permeten obtenir guanys milionaris

Un dels grups més actius i més prolífics en matèria de ciberatacs contra infraestructures crítiques ha estat DarkSide, responsable de l'atac a l'oleoducte Colonial Pipeline (EUA) o al distribuïdor de productes químics Brenntag (Alemanya). Amb aquests atacs, ha aconseguit que un 47% de les seves víctimes optessin per pagar el rescat. Així, en nou mesos, ha obtingut més de 70 M€, només superat per grups també responsables d'incidents igualment rellevants, com ara Ryuk (130 M€), GandCrab (130 M€) o REvil (86 M€)[67]. Curiosament, DarkSide diu que no vol atacar ni el sector sanitari, ni governs ni entitats sense ànim de lucre.



Il·lustració 10. Evolució dels ingressos de DarkSide[68].

[65] *https://paymentyearbooks.com/blogs/news/ransomware-attacks-surge-by-over-150-in-2021*
[66] *https://www.ustelecom.org/research/2021-cybersecurity-survey-critical-infrastructure-small-and-medium-sized-businesses/*
[67] *https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/*
[68] *https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin*

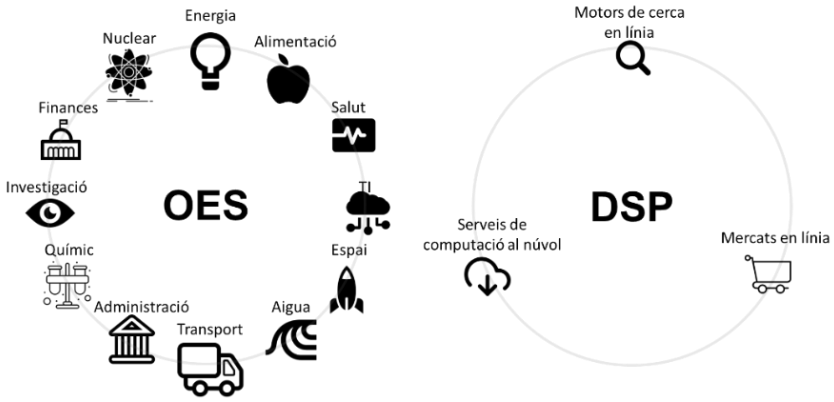
Una APT (Advanced Persistent Threat), o amenaça persistent avançada, és un atac a gran escala, subreptici, sofisticat, continu i dirigit a una entitat específica.

(font: Termcat)

Els ciberatacs a infraestructures crítiques proliferen motivats pel *ransomware* i el ciberespionatge

Els **ciberatacs a infraestructures crítiques** van créixer un **50%** el 2020 i s'estima que creixeran un **80%** aquest 2021[69]. Abans, els ciberatacs a infraestructures crítiques estaven dirigits als sectors energètics, industrials o de defensa, però arran de la **pandèmia** i amb la **irrupció del *ransomware***, les prioritats han canviat[70].

Els atacs de *ransomware* incrementen l'**efectivitat** quan **la víctima no pot fer front a una aturada** de l'activitat i es veu forçada a pagar el rescat. Així, els ciberatacs actuals es dirigeixen contra **administracions públiques, el sistema sanitari, la distribució d'aigua i aliments, els sistemes de transport**... Tots ells són operadors de serveis essencials que, en cas d'una aturada, podrien posar en **risc l'equilibri social i econòmic** (veure il·lustració 8).



Il·lustració 11. Operadors de Serveis Essencials (OES) i Proveïdors de Serveis Digitals (DSP) afectats per la Directiva NIS i les seves transposicions nacionals.

Les infraestructures crítiques que fan possible el funcionament dels serveis essencials han esdevingut un objectiu prioritari. L'operador del *ransomware* **DarkSide** ho sap molt bé: ha aconseguit més de **70 M€** en **8 mesos**, i que el **47% de les seves víctimes paguessin** un rescat (veure il·lustració 10)[71]. Entre aquestes víctimes hi ha l'operador de l'oleoducte **Colonial Pipeline** (EUA) o l'empresa de distribució de productes químics **Brenntag** (Alemanya) [72].

Tanmateix, els grups cibercriminals que malden per lucrar-se econòmicament amb atacs de *ransomware* no són l'única amenaça. En el món actual, els **conflictes entre els estats** tenen un reflex a **Internet**: els rivals geopolítics cerquen de **perjudicar l'adversari amb atacs cibernètics a les seves infraestructures crítiques**. Sovint, aquests atacs es duen a terme a través de grups APT que, amb el patrocini dels estats, esdevenen el braç executor a la xarxa. Així, per exemple, l'**Índia** investiga si l'apagada que va viure la ciutat de Bombai l'octubre del 2020 està **vinculada a un ciberatac** de la Xina i motivat per un litigi fronterer. L'atac que va deixar sense electricitat 18 milions de persones durant 12 hores va afectar els serveis de trens, el mercat de valors... Els hospitals van haver de recórrer a generadors d'emergència per poder operar amb normalitat[73].

[69] *https://diarioti.com/aumentan-los-ataques-de-ransomware-contra-infraestructura-critica/116703*
[70] *https://diarioti.com/aumentan-los-ataques-de-ransomware-contra-infraestructura-critica/116703*
[71] *https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin*
[72] *https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/*
[73] *https://economictimes.indiatimes.com/news/politics-and-nation/is-the-mumbai-blackout-last-year-connected-to-the-ladakh-standoff/articleshow/81277610.cms*

La triple extorsió és un ciberatac que consisteix a extorsionar la víctima amb la combinació de tres pràctiques: les dues corresponents a la doble extorsió més un atac de DDoS en el qual s'exigeix un pagament a canvi d'aturar-lo.

Els atacs de *ransomware* traspassen línies vermelles amb els atacs a Colonial Pipeline, la productora de carn JBS i el sistema sanitari d'Irlanda

Els ciberatacs a infraestructures crítiques han esdevingut un fet habitual (veure il·lustració 9), però **tres incidents han destacat especialment**. La raó és ben diàfana: han posat de relleu les **terribles conseqüències** que un incident cibernètic pot provocar.

L'atac a l'**operador de l'oleoducte Colonial Pipeline** (EUA) ha estat un cas especialment rellevant pel gran impacte. La companyia va haver de **pagar un rescat de gairebé 4 M€** per recuperar l'activitat després de ser víctima de *ransomware*. L'FBI va atribuir l'atac al grup **DarkSide**, que opera des de Rússia. Tot i que el grup va publicar un comunicat en què afirmava que el seu objectiu era "guanyar diners i no generar problemes a la societat", van causar una autèntica **crisi per la manca de benzina en quatre estats**[74]. I no ha estat l'única companyia del negoci dels oleoductes afectada: l'empresa **LineStar Integrity Sevices**, dedicada a les auditories, compliment i manteniment de les tecnologies en aquest sector, va rebre un atac de *ransomware* en el qual es van robar 70 GB d'arxius interns que es van publicar a la *dark web*[75].

Poc després, l'empresa brasilera **JBS SA**, una de les del sector del **subministrament càrnic** més grans del món, va ser atacada per un *ransomware* atribuït al grup **REvil**. JBS té 150 plantes en 15 països, més de 150.000 empleats i, si bé té la seu al Brasil, les plantes afectades estaven als EUA (on se subministra el 25% de la carn), el Canadà i Austràlia. L'atac va fer **témer que hi haguessin problemes en el subministrament de carn, així com un augment dels preus**. Entre els seus clients hi ha supermercats, cadenes de restaurants i distribuïdors de serveis d'aliments. Finalment, la companyia va **pagar al voltant de 10 M€ de rescat**, pressionada per la demanda dels clients i dels països afectats. A més, també es va confirmar el robatori d'informació[76].

Els ciberatacs contra el sector de la salut també han estat protagonistes negatius. L'atac de *ransomware* contra els **serveis sanitaris d'Irlanda**, el Health Service Executive (HSE), va afectar diversos serveis de diagnòstic, va obligar a aturar el procés de tests de la covid-19 i va forçar uns quants hospitals a cancel·lar alguns serveis d'emergència. Segons el ministre de Salut d'Irlanda, l'atac el va dur a terme un **grup de cibercriminals internacionals**, que va aprofitar una **vulnerabilitat de dia zero** que hi havia en els sistemes de tots els centres locals i nacionals. Arran de l'atac, el sistema sanitari irlandès no va poder recuperar la normalitat durant unes quantes setmanes[77].

Els atacs de DDoS segueixen els passos del *ransomware*: més recursos, objectius més ambiciosos i grans impactes en serveis essencials

Com s'avançava en l'informe del 2n semestre de 2020, la triple extorsió segueix l'embranzida creixent. Si bé és cert que s'han identificat **menys atacs DDoS**, aquests s'orienten a **crear impactes greus i perllongats en el temps per tal de poder exigir un rescat**[78]. Destaca el grup APT Fancy Lazarus, el qual s'ha dedicat a dirigir atacs DDoS a organitzacions dels EUA en els quals exigia el pagament d'uns 2 *bitcoins*[79].

[74] *https://actualidad.rt.com/actualidad/392021-colonial-pipeline-pagar-millones-hackeo*
[75] *https://www.databreaches.net/ransomware-struck-another-pipeline-firm-and-70gb-of-data-leaked/*
[76] *https://www.bbc.com/news/world-us-canada-57318965*
[77] *https://cisomag.eccouncil.org/irish-health-services-shut-down-after-being-hit-by-ransomware-attack/*
[78] *https://securelist.com/ddos-attacks-in-q2-2021/103424/*
[79] *https://www.link11.com/en/blog/threat-landscape/new-wave-ddos-extortion-campaigns-fancy-lazarus/*

Un atac de DDoS, o de denegació de servei distribuït, és un atac en què s'envien una gran quantitat de peticions falses de manera simultània a través de grups d'usuaris o de xarxes d'ordinadors zombi, distribuïts a diferents zones geogràfiques.

(font: Termcat)

Una botnet és grup d'ordinadors zombi que són controlats des d'un mateix servidor i es fan actuar conjuntament. El terme prové de l'acrònim en anglès de les paraules robot *(*bot*) i* net *(xarxa); cada dispositiu que forma part de la mateixa és anomenat bot o zombi.*

(font: Termcat)

El cibercrim es dota de nous recursos per aconseguir aquests atacs de DDoS. D'una banda, se **segueixen creant noves *botnets***, com ara Simps, especialitzada en infectar IoT vulnerables per perpetrar atacs de DDoS. Aquestes s'han d'afegir a les diferents *botnets* identificades durant el 1r trimestre: FreakOut per a Linux, Matryosh per a Android i una nova variant de Mirai. Val a dir que la proliferació de programaris maliciosos de tipus *botnet* es deu a la publicació, el 2016, del codi de la *botnet* Mirai[80]. D'una altra banda, s'ha detectat com **els cibercriminals busquen i descobreixen nous serveis i protocols per amplificar els atacs de DDoS**, o sigui, noves maneres d'utilitzar els elements connectats a Internet per multiplicar el tràfic de dades i redirigir-lo contra un objectiu determinat amb fluxos de fins a **2 Tbps**[81].

Així, els atacs de DDoS esdevenen **més intel·ligents**: a) **complexos**, perquè són més difícils de detectar, i b) **dirigits**, perquè atacaquen amb precisió objectius concrets. Així doncs, els atacs de DDoS esdevenen eines versàtils com a complement del ***ransomware***. Un exemple: abans de l'atac de *ransomware* al sistema sanitari públic irlandès (HSE), hi va haver dos o tres atacs de DDoS. Tot i que la relació no està demostrada, és més que probable que fos una **tècnica de distracció**[82].

Els atacs de DDoS, igual que els de *ransomware*, també apunten a les **infraestructures crítiques**. En aquest sentit, destaquen els **atacs a proveïdors de serveis d'Internet** (ISP). Així, s'ha vist com un atac a l'empresa de telecomunicacions ASAC, amb el *ransomware* Zeppelin, deixava inoperatius els webs del Tribunal de Cuentas, el Consejo de Seguridad Nuclear i diversos ajuntaments espanyols[83]. I, anàlogament, un atac de DDoS dirigit als proveïdors d'ISP Belnet va bloquejar els webs i l'accés a Internet de més de 200 organitzacions de Bèlgica, incloent-hi el Parlament i ministeris governamentals[84]. Es constata, doncs, que els ISP són objectiu d'atacs DDoS. Un altre cas: el proveïdor Ireland Nova (Irlanda) també va deixar d'oferir serveis arran d'un atac DDoS[85].

També són objectiu dels atacs de DDoS les institucions educatives que, actualment, depenen d'Internet per al desenvolupament de les seves operacions. A França, la plataforma del **programa Ma classe a la maison** va ser objecte de ciberatacs que en van malmetre el funcionament. Tot i que encara no està confirmat, probablement es tractava d'atacs de DDoS, malgrat que es va acusar el govern de mala preparació[86].

Les plataformes de videojocs també són un objectiu prioritari dels atacs de DDoS. Els atacs als servidors de Titanfall i Titanfall 2 van afectar l'experiència dels jugadors. L'amenaça és tan real que la nova versió del videojoc Apex Legends, en cas d'atac, expulsa els jugadors i els compensa per les pèrdues ocasionades[87].

[80] *https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/*
[81] *https://securelist.com/ddos-attacks-in-q1-2021/102166/*
[82] *https://www.irishtimes.com/news/health/bitcoin-ransom-will-not-be-paid-following-cyber-attack-on-hse-computer-systems-1.4564957*
[83] *https://www.abc.es/espana/abci-ciberataque-deja-inoperativas-webs-tribunal-cuentas-consejo-seguridad-nuclear-y-varios-ayuntamientos-202105110956_noticia.html*
[84] *https://www.zdnet.com/article/this-massive-ddos-attack-took-large-sections-of-a-countrys-internet-offline/*
[85] *https://securelist.com/ddos-attacks-in-q2-2021/103424/*
[86] *https://techxplore.com/news/2021-04-french-homeschooling-hackers-russia-china.html*
[87] *https://www.nme.com/news/gaming-news/respawn-updates-apex-legends-to-defend-players-against-ddos-attacks-2967418*

Arran de l'escalada en la gravetat dels ciberatacs, les institucions governamentals s'alien amb la ciberseguretat com a prioritat

Queda clar com un **ciberatac contra una infraestructura crítica** pot provocar un greu **impacte** en el subministrament de **serveis essencials** per a la societat. Conscients d'aquesta amenaça, **institucions governamentals** de tot el món estan decidides a actuar[88].

Diverses institucions governamentals han mostrat públicament i de manera efusiva el seu posicionament. L'**OTAN** va emetre un comunicat en què comparava els atacs cibernètics amb els atacs armats, i afirmava la disposició a "emprar la gamma completa de capacitats en tot moment per **dissuadir activament, defensar-se i contrarestar tot l'espectre d'amenaces cibernètiques**, incloses les realitzades com a part de campanyes híbrides, d'acord amb el dret internacional"[89]. En la mateixa línia, els països del **G-7** van exigir que Rússia prengués accions contra grups cibercriminals que hi havia al darrere dels atacs de *ransomware*. I, per la seva banda, el **Regne Unit** va exigir a Moscou que aturés el comportament desestabilitzador i les activitats malicioses[90]. Val a dir que el **president rus**, Vladimir Putin**,** va refusar totes les acusacions sobre la responsabilitat del seu país en els atacs cibernètics, i va al·legar que eren acusacions infundades i sense cap mena d'evidència[91].

A l'altra banda de l'oceà, la **Casa Blanca** va presentar un programa per a incrementar la seguretat de les infraestructures crítiques davant del que considera com una "amenaça creixent"[92]. Precisament, els **EUA i el Regne Unit** col·laboraran conjuntament per **liderar la ciberseguretat mundial** amb l'objectiu de protegir les seves infraestructures de ciberatacs. Entre altres accions, mantindran una **llista negra** de ciberatacants, iniciaran **procediments sancionadors** i dirigiran **accions ofensives** per inhabilitar-los. Ambdós governs van anunciar la revisió de la Carta Atlàntica, signada durant la 2a Guerra Mundial, per incloure els nous reptes en matèria de ciberseguretat[93].

La **cooperació internacional** és clau per fer front al *ransomware*, ja que les bandes cibercriminals aprofiten les fronteres i l'entramat financer global per actuar impunement. Així, cal destacar iniciatives com la creació de l'aliança ***Ransomware Task Force***, liderada per l'organització sense ànim de lucre IST (Institute for Security + Technology), que té l'objectiu d'**interrompre el negoci dels ciberdelinqüents** en les diferents fases de l'acció delictiva associada al *ransomware*. Engloba **60 entitats públiques i privades** de perfils diversos, com ara desenvolupadors de programari, proveïdors de ciberseguretat, companyies de serveis financers, organitzacions sense ànim de lucre, institucions acadèmiques i agències governamentals. Destaquen alguns grans noms com el Departament de Justícia dels EUA, l'Europol, el National Cybersecurity Center (NCSC) del Regne Unit, Amazon, Cisco, FireEye i Microsoft[94].

A la **UE**, aquests ciberatacs a infraestructures crítiques han arribat enmig del desenvolupament de la denominada **Directiva NIS 2**[95]. Aquesta revisió de l'actual directiva NIS **planteja incorporar** un marc europeu unificat de mesures de ciberseguretat, a més de les entitats essencials que operen en sectors crítics (actualment ja incloses en la Directiva NIS), **altres entitats importants**. L'objectiu és **protegir les infraestructures crítiques** dels atacs a la cadena de

La Directiva NIS (en anglès, Network and Information Security*) és una legislació que entrà en vigor l'agost de 2016 per millorar la seguretat en xarxes i sistemes d'informació pels Estats de la Unió Europea. Principalment, aquesta legislació estableix cinc mesures concretes que han d'assolir tots els estats membres: una estratègia nacional, un grup de cooperació entre els estats membres, una xarxa CSIRT, unes condicions de seguretat per a operadors de serveis essencials i proveïdors de serveis digitals, i unes obligacions de ciberseguretat per a les autoritats nacionals.*

L'atac a la cadena de subministrament és un ciberatac en què el ciberdelinqüent ataca alguna de les parts de la cadena de producció d'un producte tecnològic amb l'objectiu d'afectar tots aquells que en facin ús.

[88] *https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks*
[89] *https://www.theregister.com/2021/06/15/nato_final_communique_cyber_policy/*
[90] *https://www.reuters.com/world/europe/g7-demand-action-russia-cybercrimes-chemical-weapon-use-2021-06-13/*
[91] *https://www.nytimes.com/es/2021/06/18/espanol/ciberataques-rusos.html*
[92] *https://www.segurilatam.com/actualidad/infraestructuras-criticas-casa-blanca-los-ataques-de-ransomware-se-intensificaran_20210608.html*
[93] *https://www.databreachtoday.in/uk-plans-for-enhanced-cybersecurity-role-a-16868*
[94] *https://threatpost.com/gov-task-force-ransomware-economy/165715/*
[95] *https://ec.europa.eu/commission/presscorner/detail/es/ip_20_2391*

Una botnet és grup d'ordinadors zombi que són controlats des d'un mateix servidor i es fan actuar conjuntament. El terme prové de l'acrònim en anglès de les paraules robot *(*bot*) i* net *(xarxa); cada dispositiu que forma part de la mateixa és anomenat bot o zombi.*

(font: Termcat)

subministrament[96]. A això cal sumar-hi el fet que el 2023 entrarà en funcionament una unitat anomenada **Joint Cyber Unit**, en la qual hi participen alguns sectors públics i privats dels estats membres. El seu objectiu és millorar les defenses i assegurar una resposta europea coordinada davant d'una crisi cibernètica[97].

Els cibercrim ja no actua impunement: grans operacions policials persegueixen els ciberdelinqüents amb els operadors de *ransomware* en el punt de mira

Gràcies a les aliances internacionals i a les accions que s'estan duent a terme des dels sectors públic i privat, **la lluita contra els grans operadors cibercriminals ha pres una nova dimensió**. El 1r trimestre van destacar les operacions policials exitoses contra el *ransomware* **Netwalker**[98], la *botnet* **Emotet** i els **mercats Darknet** i **JokerStash**. Durant el 2n trimestre, noves operacions han estat dirigides contra els operadors de *ransomware*.

Així, gràcies a la col·laboració entre organitzacions del sector públic i privat, tres presumptes membres del càrtel del *ransomware* **Egregor** van ser detinguts a Ucraïna, en una ofensiva duta a terme per les autoritats franceses i ucraïneses[99]. Poc després, precisament també a Ucraïna, les autoritats policials van anunciar que havien arrestat sis presumptes membres de l'operador de *ransomware* **Clop**. Les autoritats van afirmar que els acusats estaven involucrats en ciberatacs dirigits contra organitzacions de Corea del Sud i els EUA, entre les quals hi havia les **universitats de Stanford**, **Maryland** i **Califòrnia**[100].

Més enllà dels esforços internacionals en la lluita contra el *ransomware*, cal destacar les **actuacions policials a Catalunya** contra el cibercrim. Així, la Policia Nacional espanyola va detenir, a la comarca del **Baix Camp**, set persones investigades per diverses **estafes arreu de l'Estat**. Es dedicaven a perpetrar fraus a través de coneguts portals web per a la compravenda i lloguer d'habitatges: hi anunciaven **falses ofertes de lloguer de vacances** a localitats turístiques espanyoles, per a les quals demanaven una paga i senyal[101]. En paral·lel, una complexa recerca dels Mossos d'Esquadra va aconseguir detenir a **Reus** quatre presumptes autors d'una **estafa** de gairebé **70.000 €** a diversos clients d'una mateixa **entitat bancària**. Les víctimes havien fet ús d'un **codi SMS** per extreure diners d'un **caixer automàtic**, però es van trobar que algú altre s'havia anticipat des d'un altre caixer. Gràcies a les investigacions, es va identificar que el cervell de la trama era un empleat dels serveis informàtics bancaris amb accés als codis per validar reintegraments des de caixers automàtics[102].

[96] *https://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari19-2021-arteaga-evaluacion-y-revision-de-la-directiva-nis-2-0*
[97] *https://www.securityweek.com/eu-announces-new-joint-cyber-unit-protect-against-critical-attacks*
[98] *https://www.securityweek.com/netwalker-ransomware%E2%80%99s-sites-seized-law-enforcement*
[99] *https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html*
[100] *https://www.databreachtoday.eu/ukraine-arrests-6-clop-ransomware-operation-suspects-a-16885*
[101] *https://catalunyadiari.com/tarragonadigital/successos/policia-nacional-desarticula-dos-grups-estafadors-baix-camp*
[102] *https://www.lavanguardia.com/local/tarragona/20210428/7384709/estafa-entidad-bancaria-reus-detenidos-clientes.html*

Recomanacions

- **Les organitzacions han d'elaborar anàlisis de riscos periòdiques i plans estratègics en matèria de ciberseguretat i resiliència per fer front als canvis socials i tecnològics constants.**
- **Les organitzacions han de disposar d'un pla de continuïtat de negoci i un pla de recuperació de desastres, i han de validar que ha estat verificat a través de simulacres que impliquin els proveïdors.**
- **Les organitzacions han de promoure periòdicament programes de seguretat de la informació a tots els socis, empleats, col·laboradors, clients i proveïdors.**
- **Les organitzacions han de protegir i custodiar les còpies de seguretat, tot fent-les fora de línia i amb la garantia que estiguin lliures de *malware*.**
- **Les organitzacions han d'emmagatzemar les dades personals amb xifratge segur per evitar que un intrús les pugui robar en text pla.**
- **Les organitzacions s'han d'aproximar a models de confiança zero, amb la segregació dels serveis interns de la xarxa empresarial i amb la disposició de protecció perimetral.**
- **Els responsables de TI han de vetllar per mantenir actualitzats els sistemes operatius i el programari, així com els *antimalware* o antivirus, amb els darrers patrons de codi maliciós.**
- **Els responsables de TI han de mantenir actualitzats i avaluar la seguretat dels accessos remots, en especial RDP, VPN i Citrix.**
- **Els administradors de sistemes, i si és possible tota la resta d'usuaris, han de disposar d'accessos amb doble factor d'autenticació.**

Fets rellevants

- Colonial Pipeline va poder reiniciar les operacions després de pagar el rescat per un atac de *ransomware*. L'operadora de la xarxa d'oleoductes de l'est dels EUA es va veure obligada a pagar un rescat de 4 M€ en un atac de *ransomware* que l'FBI va atribuir al grup DarkSide, que opera des de Rússia. L'aturada de més de cinc dies en el subministrament de combustible va provocar una crisi a quatre estats nord-americans. El vector d'atac podria estar relacionat amb la manca de doble factor d'autenticació (2FA) en un compte de VPN en desús. Val a dir que, posteriorment, es va recuperar una part dels diners pagats a través del compromís del criptomoneder dels atacants[103]
- La brasilera JBS SA va ser víctima d'un atac de *ransomware* atribuït al grup REvil (o Sodinokibi). JBS té 150 plantes a 15 països i més de 150.000 empleats. Les plantes afectades estaven als EUA, el Canadà i Austràlia. També es va confirmar el robatori d'informació de la companyia. L'atac va fer témer per la manca de subministrament de carn i l'augment dels preus, ja que entre els clients de JBS hi ha supermercats, cadenes de restaurants i distribuïdors de d'aliments. Finalment, la companyia va pagar al voltant de 10 M€ de rescat[104].
- L'Irish Health Service Executive (HSE) va comunicar que un atac de *ransomware* va afectar diversos serveis de diagnòstic, va obligar a aturar el procés de tests de la covid-19 i va forçar uns quants hospitals a cancel·lar alguns serveis d'emergència. Segons el ministre, l'atac el va dur a terme un grup de cibercriminals internacional. Es va apuntar que el grup va aprofitar una vulnerabilitat de dia zero desconeguda en els sistemes de tots els centres locals i nacionals. L'organització no preveu que es pugui recuperar la normalitat durant unes quantes setmanes. A més a més, a final de maig, es van detectar 520 registres de dades personals de pacients publicades[105].
- El distribuïdor de productes químics Brenntag (Alemanya) va pagar un rescat de 3,5 M€ en un atac del grup de *ransomware* DarkSide. Amb aquest pagament es volien obtenir les claus de xifratge i evitar la filtració de 150 GB de dades robades a Brenntag North America, filial de l'empresa alemanya. Sembla que els atacants van obtenir l'accés a la xarxa corporativa després de comprar unes credencials a la *dark web*[106].
- L'aeroport internacional de Narita, molt a prop de Tòquio, es va veure afectat per una important fuita de dades. Els atacants van robar dades de control de trànsit aeri, horaris de vols i informació sobre operacions comercials. El robatori es va produir per un accés no autoritzat a la plataforma al núvol de compartició d'arxius ProjectWEB de Fujitsu, utilitzada per agències japoneses. Els atacants van obtenir més de 76.000 adreces de correu electrònic i informació de projectes de diverses agències governamentals japoneses[107].
- Aparentment, Israel va confirmar les acusacions d'estar al darrere d'un atac cibernètic a la principal instal·lació nuclear de l'Iran: el reactor de Natanz. El ciberatac es va dur a terme en un moment crític, en el qual es pretenia accelerar la producció d'urani enriquit. L'atac va provocar un tall d'energia elèctrica al país. El primer ministre israelià va declarar que "la lluita contra l'Iran, col·laboradors i els esforços d'armament és una missió enorme"[108].
- L'OTAN va emetre un comunicat en què comparava els atacs cibernètics amb els atacs armats. En el comunicat s'assegurava que està disposada a "emprar la gamma completa de capacitats en tot moment per dissuadir activament, defensar-se i contrarestar tot l'espectre d'amenaces cibernètiques, incloses les realitzades com a part de campanyes híbrides, d'acord amb el dret internacional". El document considera com a amenaces tant Rússia com la Xina: la primera està etiquetada com a "agressiva"; la segona, "enèrgica" i que "presenta desafiaments sistèmics"[109].

[103] *https://actualidad.rt.com/actualidad/392021-colonial-pipeline-pagar-millones-hackeo*
[104] *https://www.theverge.com/2021/6/3/22466003/jbs-cyberattack-fbi-revil-sodinokibi-criminal-group*
[105] *https://cisomag.eccouncil.org/irish-health-services-shut-down-after-being-hit-by-ransomware-attack/*
[106] *https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/*
[107] *https://www.zdnet.com/article/various-japanese-government-entities-had-data-stolen-in-cyber-attack-report/*
[108] *https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility*
[109] *https://abcnews.go.com/Politics/us-nato-expose-china-malicious-cyber-activities/story?id=78919558*

El *ransomware* explota el pagament de rescats per part de les ciberassegurances i el model de negoci d'aquestes se'n ressent

Les organitzacions consideren que els ciberincidents constitueixen una de les seves principals amenaces i recorren a la contractació de pòlisses de ciberassegurança. El cibercrim ha atacat amb *ransomware* les organitzacions ciberassegurades per sol·licitar rescats elevats, i les empreses asseguradores s'han vist obligades a apujar el preu de les primes o a desestimar el pagament del rescat. En aquest context, el sector educatiu ha estat un objectiu especialment atacat durant el 2n trimestre.

Amb la pandèmia, les organitzacions han accelerat la seva transformació digital i han canviat les seves preocupacions: a l'Estat espanyol, un 58% de les organitzacions considera els ciberincidents com la principal amenaça. Per aquest motiu, moltes sol·liciten serveis de ciberassegurança.

Els sinistres de les asseguradores causats per *ransomware* creixen any rere any de forma exponencial i, en conseqüència, també creix l'import de les primes de ciberassegurancça. Es constata que el cibercrim s'ha beneficiat del pagament de rescats a través d'assegurances per atacar les empreses que disposen d'aquest servei i exigir rescats elevats.

En aquest context, els cibercriminals fins i tot han atacat asseguradores per obtenir llistes de clients ciberassegurats i perquè, òbviament, disposen del capital per fer front al rescat. Aquest trimestre, la companyia CNA Financial ha fet el pagament més elevat que es coneix fins avui: 34 M€.

Les asseguradores han vist que minvaven les reserves de capital per fer front als ciberriscos, i s'han vist obligades a augmentar les primes entre un 25% i un 40%, o a deixar de cobrir els pagaments per atacs de *ransomware*.

En paral·lel, aquest trimestre, el sector educatiu ha destacat pel gran nombre de ciberatacs rebuts. No és estrany, doncs, que en aquest cas les pòlisses de ciberassegurança hagin augmentat un 60%.

Aspectes clau:

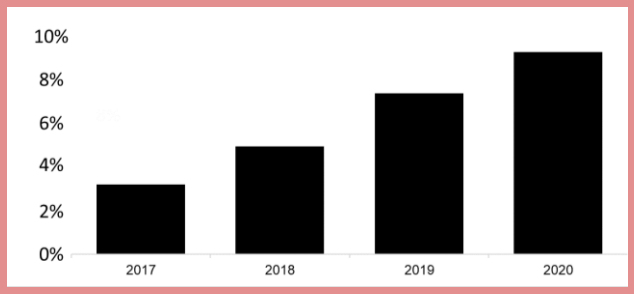
- **El *ransomware* s'ha beneficiat de les ciberassegurances per garantir el cobrament i augmentar els preus dels rescats**
- **La cartera de clients de les ciberasseguradores ha estat un objectiu prioritari del *ransomware***
- **Les ciberassegurances es veuen obligades a apujar o a desestimar el pagament de rescats**
- **El sector educatiu viu una onada de ciberatacs sense precedents i experimenta l'augment de les primes per a ciberassegurances**

Baròmetre

La pandèmia ha accelerat la transformació digital i els ciberincidents han esdevingut una de les principals preocupacions de les organitzacions. Moltes opten per transferir els riscos digitals a les ciberassegurances que, davant de la proliferació del *ransomware*, encareixen les primes o desestimen fer pagaments.

El creixement dels sinistres per atacs de *ransomware* s'accentua any rere any

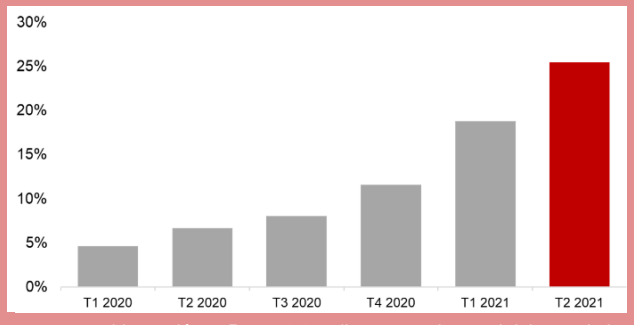
Gairebé el 70% de la sinistralitat en les pòlisses de ciberassegurança té l'origen en atacs de *ransomware*, compromís de dades personals i enginyeria social. Pel que fa als sinistres causats exclusivament per *ransomware*, el creixement anual dels sinistres cibernètics s'ha triplicat.



Il·lustració 12. Percentatge d'augment anual dels sinistres de ciberassegurances causats per atacs de ransomware[110].

Les primes de les ciberassegurances en continu augment

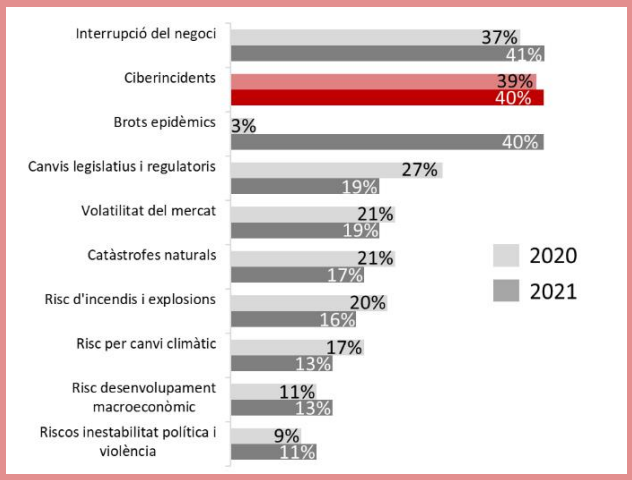
El preu mitjà de les assegurances per incidents cibernètics no ha deixat de pujar el darrer any i mig. Durant el 2n trimestre de 2021, l'increment ha estat d'un 25,5%, davant del 18% del 1r trimestre. L'increment en el nombre de ciberatacs i els impactes econòmics cada vegada més grans han contribuït a aquest augment continuat.



Il·lustració 13. Percentatge d'augment trimestral del preu de les ciberassegurances[111].

Les ciberasseguradores situen els ciberincidents entre els principals riscos

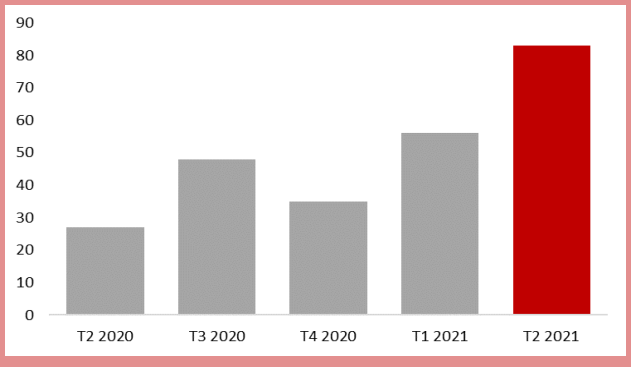
Els incidents cibernètics s'han convertit en una de les principals preocupacions per a les organitzacions. En una enquesta a entitats de tot el món, el 40% situa els ciberincidents entre els tres principals riscos de 2021. A l'Estat espanyol, el 58% afirma que els ciberincidents són la principal preocupació.



Il·lustració 14. Principals preocupacions de les organitzacions[112].

Augment dels atacs de *ransomware* al sector educatiu durant el segon trimestre

Durant el 2n trimestre, el sector educatiu ha viscut un augment del 50% dels atacs de *ransomware* respecte del trimestre anterior. Però aquest augment ha estat del 200% respecte del mateix període de fa un any. El motiu és que, especialment durant els mesos de març i abril, hi ha hagut una autèntica onada d'atacs.



Il·lustracióc 15. Presència als mitjans especialitzats d'incidents de ransomware *al sector educatiu (font: Agència).*

[110] *https://www.segurostv.es/data/informes/ESTUDIO-CIBERSEGURIDAD-ESPANA-2021-AON_v2.pdf*
[111] *https://www.ciab.com/resources/q2-p-c-market-survey-2021/*
[112] *https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html*

El *ransomware* ha tret profit de les ciberassegurances per garantir el cobrament dels rescats i augmentar-ne l'import

Arran de la pandèmia, moltes organitzacions han accelerat la seva **transformació digital** i, al mateix temps, han vist com **canviaven** les seves **preocupacions**. De fet, un **58%** de les empreses de l'Estat espanyol consideren que els **ciberincidents són la principal amenaça** a la qual estan exposades, seguida dels brots pandèmics i, finalment, la interrupció del negoci (veure il·lustració 14)[113,114]. Així, per tal de fer front a l'impacte d'un incident cibernètic, les organitzacions contracten **ciberassegurances**.

Entre la gran varietat d'**incidents cibernètics reclamats** a les asseguradores, destaquen els causats per ***ransomware***, perquè mantenen un creixement exponencial any rere any (veure il·lustració 12). Als EUA, durant la 1a meitat de 2020, els sinistres per *ransomware* van representar el **41%** del nombre total de les reclamacions d'assegurances cibernètiques[115].

Segons aquestes xifres es podria deduir que moltes víctimes de *ransomware* es veuen beneficiades pel fet **que l'assegurança s'hagi fet càrrec del rescat**, però la realitat és que aquest fet **no garanteix la recuperació de la informació xifrada**. Un estudi de Sophos indica que, després del pagament, es recupera una **mitjana del 65%** de la informació, que tan sols un **8%** de les organitzacions que paguen el rescat recuperen **tota la informació** i que un **29%** no n'arriba a recupera ni **la meitat**[116]. Tanmateix, moltes víctimes de *ransomware* prefereixen aquesta alternativa que no pas haver d'afrontar conseqüències com les que va patir l'empresa noruega Norsk Hydro ASA el 2019[117] (amb pèrdues de més de 50 M€) o l'atac recent al **sistema sanitari d'Irlanda** (amb pèrdues que poden arribar als **500 M€**)[118].

A més, cal destacar que els **pagaments** d'un rescat a un grup cibercriminal esdevenen un **finançament** de la seva **activitat delictiva** i alimenten una **espiral d'augment de preus** dels rescats. El fet que les ciberassegurances, amb les notables capacitats econòmiques, garanteixin el pagament dels rescats promou que el cibercrim s'atreveixi a exigir imports encara més elevats. En aquest sentit, cal destacar com els imports dels **rescats** han mantingut una **tendència sempre creixent** fins a final de 2020 i, avui dia, l'import mitjà d'un rescat està en els **118.000 €**[119].

Les asseguradores i els seus clients esdevenen objectius del *ransomware*

A més d'afavorir l'escalada dels rescats, el fet que les asseguradores s'ocupin de pagar-los comporta una altra conseqüència negativa: les **empreses ciberassegurades** s'han convertit en **objectiu** dels ciberatacants. I és que atacar una organització amb una ciberassegurança que inclogui els atacs de *ransomware* és una **garantia addicional per al cobrament d'un rescat**.

[113] *https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2021-covid-trio.html*
[114] *https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html*
[115] *https://markets.businessinsider.com/news/stocks/coalition-releases-cyber-insurance-claims-report-detailing-increased-ransomware-demands-in-2021-1030649887*
[116] *https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx*
[117] *https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/*
[118] *https://heimdalsecurity.com/blog/expenses-from-ransomware-attack-against-ireland-health-service-executive-exceed-600m/*
[119] *https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority*

Precisament, un integrant del grup de *ransomware* **REvil** va advertir que **les organitzacions ciberassegurades "són de les més llamineres"**. Però va afegir que l'interès residia en **atacar primer les asseguradores**, obtenir la seva **llista de clients** i, posteriorment, realitzar atacs dirigits contra les empreses assegurades[120]. En aquest sentit, val la pena esmentar el cas de la corredoria d'assegurances **One Call Insurance** (Regne Unit), que va ser víctima d'un atac de *ransomware* amb el **robatori de la informació** dels seus clients; es va exigir un rescat de **17 M€** per no fer-la pública[121].

El fet que les **empreses asseguradores** disposin de les dades dels seus clients no és l'únic motiu pel qual són objectius d'atacs. També ho és el fet que són entitats que **poden fer front a grans pagaments**. Ho demostra el rescat rècord de **34 milions d'euros** que va pagar el **CNA Financial** (EUA), una companyia financera que ofereix diferents productes de ciberassegurances[122]. Això sí, per tal d'evitar riscos de sanció, la companyia va optar per consultar i compartir informació amb l'FBI i amb el Departament del Tresor[123].

Les ciberassegurances es veuen obligades a apujar les primes o excloure el pagament de rescats

L'escalada en l'import dels rescats és prou evident. Durant el trimestre, s'han succeït diversos **incidents de *ransomware*** amb peticions de rescat per **sobre dels 10 M€**: l'empresa francesa **Asteelflash**, que fabrica components electrònics, va rebre una petició de 20 M€[124]; la farmacèutica francesa **Pierre Fabre**, 21 M€[125]; el **districte escolar de Florida** (EUA), 34 M€[126]; la companyia nord-americana **CNA Financial**, 34 M€[127], per posar només alguns exemples.

La conseqüència d'haver d'assumir uns rescats tan importants és que les assegurances s'han vist obligades a **replantejar el preu de les primes**. De fet, més del **70%** dels membres de The Council of Insurance Agents & Brokers dels EUA van informar d'una **disminució de les reserves de capital per assumir les cobertures de ciberriscos**[128]. Així, les primes de les ciberassegurances han augmentat progressivament cada any (veure il·lustració 13)[129].

Enmig d'aquesta **escalada de preus** i, probablement, a causa dels estralls econòmics de la pandèmia, no totes les empreses poden pagar els serveis d'una ciberassegurança. Del 2019 al 2020, **més empreses** amb **facturació superior a 250 M€** contracten pòlisses de ciberassegurança (han passat del 44% al 68%); en canvi, **menys pimes** opten per transferir el risc cibernètic a una asseguradora (del 56% al 32%)[130].

En altres casos, les asseguradores no en tenen prou amb l'augment dels preus de les pòlisses. Arriben a haver de **limitar la cobertura de l'assegurança en casos d'extorsió** i, fins i tot, a **deixar d'emetre pòlisses** que incloguin el pagament de rescats per *ransomware*[131,132].

[120] *https://grahamcluley.com/ransomware-gang-says-it-targets-firms-with-cyber-insurance/*
[121] *https://www.computing.co.uk/news/4031733/insurer-falls-victim-ransomware-attack-darkside-gang*
[122] *https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack*
[123] *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*
[124] *https://www.bleepingcomputer.com/news/security/asteelflash-electronics-maker-hit-by-revil-ransomware-attack/*
[125] *https://www.bleepingcomputer.com/news/security/leading-cosmetics-group-pierre-fabre-hit-with-25-million-ransomware-attack/*
[126] *https://www.foxnews.com/us/florida-school-district-ransomware-attack-hackers*
[127] *https://www.cybersecuritydive.com/news/cna-financial-ransomware-payment-treasury-sanctions/600591/*
[128] *https://insurance-edge.net/2021/06/10/the-thing-about-ransomware-is-that-its-not-about-the-ransom/*
[129] *https://www.theregister.com/2021/07/05/cyber_insurance_report/*
[130] *https://www.segurostv.es/data/informes/ESTUDIO-CIBERSEGURIDAD-ESPANA-2021-AON_v2.pdf*
[131] *https://www.segurostv.es/data/informes/ESTUDIO-CIBERSEGURIDAD-ESPANA-2021-AON_v2.pdf*
[132] *https://www.howdengroup.com/sites/g/files/mwfley566/files/inline-files/Howden%20Cyber%20Insurance%20-%20A%20Hard%20Reset%20report_1.pdf*

El fet que les ciberassegurances excloguin el pagament de rescats en casos d'extorsió va clarament en contra dels interessos del cibercrim. Probablement per aquest motiu, l'asseguradora **AXA**, després d'anunciar que **deixava d'emetre noves pòlisses d'assegurança pel pagament de rescats a França**, va ser **víctima** d'una **ofensiva cibernètica**[133]. El ciberatac va impactar les operacions a Tailàndia, Malàisia, Hong Kong i les Filipines. En aquesta ofensiva, el *ransomware* Avaddon va impactar els serveis d'assistència, i també es van robar 3 TB de dades. Però el drama no s'acaba aquí: també es van dirigir diversos atacs de DDoS contra els seus webs[134].

El sector educatiu viu una onada de ciberatacs sense precedents i experimenta l'augment de les primes de ciberassegurances

La **covid-19 ha canviat el sector educatiu** perquè ha incorporat abastament les noves tecnologies i Internet per mantenir l'activitat formativa durant la pandèmia. Ara bé, la conseqüència és que el **nivell d'exposició** als ciberatacs s'ha accentuat, així com la **dependència** de les tecnologies digitals.

Aquesta situació coincideix amb les **motivacions del cibercrim** per atacar el sector educatiu. D'una banda, el sector educatiu actual és molt més **sensible a l'extorsió a través d'un atac de *ransomware***, que podria bloquejar l'activitat dels centres formatius o les classes en línia. Tenim el cas del **districte escolar de Florida,** que va ser víctima d'un *ransomware* que va interrompre la xarxa escolar i va aturar diversos serveis; els ciberdelinqüents demanaven un rescat de **34 M€**, possiblement el **més elevat mai sol·licitat a un centre educatiu**[135]. D'una altra banda, el **gran volum de dades personals** de què disposa el sector educatiu és un actiu de valor; aquestes dades es poden robar i fer servir per amenaçar de publicar-les si no es paga un rescat, o es poden vendre directament al mercat negre. Precisament, la **Universitat de Còrdova** (UCO) va veure com li robaven informació confidencial i era extorsionada per evitar-ne la publicació[136].

Així les coses, podem dir que, el 2020, el **44%** de les entitats del sector educatiu han estat **víctima d'atacs de *ransomware*** i lidera la taula del **sector més afectat**[137]. Per tant, l'augment de la sinistralitat també ha provocat un **augment** de les **primes de les ciberassegurances** en aquest sector. A l'Estat espanyol, l'increment de les primes del sector educatiu ha estat del **60%** durant la primera meitat de 2021[138]. Si ho comparem amb els EUA, però, allà han experimentat increments de fins al **300%**[139].

Durant el 2n trimestre de 2021, els ciberatacs contra aquest sector han estat una constant (veure il·lustració 16). A l'Estat espanyol, per exemple, la **Universitat de Castilla La Mancha** (UCLM) va perdre el servei web pels efectes d'un *ransomware*[140].

A Europa també s'ha viscut aquesta escalada d'atacs de *ransomware* al sector educatiu. La **Universitat de Montpellier** (França) va veure com un *ransomware* afectava a xarxa wifi, les connexions VPN i unes quantes funcions administratives[141]. El **National College of Ireland** (NCI) i la **Technological**

[133] *https://www.cpomagazine.com/cyber-security/frances-largest-insurer-will-no-longer-cover-ransomware-payments/*
[134] *https://www.securityweek.com/axa-confirms-ransomware-attack-impacted-operations-asia*
[135] *https://www.foxnews.com/us/florida-school-district-ransomware-attack-hackers*
[136] *https://www.diariocordoba.com/cordoba-ciudad/2021/06/04/policia-nacional-investiga-ciberataque-uco-52620424.html*
[137] *https://diarioti.com/aumentan-los-ataques-de-ransomware-contra-infraestructura-critica/116703*
[138] *https://www.segurostv.es/data/informes/ESTUDIO-CIBERSEGURIDAD-ESPANA-2021-AON_v2.pdf*
[139] *https://www.businessinsurance.com/article/20210712/NEWS06/912342944/Schools-hit-with-cyber-price-hikes*
[140] *https://www.cmmedia.es/noticias/castilla-la-mancha/la-universidad-de-castilla-la-mancha-uclm-sufre-un-ciberataque-ransonware/*
[141] *https://www.lemagit.fr/actualites/252499046/Un-virus-affecte-les-services-informatiques-de-luniversite-de-Montpellier*

Universtity (TU) de Dublín també van ser víctimes d'atacs de *ransomware*. Els ciberatacs va obligar a suspendre el funcionament de la plataforma Moodle, el servei de biblioteca i la intranet dels estudiants del NCI, i es van haver de suspendre les classes durant alguns dies[142].

Cal destacar, també, el que probablement és un dels atacs més destacats contra el sector educatiu. Al Regne Unit, un atac de *ransomware* a la **cadena d'acadèmies Harris Federation** va impactar els sistemes d'informació, els servidors de correu electrònic i les línies telefòniques; va afectar **37.000 alumnes** i una dotzena de centres[143].

Recomanacions

- **Les organitzacions han d'evitar el pagament de rescats en cas d'extorsió per part de grups cibercriminals.**
- **Les organitzacions han de desplegar mesures de ciberseguretat complementàries, independentment de si es contracta o no una ciberassegurança.**
- **Les organitzacions han de protegir i custodiar les còpies de seguretat, tot fent-les fora de línia i assegurant que estiguin lliures de *malware*.**
- **Les organitzacions han de disposar d'un pla de continuïtat de negoci i un pla de recuperació de desastres. A més a més, han de validar que ha estat verificat amb un simulacre d'atac de *ransomware* i de DDoS.**
- **Les organitzacions han d'emmagatzemar les dades personals amb xifratge segur per evitar que un intrús pugui robar-les en text pla.**
- **Les organitzacions han de realitzar anàlisis de riscos en matèria de privacitat (Avaluació d'Impacte de Dades Personals) per tal d'establir les mesures de protecció adequades de les dades personals.**

[142] *https://www.bleepingcomputer.com/news/security/ransomware-hits-tu-dublin-and-national-college-of-ireland/*
[143] *https://heimdalsecurity.com/blog/harris-federation-hit-with-ransomware/*

Fets rellevants

- Un integrant del grup cibercriminal REvil va advertir que les empreses que tenen ciberassegurança serien objectiu dels seus ciberatacs. L'integrant del grup va comentar, en una entrevista, que les organitzacions ciberassegurades "són les més llamineres". Destacava l'interès en atacar primer les asseguradores, obtenir la seva base de clients i, posteriorment, realitzar atacs dirigits contra les empreses assegurades contra incidents cibernètics[144].
- L'asseguradora CNA Financial, una de les companyies d'assegurances més grans dels EUA, va ser víctima d'un atac amb el *ransomware* Phoenix Locker. A causa del ciberatac, els empleats no podien accedir als sistemes de l'empresa i també es van robar dades confidencials. La companyia va arribar a un acord per al pagament de 34 M€ per restaurar els sistemes i evitar que es filtrés la informació robada. És el pagament més elevat mai publicat[145].
- L'asseguradora One Call (Regne Unit) va ser víctima d'un atac de *ransomware* amb robatori de dades. L'atac fou perpetrat pel grup DarkSide, el qual va reclamar 17 M€ a canvi de lliurar les claus de desxifratge i de no fer públiques les dades robades. Ara com ara, no s'ha confirmat el pagament de cap rescat i s'interpreta que la companyia disposava de sistemes de suport i còpies de seguretat. La companyia també va dur a terme una anàlisi per confirmar si les dades s'havien vist compromeses. [146].
- AXA (França) va confirmar que les seves operacions a l'Àsia van quedar afectades a causa d'un atac de *ransomware* i atacs de DDoS. Els ciberdelinqüents van atacar els sistemes d'AXA a Hong Kong, Tailàndia, les Filipines i Malàisia, i van afirmar que havien robat 3 TB de dades. L'incident es va produir una setmana després que el gegant de les assegurances anunciés que deixava d'oferir pòlisses d'assegurança per als pagaments per *ransomware* a França. S'ha especulat que es podria tractar d'una represàlia[147].
- Funcionaris de la ciutat de Califòrnia han admès que el 2019 van utilitzar la seva ciberassegurança per pagar un rescat de 54.000 €. Es dona el cas que, poc després del pagament, van trobar una clau gratuïta per al desxifrat de la informació[148].
- El grup cibercriminal Conti va exigir un rescat de més de 34 M€ al districte escolar de Florida després d'un atac de *ransomware*. Conti justificava l'elevat rescat pels gairebé 4.000 M€ de pressupost anual del districte escolar, el 6è més gran dels EUA, amb 261.000 alumnes i 110.000 estudiants adults, en més de 300 centres. L'atac va bloquejar tota la xarxa escolar i va interrompre diversos serveis. [149].
- La Universitat de Castilla La Mancha va ser víctima d'un atac de *ransomware* i, tot i que es va aconseguir tancar les connexions externes quan es va detectar la intrusió, va afectar alguns dels serveis digitals del centre. Els equips d'estudiants, professors i investigadors no van quedar afectats. Tot indica que l'objectiu del ciberatac era la infraestructura tecnològica i no pas els equips de la comunitat universitària[150].
- La Brigada de Delictes Informàtics de la Policía Nacional espanyola va investigar el robatori de dades de la Universitat de Còrdova perpetrat pels responsables del *ransomware* Conti. Els ciberdelinqüents van publicar 20 documents (el 5% de la informació confidencial) per provar el robatori i, així, forçar el rescat[151].
- A França, coincidint amb l'inici del programa educatiu *Ma classe à la maison*, la plataforma per a l'estudi a distància, es van produir una sèrie de ciberatacs que van provocar aturades i mal funcionament. El ministre d'Educació va apuntar, com a responsables, grups de ciberdelinqüents estrangers, però molts pares de la comunitat educativa van culpar el govern francès per falta de preparació[152].

[144] *https://grahamcluley.com/ransomware-gang-says-it-targets-firms-with-cyber-insurance/*
[145] *https://www.zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/*
[146] *https://www.insurancebusinessmag.com/uk/news/cyber/one-call-insurance-hit-by-ransomware-255978.aspx*
[147] *https://www.securityweek.com/axa-confirms-ransomware-attack-impacted-operations-asia*
[148] *https://threatpost.com/conti-40m-ransom-florida-school/165258/*
[149] *https://www.databreaches.net/es-university-of-castilla-la-mancha-uclm-suffers-a-ransomware-attack/*
[150] *https://www.cmmedia.es/noticias/castilla-la-mancha/la-universidad-de-castilla-la-mancha-uclm-sufre-un-ciberataque-ransonware/*
[151] *https://www.diariocordoba.com/cordoba-ciudad/2021/06/04/policia-nacional-investiga-ciberataque-uco-52620424.html*
[152] *https://techxplore.com/news/2021-04-french-homeschooling-hackers-russia-china.html*

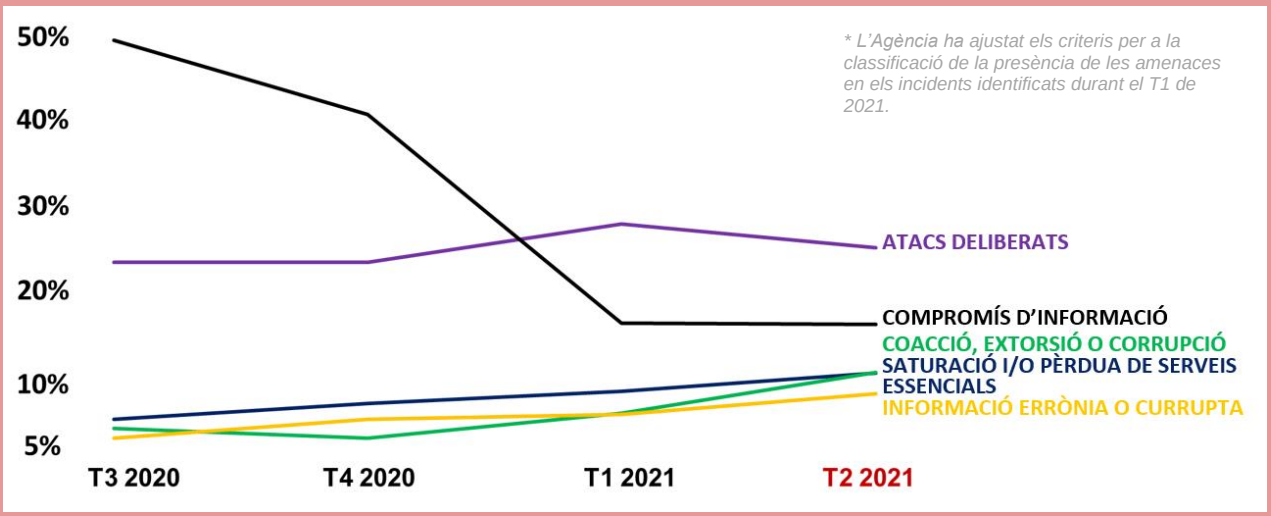
Top 5 de ciberamenaces

Tenint en compte el nombre d'incidents que s'han esdevingut durant el 2n trimestre de 2021, a continuació es mostra l'evolució de les cinc **ciberamenaces** més rellevants i se'n destaquen els esdeveniments més significatius.

Una ciberamenaça 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.

2T 2021	vs	1T 2021	Ciberamenaces[153]
1	=	1	**Atacs deliberats** *Difusió i/o execució de programari maliciós, accés lògic o físic no autoritzat, o abús de privilegis d'accés sobre els sistemes d'informació.*
2	=	2	**Compromís i/o pèrdua d'informació** *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.*
3	▲	4	**Coacció, extorsió o corrupció** *Persuasió il·legítima, intimidació o suborn per obligar una víctima a cometre accions il·lícites o delictives contra els actius d'informació.*
4	▼	3	**Saturació i/o pèrdua de serveis essencials** *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.*
5	=	5	**Informació errònia o corrupta** *Informació errònia o corrupta que implica que el contingut lògic estigui organitzat d'una manera no apropiada, faltin dades o no sigui vàlid.*

▲ *Puja* ▼ *Baixa* = *Es manté*



** L'Agència ha ajustat els criteris per a la classificació de la presència de les amenaces en els incidents identificats durant el T1 de 2021.*

[153] *Catàleg d'amenaces de l'Agència de Ciberseguretat de Catalunya.*

1. Atacs deliberats

El cibercrim encara aprofita els temes d'actualitat per realitzar campanyes de *phishing* amb l'objectiu de robatori dades personals o programari maliciós. A banda dels tradicionals esquers relacionats amb el pagament d'impostos durant la campanya de la renda, també s'ha fet ús de la cerimònia dels Oscar, la fusió de CaixaBank i Bankia o l'aparició del passaport sanitari.

01/04. Campanya de *phishing* contra el sector educatiu als EUA. A final de març, l'IRS (Internal Revenue Service), encarregat de la recaptació fiscal i del compliment de lleis tributàries, va alertar estudiants i personal de les universitats d'una campanya en la qual se n'usurpava la identitat. Amb l'ús del reemborsament d'impostos com a reclam, l'objectiu del *phishing* era obtenir informació personal i dades financeres[154].

05/04. Suplantació de la pàgina web de l'Agencia Tributaria per forçar la descàrrega d'un programari maliciós. Una de les campanyes identificades presentava el tema "Acción Fiscal" o "Factura no pagada – Gobierno de Espanya", però se sospita que podria haver-n'hi d'altres. Els correus s'enviaven des de dominis com ara "agencia-tributaria26" per confondre les víctimes i incloïen logotips oficials per donar-ne credibilitat. Els correus informaven d'una acció fiscal i subministraven un enllaç que, en comptes de dirigir a la Sede Electrónica, descarregava un *malware*[155].

23/04. La cerimònia de lliurament dels Oscar serveix per difondre programari maliciós i robar dades sensibles. Diferents grups de ciberatacants van aprofitar la cerimònia dels premis de l'Acadèmia de Cinema nord-americana, que enguany es va celebrar en format virtual, per crear webs que oferien la descàrrega il·legal de les pel·lícules nominades a canvi d'un pagament. Ara bé, els webs permetien robar les dades de les targetes de crèdit o incloïen programari maliciós en les descàrregues[156].

15/06. Alerta de campanyes de *phishing* a clients de BBVA, CaixaBank i Banco Santander. S'ha alertat de campanyes de *phishing* dirigides als clients de les entitats bancàries BBVA, CaixaBank i Banco Santander. En el cas de CaixaBank, la campanya és especialment adequada als temps actuals: avisa de l'anunci de la fusió amb Bankia com a pretext per dirigir la víctima a pàgines web falses i robar-li les dades personals[157].

17/06. Google Docs s'utilitza per esquivar els controls d'anti-*phishing*. Els ciberatacants difonen enllaços legítims de documents publicats a la plataforma Google Docs, els quals contenen documents maliciosos que reenvien l'usuari a un web que suplanta la pàgina d'autenticació de Google. L'objectiu és robar les credencials. Com que l'enllaç enviat és legítim, no és detectable per les eines d'anti-*phishing* convencionals[158].

23/06. Campanya de *phishing* al Regne Unit que ofereix passaports sanitaris en nom de l'NHS. Els correus contenien un enllaç a un web fals del NHS (National Health Service) en el qual se sol·licitava informació personal i un pagament en concepte de despeses de gestió per obtenir el passaport sanitari. La policia va advertir d'aquesta campanya i va animar els ciutadans a denunciar-ho a les autoritats i agències de ciberseguretat[159].

[154] *https://hotforsecurity.bitdefender.com/blog/irs-warns-of-phishing-campaign-targeting-university-students-and-staff-25577.html*
[155] *https://www.osi.es/es/actualidad/avisos/2021/04/correo-suplantando-la-agencia-tributaria-que-busca-descargar-malware-en-tu*
[156] *https://threatpost.com/oscar-bait-hackers-nominated-phishing-malware/165583/*
[157] *https://www.rtve.es/noticias/20210615/phishing-caixabank-cuenta-suspendida/2103844.shtml*
[158] *https://threatpost.com/google-docs-host-attack/166998/*
[159] *https://www.express.co.uk/life-style/life/1453497/scam-warning-covid-vaccine-digital-coronavirus-passport-email-police*

2. Compromís i/o pèrdua d'informació

S'han descobert algunes de les recol·leccions de credencials més grans de la història, però també grans bases de dades amb informació extreta de les xarxes socials a través de *scrapping*. També s'han produït noves fuites de dades a partir d'atacs de *ransomware* amb robatori de dades o arran d'errors de configuració .

05/06. Ciberatac a la web de la RFEF i exposició de dades sensibles. La Real Federación Española de Fútbol (RFEF) va recomanar als empleats i directius que canviessin les contrasenyes, després que s'identifiqués un ciberdelinqüent que subhastava informació confidencial de l'entitat. Tanmateix, la Federació va comunicar que la major part de la informació recollida pel ciberdelinqüent ja era pública[160].

10/06. 26 milions de contrasenyes a la venda a la *dark web*, obtingudes d'una *botnet* a partir de 3 milions de dispositius Windows infectats. La *botnet* d'*infostealers* anomenada Raccoon, que s'hauria difós amb versions no legals d'Adobe, videojocs i el sistema operatiu Windows, en podria ser la responsable. Va aconseguir robar les contrasenyes d'1,5 milions de comptes de Facebook i més de 20 milions d'altres plataformes, emmagatzemades pels usuaris a Chrome. També va recopilar 2.000 milions de *cookies* d'accés, 1 milió d'imatges i 650.000 documents en format word i pdf[161].

15/06. El contractista del govern dels EUA d'armes nuclears Sol Oriens, víctima d'un ciberatac amb robatori de dades. REvil afirma que va robar dades comercials i dades d'empleats, com ara informació salarial i números de la seguretat social. Com a prova, REvil va publicar imatges de documents amb dades contractuals, nòmines i un informe de salaris. La banda va amenaçar de compartir "documentació i dades rellevants a les agències militars que triés" i va afirmar que ja havia començat la subhasta de les dades robades[162].

16/06. Detectada una campanya d'espionatge xinesa activa des de 2014. Es creu que aquesta campanya de ciberatacs està perpetrada pel grup APT xinès RedFoxtrot, vinculat a l'exèrcit d'aquest país, i que té com a objectiu obtenir intel·ligència militar dels països veïns. En els últims sis mesos, diversos contractistes de defensa i aeroespacials de l'Índia, empreses de telecomunicacions de l'Afganistan, l'Índia, Kazakhstan i del Pakistan, així com diverses institucions nacionals i estatals de la regió, haurien estat víctimes d'aquesta campanya[163].

25/06. Un grup d'investigadors va detectar una bases de dades exposada públicament amb dades de 800 milions de registres d'usuaris de Wordpress. La base de dades pertanyia al proveïdor d'allotjament web DreamHost. Alguna informació estava relacionada amb usuaris d'institucions educatives i governamentals, ja que incloïen les extensions .edu i .gv en l'adreça de correu[164].

[160] *https://www.vozpopuli.com/espana/rfef-ciberataque-web.html*
[161] *https://www.bankinfosecurity.com/blogs/26m-passwords-exposed-in-botnet-data-leak-p-3054*
[162] *https://securityaffairs.co/wordpress/118968/security/revil-ransomware-sol-oriens.html*
[163] *https://therecord.media/sprawling-cyber-espionage-campaign-linked-to-chinese-military-unit/*
[164] *https://www.infosecurity-magazine.com/news/cloud-database-exposes-800m/*

3. Coacció, extorsió o corrupció

El cibercrim segueix dirigint campanyes de *ransomware* contra organitzacions amb l'objectiu d'extorsionar-les a canvi de desblocar els sistemes d'informació o evitar la filtració de dades confidencials. Tanmateix, l'extorsió es consolida en altres formes, com atacs de DDoS que exigeixen un rescat per cessar o amb l'ús de dades robades per extorsionar els afectats.

29/04. El Tribunal de Justícia de l'Estat de Rio Grande do Sul (Brasil), afectat per un atac de *ransomware* amb una doble extorsió de gairebé 5 M€. Poc després de l'inici de l'atac, el TJRS es va dirigir als empleats a través del compte oficial de Twitter per advertir que no accedissin a la xarxa: "El TJRS informa que s'enfronta a una inestabilitat en els sistemes informàtics. L'equip de seguretat aconsella als usuaris interns que no accedeixin a ordinadors remotament, ni que iniciïn cap sessió en ordinadors a dins de la xarxa TJ"[165].

11/05. Una nova campanya de *phishing* dirigida a influenciadors de Facebook i Instagram. Els cibercriminals intentaven prendre el control dels comptes dels influenciadors amb milers de seguidors amb l'objectiu de demanar un rescat a canvi de recuperar el compte. Es feien passar per membres del personal de Facebook o d'Instagram, i intentaven portar les víctimes a llocs web maliciosos per robar-los informació i credencials[166].

14/05. Campanya d'extorsió als clients de la companyia de criptomonedes Ledger a partir de les dades filtrades el juliol de 2020. Els ciberdelinqüents advertien les víctimes que havien estat *hackejades* i que, si no pagaven al voltant de 800 €, utilitzarien les seves dades per subscriure's a llocs web amb continguts sexualment explícits amb menors[167].

17/05. L'FBI alerta de noves campanyes d'extorsió dirigides a familiars de persones desaparegudes. Els ciberdelinqüents identifiquen gent desapareguda a les xarxes socials, recopilen informació sobre la víctima i els familiars amb l'objectiu d'exigir un rescat d'entre 4.000 i 8.000 € per un suposat segrest. Tot plegat sense haver tingut mai contacte amb la persona desapareguda[168].

10/06. Onada d'atacs de DDoS amb extorsió perpetrada pel grup APT Fancy Lazarus. La campanya d'atacs va començar durant la segona meitat de 2020. El grup APT s'ha dedicat a dirigir correus electrònics amenaçadors a companyies de diferents sectors com l'energia, finances, assegurances o manufactura, entre d'altres. En els correus demanen 2 *bitcoins* per tal d'evitar atacs DDoS abans d'una data concreta. Si no es fa el pagament, la quantitat es dobla i s'incrementa un *bitcoin* per dia.[169].

18/06. Compromesa una plataforma classificada de l'OTAN. Uns ciberatacants, declarats "políticament motivats", van comprometre l'empresa everis, proveïdora de serveis d'accés a la informació d'una plataforma de serveis al núvol de l'OTAN. Van obtenir accés al codi font associat, documentació i diversos *datasets*. I, fins i tot, van tenir l'oportunitat d'esborrar-la. Van exigir a everis un pagament de 14.500 XMR (aproximadament 2 M€) per evitar la publicació de les dades, i van difondre missatges irònics sobre la possible compartició amb els serveis d'intel·ligència russos. Val a dir que, inicialment, els atacants estaven interessats en les subsidiàries d'everis a l'Amèrica Llatina[170].

[165] *https://www.bleepingcomputer.com/news/security/brazils-rio-grande-do-sul-court-system-hit-by-revil-ransomware/*
[166] *https://noticiasseguridad.com/seguridad-informatica/nueva-campana-de-phishing-apuntando-contra-influencers-de-facebook-e-instagram/*
[167] *https://www.itsecuritynews.info/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign/*
[168] *https://www.welivesecurity.com/2021/05/18/scams-target-families-missing-persons-fbi-warns/*
[169] *https://www.proofpoint.com/us/newsroom/news/fancy-lazarus-criminal-group-launches-ddos-extortion-campaign*
[170] *https://ddosecrets.substack.com/p/exclusive-nato-classified-cloud-platform*

4. Saturació i/o pèrdua de serveis essencials

Els atacs de *ransomware* han estat els principals culpables de la interrupció del negoci de milers d'organitzacions de tot el món. Els atacs de DDoS també han provocat greus afectacions, especialment en incidents dirigits a empreses proveïdores de serveis d'Internet, que han deixat sense suport els seus clients.

23/04. Un ciberatac deixa la pàgina web de l'INE i de diversos ministeris inoperatius. El primer web que va deixar de funcionar va ser el de l'Instituto Nacional de Estadística (INE), inoperatiu durant més de 12 hores. Després, li va tocar el torn a les pàgines oficials del Ministeri d'Educació i Cultura, del Ministeri de Justícia i del Ministeri d'Assumptes Econòmics i Transformació Digital (Mineco), així com les seus electròniques[171].

05/05. Un atac de DDoS afecta més de 200 organitzacions de Bèlgica, inclosos el Parlament i alguns ministeris. L'atac es va dirigir a l'empresa Belnet, l'ISP de les institucions educatives, centres de recerca, instituts científics i diverses institucions governamentals. Alguns debats i comissions parlamentàries es van haver d'ajornar perquè els usuaris no podien accedir als serveis virtuals necessaris. L'atac es va allargar durant un dia, va saturar llocs web, i va inhabilitar els sistemes interns i els accessos a Internet. Va resultar difícil de bloquejar perquè s'apunta que els atacants canviaven de tècniques del flux de dades enviat recurrentment[172].

10/05. Un atac de *ransomware* a l'empresa de telecomunicacions ASAC deixa inoperativa les webs del Tribunal de Cuentas, el Consejo de Seguridad Nuclear i alguns ajuntaments com els d'Oviedo, Fuenlabrada i Cáceres. El 8 de maig, durant una revisió rutinària, es va identificar un atac amb el *ransowmare* Zeppelin. L'atac xifrava part dels sistemes, de manera que l'empresa va bloquejar les comunicacions i va deixar els clients sense servei web. Tot indica que no va haver-hi robatori de dades[173].

08/06. Una fallada global deixa milers de pàgines d'Internet sense servei. Webs com la del diari El País, Amazon, Twitch, The New York Times o Reddit van poder recuperar la normalitat després de tenir problemes d'accés a causa d'un incident a la xarxa de distribució de continguts Fastly[174].

09/06. Tres mesos després del ciberatac al SEPE, el Ministerio de Trabajo y Seguridad Social, víctima d'un atac de *ransomware* que en paralitza l'activitat. El ciberatac va afectar la pàgina web i els serveis interns, ja que es va poder aïllar la xarxa infectada. No obstant això, va haver de paralitzar-se l'activitat de 5.500 funcionaris del ministeri, de l'Instituto de Trabajo, el Fondo de Garantía Salarial (FOCAGA) i l'Instituto Nacional de Seguredad y Salud en el Trabajo durant més de dues setmanes. No es va informar si s'ha tractat del *ransomware* Ryuk, el mateix que va afectar el SEPE [175,176].

[171] *https://unaaldia.hispasec.com/2021/04/ciberataques-coordinados-dejan-inoperativas-la-web-del-ine-y-de-varios-ministerios.html*
[172] *https://www.welivesecurity.com/2021/05/05/belgium-government-websites-offline-ddos-attack/*
[173] *https://www.xataka.com/seguridad/ciberataque-al-servicio-nube-asac-bloquea-ayuntamientos-como-oviedo-multiples-organismos-nacionales*
[174] *https://www.bleepingcomputer.com/news/security/stackoverflow-twitch-reddit-others-down-in-fastly-cdn-outage/*
[175] *https://cincodias.elpais.com/cincodias/2021/06/09/companias/1623233891_774070.html*
[176] *https://www.elindependiente.com/economia/2021/06/24/5-500-funcionarios-del-ministerio-de-trabajo-no-pueden-usar-sus-ordenadores-15-dias-despues-del-ciberataque/*

5. Informació errònia o corrupta

Els atacs de *ransomware* han tingut un paper cabdal en l'alteració de la integritat de les dades d'organitzacions de tot el món. En alguns casos, els atacs de *ransomware* han amagat una motivació geopolítica i estaven dirigits a eliminar la informació, sense demanar rescat. En altres casos, però, s'ha utilitzat directament un programari *wiper*. Destaca, també, la detecció d'un misteriós programari maliciós que formata els dispositius NAS connectats a la xarxa d'un fabricant determinat.

Un wiper és un programari maliciós que té la intenció de destruir sistemes i/o dades amb l'objectiu de generar danys a la víctima.

06/05. Un atac de *ransomware* contra un centre d'iniciatives mediambientals causa la pèrdua de dades. El centre, en un comunicat, va anunciar l'atac i va concloure que treballava per tornar a la normalitat. Tanmateix, van admetre que s'havien perdut tots els arxius des d'abril de 2020.[177].

27/05. Un grup cibercriminal simula atacs de *ransomware* per atacar objectius israelians i esborrar-ne informació. El col·lectiu de ciberatacants, amb el nom d'Agrius, es vincula a l'Iran. Els atacs se succeeixen des de fa un any i utilitzen les variants de *malwares* anomenades Apostle i Deadwood, de tipus *wiper*, amb l'objectiu de simular un atac de *ransomware* i confondre les víctimes.[178].

14/06. Un ex-empleat, detingut per dirigir un ciberatac a l'empresa que l'havia acomiadat, per venjança. El detingut va aconseguir accedir als sistemes de l'empresa i esborrar parcialment un programari que permetia donar servei a un client important. Per dur a terme l'atac, l'ex-empleat va utilitzar la wifi de la seva parella sentimental, pensant-se que podia passar desapercebut.[179].

25/06. Formaten dispositius NAS i discos durs de la marca Western Digital connectats a la xarxa. Diversos usuaris dels dispositius d'emmagatzematge My Book Live han vist desaparèixer les dades dels seus dispositius, fins i tot connectats a una xarxa interna o darrere d'un tallafoc. Tot apunta que existeix un *exploit* que permet l'execució remota de codi en uns dispositius que, des de 2015, ja no disposen d'actualitzacions del fabricant. La companyia va recomanar als usuaris desconnectar els dispositius de la xarxa[180].

28/06. Un ciberatacant xifra una base de dades de 250 GB de notícies utilitzada en el servei RSS de la companyia NewsBlur. El ciberatacant, probablement novell, va aconseguir accés a la base de dades mentre el lector de RSS era traslladat a un contenidor Docker i la base de dades MongoDB va quedar exposada durant tres hores. Afortunadament, els responsables de NewsBlur disposaven de l'original i van poder recuperar-la en poques hores[181].

[177] *https://www.databreaches.net/fr-ransomware-attack-on-environmental-center-resulted-in-data-loss/*
[178] *https://www.databreachtoday.com/suspected-iranian-group-wages-wiper-attacks-on-israel-a-16756*
[179] *https://www.malagahoy.es/malaga/Detenido-Malaga-ataque-informatico-empresa-despedido_0_1583243065.html*
[180] *https://threatpost.com/my-book-live-wiped-rce-attacks/167270/*
[181] *https://www.securityweek.com/newsblur-restores-service-after-hacker-wipes-database*

Conclusions

L'**activitat cibercriminal** continua el camí de batre **nous rècords** i **traspassa línies vermelles**. L'escalada en la magnitud dels atacs i la importància dels objectius provoca que els impactes no parin de créixer i esdevinguin una autèntica **amenaça per a l'estabilitat social i econòmica de la societat digital**.

D'entrada, cal destacar les afectacions a la **ciutadania**. A Catalunya, només aquest trimestre, s'haurien pogut filtrar dades personals de fins al **50% de la població**. Així mateix, s'han identificat bases de dades amb credencials de dimensions extraordinàries: aproximadament, una mitjana de **dues contrasenyes per cada habitant del planeta**. I, atès que el ciberespai no oblida, cal sumar-hi l'**històric de dades personals filtrades amb anterioritat**. Però el pitjor està encara ha d'arribar, ja que tota aquesta informació permetrà dur a terme **campanyes de ciberatacs** de *credential stuffing* per obtenir l'accés als comptes personals o professionals, així com incomptables formes de suplantació d'identitat o fraus. Amb un detall afegit: amb l'ús de la IA, les possibilitats es multipliquen. Per tant, ja no hi ha excusa: cal **conscienciar** i utilitzar accessos amb **doble factor** d'autenticació.

Les **infraestructures crítiques** també han estat objectiu d'un cibercrim **hàbil** i que sap com **actuar amb impunitat**. Durant aquest trimestre, els atacs de ***ransomware*** i **DDoS** han afectat els serveis essencials per a la ciutadania. Arran de la gravetat dels incidents, les **institucions governamentals** col·laboren per combatre el cibercrim: **les fronteres** i **estructures financeres internacionals** no han de suposar un **impediment** per a les autoritats que persegueixen els ciberdelinqüents. Les nombroses **accions policials i detencions** dels darrers temps són una prova d'aquest pas endavant.

Aquest context afecta l'àmbit dels **negocis**. Cada vegada més, es contracten **ciberassegurances** per pal·liar les conseqüències d'un ciberatac. El plantejament pot ser efectiu per fer front des d'un punt de vista econòmic a un incident cibernètic, però, **en els casos d'extorsió, la solució no és tan senzilla**. El pagament dels rescats **reforça l'activitat del cibercrim** i promou la **pujada dels imports dels rescats**. A més a més, **no garanteix la recuperació** de tota la informació segrestada. Per aquest motiu, en cas de ser víctimes d'un *ransomware*, per sobre de tot, cal **evitar que el pagament constitueixi l'única alternativa** per a la supervivència. D'aquesta manera, és necessari implantar **mesures de ciberseguretat** per prevenir i minimitzar les conseqüències d'un atac. La primera i imprescindible: la disponibilitat d'unes **còpies de seguretat** actualitzades i fora de línia.

Com es constata, doncs, el cibercrim desplega uns atacs cibernètics **sense precedents**. Per tant, per fer-hi front, cal **innovació** amb l'objectiu d'esdevenir **més digitalment avançats i segurs que mai**.

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

ciberseguretat.gencat.cat

desembre de 2021