AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Informe de tendències de ciberseguretat

1r trimestre de 2021

El repte d'una recuperació econòmica digital i segura

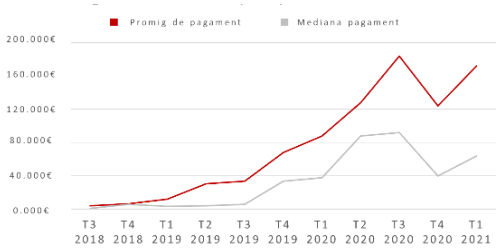
Índex

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

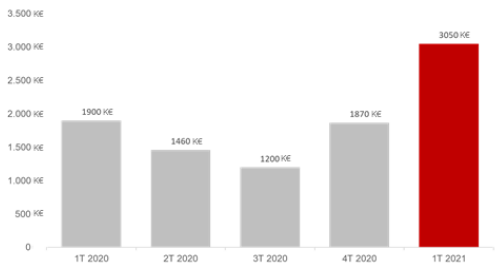
Ha estat notícia. El **2 de març** de 2021, Microsoft publicava un comunicat extraordinari on informava de **quatre vulnerabilitats crítiques** identificades al programari de **MS Exchange Server** i es publicaven els **pegats** pertinents. A partir d'aquesta data, els **ciberatacs** tractant d'explotar les vulnerabilitats es van multiplicar. A Catalunya, en l'àmbit de l'Administració Pública, han estat afectades al voltant de **108 IP** i l'**Hospital Dexeus Dona** va resultar víctima d'un ciberatac que precisament afectava el seu servidor MS Exchange.



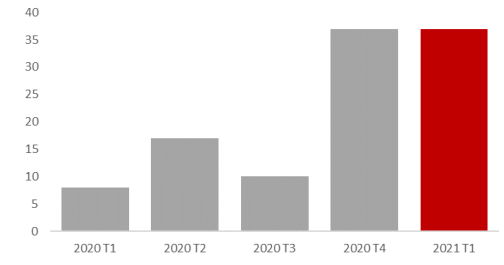
El preu mitjà dels rescats van decréixer a finals de 2020, però el 2021 ha recuperat la tendència a l'alça.

El cibercrim amenaça els plans de recuperació econòmica i transformació digital amb noves tècniques en els atacs de *ransomware*, DDoS complexos i robatoris de dades. El pla **NextGenEU** preveu grans inversions en tecnologia per transformar la societat: concretament, **160.000 M€** per a la **transformació digital**. Ara bé, el desplegament de tecnologies digitals haurà de fer front a un cibercrim que evoluciona i fa ús de tècniques molt sofisticades. El **77%** dels atacs de *ransomware* utilitza la **doble extorsió**, els atacs **es dirigeixen a directius** per tenir accés a informació sensible i impacten **organitzacions més grans**. L'import mitjà del **rescat** ja arriba aproximadament als **180.000 €**. Hi ha **menys** atacs de **DDoS**, però són més **volumètrics i complexos**, i tres dels cinc atacs DDoS més grans detectats per Akamai s'han dut a terme durant l'any 2021. Les **fuites de dades** no paren de créixer i el **mercat negre** s'omple d'informació per realitzar noves ofensives.

La ciberseguretat esdevé una prioritat: pressupostos més grans, ajuts, regulacions, sancions per incompliments i accions policials contra l'activitat cibercriminal. La **ciberseguretat** ha esdevingut un aspecte indispensable i estratègic per a la **transformació digital** de la societat, un **pilar** essencial per a la **recuperació econòmica**. Els **pressupostos** de ciberseguretat augmenten i les administracions ofereixen **ajuts econòmics**. Es calcula que hi haurà un creixement d'un **12,5% del mercat mundial** de la ciberseguretat i un **8,1% a l'Estat espanyol**. S'amplia la normativa en matèria de ciberseguretat amb el ***Real Decreto 43/2021*** i les autoritats de protecció de dades incrementen la **severitat i el nombre de sancions** per incompliments de l'**RGPD**. Així, s'imposen **multes de rècord**, entre les quals val la pena ressenyar els **8,1 M€** a **Vodafone**. Cada vegada més, amb la col·laboració internacional, així com entre el sector públic i el privat, les **autoritats policials** actuen contra el **cibercrim**. El principal exemple és l'ofensiva que va acabar amb el **tancament** de la perillosa ***botnet* Emotet**.



Només en el 1r trimestre de 2021, els fons inversors en el sector de la ciberseguretat han superat els 3.000 M€, gairebé la meitat de tot el 2020.



Els ciberatacs a la cadena de subministrament han crescut gairebé un 350% respecte del 1r trimestre de 2020.

Els ciberatacs exploten la confiança en el consum digital, el subministrament de productes i serveis TIC, i la distribució de vacunes. El cibercrim explota la **confiança** en què es basen les **relacions comercials** en la nova realitat digital. El **consum digital** és atacat a través de la **usurpació de la identitat** dels actors que hi participen. Així, el **16% del *phishing*** suplanta **empreses de comerç electrònic**. Respecte el 1r trimestre de l'any passat, es constata un increment del **350%** dels ciberatacs dirigits a la **cadena de subministrament**, amb l'objectiu d'impactar un gran nombre de víctimes, amb especial focus en els **serveis i productes TIC**. La **cadena de distribució de les vacunes**, pel fet de ser un element essencial i pel fet de tenir un alt valor estratègic, també ha estat objectiu de **ciberatacs**, amb un augment del **189%** entre desembre i febrer. En aquest context d'amenaça cibernètica, solucions com ara el **Certificat Verd** busquen establir una base de **confiança, seguretat i privadesa**, per garantir la mobilitat de la ciutadania lliure de virus.

Un sistema on-premise s'allotja dins de les instal·lacions de l'organització que en fa ús.

El SaaS és un model de distribució de programari en el qual un proveïdor de serveis al núvol allotja les aplicacions i n'ofereix l'ús als seus clients a través d'Internet.

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

(font: Termcat)

Ha estat notícia

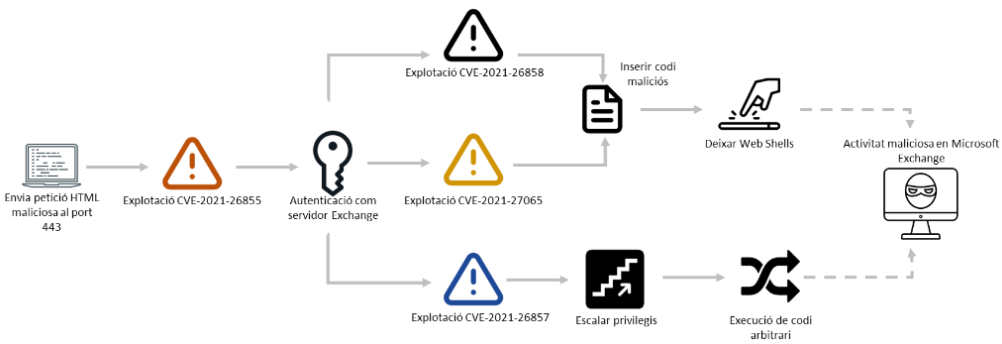
El 2 de març de 2021, Microsoft publicava els pegats de seguretat per a quatre vulnerabilitats crítiques identificades en el programari MS Exchange Server. La publicació dels pegats va originar un augment extraordinari dels ciberatacs. A l'Administració pública catalana, 108 servidors amb MS Exchange van resultar afectats per les vulnerabilitats.

Les vulnerabilitats permeten accedir a servidors de MS Exchange sense credencials, extreure informació i injectar programari maliciós

Microsoft Exchange Server és un **popular servidor de correu electrònic, calendari, contactes** i diverses **aplicacions per al treball en grup** que ha esdevingut una eina de comunicació essencial per a les organitzacions. Els **servidors** MS Exchange són sistemes d'informació centrals, allotgen **grans volums d'informació sensible** (com ara el contingut dels correus electrònics, usuaris i contrasenyes, també dels administradors) i disposen d'accés a la resta de la xarxa corporativa.

Microsoft l'ofereix en modalitats *on-premise* i Saas. En la modalitat *on-premise*, **els clients adquireixen una llicència i s'ocupen de la seva instal·lació i manteniment**, mentre que en la modalitat SaaS és Microsoft qui s'ocupa de fer-ho a canvi d'un pagament mensual. Quan es detecta una vulnerabilitat, en una solució *on-premise,* **el client és el responsable de la instal·lació dels pegats corresponents**.

En aquest sentit, el 1r trimestre de 2021 es van detectar **quatre** vulnerabilitats als servidors de MS Exchange, **classificades** pel fabricant com a **crítiques** i que afectaven gairebé **400.000 servidors** de tot el món (versions 2013, 2016 i 2019)[1,2]. En l'àmbit de l'**Administració pública catalana**, les vulnerabilitats han afectat **108 adreces IP** de servidors de MS Exchange utilitzats per ajuntaments, administracions locals, organismes públics, universitats i centres de recerca i hospitals públics, entre d'altres[3].



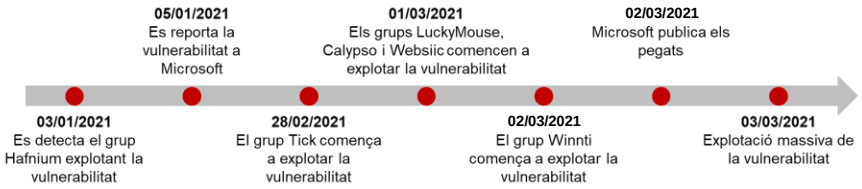
Il·lustració 1. Esquema d'explotació de vulnerabilitats detectades a MS Exchange Server[4].

[1] *https://www.bleepingcomputer.com/news/security/microsoft-92-percent-of-exchange-servers-safe-from-proxylogon-attacks/*
[2] *https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/10886-ccn-cert-al-02-21-vulnerabilidades-zero-day-en-microsoft-exchange.html*
[3] *Font: Agència de Ciberseguretat de Catalunya*
[4] *https://www.bleepingcomputer.com/news/security/the-microsoft-exchange-hacks-how-they-started-and-where-we-are/*

Un **butlletí oficial** emès per l'Agència de Ciberseguretat de Catalunya se'n va fer ressò i va publicar el detall d'aquestes vulnerabilitats crítiques[5]. Descriu com un ciberatacant podria explotar, en primer lloc, la vulnerabilitat CVE-2021-26855, només coneixent la **IP pública** del servidor i un **compte de correu electrònic** per autenticar-se. La resta de vulnerabilitats per dur a terme les diferents accions malicioses s'explotarien després. El ciberatacant tindria l'opció d'**executar codi remot amb privilegis de sistema** a través de la vulnerabilitat CVE-2021-26857, o bé **escriure un arxiu a qualsevol ruta del servidor** i **controlar el sistema** fent ús de les vulnerabilitats CVE-2021-26858 o CVE-2021-27065.

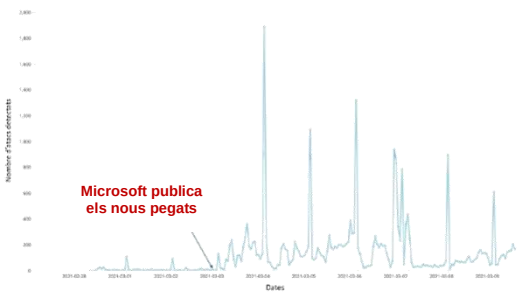
La publicació dels pegats va ser l'origen d'un augment extraordinari dels atacs

El 5 de gener de 2021, un investigador de l'empresa de ciberseguretat taiwanesa DEVCORE[6] es va posar en contacte amb Microsoft per **notificar el descobriment** de la vulnerabilitat CVE-2021-26855. L'afer no es va acabar aquí i, durant les setmanes següents, Microsoft va rebre diversos avisos d'**atacs que explotaven altres vulnerabilitats desconegudes**[7,8]. Al darrere, s'hi identificaven grups APT amb capacitats avançades, com Hafnium[9], Tick, LuckyMouse, Calypso o Winnti, entre d'altres.



Il·lustració 2. Cronograma de la publicació dels pegats de MS Exchange.

A partir del 2 de març, un cop Microsoft **va publicar els pegats** i les vulnerabilitats van esdevenir públiques, **els atacs es van incrementar de manera excepcional**. Una setmana després, Microsoft informava que un 25% dels 400.000 servidors afectats encara no disposaven dels pegats instal·lats i eren vulnerables als ciberatacs.



Il·lustració 3. Deteccions de ciberatacs explotant la vulnerabilitat CVE-2021-26855[10].

[5] *https://ciberseguretat.gencat.cat/web/.content/PDF/Avisos/Butlleti-de-seguretat-Vulnerabilitats-Microsoft-Exchange-marc-2021.pdf*
[6] *https://www.bleepingcomputer.com/news/security/the-microsoft-exchange-hacks-how-they-started-and-where-we-are/*
[7] *https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/*
[8] *https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/*
[9] *https://attack.mitre.org/groups/G0125/*
[10] *https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/*

Així doncs, el 18 de març de 2021[11], l'explotació de les vulnerabilitats als servidors de MS Exchange ja era generalitzada, motiu pel qual Microsoft **va publicar** una **eina** per tal d'automatitzar algunes parts del procés de detecció i d'aplicació del pegat[12].

Organitzacions diverses de tot el món s'han vist afectades per les vulnerabilitats de MS Exchange, també a Catalunya

L'explotació de les vulnerabilitats de MS Exchange s'ha utilitzat per dur a terme diversos atacs de ***ransomware***[13,14,15,16] i difondre ***malware***, com ***backdoors***[17] o programari per a la **mineria furtiva**[18]. En aquest sentit, es va identificar una campanya de difusió de *backdoors* que va arribar a afectar **21.000 servidors**[19]. Els ciberatacs contra entitats governamentals dels EUA[20], el parlament de Noruega[21] i sis agències de govern alemanyes[22] han evidenciat com les vulnerabilitats també s'han aprofitat en **campanyes de ciberespionatge**.

A Catalunya, l'Hospital privat **Dexeus Dona**, va ser víctima d'un ciberatac contra el seu servidor MS Exchange. Afortunadament, els serveis de ciberseguretat de l'hospital van reaccionar ràpidament i van suspendre els serveis de la plataforma de correu electrònic com a mesura cautelar. Ara bé, el centre va haver de **reprogramar** les visites d'uns **2.000 pacients**[23].

Els ciberatacs han impactat arreu del món. L'**Autoritat Bancària Europea**, a París, es va veure obligada a **desconnectar els servidors i supervisar els sistemes** com a mesura de precaució[24]. Als **EUA**, es calcula que **30.000 organitzacions** van ser objectiu de ciberatacs[25], fins al punt que la *Cibersecurity & Infrastructure Security Agency* (CISA) va ordenar l'actualització de les aplicacions de MS Exchange o, en el seu defecte, la desconnexió immediata[26]. A **Àsia**, la multinacional taiwanesa d'ordinadors i dispositius electrònics **Acer Inc**. va ser víctima del robatori d'informació i d'un atac de ***ransomware***[27].

Finalment, cal destacar que un **7% dels afectats** per aquests ciberatacs han estat **proveïdors de software**. Aquests casos són especialment significatius perquè la intrusió dels ciberatacants podria derivar en la instal·lació de codi maliciós en el programari legítim, tal i com va passar en el cas de **Solarwinds** (darrer trimestre de 2020[28]). Les conseqüències, doncs, seran visibles a mitjà i llarg termini[29].

[11] *https://www.rapid7.com/blog/post/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day/*
[12] *https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/*
[13] *https://blog.malwarebytes.com/ransomware/2021/03/ransomware-is-targeting-vulnerable-microsoft-exchange-servers/*
[14] *https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/*
[15] *https://securityaffairs.co/wordpress/115912/malware/black-kingdom-microsoft-exchange.html*
[16] *https://www.bankinfosecurity.com/hades-ransomware-gang-linked-to-exchange-attack-a-16293*
[17] *https://www.microsoft.com/security/blog/2021/03/12/protecting-on-premises-exchange-servers-against-recent-attacks/*
[18] *https://www.bleepingcomputer.com/news/security/microsoft-exchange-exploits-now-used-by-cryptomining-malware/*
[19] *https://krebsonsecurity.com/2021/03/no-i-did-not-hack-your-ms-exchange-server/*
[20] *https://www.ccn-cert.cni.es/informes/abstracts/5753-zero-day-exchange-server-hafnium/file.html*
[21] *https://www.cyberdefensemagazine.com/hackers-stole-data/*
[22] *https://www.tellerreport.com/tech/2021-03-09-%0A---german-government-victim-of-cyber-attack-via-microsoft-mail-servers%0A--.rJQV2lXBQO.html*
[23] *https://cronicaglobal.elespanol.com/vida/dexeus-mujer-reprograma-pruebas-ataque-informatico_458572_102.html*
[24] *https://thehackernews.com/2021/03/microsoft-exchange-hackers-also.html*
[25] *https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/*
[26] *https://noticiasseguridad.com/seguridad-informatica/gobierno-de-e-u-ordena-cerrar-o-actualizar-aplicaciones-de-microsoft-exchange-para-proteger-a-agencias-federales-de-los-hackers-chinos/*
[27] *https://www.pandasecurity.com/es/mediacenter/adaptive-defense/acer-rescate-ransomware/*
[28] *https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know*
[29] *https://blog.checkpoint.com/2021/03/11/exploits-on-organizations-worldwide/*

El cibercrim amenaça els plans de recuperació econòmica i transformació digital amb noves tècniques en els atacs de *ransomware*, DDoS complexos i robatoris de dades

El pla NextGenEU preveu grans inversions per transformar la societat. Ara bé, el desplegament de tecnologies digitals haurà d'enfrontar-se a un cibercrim que evoluciona i fa ús de tècniques molt sofisticades. Els atacs de *ransomware* consoliden l'ús de la doble extorsió i es dirigeixen a directius i organitzacions més grans. Els atacs de DDoS són menys, però són més volumètrics i complexos. Les fuites de dades no paren de créixer i el mercat negre s'omple d'informació per realitzar nous ciberatacs. Els estats patrocinen grups cibercriminals per robar informació o atacar infraestructures crítiques.

El pla NextGenerationEU preveu un fons de 800.000 M€ per transformar i recuperar l'economia. Comportarà un gran desplegament de tecnologies digitals i nous riscos en matèria de ciberseguretat.

Els atacs de *ransomware* amb doble extorsió es consoliden (un 77%) i es contacten mitjans de comunicació i clients de les víctimes per forçar el pagament del rescat. Els atacs es dirigeixen contra directius per tal d'accedir a informació més sensible, i les empreses grans, l'administració pública i el sistema sanitari són objectius preferents. Es realitzen menys atacs de DDoS, però són més volumètrics i complexos per esquivar les proteccions anti-DDoS. Darrerament, les *botnets* utilitzades en atacs de DDoS de baixa intensitat s'empren per a la criptomineria furtiva (*cryptojacking*) arran de l'alt valor de les criptomonedes. El nombre d'incidents de fuites de dades i la informació filtrada creixen i tornen a les elevades xifres d'abans de la pandèmia, però s'identifica més activitat al mercat negre pel valor potencial de les dades per fer nous ciberatacs. A tot aquest clima cal afegir-hi el fet que la competència geoestratègica global promou que els estats patrocinin grups cibercriminals que roben informació estratègica o ataquen infraestructures crítiques.

Aspectes clau:

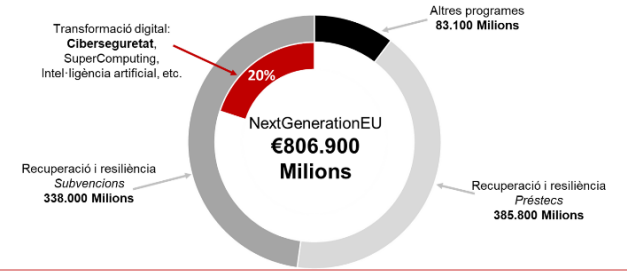
- **El cibercrim, en constant adaptació, buscarà explotar les noves tecnologies desplegades en el marc dels plans de transformació digital.**
- **Després d'incorporar la doble i triple extorsió, els operadors de *ransomware* depuren les seves tècniques i ataquen organitzacions cada vegada més grans, l'administració pública i els centres sanitaris.**
- **Menys atacs de DDoS durant el 1r trimestre, però més potents i elaborats; augmenta la difusió de criptominers furtius.**
- **Les dades personals filtrades, en menys incidents però amb més importants, tenen l'origen en errors de configuració i fan créixer el mercat negre per ser utilitzades en nous ciberatacs.**
- **Amb motivacions geopolítiques, s'intensifiquen amb atacs contra agències governamentals i infraestructures crítiques.**

Baròmetre

Les ciberamenaces posen en risc la transformació digital en què s'ha de basar la recuperació econòmica. Els atacs de *ransomware*, el robatori de dades, els atacs DDoS i l'augment de la mineria són una font d'ingressos principal per al cibercrim.

La nova economia aposta per la digitalització... segura

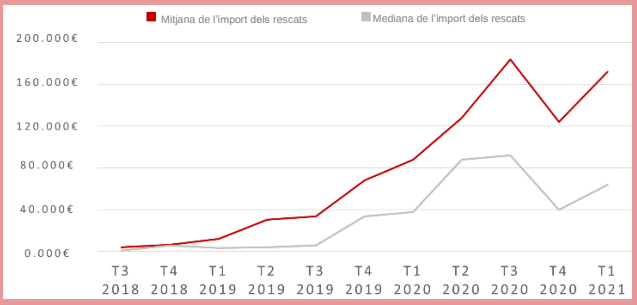
La UE ha posat en marxa el pla NextGenerationEU, un fons de més de 800.000 M€ destinats a la recuperació econòmica a partir d'una transició digital sostenible. Un 20% del pressupost estarà dedicat a la transformació digital, i la ciberseguretat ha d'esdevenir una part essencial per tal que es pugui efectuar de manera segura.



Il·lustració 4. Pressupost NexttGenerationEU [30].

L'import dels rescats del *ransomware* augmenta de nou

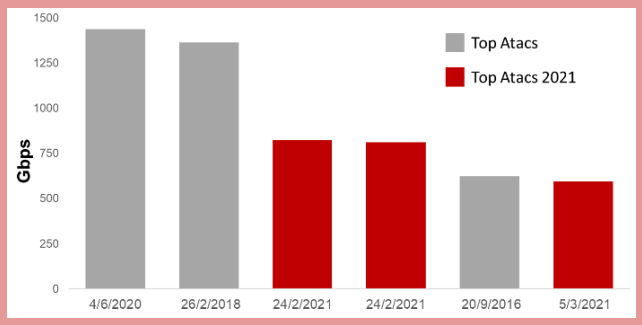
El darrer trimestre de 2020, l'import mitjà dels rescats va baixar respecte del trimestre anterior. No obstant això, ha crescut un 43% durant el primer trimestre de 2021 i ha superat els 180.000 €. Els cibercriminals han adoptat nous factors d'extorsió, com ara el robatori d'informació i l'amenaça de fer-la pública, per mantenir els ingressos.



Il·lustració 5. Evolució de la mitjana i la mediana de l'import dels rescats per atacs de ransomware[31].

Menys atacs de DDoS, però més volumètrics i difícils de bloquejar

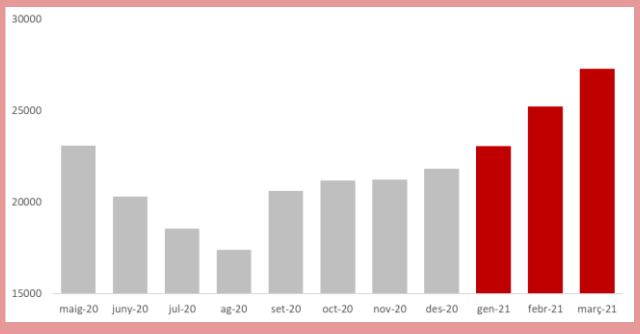
El nombre d'atacs de DDoS ha baixat durant els darrers mesos. Tot i això, aquests són més volumètrics i complexos, o sigui, difícils d'identificar i bloquejar. Tres dels sis atacs DDoS més grans mai registrats per Akamai s'han produït el 2021.



Il·lustració 6. Principals atacs DDoS registrats per Akamai[32].

La criptomineria furtiva creix

La difusió de *malware* de criptomineria furtiva (*cryptojacking*) va baixar amb la caiguda del preu del *bitcoin* durant el 2018 i 2019. Ara bé, la prosperitat del valor de les criptomonedes iniciat el darrer trimestre de 2020 ha promogut un canvi de dinàmica. Així, el 1r trimestre de 2021 respecte del 4t trimestre de 2020, s'ha detectat un increment del 17% en la difusió de *malware* de criptomineria furtiva a Europa[33]. Durant el mes de març, no només el nombre de deteccions va arribar al màxim, sinó que l'aparició de noves versions de *malwares* de mineria es va quadruplicar.



Il·lustració 7. Nombre d'usuaris infectats amb criptominers a Europa des de maig de 2020 a març de 2021[34].

[30] https://op.europa.eu/en/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-es
[31] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[32] https://securityboulevard.com/2021/03/2021-volumetric-ddos-attacks-rising-fast/
[33] https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/
[34] https://securelist.com/it-threat-evolution-q1-2021-non-mobile-statistics/102425/

El cibercrim, en constant adaptació, buscarà explotar les noves tecnologies desplegades en el marc dels plans de transformació digital

El ***World Economic Forum*** (WEF), en l'**informe de riscos globals de 2021**, situa el risc d'una fallada de **ciberseguretat** entre els de **més probabilitat i impacte**. Si es compara amb les conclusions dels darrers anys, ara els principals riscos globals venen marcats per la crisi sanitària de la covid-19 i els relacionats amb el canvi climàtic. Però la **ciberseguretat** es manté en **posicions destacades**[35].

Clarament, la rellevància de la ciberseguretat està impulsada per l'aparició de **tecnologies digitals emergents**, les quals estan esdevenint un pilar fonamental en el desenvolupament de la societat per la seva **capacitat transformadora**. De fet, per sortir de la **crisi econòmica i social** generada per la covid-19, la UE aposta per invertir en tecnologies digitals com les **xarxes 5G, la intel·ligència artificial, la robòtica,** etc. A través del pla de recuperació **NextGenerationEU**, s'impulsarà el paquet d'estímul financer més gran que hagi desplegat la UE en un pressupost. En total, seran **800.000 M€** entre els anys 2021 i 2027, amb l'objectiu d'assolir una UE més ecològica, digital i *resilient* (veure il·lustració 4)[36].

Ara bé, el **desplegament de noves tecnologies i projectes** de gran envergadura promogut pels fons NextGenerationEU comportarà **reptes** igualment importants en matèria de **ciberseguretat**. El **cibercrim**, que ha demostrat a bastament com s'adapta a la situació conjuntural en cada moment, ben segur que posarà el seu **punt de mira en les noves iniciatives digitals**. Per aquest motiu, la ciberseguretat esdevindrà un element cabdal per tal de construir una **UE digitalment avançada**, però també **resilient i segura**. El pla NextGenerationEU ha de garantir la transformació de la societat del vell continent, sí, però només ho aconseguirà si garanteix la **confiança en unes tecnologies emergents segures**.

La resiliència és la capacitat d'un sistema informàtic de recuperar-se davant d'un atac.

(font: Termcat)

La necessitat de ciberseguretat dels propers anys vindrà acompanyada de la preocupació per la **manca de professionals i talent** en la matèria. A dia d'avui, la **demanda de professionals** de la ciberseguretat ja és elevada i no està coberta, però amb iniciatives com el pla NextGenerationEU **la situació s'agreujarà** encara més. En concret, s'estima que seran necessaris molts especialistes pel que fa a la seguretat en el desenvolupament d'aplicacions o seguretat al núvol[37].

A l'Estat espanyol, actualment ja queda palesa la necessitat d'augmentar el **nivell de preparació** en matèria de ciberseguretat. Només el **44%** de les empreses té una visió concreta de l'estratègia en ciberseguretat a seguir, i coneix les noves oportunitats i amenaces que es presenten[38]. En canvi, en relació amb la transformació digital, el **56%** de les empreses compta amb **plans concrets de transformació digital** per liderar els canvis necessaris[39]. El desajust que hi ha entre plans de digitalització i compromís amb la ciberseguretat és prou evident, i posa de manifest que encara queda molta feina per fer. Especialment si es pensa en l'horitzó del pla NextGenerationEU, que ha de revolucionar la transformació digital a Europa en els pròxims anys.

[35] *http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf*
[36] *https://ec.europa.eu/info/strategy/recovery-plan-europe_es*
[37] *https://www.forbes.com/sites/louiscolumbus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/*
[38] *https://www.minsait.com/es/actualidad/insights/ascendant-2020-21-ciberseguridad*
[39] *https://factorialhr.es/blog/transformacion-digital-empresas-espana/*

El ransomware, o programari de segrest, és un programari maliciós que restringeix totalment o parcialment l'accés als fitxers d'un dispositiu fins que no es paga una determinada quantitat de diners.

(font: Termcat)

La doble extorsió és un ciberatac que consisteix a extorsionar la víctima amb la combinació de dues pràctiques: un atac de ransomware *acompanyat del robatori de dades i l'amenaça de la publicació si no es fa el pagament d'un rescat.*

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..

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

(font: Termcat)

Després d'incorporar la doble i triple extorsió, els operadors de *ransomware* depuren les seves tècniques i ataquen organitzacions cada vegada més grans, l'administració pública i els centres sanitaris

Els atacs de *ransomware* no han deixat d'evolucionar i ja incorporen habitualment la doble extorsió. Durant el 1r trimestre de 2021, el **77%** dels atacs de *ransomware* **robaven i amenaçaven de filtrar les dades de les víctimes**, una xifra que representa el **10% més** que el trimestre anterior[40]. I, per a més inri, diferents grups cibercriminals han anunciat la utilització de la triple extorsió, amb la incorporació d'atacs DDoS. Grups com ara Clop i REvil són exemples d'aquesta evolució.

No només s'han incorporat nous factors d'extorsió, també es depuren les **tècniques d'atac** per incrementar-ne l'impacte. D'una banda, es fa ús de **trucades telefòniques a periodistes o a socis** de les entitats afectades per **pressionar** encara més les companyies[41]. D'altra banda, els atacs es dirigeixen contra **alts executius** per poder accedir a **informació confidencial més sensible i crítica**. També, cal destacar com, durant aquest 1r trimestre, s'ha fet ús de l'**explotació de noves vulnerabilitats**, en especial les identificades en servidors de **MS Exchange**[42] (veure capítol Ha estat notícia).

A més a més, s'ha constatat que les **organitzacions objectiu** dels atacs de *ransomware* són cada vegada **més grans**. La mida mitjana de les entitats víctimes de *ransomware* ha crescut un **400%** en un any i, actualment, és de **612 treballadors**[43]. Destaca el cas del fabricant d'ordinadors **ACER** que, amb més de 7.000 empleats[44], va rebre un atac de *ransomware* a través de l'explotació de les vulnerabilitats de MS Exchange i en el qual es va exigir un pagament de **43 M€**. A dia d'avui, es tracta d'un **import rècord**[45].

Amb els factors d'extorsió addicionals i les noves tècniques, els ciberdelinqüents poden pressionar les víctimes amb l'exigència de **rescats més elevats**. Si bé l'import mitjà dels rescats va experimentar una davallada a final del 4t trimestre del 2020, el 1r trimestre de 2021 ha pujat un **43%** i ha arribat als **182.000 €**, gairebé el doble que fa un any (veure il·lustració 5)[46]. La intensa activitat dels **nous grups cibercriminals**, com els que hi ha al darrere dels *ransomwares* de Clop o Darkside, els quals han entrat en el *top 10* dels principals grups cibercriminals per primer cop, hi ha contribuït sensiblement[47].

L'**administració i el sector públic** de l'**Estat** han estat objectiu de l'increment i la virulència dels atacs de *ransomware*. De fet, els incidents han estat una constant durant el 1r trimestre. El ***Servicio Público de Empleo Estatal*** (SEPE) va ser víctima del *ransomware* Ryuk, el qual va paralitzar l'activitat de l'organisme, tant a les **710 oficines** que presten servei presencial com a les **52 telemàtiques**[48]. L'**Àrea Metropolitana de Barcelona** (AMB) també va ser víctima d'un *ransomware* de característiques molt similars[49]. Tots dos organismes asseguren que no van tenir fuites de dades. Els ajuntaments també han tingut el seu capítol particular. L'**Ajuntament de Sitges** va ser objecte d'un intent de xifratge dels seus sistemes i, tot i que es va limitar l'accés a la xarxa del consistori des de l'exterior com a mesura de protecció, es van poder

[40] *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020*
[41] *https://securityaffairs.co/wordpress/115345/cyber-crime/revil-ransomware-ddos-voice-calls.html*
[42] *https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report*
[43] *https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report*
[44] *https://www.acer-group.com/sustainability/en/staff-structure.html*
[45] *https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/*
[46] *https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound*
[47] *https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report*
[48] *https://www.computing.es/seguridad/noticias/1124280002501/ciberataque-paraliza-sepe-toda-espana.1.html*
[49] *https://www.muyseguridad.net/2021/03/16/area-metropolitana-de-barcelona/*

El cryptojacking, o mineria furtiva, és una pràctica fraudulenta consistent a utilitzar la capacitat de càlcul computacional d'un dispositiu aliè per fer criptomineria sense el coneixement del propietari.

(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)

organitzar les eleccions autonòmiques catalanes amb normalitat, celebrades pocs dies més tard.[50] L'**Ajuntament d'Arenys de Mar** també va viure un atac que va paralitzar totalment les operacions informàtiques[51], com els consistoris de **Cambrils**[52] i de **Castelló de la Plana**[53].

El **sector sanitari** tampoc ha escapat dels atacs de *ransomware*. De fet, els hospitals han estat un dels **principals objectius** dels cibercriminals des de l'inici de la pandèmia. Destaquen diversos atacs a **hospitals francesos**, que han portat el **govern** a **prendre mesures** dràstiques. El president francès, Emmanuel Macron va prometre una inversió de **1.000 M€** en ciberseguretat, com a resposta als continus atacs al sector sanitari. Segons Macron aquests atacs mostren "la vulnerabilitat i la importància de fer un pas endavant en inversions en ciberseguretat"[54].

Menys atacs de DDoS durant el 1r trimestre, però més potents i elaborats; augmenta la difusió de criptominers furtius

Durant l'any 2020, el **nombre d'atacs de DDoS** va créixer més del **154%** respecte de 2019. No obstant això, la tendència a l'alça es va aturar en el darrer trimestre del 2020 i ha continuat **a la baixa en el 1r trimestre del 2021**[55].

Ara bé, segons Akamai, els atacs de DDoS presenten **magnituds més grans**, **més complexitat** i **persistència**. En aquest sentit, el 1r trimestre de 2021, han estat detectats **3 dels 5 atacs més grans registrats** mai per Akamai (veure il·lustració 6)[56]. D'aquests atacs, el més volumètric, amb **824 Gbps**, es va dirigir contra una empresa d'apostes europea. A més, es tractava d'un atac de DDoS complex, atès que es va utilitzar el protocol de xarxa *Datagram Congestion Control Protocol* (DCCP), diferent del tràfic TCP o UDP utilitzat habitualment en aquest tipus d'atacs. L'objectiu era **esquivar les mesures de protecció anti-DDoS**. L'altre atac, el mateix dia, es va dirigir contra una empresa de videojocs asiàtica amb una ràfega de **812 Gbps**. Pel que fa a la persistència, Akamai també informa d'un altre atac amb un flux de dades sostingut per sobre de **200 Gbps** durant més de **9 hores**[57].

Els atacs DDoS dels últims mesos també evidencien una orientació clara a l'exigència d'un rescat (**RDDoS** o *Rescue* DDoS), una pràctica a través de la qual els ciberdelinqüents extorsionen la víctima amb la **saturació de les comunicacions** mentre no faci el **pagament d'un rescat**[58]. En aquest sentit, des del darrer trimestre de 2020, l'empresa de ciberseguretat Cloudflare constata una tendència a l'alça de les campanyes de RDDoS per extorsionar organitzacions i apunta que un **13%** dels seus clients n'han estat víctimes[59].

El **motiu** que hi ha al darrere del **descens** del nombre d'atacs de **DDoS** podria ser l'**augment del preu de les criptomonedes**. A causa d'aquest increment, el *cryptojacking*, o **criptomineria furtiva**, ha esdevingut un **bon negoci**. Així, segons Kaspersky, els cibercriminals que operen les *botnets* treuen **més beneficis** difonent miners o minant directament que no pas **llogant-les per**

[50] *https://www.lavanguardia.com/local/catalunya/20210219/6256322/mossos-esquadra-investigan-ataque-informatico-ayuntamiento-sitges.html*
[51] *https://www.lavanguardia.com/local/barcelona/20210122/6189766/veintena-ayuntamientos-atacados-ciberdelincuentes.html*
[52] *https://www.diaridetarragona.com/costa/Los-hackers-piden-al-Ayuntamiento-de-Cambrils-un-rescate-en-bitcoins-para-desbloquear-su-servidor-20201223-0035.html*
[53] *https://www.xataka.com/seguridad/ayuntamiento-castellon-sufre-ciberataque-se-queda-acceso-al-sistema-informatico-web-municipal-portal-tributario*
[54] *https://www.lemagit.fr/actualites/252496034/Cyberattaques-BVA-et-la-mutuelle-nationale-des-hospitaliers-allongent-la-liste*
[55] *https://www.ehackingnews.com/2021/02/ddos-attacks-increase-by-154-in-2020.html*
[56] *https://securityboulevard.com/2021/03/2021-volumetric-ddos-attacks-rising-fast/*
[57] *https://cybersecuritynews.com/ddos-attacks-peaked-at-800gbps/*
[58] *https://www.bleepingcomputer.com/news/security/800gbps-ddos-extortion-attack-hits-gambling-company/*
[59] *https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1/*

Un servidor C&C és un ordinador central que emet ordres a una xarxa de zombis i rep informes de tornada dels mateixos zombis.

(font: Termcat)

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

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.

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)

realitzar atacs de DDoS[60]. Així, és possible que servidors C&C hagin perfilat les seves xarxes de bots perquè dediquin la potència informàtica per minar i obtenir criptomonedes.

En aquesta línia, cal destacar com la **pujada del valor de les criptomonedes** ha intensificat la difusió de ***malware* per a la mineria furtiva**. Durant el darrer trimestre del 2020, aquesta pràctica va augmentar un **53%**, i la tendència ha continuat durant el 1r trimestre amb un creixement del **17%** (veure il·lustració 7)[61]. Cal destacar el cas de l'ús d'**imatges de disc** amb *malware* de *criptojacking* incorporades en els contenidors disponibles a Docker Hub, de les quals se n'haurien fet aproximadament **20 milions de descàrregues**[62].

Les dades personals filtrades, en menys incidents però amb més importants, tenen l'origen en errors de configuració i fan créixer el mercat negre per ser utilitzades en nous ciberatacs

Els **incidents** amb fuita de dades són **menys en nombre**, però cada vegada són **més massius**. El **número d'incidents** segueix una tendència a la baixa: és un **28%** inferior respecte el 1r trimestre de 2020 i està un **12% per sota del trimestre passat**. Ara bé, segueix pujant el volum de registres filtrats: creix un **96%** respecte el 1r trimestre de 2020 i ni més ni menys que un **1.435% respecte el trimestre passat**.

Val la pena destacar la quantitat d'incidents causats per **errors de configuració**, els quals s'han incrementat un **310%** durant els darrers mesos[63], principalment a causa dels **serveis d'emmagatzematge al núvol** mal configurats. Es calcula que el **93%** de les implementacions al *cloud* han estat l'origen de més de **200 bretxes** en els últims **dos anys**, les quals han exposat més de **30.000 milions** de registres de dades personals[64].

Són moltes les fuites de dades causades per errors de configuració que s'han viscut durant el darrer trimestre. **Socialarks**, una empresa dedicada a la gestió de xarxes socials, va experimentar la filtració de dades personals de més de **200 milions d'usuaris** de Facebook, Instagram i LinkedIn. La causa va ser un motor de cerca **ElasticSearch** insegur que allotjava **408 GB** de dades personals d'usuaris de les xarxes socials. Tot indica que les dades filtrades s'haurien obtingut massivament mitjançant eines de *scrapping*[65]. Un altre exemple és la fuita d'FBS, un corredor de comerç en línia amb seu a Xipre i utilitzat per milions de comerciants de més de **190 països**: es van exposar més de **16.000 milions de registres** de dades personals per un error de configuració, novament en un servidor **ElasticSearch**. Es tracta d'una fuita extraordinàriament gran, oimés si es té en compte que, durant tot 2020, es van filtrar **37.000 milions de registres**; així, la fuita de FBS equivaldria al **43%**[66] del total. La filtració incloïa informació d'identificació personal (PII), com ara informació financera, documents governamentals i, fins i tot, contrasenyes en text pla[67].

[60] *https://www.kaspersky.com/about/press-releases/2021_a-matter-of-profit-ddos-attacks-in-q4-2020-dropped-by-a-third-compared-to-q3-as-cryptomining-is-on-the-rise*
[61] *https://chaslescorp.com/coin-mining-malware-volumes-soar-53-in-q4-2020/*
[62] *https://threatpost.com/malicious-docker-cryptomining-images/165120/*
[63] *https://www.hackerone.com/resources/hackerone/the-rise-of-misconfiguration-and-supply-chain-vulnerabilities*
[64] *https://solutionsreview.com/cloud-platforms/accurics-93-percent-of-cloud-deployments-featured-misconfigured-storage-services/*
[65] *https://hotforsecurity.bitdefender.com/blog/over-200-million-facebook-instagram-and-linkedin-profiles-exposed-through-unsecured-database-held-by-chinese-startup-25067.html*
[66] *https://www.securityinfowatch.com/cybersecurity/press-release/21207207/riskbased-security-risk-based-security-releases-its-yearend-2020-data-breach-report*
[67] *https://securityaffairs.co/wordpress/115925/data-breach/fbs-data-breach.html*

El credential stuffing, o farciment de credencials, és una tècnica d'atac que utilitza credencials robades, normalment adreces de correu electrònic, noms d'usuari i contrasenyes, per accedir sense autorització als comptes d'usuari. Utilitza com a premissa que els usuaris reutilitzen les mateixes contrasenyes en diferents comptes.

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 d'encriptació, dels paquets a diferents punts remots, i utilitza infraestructures públiques de transport.

(font: Termcat)

Les **dades filtrades** s'utilitzen, cada vegada més, per a l'**extorsió** de les organitzacions que les custodiaven amb l'amenaça de publicar-les. El fet és que la revelació d'una fuita de dades pot comportar importants **sancions econòmiques** per incompliment de les lleis de protecció de dades personals, així com la **pèrdua de reputació**. És el cas del **centre terapèutic Vastaamo** (Finlàndia), que va patir el **robatori** de les notes terapèutiques d'uns **40.000 pacients**. L'entitat va encobrir l'atac, però posteriorment els pacients van ser extorquits directament pels ciberdelinqüents i el centre, finalment, s'ha declarat en **fallida** durant el 2021[68].

En altres casos, les dades filtrades s'utilitzen per dur a terme **nous ciberatacs**. Per exemple, la plataforma Spotify va identificar un atac de *credential stuffing* dirigit contra **100.000 usuaris**, en el qual es feia servir una base de dades amb informació recopilada de **fuites anteriors**[69]. Un altre cas sonat és el de T-Mobile, una empresa de telecomunicacions dels EUA, la qual va patir una fuita de dades que, posteriorment, va ser utilitzada per dur a terme **duplicats de targetes SIM** de telefonia mòbil. Es dona el cas que les dades robades incloïen informació que facilitava la **usurpació d'identitat** en el procés de sol·licitud de duplicats de targeta SIM[70].

No hi ha cap mena de dubte que la utilitat de les dades personals filtrades n'incentiva el valor. Això es constata en una major **activitat en el mercat negre** a la *dark web*, on **es venen** o **es comparteixen** dades personals en diferents fòrums[71]. El preu varia en funció de la sensibilitat de les dades, el seu potencial per ajudar a dur a terme nous atacs i la quantitat de registres. Així, no fa pas gaire, experts en seguretat van descobrir la venda de més de **21 milions de registres** d'usuaris en un fòrum de ciberdelinqüents informàtics; s'hi incloïen credencials d'usuari de tres serveis diferents *VPN* d'Android: **SuperVPN** (amb més de 100 milions d'instal·lacions a Play Store), **GeckoVPN** (més de 10 milions d'instal·lacions) i **CatVPN** (més de 50.000 instal·lacions). En aquestes fuites hi havia noms, adreces, contrasenyes, informació de targeta de crèdit... Un conjunt de dades que obren la possibilitat de perpetrar un gran ventall d'activitats fraudulentes[72].

La ciberamenaça amb motivacions geopolítiques s'intensifica amb atacs contra agències governamentals i infraestructures crítiques

Els **ciberatacs patrocinats per estats** han estat una constant aquest darrer trimestre. Les **tensions geopolítiques** entre Washington i les altres dues grans potències, Rússia i la Xina, en són un dels motius principals. Aquests ciberatacs són utilitzats com a **armes diplomàtiques i polítiques**, per demostrar obertament que si un estat pot realitzar ciberatacs contra un altre és que en coneix els punts febles i que no tem un pols cibernètic[73].

Un exemple d'aquesta tensió és el ciberatac a la cadena de subministrament de **Solarwinds** de finals de 2020, que encara cueja. Les **autoritats nord-americanes** apunten que forma part d'una **campanya de *hacking* molt sofisticada d'origen rus** que tenia com a objectiu nou agències governamentals i 100 empreses privades; a més d'utilitzar la difusió de programari maliciós a través del *software* legítim de Solarwinds, en un 30% dels

[68] https://www.computerweekly.com/news/252496227/Hacked-Finnish-therapy-business-collapses
[69] https://www.darkreading.com/attacks-breaches/spotify-hit-with-another-credential-stuffing-attack/d/d-id/1340083
[70] https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/
[71] https://www.ehackingnews.com/2021/03/data-of-21-million-vpn-users-leaked.html
[72] https://www.ehackingnews.com/2021/03/data-of-21-million-vpn-users-leaked.html
[73] https://www.france24.com/es/ee-uu-y-canad%C3%A1/20210309-eeuu-joe-biden-ciberespionaje-rusia-china

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 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)

*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)

casos s'han identificat altres tècniques de ciberatac. També s'ha identificat la intrusió a través d'accessos de terceres parts a comptes d'Office 365, Azure i Amazon Web Services, amb l'ús de tècniques més rudimentàries com ara el *phishing* o el descobriment de contrasenyes dels comptes d'administrador[74].

Des de l'altra banda, el **govern rus** també té la ciberseguretat ben present a la seva agenda. Ha emès una guia de ciberseguretat per a les empreses russes, amb l'excusa que estan en risc de ser objecte de **ciberespionatge per part dels EUA** com a **represàlia** per l'atac de SolarWinds. El missatge afirmava que l'administració de Joe Biden amenaçava amb **atacs** contra la **infraestructura crítica russa**[75].

L'ofensiva cibernètica entre els estats té, al darrere, **grups cibercriminals molt capacitats**. Focalitzen els atacs en agències governamentals, per obtenir informació estratègica, o en infraestructures crítiques, per causar un impacte greu a un rival geoestratètic. En aquest sentit, en els darrers mesos, els ciberatacs contra infraestructures de **serveis bàsics, com ara l'energia elèctrica, l'aigua, el petroli o el gas**, han estat notícia[76]. Als EUA, la **planta de tractament d'aigua** d'Oldsmar, a Florida, va ser víctima d'un atac cibernètic. Tot i que no sembla que els autors de l'atac tinguessin una motivació geopolítica, el fet és que van aconseguir internar-se al sistema a través de **TeamViewer** i van arribar a **modificar els nivells d'hidròxid de sodi**[77].

En alguns casos, els responsables dels atacs són grups APT que disposen del **suport d'un estat**. En aquest sentit, s'ha de destacar que, per causa de les intenses tensions frontereres entre l'Índia i la **Xina**, diversos investigadors en ciberseguretat han identificat grups patrocinats per l'estat xinès que han encetat una **campanya concertada** contra infraestructures crítiques de l'Índia, inclosa la **xarxa elèctrica del país i dos ports marítims**. Però les acusacions no només involucren la Xina, també s'acusa la **Índia** d'estar darrere d'un grup APT que ha patrocinat atacs de *phishing* dirigits a entitats governamentals i militars xineses[78].

En els temps actuals, l'ofensiva cibernètica amb motivacions geopolítiques s'ha evidenciat en un **increment dels atacs a la cadena de subministrament de la vacuna**. Es té constància de grups cibercriminals subvencionats per estats que han realitzat campanyes de ciberatacs contra centres de recerca del coronavirus, fabricants de vacunes, hospitals, etc (veure capítol Els ciberatacs exploten la confiança en el consum digital, el subministrament de productes i serveis TIC, i la distribució de vacunes).

Recomanacions

- **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.**

[74] *https://www.cnet.com/news/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/*
[75] *https://www.oodaloop.com/briefs/2021/01/25/russian-government-agency-warns-firms-of-us-attack/*
[76] *https://www.zdnet.com/article/these-four-new-hacking-groups-are-targeting-critical-infrastructure-warns-security-company/*
[77] *https://www.techrepublic.com/article/fbi-secret-service-investigating-cyberattack-on-florida-water-treatment-plant/*
[78] *https://thehackernews.com/2021/03/chinese-hackers-targeted-indias-power.html*

- **Les organitzacions han de realitzar anàlisis de riscos en el tractament de dades personals (Avaluació d'Impacte de Dades Personals) per tal d'establir les mesures de protecció adequades a les dades personals que garanteixin el compliment normatiu.**
- **Les organitzacions han de realitzar campanyes de conscienciació en matèria de ciberseguretat entre els empleats, socis, 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 han d'aproximar models de confiança zero amb la segregació dels serveis interns de la xarxa empresarial i disposar de protecció perimetral.**
- **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. Per exemple: atacs de *ranomware*, de DDoS...**
- **Les organitzacions han de disposar de proteccions anti-DDoS per als recursos essencials visibles des d'Internet.**
- **Les administracions governamentals han d'elaborar anàlisis de riscos periòdiques i plans estratègics en matèria de ciberseguretat i resiliència per fer front als constants canvis socials i tecnològics.**

Fets rellevants

- L'Àrea Metropolitana de Barcelona (AMB), víctima d'un atac de *ransowmare*. Arran d'aquest atac, es van veure afectats els serveis de tramitació electrònica, altres serveis digitals i les instal·lacions que gestiona aquest ens[79].
- El *Servicio Público de Empleo Estatal* (SEPE) va patir un ciberatac amb el *ransomware* Ryuk, que va paralitzar l'activitat a tot l'Estat, tant a les 710 oficines de servei presencial com a les 52 finestretes telemàtiques. Un mes després del ciberatac, calia fer el pagament de prestacions i no s'atenien noves demandes dels ciutadans. No es va informar si els ciberatacants van fer petició de rescat, raó per la qual hi ha la sospita que la motivació de l'atac era simplement causar danys[80].
- En un atac de *ransomware* a l'ajuntament de Sitges, els actors maliciosos van intentar esborrar les còpies de seguretat del sistema i xifrar-ne la informació, però no van afectar els serveis orientats a la ciutadania. Després de l'atac, l'ajuntament va restringir el teletreball i l'accés des de l'exterior a la xarxa municipal[81].
- Un atac de *ransomware* va paralitzar l'ajuntament de Castelló de la Plana. Els serveis del web municipal, la seu electrònica, el portal tributari, així com el sistema informàtic intern, van quedar sense accés a les dades[82].
- L'ajuntament de la ciutat francesa de Houllies va quedar paralitzat per un atac de *ransomware* que va bloquejar la pàgina web, així com els serveis municipals de TI. Els processos digitals i el correu electrònic van deixar de funcionar. Tot i que no es van donar detalls de l'atac, tot apunta cap a un atac de *ransomware*[83].
- La *Feria Virtual Internacional de Tecnologia para el Proceso Industrial* de L'Hospitalet de Llobregat es va haver de posposar per causa d'un ciberatac. L'organització va anunciar l'ajornament després de rebre, el primer dia de l'esdeveniment, milers de visites provinents de l'Iran, el Sudan i Corea del Nord, entre altres, que van afectar l'accés dels visitants[84].
- Es va detectar un atac de DDoS amb extorsió de rècord, amb un flux de 800 Gbps contra una empresa de jocs i apostes d'Europa. Es tractava d'un atac complex, pel fet d'utilitzar el protocol de xarxa *Datagram Congestion Control Protocol* (DCCP), diferent del tràfic TCP o UDP utilitzat habitualment, amb l'objectiu d'esquivar les mesures de protecció anti-DDoS[85].
- L'empresa de *trading* FBS va exposar 20 TB de dades amb 16.000 milions de registres que incloïen dades personals de milions de clients de la companyia. La informació estava accessible en un servidor d'Elasticsearch sense les mesures de seguretat necessàries[86].
- Es van filtrar 4.000 documents de l'Agència de Protecció del Medi Ambient d'Escòcia (SEPA) arran de la negativa a pagar un rescat. Els ciberatacants havien perpetrat un atac de *ransomware* durant les festes de Nadal, van xifrar el sistema de correu electrònic i contactes, i van robar la informació[87].
- El mes de gener de 2021, les dades personals de 223 milions ciutadans brasilers i més de 104 milions de matrícules de vehicles es van detectar en una base de dades a la venda al mercat negre. L'*Autoridade Nacional de Proteção de Dados*, creada a partir de l'entrada en vigor de la *Lei Geral de Proteção de Dados* (LGPD) de 2020, va alertar els ciutadans de futures campanyes de *phishing*[88].
- La planta de tractament d'aigua d'Oldsmar, a l'estat nord-americà de Florida, va ser víctima d'una intrusió cibernètica. Els atacants van accedir-hi a través dels accessos de TeamViewer i van aconseguir modificar els nivells d'hidròxid de sodi (sosa càustica): de 100 a 11.100 parts per milió, amb el risc d'enverinament de més de 15.000 persones. Afortunadament, un operador va detectar el moviment i el va corregir sense més conseqüències. L'accés remot va ser desactivat després de l'incident[89].

[79] *https://www.elperiodico.com/es/barcelona-metropolitana/20210315/amb-victima-ciberataque-paralizado-servicios-11579815*
[80] *https://www.xataka.com/seguridad/asi-ryuk-ransomware-que-ha-dejado-tumbado-al-sepe-que-antes-tumbo-a-otros-muchos/*
[81] *https://www.eixdiari.cat/societat/doc/94306/els-mossos-desquadra-investiguen-un-atac-informatic-a-lajuntament-de-sitges.html*
[82] *https://www.xataka.com/seguridad/ataque-ransomware-hospital-moises-broggi-barcelona-colapsa-algunos-servicios-secundarios*
[83] *https://www.databreaches.net/fr-yvelines-the-town-of-houilles-paralyzed-by-a-cyberattack/*
[84] *http://www.lafarga.com/corporatiu/un-ciberataque-obliga-a-aplazar-la-feria-virtual-internacional-de-tecnologia-para-el-proceso-industrial/*
[85] *https://www.bleepingcomputer.com/news/security/800gbps-ddos-extortion-attack-hits-gambling-company/*
[86] *https://securityaffairs.co/wordpress/115925/data-breach/fbs-data-breach.html*
[87] *https://tfun.org/2021/01/24/ransomware-group-published-more-than-4000-sepas-files-online/*
[88] *https://brasil.elpais.com/brasil/2021-01-26/todos-os-brasileiros-estao-com-seus-dados-a-venda-e-ha-muito-pouco-o-que-se-pode-fazer-para-se-proteger.html*
[89] *https://www.techrepublic.com/article/fbi-secret-service-investigating-cyberattack-on-florida-water-treatment-plant/*

La ciberseguretat esdevé una prioritat: pressupostos més grans, ajuts, noves regulacions, sancions per incompliments i accions policials contra l'activitat cibercriminal

La ciberseguretat ha esdevingut un aspecte indispensable i estratègic per a la transformació digital de la societat que ha de servir de fonaments per a la recuperació econòmica. Els pressupostos en ciberseguretat augmenten i les administracions ofereixen ajuts econòmics. Neix el *Real Decreto 43/2021* ampliant la regulació en ciberseguretat actual i les autoritats en matèria de protecció de dades apliquen més sancions i més severes als incompliments normatius; a l'Estat espanyol s'imposen multes de rècord. Nombroses accions policials, amb col·laboració internacional, així com entre el sector públic i el privat, promouen operacions contra el cibercrim, com en el tancament de la *botnet* Emotet.

La ciberseguretat ha esdevingut un aspecte estratègic per fer possible la transformació digital de la societat sobre la qual s'ha de construir la recuperació econòmica després dels estralls de la covid-19. A més, la ciberseguretat és imprescindible per fer front al 20% d'increment del nombre de ciberatacs que es va identificar el 2020. Així, es calcula que hi haurà un creixement del mercat de la ciberseguretat d'un 12,5% al món i un 8,5%, a l'Estat espanyol. Per contribuir en aquest increment de despesa en ciberseguretat, el govern de l'Estat preveu 450 M€ i la Generalitat promou ajuts com el programa de cupons d'ACC1Ó a la competitivitat de l'empresa.

Més enllà de les inversions i ajuts, l'Estat espanyol reforça la seva normativa. Després de la transposició de la Directiva NIS, s'ha publicat el *Real Decreto 43/2021* pel seu desenvolupament, amb impacte en els Operadors de Serveis Essencials (OES) i els Proveïdors de Serveis Digitals (DSP). D'altra banda, després de gairebé tres anys de l'entrada en vigor de l'RGPD, les sancions creixen pel que fa al nombre i import. L'AEPD és qui més ha sancionat, amb multes milionàries durant el 1r trimestre de 2021.

La col·laboració policial coordinada entre països, i entre el sector públic i privat, ha permès desmantellar grups cibercriminals. Les activitats criminals més cercades han estat dirigides als responsables de les activitats criminals més actives: *ransomware*, *botnets*, mercats negres, ciberatacs a les botigues en línia, estafes de *smishing* i duplicats de targetes SIM. Destaca el tancament de la *botnet* Emotet, una greu amenaça des del 2014.

Aspectes clau:

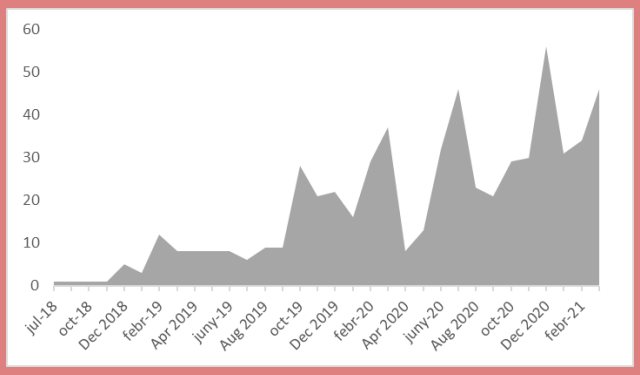
- **En resposta als reptes de la transformació digital i l'increment dels ciberatacs, augmenta el pressupost i se segueix desenvolupant la normativa de ciberseguretat.**
- **Després d'una fase de transició, les sancions de l'RGPD esdevenen més severes: l'Estat espanyol és qui més sanciona i amb quantitats més elevades.**
- **Les forces de l'ordre actuen contra l'activitat del cibercrim: *ransomware*, *botnets*, mercats negres, ciberatacs a les botigues en línia, estafes de *smishing* i duplicats de targetes SIM.**

Baròmetre

La recuperació econòmica dels estralls de la pandèmia serà digital. Per assegurar-ne l'èxit, calen mesures per reforçar el nivell de ciberseguretat i el nivell de confiança digital. En aquest context, creix l'exigència pel compliment de l'RGPD, les forces de l'ordre intensifiquen les accions contra les activitats cibercriminals, els pressupostos en ciberseguretat creixen i es desenvolupa nova normativa per tal de reforçar les capacitats del teixit econòmic digital.

Les sancions per incompliment de l'RGPD són més i més altes

Des de l'entrada en vigor de l'RGPD, el nombre de sancions ha crescut paulatinament. El 1r trimestre de 2021, el nombre de sancions ha estat un 35% superior respecte del 1r trimestre de 2020. L'Estat espanyol s'ha convertit en el país amb més sancions.



Il·lustració 88. Sancions/mes per incompliment normatiu de l'RGPD[90].

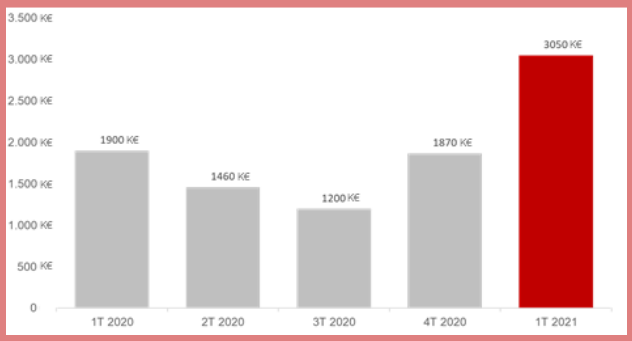
Els imports de les sancions s'han disparat des de desembre de 2020 a l'Estat espanyol. De fet, tres de les cinc sancions més importants fixades per l'AEPD s'han produït durant el 1r trimestre de 2021. A final de 2020, l'RGPD acumulava 112 M€ en concepte de sancions a tota la UE.

Data	Sanció (€)	Entitat Sancionada
11/3/2021	8.150.000	Vodafone España, S.A.U.
13/1/2021	6.000.000	Caixabank S.A.
11/12/2020	5.000.000	Banco Bilbao Vizcaya Argentaria, S.A.
15/3/2021	600.000	Air Europa Lineas Aereas, SA.
11/6/2019	250.000	Professional Football League (LaLiga)

Il·lustració 9. Principals sancions fixades per l'AEPD en base a l'RGPD[91].

Els fons per a la ciberseguretat arriben a xifres rècord durant el 1r trimestre

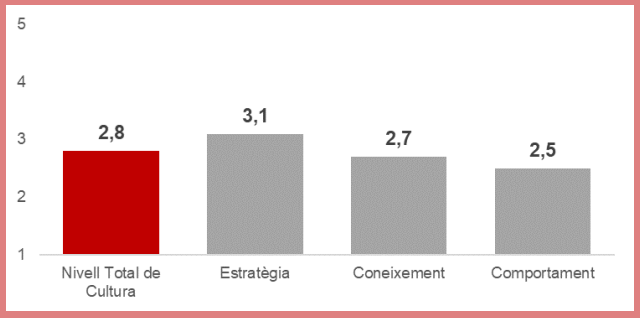
Els fons destinats a la indústria de la ciberseguretat van arribar als 6.000 M€ el 2020, i s'ha convertit en el cinquè sector amb més finançament al món. La tendència a l'alça continua i, en només un trimestre de 2021, s'ha arribat als 3.000 M€ invertits a tot el món, aproximadament la meitat de tot el 2020.



Il·lustració 90. Fons destinats al sector de la ciberseguretat al món[92].

Cal desenvolupar la cultura en ciberseguretat de les empreses de l'Estat

Les empreses de l'Estat espanyol necessiten fer un pas endavant en matèria de ciberseguretat si volen fer front als reptes digitals i a l'augment dels atacs cibernètics. Un informe de PwC valora el nivell cultural de les empreses de l'Estat amb un 2,8 sobre 5. Això significa poca maduresa i un marge de millora important i necessari. Les companyies amb una millor cultura en ciberseguretat són les que tenen més de 10.000 empleats, precisament les que disposen d'un pressupost més elevat i un grau més gran d'exposició a les amenaces.



Il·lustració 101. Avaluació del nivell de cultura en ciberseguretat de les empreses a l'Estat espanyol, per PwC[93].

[90] *https://www.enforcementtracker.com/?insights*
[91] *https://www.enforcementtracker.com/*
[92] *https://about.crunchbase.com/cybersecurity-research-report-2021/*
[93] *https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html*

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.*

En resposta als reptes de la transformació digital i l'increment dels ciberatacs, augmenta el pressupost i se segueix desenvolupant la normativa de ciberseguretat

La **ciberseguretat** ha esdevingut un aspecte indispensable i estratègic per fer possible la **transformació digital** de la societat. El creixement de l'amenaça cibernètica hi té molt a veure: el 2020 es van detectar **119.000 ciberatacs/minut**, un **20%** més que el 2019[94].

Per aquest motiu, els **fons d'inversió globals en ciberseguretat** augmentaran més d'un **10%** durant el 2021[95] i, només durant el 1r trimestre de l'any 2021, els fons han arribat als **3.000 M€**, la meitat del total registrat el 2020[96] (veure il·lustració 10). Aquestes xifres evidencien els bons auguris de creixement del sector. En aquest sentit, s'estima que el mercat mundial de seguretat cibernètica ha mogut **130.000 M€** el 2020 i es calcula un creixement anual del **12.5%** (superarà els **350.000 M€** el **2028**[97]). A l'Estat espanyol, la predicció és que el mercat de la ciberseguretat creixi un **8,1%** respecte del 2020 i que arribi als **1.324 M€**[98].

En la mateixa línia, el Govern de l'Estat espanyol destinarà **11.000 M€** a digitalitzar les pimes, l'Administració i la formació tecnològica de la ciutadania fins al 2023[99]; d'aquests, **450 M€** estaran **destinats a la ciberseguretat**[100]. Aquest és un pas endavant important, ja que es creu un **86%** de les empreses espanyoles **no tenen una cultura suficient de ciberseguretat**[101] (veure il·lustració 11). Anàlogament, el Govern de la Generalitat de Catalunya ha concedit els **cupons ACC1Ó** a la competitivitat de l'empresa, un **programa d'ajuts** dirigit a pimes per a la contractació de serveis d'innovació i implementació de tecnologies que incloguin aspectes relacionats amb la transformació tecnològica cap a la indústria 4.0. El programa inclou la **ciberseguretat**, però també la Internet de les Coses (IoT), el Big Data, la Intel·ligència Artificial, el *blockchain*...[102].

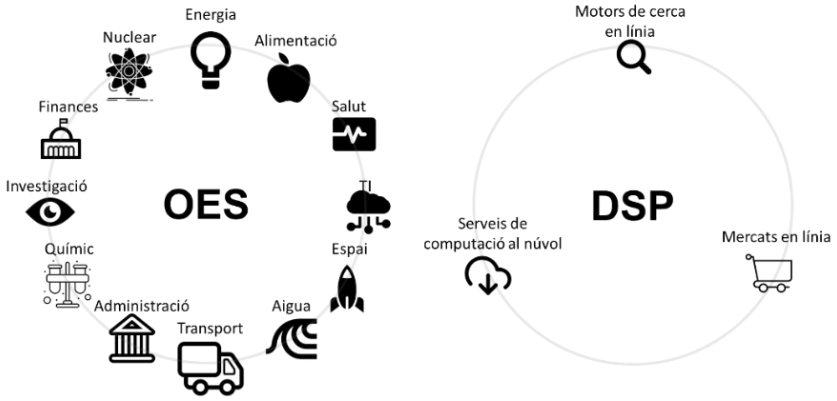
Més enllà de les inversions i ajuts en ciberseguretat, l'Estat espanyol ha procedit a **reforçar la normativa**. Així, després de transposar la Directiva NIS de la UE amb el *Real Decreto-Ley 12/2018 de Seguridad de las redes y sistemas de información*, el 26 de gener del 2021 publicava detalls per al seu desenvolupament mitjançant el *Real Decreto 43/2021*[103]*.* Aquest reial decret té impacte en dos tipus d'entitats: els **Operadors de Serveis Essencials** (OES) i els **Proveïdors de Serveis Digitals** (DSP). També, identifica les **autoritats** per exercir funcions tant de **vigilància** com **sancionadores**, i els **equips de resposta a incidents** de seguretat informàtica de referència[104].

[94] *https://www.itdigitalsecurity.es/endpoint/2021/02/en-2020-se-detectaron-119000-amenazas-por-minuto-un-20-mas-que-en-2019*
[95] *https://www.helpnetsecurity.com/2021/01/26/cybersecurity-investments-2021/*
[96] *https://about.crunchbase.com/cybersecurity-research-report-2021/*
[97] *https://www.globenewswire.com/news-release/2021/03/17/2194254/0/en/Global-Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html*
[98] *https://www.redseguridad.com/actualidad/ciberseguridad/el-sector-de-la-ciberseguridad-crecera-hasta-llegar-a-los-1-324-millones-de-euros-en-2021-en-espana_20210222.html*
[99] *https://elpais.com/tecnologia/2021-01-27/el-gobierno-destinara-11000-millones-a-digitalizar-las-pymes-la-administracion-y-a-mejorar-la-formacion-tecnologica.html*
[100] *https://www.xataka.com/pro/academia-hacker-estatal-inversion-450-millones-euros-asi-quiere-gobierno-impulsar-ciberseguridad-espanola*
[101] *https://confilegal.com/20210129-el-86-de-las-empresas-espanolas-carecen-de-cultura-de-ciberseguridad/*
[102] *http://www.accio.gencat.cat/ca/serveis/cercador-ajuts-empresa/ajutsiserveis/20239_Cupons_Industria4.0*
[103] *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192*
[104] *https://www2.deloitte.com/es/es/pages/risk/articles/transposicion-directiva-nis.*

CISO (Chief Information Security Officer) és el director de seguretat de la informació d'una organització i màxim responsable de garantir els seus bens i tecnologies d'informació.

L'RGPD és un reglament europeu d'obligat compliment 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 a risc.



Il·lustració 12. Operadors de Serveis Essencials (OES) i Proveïdors de Serveis Digitals (DSP) afectats per la Directiva NIS i les seves transposicions nacionals.

La norma estableix un **marc estratègic i institucional de seguretat** per a les xarxes i sistemes d'informació, en el qual es desenvolupa la **supervisió del compliment de les obligacions** per als operadors de serveis essencials i serveis digitals, així com la **gestió dels incidents de ciberseguretat**. Destaca l'article 11.2 on s'estableix que el **CCN-CERT** esdevé el responsable d'exercir la coordinació nacional de la resposta tècnica dels CSIRT en els incidents d'especial gravetat[105]. En els articles 8 i 9, s'estipula la **notificació d'incidents** i obliga els operadors de serveis essencials a informar dels incidents que puguin alterar significativament els seus serveis o afectar les seves xarxes i sistemes d'informació[106]. Un altre aspecte rellevant és que les empreses afectades pel reial decret estan obligades a designar una **persona, entitat o òrgan col·legiat** com a **Responsable de Seguretat de la Informació** o CISO. Aquesta figura exercirà de punt de contacte amb l'autoritat competent i supervisarà que l'empresa compleixi amb els requisits de ciberseguretat que exigeix la normativa[107].

Al mateix temps, a la **UE** s'ha adoptat la proposta per revisar la Directiva NIS amb l'objectiu de resoldre les seves deficiències i donar lloc a la **Directiva NIS 2.0**. En aquesta nova Directiva, s'inclouen **nous sectors** en base a la seva **importància per la societat i l'economia**, eliminant la distinció entre OES i DSP. Ara, la proposta està subjecta a la discussió i l'aprovació dels Estats[108].

Després d'una fase de transició, les sancions de l'RGPD esdevenen més severes: l'Estat espanyol és qui més sanciona i amb quantitats més elevades

Per combatre les amenaces cibernètiques, les autoritats no només han de perseguir l'activitat dels ciberdelinqüents, també han de **promoure** que la **ciutadania i les empreses** apliquin les **mesures de ciberseguretat adequades**. En aquesta línia, l'RGPD és una normativa que estableix la necessitat de protegir les dades personals dels ciutadans de la UE i, en cas d'incompliment, estableix **sancions** que poden arribar als **20 M€** o al **4% del volum de negoci anual** per a les empreses[109].

[105] *https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/10774-publicado-en-el-boe-el-real-decreto-ley-de-transposicion-de-la-directiva-europea-nis.html*
[106] *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-*
[107] *https://edorteam.com/importantes-cambios-ciberseguridad-empresas-real-decreto-43-2021/*
[108] *https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union*
[109] *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

L'RGPD és vigent des del 25 de maig de 2018. Tanmateix, durant els dos primers anys de vida, les **multes** establertes han estat molt **lluny dels imports màxims exigibles**. Ha estat durant els darrers mesos de 2020 i el 1r trimestre de 2021 que les tant el nombre com la quantitat de les **sancions s'han incrementat sensiblement** (veure il·lustració 8)[110].

Aquesta **crescuda de l'import de les sancions** de l'RGPD es constata clarament a l'**Estat espanyol** (veure il·lustració 9). Des del 2019, la multa més elevada que havia imposat l'*Agencia Española de Protección de Datos* (AEPD) eren els **250.000 €** de la *Liga de Futbol Profesional* (LFP). Ara bé, el desembre del 2020, el **BBVA** rebia una sanció de **5 M€**[111] i s'obria una nova etapa de sancions elevades. Així, el 1r trimestre del 2021, **CaixaBank** ha estat sancionada amb **6 M€**[112], i l'empresa de telecomunicacions **Vodafone** ha rebut la multa rècord de **8,1 M€**[113]. Aquest trimestre, només han estat superades per una sanció de l'**agència alemanya**: **10 M€** a l'empresa de venda en línia de dispositius electrònics **Notebooksbilligerde**[114]. L'AEPD també ha sancionat amb **600.000 €** a Air Europa Líneas Aéreas[115] i a Redes Eléctricas Inteligentes S.A.U amb **200.000 €**[116]. Amb aquestes multes, l'AEPD situa l'Estat espanyol entre els cinc països que han acumulat sancions econòmiques més elevades.

Il·lustració 13. Top 5 d'estats segons l'acumulat de sancions de l'RGPD.

L'Estat espanyol no només destaca per l'increment de l'import de les multes, també és el país que més sancions ha imposat en la història de l'RGPD.

Il·lustració 14. Top 5 de països segons el nombre de sancions de l'RGPD.[117]

De la mateixa manera, en altres països, també s'han fixat noves sancions milionàries que estableixen un rècord nacional. A Noruega, per exemple, s'ha multat amb **10 M€** l'app de la cites **Grindr**[118].

Les forces de l'ordre actuen contra l'activitat del cibercrim: *ransomware*, *botnets*, mercats negres, ciberatacs a les botigues en línia, estafes de *smishing* i duplicats de targetes SIM

Amb l'objectiu d'assegurar un **entorn propici per a la transformació digital** venidora, és imprescindible **fer front a la ciberdelinqüència**, cada vegada més coordinada i capacitada. Així ho entenen les autoritats que, durant el 1r trimestre

[110] *https://www.enforcementtracker.com/?insights*
[111] *https://confilegal.com/20201214-la-aepd-impone-5-millones-de-euros-de-sancion-al-bbva-por-vulnerar-tres-articulos-del-rgpd-la-mas-alta-de-la-historia-de-la-autoridad/*
[112] *https://www.xataka.com/legislacion-y-derechos/multa-record-agencia-proteccion-datos-a-caixabank-6-millones-euros-forzar-cesion-datos-personales*
[113] *https://www.xataka.com/legislacion-y-derechos/multa-record-a-vodafone-espana-aepd-8-1-millones-euros-saltarse-proteccion-datos-no-frenar-acciones-comerciales-cuando-se-les-pedia*
[114] *https://www.zdnet.com/article/gdpr-german-laptop-retailer-fined-eur10-4m-for-video-monitoring-employees/*
[115] *https://www.preferente.com/noticias-de-transportes/noticias-de-aerolineas/air-europa-multa-de-600-000e-por-el-ataque-a-datos-de-sus-clientes-307957.html*
[116] *https://www.aepd.es/es/documento/ps-00197-2020.pdf*
[117] *https://www.enforcementtracker.com/*
[118] *https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-intention-issue-eu-10-million-fine-grindr-llc_en*

de 2021, han desplegat un gran nombre d'**operacions contra el cibercrim**, les quals han exigit la **cooperació internacional**, així com entre les **forces de l'ordre i les empreses de ciberseguretat**.

Una de les operacions més rellevants ha estat el **desmantellament de la *botnet* Emotet**. La policia de **sis països europeus**, així com del **Canadà** i dels **EUA**, va completar una operació conjunta per **detenir els responsables** i **prendre el control dels servidors** d'Internet utilitzats per executar i controlar la xarxa de *malware* coneguda com Emotet[119]. El cas és que Emotet, un programari maliciós nascut el 2014, s'havia convertit en la *botnet* més perillosa per la seva capacitat d'infecció i pel fet de ser utilitzada en importants campanyes de distribució de *ransomware*[120].

Parlant de ciberamenaces, els atacs de *ransomware* són una de més rellevants dels darrers temps, motiu pel qual **les accions policials contra els operadors de programari de segrest s'han intensificat**. És destacable com les autoritats franceses i ucraïneses van poder **localitzar i detenir tres membres** de l'operador de *ransomware* **Egregor**. Les detencions van ser el resultat d'una investigació a partir d'una sèrie de ciberatacs contra empreses franceses com **Ubisoft**, **Gefco** i **Ouest France**[121]. Anàlogament, l'operador del *ransomware* **NetWalker** també ha estat objectiu de les accions de la justícia nord-americana en col·laboració amb cossos policials internacionals. Van aconseguir tombar part de la infraestructura tecnològica i emetre càrrecs contra els responsables de Netwalker i, fins i tot, recuperar part de les desenes de milions d'euros pagats per part de les víctimes. Netwalker ha estat un *ransomware* especialment perillós i actiu contra el sector sanitari durant la pandèmia de la covid-19.[122].

El **mercadeig de dades personals robades**, utilitzades per dur a terme ciberatacs, també s'ha convertit en una autèntica amenaça. Per aquest motiu, les accions contra els **mercats negres de la *dark web*** també han estat recurrents. En aquest sentit, **Joker's Stash**, probablement la botiga de targetes de crèdit més antiga i coneguda a la web fosca, **va anunciar el seu tancament** el 15 de febrer, després que la Interpol i l'FBI confisquessin els seus servidors[123]. D'altra banda, la policia alemanya va tancar **DarkMarket**, el "mercat negre més gran del món". En el moment del tancament, tenia gairebé **500.000 usuaris,** més de **2.400 venedors** i acumulava **140 M€ en transaccions**, ja que, segons l'Europol, la pandèmia de coronavirus ha portat gran part del comerç de narcòtics a operar en línia. Un ciutadà australià de 34 anys, que es creu que era l'operador de DarkMarket ,va ser **arrestat** a prop de la frontera germano-danesa i més de **20 servidors** a Moldàvia i Ucraïna van ser confiscats[124].

Las autoritats també han perseguit els ciberdelinqüents responsables de **ciberatacs contra el comerç electrònic**. Precisament, la Interpol va **detenir tres ciberdelinqüents** que es dedicaven a injectar codi maliciós als formularis de les botigues en línia per robar les dades dels clients de les botigues en línia. En aquest cas, la Interpol va col·laborar amb l'empresa de ciberseguretat Group-IB per descobrir **centenars de webs de comerç en línia que havien estat infectats** en diferents punts de tot el planeta[125]. Així mateix, la Interpol també va detenir 5 persones que formaven part del **grup cibercriminal InfinityBlack**, responsable de la distribució de *malware*, eines de pirateria, fraus i el robatori de credencials[126].

[119] *https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action*
[120] *https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action*
[121] *https://therecord.media/frances-lead-cybercrime-investigator-on-the-egregor-arrests-cybercrime/*
[122] *https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware*
[123] *https://unaaldia.hispasec.com/2021/01/jokers-stash-conocida-tienda-en-la-deep-web-anuncia-su-cierre.html*
[124] *https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down*
[125] *https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/INTERPOL-contribuye-a-la-detencion-de-unos-ciberdelincuentes-que-atentaban-contra-sitios-web-de-compra-en-linea*
[126] *https://www.cyberdefensemagazine.com/law-enforcement-agencies-dismantled-infinity-black-hacker-group/*

A **Catalunya**, el Mossos d'Esquadra, en col·laboració amb la *Policía Nacional* espanyola, també han actuat contra el cibercrim amb èxit. Van **detenir deu persones** a L'Hospitalet de Llobregat en una operació contra els responsables d'una campanya de **duplicat de targetes SIM** que havia afectat **més d'un centenar de víctimes** de tot l'Estat espanyol i havia aconseguit robar **600.000 €**[127]. També, durant el 1r trimestre de 2021, els Mossos d'Esquadra van **detenir quatre persones**, d'entre 19 i 27 anys, que havien enviat **71.000 SMS** amb enllaços maliciosos que portava les víctimes a un web on se suplantaven entitats bancàries i operadors mòbils per robar-los les credencials[128]. I de forma molt similar, a València, els agents de la *Policía Nacional* van **detenir un home** de 25 anys com a presumpte autor d'un delicte d'estafa després d'obtenir, també mitjançant l'*smishing*, **dades de més de 4.000 targetes bancàries**, **comprar en diferents comerços** i **retirar diners en caixers automàtics**.

Recomanacions

- **Les organitzacions han de realitzar campanyes de conscienciació i formació en matèria de ciberseguretat entre els treballadors, socis i col·laboradors per capacitar-los contra les amenaces cibernètiques.**
- **Les organitzacions han d'elaborar i desplegar un pla de compliment normatiu proactiu, que identifiqui els marcs reguladors interns i externs aplicables, que apliqui les directrius i normes emeses, i que avaluï periòdicament el nivell de compliment.**
- **Les organitzacions han de realitzar un Estudi d'Impacte de Protecció de Dades (EIPD), en el qual s'analitzin els riscos i s'estableixin mesures de protecció adequades per garantir la seguretat i la privacitat de les dades de caràcter personal.**
- **Les organitzacions han de disposar de les mesures tècniques i organitzatives adients per detectar i notificar els incidents cibernètics a les autoritats competents en la matèria i informar les agències de ciberseguretat.**
- **Les organitzacions que tractin dades de caràcter personal han de notificar a les autoritats de protecció de dades les violacions de seguretat que afectin als drets i llibertats de les persones físiques que hagin estat objecte del tractament.**
- **Les organitzacions han d'elaborar anàlisis de riscos que identifiquin, especialment, els actius crítics i que despleguin mesures de prevenció, protecció i resposta proporcionals.**
- **Les organitzacions han d'elaborar plans de seguretat per desplegar les mesures de ciberseguretat pertinents i cercar opcions de finançament o ajudes econòmiques dels estaments públics.**
- **Les administracions governamentals han de revisar els seus plans estratègics de col·laboració en ciberseguretat i resiliència per fer front a les constants oportunitats de canvi social, tecnològic i climàtic com a mínim cada dos anys.**

[127] *https://cronicaglobal.elespanol.com/vida/cibercrimen-detenidos-estafar-victimas_358704_102.html*
[128] *https://www.ara.cat/societat/cau-grup-criminal-estafava-enviant-milers-sms-enllacos-fraudulents_1_3890631.html*

Fets rellevants

- Multa rècord de l'AEPD a Vodafone Espanya: 8,1 M€. Sembla que Vodafone encara no ha explicat la raó per la qual els usuaris que han sol·licitat cancel·lar les seves dades per rebre accions de màrqueting continuen rebent-les. És la multa més important imposada per l'AEPD a l'Estat espanyol[129].
- L'AEPD sanciona amb 6 M€ CaixaBank per incompliment de l'RGPD i la LOPDGDD arran de la denúncia d'un client "per imposar-li l'obligació d'acceptar les noves condicions en matèria de protecció de dades personals, en concret la relativa a la cessió de les dades personals a totes les empreses del grup". L'AEPD ha desestimat una tercera sanció pel tractament automatitzat de perfils[130].
- WhatsApp podria ser multada amb fins a 50 M€ per no informar eficaçment els seus usuaris de la UE sobre com les dades serien compartides amb Facebook, segons informa la *Data Protection Commission* d'Irlanda[131].
- Les autoritats policials dels EUA i Europa han requisat llocs de la web fosca associats a les operacions del *ransomware* NetWalker. En un informe d'agost de 2020, els investigadors de seguretat de McAfee van estimar que els ingressos totals generats per NetWalker havien superat els 20 M€ el juliol de 2020. El Departament de Justícia dels EUA va assenyalar que NetWalker s'ha utilitzat en atacs contra serveis d'emergència, hospitals, forces de l'ordre, municipis, districtes escolars, col·legis, universitats i empreses privades[132].
- La policia de sis països europeus, així com del Canadà i dels EUA, va completar una operació conjunta per a prendre el control dels servidors d'Internet utilitzats per controlar la *botnet* Emotet. S'ha tractat del programari maliciós més emprat pels cibercriminals durant el desembre de 2020 a l'Estat espanyol. En concret, va afectar el 15% de les companyies espanyoles, i el 7% a la resta del món[133].
- Joker's Stash, una botiga coneguda a la web fosca, el 15 de febrer va anunciar el seu tancament, després que la Interpol i l'FBI confisquessin servidors *proxy* que s'utilitzaven per mantenir dominis basats en *blockchain*. També es destaca que tan la quantitat com la qualitat de les dades publicades havien disminuït. Després d'interrompre breument l'activitat, va anunciar el tancament complet i definitiu[134].
- La policia alemanya tanca el mercat DarkMarket, el més gran del món a la web fosca, que tenia gairebé 500.000 usuaris i més de 2.400 venedors. Val a dir que la pandèmia de coronavirus ha portat gran part del comerç de carrer de narcòtics a connectar-se a Internet. Un ciutadà australià de 34 anys, que es creu que era l'operador de DarkMarket, va ser arrestat molt a prop de la frontera germano-danesa; una vintena de servidors a Moldàvia i a Ucraïna van ser confiscats[135].
- Als EUA, després de l'impacte de l'atac de SolarWinds, la Casa Blanca treballa en una odre que obligarà tots els proveïdors del govern federal a complir uns estàndards de seguretat i millorar la capacitat de coordinació contra un incident. L'objectiu és millorar la seguretat de les cadenes de subministrament de l'administració nord-americana i les agències federals[136].
- El president Emmanuel Macron promet una inversió milionària en ciberseguretat després dels continus atacs al sector sanitari. El president francès ha promès una inversió de 1.000 M€ en ciberseguretat arran de l'onada d'atacs contra hospitals durant el mes de febrer de 2021 i, de fet, durant tot el 2020. Segons Macron, aquests atacs mostren "vulnerabilitat i la importància de fer un pas endavant en inversions en ciberseguretat"[137].

[129] *https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-75000-eur-vodafone_en*
[130] *https://elpais.com/economia/2021-01-15/seis-millones-de-multa-a-caixabank-por-el-tratamiento-ilicito-de-los-datos-de-sus-clientes.html*
[131] *https://www.politico.eu/article/whatsapp-privacy-fine-data-protection-europe-50-million/*
[132] *https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware*
[133] *https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action*
[134] *https://unaaldia.hispasec.com/2021/01/jokers-stash-conocida-tienda-en-la-deep-web-anuncia-su-cierre.html*
[135] *https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down*
[136] *https://www.cyberscoop.com/cyber-executive-order-supply-chain-solarwinds/*
[137] *https://www.efe.com/efe/america/mundo/macron-defiende-una-mayor-inversion-para-proteger-hospitales-de-ciberataques/*

Els ciberatacs exploten la confiança en el consum digital, el subministrament de productes i serveis TIC, i la distribució de vacunes

El cibercrim explota la confiança en què es basen les relacions comercials de la nova realitat digital. La cadena de consum és atacada mitjançant la usurpació de la identitat dels actors que hi participen, ja siguin organitzacions o els ciutadans mateixos. A partir de l'atac de Solarwinds, es constata un increment de ciberatacs dirigits a la cadena de subministrament de productes i serveis TIC, amb l'objectiu d'impactar un gran nombre de víctimes. La cadena de distribució de les vacunes, pel fet de ser un element essencial i tenir un alt valor estratègic , també ha estat blanc dels ciberatacs. En aquest context, hi ha solucions com el Certificat Verd que busquen establir una base de confiança, seguretat i privadesa, per garantir la mobilitat lliure de virus de la ciutadania.

Els consum en línia ha crescut molt durant la pandèmia i la confiança entre consumidors i proveïdors de serveis i productes en línia és un punt feble. Els ciberdelinqüents suplanten la identitat digital d'un element confiable amb l'objectiu d'obtenir de manera fraudulenta un benefici econòmic.

Els proveïdors de software estan en el punt de mira dels ciberatacs: la motivació dels atacants és explotar la relació de confiança amb els clients. Si aconsegueixen comprometre el proveïdor, poden impactar els seus consumidors de forma massiva i sense impediments.

Un cop més, el cibercrim aprofita les necessitats generades per la pandèmia. Dirigeixen ciberatacs contra la cadena de distribució de les vacunes, un element crític i indispensable, amb l'objectiu d'aconseguir un gran impacte i influir en la lluita contra la covid-19.

Per poder recuperar la normalitat, la UE crearà el Certificat Verd, amb l'objectiu d'acreditar l'estat immunitari de la ciutadania i permetre la lliure mobilitat entre els estats membres. El certificat ha de generar confiança, garantint la privacitat dels ciutadans i prevenir falsificacions.

Aspectes clau:

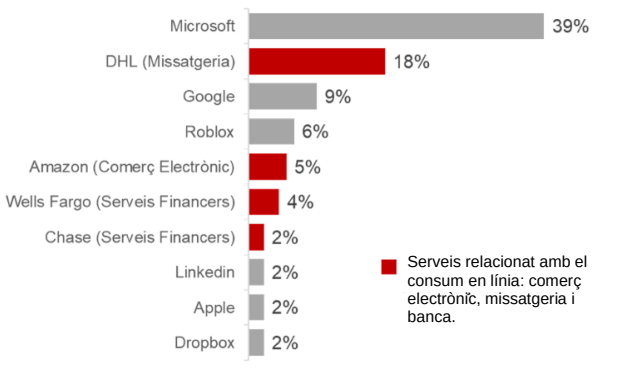
- **El cibercrim explota la confiança entre els diferents elements del consum digital mitjançant la suplantació de les marques i els consumidors.**
- **El cibercrim explota la confiança amb els proveïdors de productes i serveis TIC per dur a terme ciberatacs amb impactes massius entre els seus clients.**
- **El cibercrim ataca la cadena de subministrament de la vacuna, un entorn essencial i de confiança, amb l'objectiu de robar informació de valor estratègic i causar un impacte crític en la lluita contra la covid-19.**
- **El Certificat Verd neix amb mesures de ciberseguretat per fer front al risc de falsificació i la pèrdua de privacitat, amb l'objectiu de generar la confiança necessària per un desplegament exitós.**

Baròmetre

Els ciberdelinqüents exploten la relació de confiança entre els elements de les cadenes de subministrament del comerç electrònic, productes i serveis TIC i la mateixa vacuna. En aquest context, el Certificat Verd digital neix per ser una eina confiable i a prova de fraus, i garantir la mobilitat de persones immunitzades a la UE.

Empreses de comerç electrònic, missatgeria i banca, entre les més suplantades

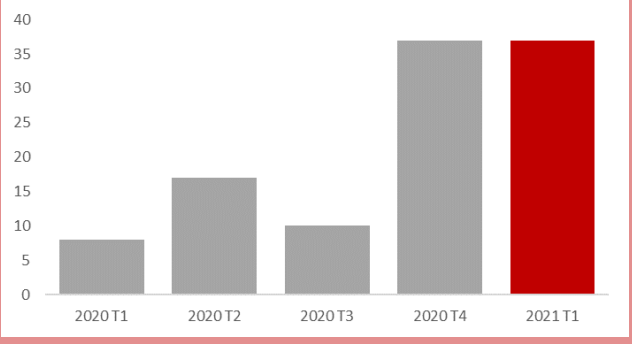
Entre les 10 empreses més suplantades en atacs de *phishing*, a banda dels gegants tecnològics, s'hi troben empreses relacionades amb el consum en línia: comerç electrònic, missatgeria i banca. El seu ús ha esdevingut intensiu durant la pandèmia.



Il·lustració 15. Principals marques suplantades en atacs de phishing *durant el 1r trimestre de 2021*[138].

Increment dels atacs cibernètics a la cadena de subministrament

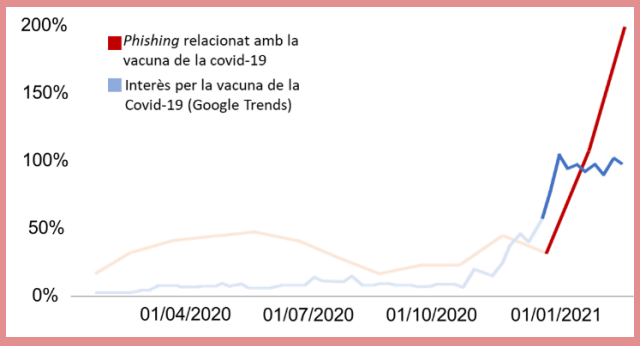
Durant dos trimestres seguits, els ciberatacs a la cadena de subministrament de productes i serveis es mantenen en cotes altes. Aquests atacs han crescut gairebé un 350% respecte del 1r trimestre de 2020.



Il·lustració 16. Incidents detectats contra la cadena de subministrament. (font: Agència)

Les campanyes de *phishing* relacionades amb la vacuna augmenten

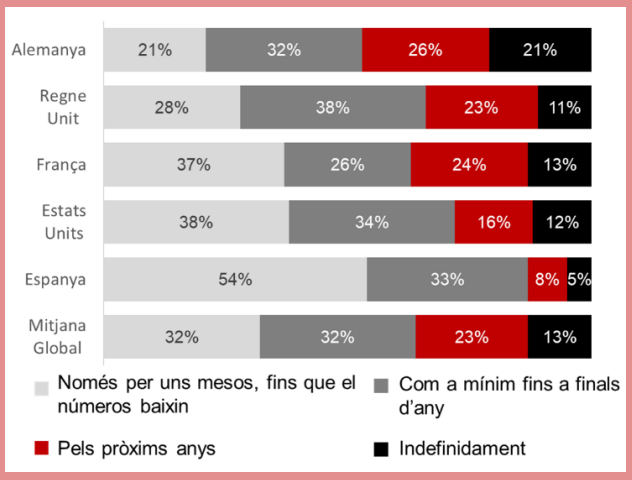
Els darrers mesos de 2020, les campanyes de *phishing* amb temàtica relacionada amb les vacunes han crescut al mateix ritme que ho feia l'interès de la ciutadania per tot allò que tenia a veure amb la vacunació. Entre el desembre de 2020 i el febrer de 2021, aquests atacs de *phishing* es van disparar un 530%.



Il·lustració 117. Relació entre el phishing *amb la vacuna com esquer i l'interès de la ciutadania en les cerques a Google* [139].

Neix el passaport sanitari

De la voluntat de restablir la normalitat neixen els passaports sanitaris per certificar la immunitat a la covid-19 i moure's lliurament entre països de la UE. La confiança de la ciutadania en el Certificat Verd no és unànime: calen mesures de ciberseguretat adequades per evitar-ne la falsificació i preservar la privacitat dels ciutadans si es vol garantir-ne l'ús.



Il·lustració 18. Opinió dels ciutadans de diferents països sobre l'ús dels passaports sanitari[140].

[138] *https://blog.checkpoint.com/2021/04/15/microsoft-continues-to-be-most-imitated-brand-for-phishing-attempts-in-q1-2021/*
[139] *https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/*
[140] *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN*

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)

Una injecció de codi, o un atac de formulari, és un atac en què el ciberdelinqüent injecta codi maliciós en el formulari de pagament d'un lloc web, per tal de poder obtenir les dades bancàries que la víctima hi introdueix i, més endavant, vendre-les al web fosc.

(font: Termcat)

El cibercrim explota la confiança entre els diferents elements del consum digital mitjançant la suplantació de les marques i els consumidors

Arran de la pandèmia, les autoritats han pres mesures de confinament i restriccions a la mobilitat entre la població. Aquest fet ha motivat que molts consumidors fessin un ús intensiu d'Internet per adquirir productes i serveis. Només a l'Estat espanyol, el comerç electrònic va marcar un nou record històric amb més de **258 milions de transaccions** durant el 3r trimestre, la qual cosa ha suposat un **creixement del 22,9%** respecte del 2019[141].

La **confiança dels consumidors en les marques** és**,** en realitat, un **punt feble** que els ciberdelinqüents aprofiten. Els ciberdelinqüents l'aprofiten per **suplantar** la identitat digital d'un element confiable amb l'objectiu d'obtenir un **benefici econòmic** de forma fraudulenta. Dirigeixen els seus ciberatacs a tos els actors del **consum digital**: des de la compra en línia fins el lliurament dels productes adquirits, inclosa la relació amb les entitats financeres i les institucions públiques pel pagament dels tributs o la sol·licitud d'ajuts.

Així, tot i que les marques més suplantades pels ciberdelinqüents en les campanyes de *phishing* són els gegants digitals, a continuació s'hi poden trobar **empreses de comerç electrònic, missatgeria i banca**: DHL 18%, Amazon 5%, i els bancs Wells Fargo 4% i Chase 2% (veure il·lustració 15)[142].

Il·lustració 19. *Elements de la cadena consum del comerç electrònic..*

Suplantació d'empreses de comerç electrònic

Durant el 1r trimestre de 2021, el **15,77%** de les **campanyes de *phishing*** han suplantat **marques de comerç electrònic**, les quals s'han convertit en sector més afectat[143]. Destaca el cas d'**Amazon**, líder absolut. Els ciberdelinqüents s'han fet passar per la marca per enviar correus electrònics als consumidors tot utilitzant noms de dominis o webs similars. Oferien a la víctima un **premi** si responia una enquesta amb l'objectiu de **robar les dades personals**[144].

Però el *phishing* no ha estat l'única forma d'explotar la confiança de les empreses de comerç electrònic amb els consumidors. Els ciberdelinqüents han aprofitat la **web legítima per explotar la confiança dels consumidors** i dur a terme la seva activitat maliciosa. A partir d'una web vulnerable, realitzen un atac d'injecció de codi als **formularis de compra** per tal de robar les dades personals

[141] *https://www.metadata.cat/noticia/1067/comerc-electronic-creix2-5-interanual-tercer-trimestre-2020*
[142] *https://www.checkpoint.com/press/2021/microsoft-continues-to-be-most-imitated-brand-for-phishing-attempts-in-q1-2021/*
[143] *https://securelist.com/spam-and-phishing-in-q1-2021/102018/*
[144] *https://www.20minutos.es/noticia/4585610/0/cuidado-ataque-phishing-amazon-suplantacion-identidad-encuestas//*

L'smishing, o pesca per SMS, és una tècnica de pesca en què s'intenta enganyar les víctimes adreçant-s'hi a través d'un SMS.

(font: Termcat)

Un troià és un programa maliciós amb una funció aparentment útil, però amb funcions addicionals amagades que faciliten l'accés no autoritzat a un sistema i el fan vulnerable.

(font: Termcat)

i bancàries que els compradors introdueixen. És preocupant destacar com un **93% dels consumidors** en línia mostren **preocupació** respecte de la seguretat dels formularis de compra[145].

Suplantació d'empreses de missatgeria

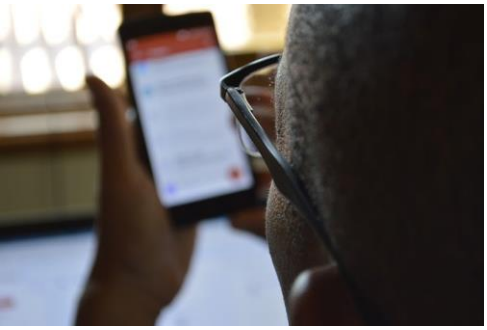
Recentment s'han detectat diferents campanyes d'*smishing* en què se suplantaven empreses relacionades amb la **distribució de paqueteria i missatgeria**. Els missatges SMS enviats als mòbils de les víctimes advertien que hi havia un paquet pendent de lliurament, i adjuntaven un **enllaç maliciós** que convidava a clicar per conèixer-ne més detalls. Empreses com **Fedex**, **Correos** o **DHL** han estat suplantades en aquestes campanyes[146,147].

En aquesta línia, a **Barcelona**, el març de 2021, els Mossos d'Esquadra van detenir quatre integrants d'una organització cibercriminal que perpetraven aquest tipus d'atac de *smishing* suplantant empreses de paqueteria. L'**SMS**, per guanyar credibilitat i confiança, fins i tot estava **personalitzat amb el nom de la víctima**. Si la víctima accedia a l'enllaç inclòs en el missatge, el seu mòbil descarregava el troià **FluBot**[148] o bé era redirigit a un **web fals** que demanava introduir dades personals. Tot apunta que els ciberdelinqüents pretenien utilitzar la informació robada per realitzar atacs de **segrest de SIM**[149].

Suplantació de l'Administració Pública

Més que mai, els consumidors utilitzen Internet per a les gestions amb l'Administració Pública, com ara en la **liquidació de tributs**, la sol·licitud de **subvencions i ajudes**, etc. I, novament, els ciberdelinqüents han fet ús de la suplantació d'identitat per treure'n benefici.

L'exemple més habitual, que es repeteix cada any coincidint amb els mesos previs a la declaració de la renda, és la **suplantació de l'Agencia Tributaria espanyola**[150]. Un altre exemple destacat durant la pandèmia ha estat la suplantació de l'**Administració Pública** en la distribució d'**ajuts socials**. Molts països han engegat campanyes d'ajuts econòmics, i els ciberdelinqüents les han utilitzat per enganyar famílies en una **situació de necessitat i vulnerabilitat**. Els ciberdelinqüents han fet ús de diferents canals, fins i tot de Whatsapp, per difondre missatges a través dels s'oferien suposats ajuts, però que en realitat buscaven **robar dades personals**[151].



Suplantació dels consumidors

Per a l'explotació de les relacions de confiança no sempre se suplanten les entitats. Els ciberdelinqüents també **es fan passar per consumidors** a l'hora de demanar productes o serveis, i utilitzen la informació robada en fuites de dades que han acabat a la venda en el **mercat negre**. Però no és l'única manera: un veí d'Argamasilla d'Alba (Ciudad Real), **conegut pels veïns de la vila**, va obtenir les **dades d'una quinzena de persones** per suplantar-ne la identitat. L'estafador va donar d'alta **targetes de crèdit** a nom de les seves

[145] *https://www.helpnetsecurity.com/2021/03/30/data-security-online-forms/*
[146] *https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-smishing-suplantando-fedex-descargar-malware*
[147] *https://www.adslzone.net/noticias/seguridad/smishing-correos-apk/*
[148] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/Butlleti-damenaca-Smishing-FluBot-marc-2021*
[149] *https://www.cyberscoop.com/barcelona-spain-police-arrest-massive-text-message-hacking-flubot/*
[150] *https://www.lavanguardia.com/economia/bolsillo/20210419/6968668/renta-2020-estafa-timo-devolucion-correo-email-que-hacer.html*
[151] *https://www.rtve.es/noticias/20210126/bulo-tarjeta-familia-ayudas-quedarse-casa-pandemia/2069700.shtml*

L'autenticació de múltiples factors es basa en un sistema de dues claus o més.

Es necessiten dos o més elements per iniciar sessió, que estiguin relacionats amb un element que sabem (contrasenya), un element que tenim (dispositiu mòbil o generador de claus) i/o una cosa que som (empremta dactilar o identificació biomètrica).

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)

Una backdoor, o porta del darrere, és un mecanisme que fa possible l'accés a una aplicació evitant les restriccions i les mesures de seguretat, sempre que se'n conegui l'existència i el funcionament.

(font: Termcat)

El zero trust és un model de seguretat que considera que no hi ha actors de confiança ni a dins ni a fora de la xarxa de l'organització. Tots els accessos a les aplicacions de l'estructura han de ser gestionats, i se'n limita l'accés i els privilegis tant de dispositius com d'usuaris. Es tracta d'un model de millora continua mitjançant l'aprenentatge i l'adaptació

víctimes, que va utilitzar per obtenir **22.000 €** amb **compres en línia** i, fins i tot, **operacions a crèdit** amb banca a distància[152].

Cal destacar que, actualment, fer ús de la **usurpació d'identitat** per cometre fraus amb bancs i comerços electrònics és més **complicada**, ja que és habitual que els serveis de pagament facin ús del doble factor d'autenticació (2FA) al telèfon mòbil per **verificar la identitat dels consumidors** quan sol·liciten una operació. Per aquest motiu, cada vegada més, l'objectiu dels ciberdelinqüents és aconseguir un **duplicat de la targeta SIM** de la víctima. Amb la targeta SIM duplicada, el ciberdelinqüent obté el control del doble factor de seguretat de la víctima: pot **restablir** les credencials dels comptes de la víctima i **validar les operacions** financeres fins **buidar els comptes bancaris**.

La companyia de telefonia mòbil **T-Mobile**, als EUA, va detectar una **fuita de dades** després d'assabentar-se que els seus clients havien experimentat **segrestos de la seva SIM**. Precisament, la **informació robada** era utilitzada per **suplantar els clients** de T-Mobile amb l'objectiu de **demanar un duplicat de la SIM**[153]. Malauradament són incidents cada vegada més habituals. A l'Estat espanyol, un home de 30 anys de **Cantàbria** va aconseguir **un duplicat de la SIM** de la víctima per realitzar **compres en línia**. La víctima creia que s'havia quedat sense cobertura i ho havia relacionat amb el canvi de companyia que, precisament, tenia programat. Quan va consultar el seu compte bancari, va constatar totes les operacions de compra fraudulentes realitzades.

El cibercrim explota la confiança amb els proveïdors de productes i serveis TIC per dur a terme ciberatacs amb impactes massius entre els seus clients

El ciberatac al fabricant de software **Solarwinds**, a final de 2020, pot haver estat un cas inspirador pel cibercrim. Un grup cibercriminal **va introduir una** *backdoor* en una actualització del programari legítim Solarwinds Orion i uns **18.000 clients** van quedar afectats. Ha estat l'**atac a la cadena de subministrament més important** que s'ha identificat fins ara[154].

Així doncs, els **atacs a la cadena de subministrament** han tingut un creixement del **350%** entre el 1r trimestre de 2020 i el de 2021 (il·lustració 16), entre els quals destaquen especialment els atacs als **proveïdors de *software***. L'objectiu dels ciberatacants és **explotar** la relació de **confiança** existent a la **cadena de subministrament del programari**, entre els fabricants i els seus clients, els quals fan ús del programari subministrat sense controls específics. Així, si els ciberatacants aconsegueixen **comprometre el proveïdor de programari**, poden aconseguir **impactar els seus clients** de forma **massiva** i **sense impediments**.

Aquest tipus d'atac **preocupa els governs d'arreu del món**, ja que l'impacte pot **afectar l'activitat econòmica i sectors estratègics**. La **Casa Blanca** està decidida a actuar i durant els primers tres mesos de 2021 ha estat treballant en una **ordre executiva** destinada a millorar la seguretat dels proveïdors i la cadena de subministrament amb el govern, i les agències governamentals hauran d'ajustar-se a models de treball *zero trust*[155].

Recentment, s'han identificat diferents atacs dirigits a **plataformes de compartició de fitxers** amb l'objectiu d'obtenir accés a la informació dels seus usuaris. Així, el *National Coordination Center for Cybersecurity* d'Ucraïna va

[152] *https://cadenaser.com/emisora/2021/01/13/ser_ciudad_real/1610535302_921211.html*
[153] *https://heimdalsecurity.com/blog/t-mobile-confirms-data-breach-and-sim-swapping-attacks/*
[154] *https://www.sgtreport.com/?s=solarwinds*
[155] *https://www.cyberscoop.com/cyber-executive-order-supply-chain-solarwinds/*

El malware, o programari maliciós, 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)

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

(font: Termcat)

detectar intents de disseminar **programari maliciós** amb documents allotjats al SEI EB, un sistema d'informació utilitzat per a l'**intercanvi de documentació** entre **entitats públiques ucraïneses**. Aquells usuaris que obrien els documents maliciosos es veien infectats amb un *malware* que permetia als ciberatacants **obtenir el control de l'equip**[156]. De forma similar, un altre grup de ciberdelinqüents va explotar una vulnerabilitat en un programari de la companyia **Accellion** (EUA), utilitzat per a la **transferència de fitxers**, la qual els va permetre l'accés a la informació dels clients. Alguns afectats ja han vist com els seus **documents confidencials** es publicaven a la *dark web*, però en podrien ser molts més, ja que més de **3.000 entitats** (entre empreses, universitats, agències governamentals i hospitals dels EUA) feien ús de la plataforma[157]. Un altre dels casos més destacats durant el mes de març de 2021 ha estat l'atac cibernètic a **SITA**, una empresa global de tecnologies de la informació, especialista en **comunicacions de transport aeri**. El ciberatac va afectar el **sistema de servei als passatgers** (PSS) utilitzat per diferents companyies aèries, de manera que **les dades de viatgers** es van veure's compromeses[158].

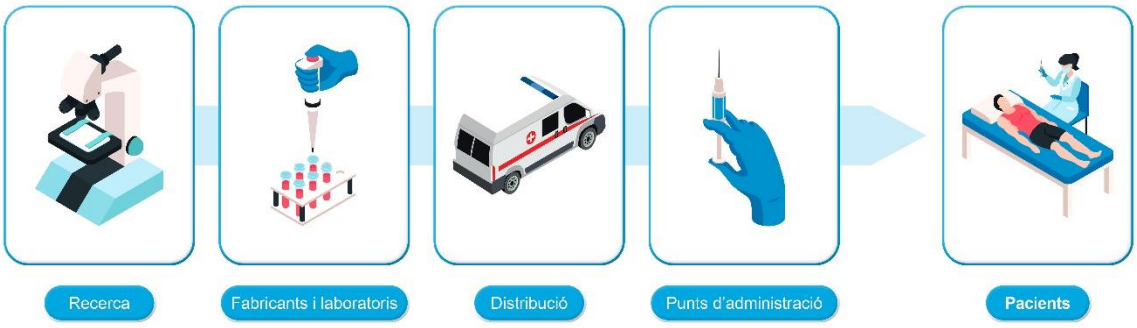
També cal destacar com els atacs de *ransomware* a un **proveïdor de serveis electrònics** poden tenir múltiples afectacions a la cadena de subministrament, ja que la dependència dels serveis pot obligar els seus clients a **aturar l'activitat**. És el cas, per exemple, de l'atac del *ransomware* Ryuk a **Esofitec**, una empresa lleidatana distribuïdora dels serveis al núvol d'Enuve, propietat d'Otenuve, la qual pertany al grup Abast. Arran de l'atac, els clients van **perdre les tres còpies de seguretat** i van haver d'invertir recursos extraordinaris per reescriure manualment les dades dels seus sistemes. Poques setmanes després, **90 despatxos professionals**, **60** dels quals **a Lleida** i alguns més a la resta de la geografia catalana, com que no van obtenir una resposta satisfactòria del proveïdor, van optar per **querellar-se** pels perjudicis ocasionats als negocis[159].

El cibercrim ataca la cadena de subministrament de la vacuna, un entorn essencial i de confiança, amb l'objectiu de robar informació de valor estratègic i causar un impacte crític en la lluita contra la covid-19

Una vegada més, el **cibercrim** ha demostrat com aprofita les **necessitats generades per la pandèmia** per realitzar **atacs oportunistes**. Actualment, el món sencer demana vacunes i la cadena de distribució ha esdevingut un element crític i indispensable. D'aquesta manera, els cibercriminals han posat el focus en les entitats involucrades en la cadena distribució de la vacuna per aconseguir un gran impacte: un **incident** en una de les baules de la cadena impacta la resta i **afecta directament en la lluita contra la covid-19**.

En aquesta línia, s'ha identificat que els atacs contra les indústries clau en la fabricació de les vacunes es van incrementar un **100%** a final de 2020[160] i, entre desembre i febrer de 2021, un **189%**[161]. Una altra dada destacada és com, amb l'**inici de la distribució de la vacuna**, els ciberatacs dirigits contra aplicacions web de salut, a través d'injecció indirecta d'*scripts* (XSS), execució remota de codi (RCE) o injecció SQL, van créixer un **51%**[162].

[156] *https://www.rnbo.gov.ua/en/Diialnist/4823.html*
[157] *https://www.insidehighered.com/news/2021/04/07/accellion-data-security-breach-latest-hit-universities*
[158] *https://gcfrng.com/2021/03/09/sita-data-breach-affects-millions-of-airline-passengers/*
[159] *https://www.segre.com/es/noticias/lleida/2021/03/17/querella_por_ciberataque_despachos_profesionales_128710_1092.html*
[160] *https://newsroom.ibm.com/2021-02-24-IBM-Security-Report-Attacks-on-Industries-Supporting-COVID-19-Response-Efforts-Double*
[161] *https://healthitsecurity.com/news/pharmacy-hospital-phishing-attacks-spike-189-amid-vaccine-rollout*
[162] *https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/*



Il·lustració 20. Actors de la cadena de distribució de la vacuna de la covid-19.

Ciberatacs als centres de recerca

La **recerca** ha estat essencial en el descobriment d'un tractament o una vacuna per a la covid-19 i la informació generada s'ha convertit en un bé de valor estratègic i cobejat. D'aquesta manera, els **centres de recerca** han estat objectiu de diversos casos de **ciberespionatge**. Ha destacat la **intrusió** que va patir la Divisió de Biologia Estructural de la **Universitat d'Oxford**, que va descobrir que es publicava informació per accedir als seus sistemes. La universitat va aconseguir bloquejar l'atac i, així, evitar un possible incident de ***ransowmare*** que hagués pogut comprometre les dades de recerca i perjudicar la resposta mèdica a la covid-19[163].

Ciberatacs a fabricants i laboratoris

Les empreses dedicades a la **producció de vacunes** han tingut un **alt nivell d'activitat** per fabricar centenars de milions de vacunes que poguessin cobrir la demanda mundial. La informació amb la qual treballen aquestes entitats també ha estat objectiu del **ciberespionatge**, sovint per part de grups cibercriminals subvencionats per estats. Precisament, a l'Índia, on es produeixen el 60% de les vacunes[164], tant l'**Institut Serum** com **Bharat Biotech** han estat objectiu d'atacs cibernètics amb l'objectiu d'obtenir **informació confidencial**, suposadament a càrrec del grup APT 10 vinculat amb el govern xinès[165].

L'spear-phishing*, o pesca dirigida, és una tècnica de pesca en què s'intenta enganyar les víctimes, habitualment individus concrets o grups específics d'usuaris vinculats a empreses importants o a institucions governamentals, adreçant-s'hi d'una manera personalitzada, sovint per correu electrònic.*

(font: Termcat)

Ciberatacs a la cadena de distribució

La distribució de les vacunes s'ha caracteritzat per la necessitat de mantenir la **cadena de fred** per tal de conservar-les a la temperatura de conservació adequada. Precisament, el coneixement d'aquest fet ha estat explotat pels cibercriminals. Ja durant el desembre de 2020 es van detectar **campanyes de *phishing* que suplantaven** l'empresa logística i proveïdora de tecnologies per la cadena del fred de la vacuna, **Haier Biomedical**[166]. Aquest tipus de campanyes de *spear-phishing* s'han repetit durant el 1r trimestre de 2021, dirigides a **44 companyies i organitzacions de 14 països d'arreu del món**; totes implicades en el transport i distribució de la vacuna[167].

[163] *https://www.welivesecurity.com/2021/02/26/oxford-university-covid19-laboratory-hack/*
[164] *https://www.pbs.org/newshour/health/covid-19-is-out-of-control-in-india-where-most-vaccines-are-made-how-did-that-happen*
[165] *https://www.reuters.com/article/us-health-coronavirus-india-china-idUSKCN2AT20P*
[166] *https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/*
[167] *https://securityintelligence.com/posts/covid-19-vaccine-global-cold-chain-security/*

Ciberatacs als centres de vacunació

Els **centres de vacunació**, com els hospitals i els punts de vacunació habilitats per a l'ocasió, duen a terme una activitat essencial en la lluita contra la pandèmia. Per aquest motiu, el cibercrim ha dirigit els **atacs de *ransomware*** contra hospitals, els quals han hagut d'**aturar les vacunacions**, així com intervencions, consultes o visites, i s'han pogut veure obligats a pagar el rescat per recuperar l'activitat. En aquesta línia, a **França**, durant el 1r trimestre de 2021, una sèrie continuada d'atacs de *ransomware* va impactar diversos centres hospitalaris. L'hospital Dax, per exemple, en plena **tasca assistencial** als malalts de covid-19 i enmig del **procés de vacunació**, es va veure obligat a **reduir l'activitat**, tot i que **no va tenir conseqüències pels pacients**[168].

Ciberatacs a la ciutadania

La **ciutadania**, que veu en la vacuna l'esperança a una tornada a la normalitat, ha estat contínuament objecte de **campanyes de *phishing* i fraus relacionats amb el vaccí**. S'ha constatat com el ***phishing*** amb temàtica sobre la vacuna ha augmentat un **530%** entre els mesos de desembre de 2020 i febrer de 2021, al mateix temps que creixia l'interès de la ciutadania pel tema (veure il·lustració 17)[169].

Més enllà del *phishing*, els ciutadans s'han pogut veure temptats per comprar vacunes en algun mercat negre d'Internet. De fet, el nombre d'**anuncis al web fosc relacionats amb les vacunes** ha augmentat un **300%** des de gener de 2021. S'ofereixen vacunes per preus que varien entre els **400 i els 800 €**, aproximadament: AstraZeneca, Sputnik, Johnson & Johnson, etc[170]. Ara bé, són vacunes sense cap tipus de garantia: no s'assegura el correcte manteniment de la cadena de fred i difícilment se'n pot comprovar la procedència o traçabilitat.

El Certificat Verd neix amb mesures de ciberseguretat per fer front al risc de falsificació i la pèrdua de privacitat, amb l'objectiu de generar la confiança necessària per un desplegament exitós

Per a la recuperació de la normalitat i, al mateix temps, assegurar-se que no es propaga el virus, esdevé imprescindible disposar d'una **eina confiable** per **garantir la circulació de persones lliures de covid-19**. Per aquesta raó, el 17 de març de 2021, la UE va proposar la creació del **Certificat Verd** amb l'objectiu que les persones puguin **acreditar el seu estat immunitari** i **moure's amb llibertat entre els estats membres**. El Certificat Verd ha d'esdevenir la prova que el ciutadà ha estat vacunat, que ha rebut un resultat de prova PCR negativa o que té anticossos per haver passat la malaltia[171]. Així, qualsevol ciutadà de la UE que estigui en possessió d'aquest Certificat Verd quedarà **exempt de restriccions a la lliure circulació** (proves, quarantenes, etc.) quan viatgi[172]. Aquest certificat estarà disponible gratuïtament en suport paper i en suport digital, i inclourà un **codi QR** per garantir-ne l'autenticitat.

[168] *https://portswigger.net/daily-swig/dax-cote-dargent-hospital-in-france-hit-by-ransomware-attack*
[169] *https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/*
[170] *https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/*
[171] *https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1181*
[172] *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0140&from=EN*

Un Gateway és un unitat funcional que permet la connexió entre xarxes d'àrea local amb una arquitectura de xarxa diferent.

(font: Termcat)

Ara bé, per tal que el Certificat Verd esdevingui una eina útil, ha de generar la confiança suficient. De fet, a l'Estat espanyol, un **54%** accepta l'ús del certificat **només mentre les xifres de malalts siguin altes**, i únicament un **5%** l'accepta **sense restriccions** (veure il·lustració 18). Així, per aconseguir ser una eina confiable, el Certificat Verd ha de garantir la **privacitat dels ciutadans** i estar **protegit de falsificacions**.

Per aquest motiu, el certificat només disposa de la **informació mínima necessària**, com ara el nom, la data de naixement, l'emissor del certificat i un identificador únic, a més del motiu pel qual el posseïdor disposa d'immunitat.[173]. Són les dades mínimes per garantir la identificació del portador, i només estaran disponibles en el mateix certificat i en les bases de dades nacionals. Mai passaran per cap sistema o servidor exterior.

Així mateix, el Certificat disposa de les característiques necessàries per acreditar-ne l'**autenticitat** i **traçabilitat**. Per fer-ho possible, el primer aspecte rellevant és que **només els centres emissors acreditats podran emetre els Certificat** (per exemple, hospitals, autoritats sanitàries, etc.). El segon és que estarà **signat per una clau digital privada** en mans dels centres emissors i que estarà degudament emmagatzemada i protegida per cada estat membre. En el moment de viatjar a un país nou, **s'escanejarà el codi QR** del viatger i, a través d'un *gateway* centralitzat, **s'accedirà a la clau pública** de la signatura que permetrà validar-ne l'origen i l'autenticitat[174]. Així, es garanteix que únicament es farà ús de les claus de firma i **no s'emmagatzemarà cap dada personal**.

Il·lustració 2112. Procés de certificació i validació del Certificat Verd..

Aquestes mesures de seguretat permeten minimitzar el **risc de falsificacions**, que és molt real, especialment si es té en compte l'experiència. Des del 5 de març de 2020, ja es demanava el certificat d'una **prova PCR o d'antígens negativa** quan es viatjava des d'una zona de risc, però al mateix temps començava la **venda i l'ús de certificats falsificats**[175]. L'Europol va alertar del comerç fraudulent d'aquest tipus de certificats amb preus que oscil·laven entre **100 i 300 €**[176].

El Certificat Verd **no és un cas aïllat**. La *International Air Transport Association* (IATA) va presentar una iniciativa a través d'una app mòbil, el IATA Travel Pass[177], per ajudar els passatgers de les línies aèries a **emmagatzemar i gestionar les seves certificacions verificades** de proves o vacunes. Busca facilitar els processos de gestió dels requisits sanitaris per viatjar d'acord amb el **Reglament Sanitari Internacional** promogut per l'OMS[178].

[173] *https://www.schengenvisainfo.com/news/eu-vaccine-chief-says-vaccine-passports-to-be-launched-in-june-unveils-document-prototype/*
[174] *https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2781*
[175] *https://abcnews.go.com/US/increased-vaccine-passports-lead-scams-experts-warn/story?id=76754919*
[176] *https://www.europol.europa.eu/sites/default/files/documents/ewn_-_illicit_sales_of_false_negative_covid-19_test_certificates.pdf*
[177] *https://www.iata.org/en/programs/passenger/travel-pass/*
[178] *https://www.who.int/ihr/ports_airports/icvp/es/*

Recomanacions

- **Els usuaris, davant d'un correu sospitós, han de validar l'autenticitat de l'adreça del remitent, consultar directament amb el remitent per un altre mitjà o consultar amb el servei tècnic.**
- **Els usuaris han d'ignorar els correus electrònics amb remitent desconegut, en especial quan sol·licitin credencials o que incloguin un fitxer adjunt.**
- **Els usuaris no han de revelar credencials a tercers, ni de forma escrita (en el cas del *phishing* o l'*smishing*) ni de forma oral (en el cas del *vishing*).**
- **Els usuaris han de fer ús del doble factor d'autenticació per als comptes de serveis en línia, en especial pel que fa a l'operativa financera.**
- **Els usuaris han de tenir en compte que la informació que exposen a les xarxes socials pot ser utilitzada per un atacant per usurpar-los la identitat.**
- **Els usuaris, en cas de pèrdua del servei del telèfon mòbil sense motiu, han de validar amb l'operador que no s'ha sol·licitat un duplicat de la targeta SIM sense consentiment. En cas afirmatiu: sol·licitar la inhabilitació de la targeta replicada.**
- **Les organitzacions han d'utilitzar proveïdors de serveis de correu electrònic que implementin tecnologies *antispam* i *antiphishing*.**
- **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 d'habilitar accessos amb doble factor d'autenticació per a tots els usuaris, en especial els administradors de sistemes.**
- **Les organitzacions han de disposar de còpies de seguretat actualitzades i fora de línia, per evitar que puguin ser xifrades a través d'un *ransomware*.**
- **Les organitzacions han d'emmagatzemar les dades personals amb un xifratge segur per evitar que un intrús pugui robar-les en text pla.**
- **Les organitzacions han d'elaborar anàlisis de riscos amb la identificació, especialment, dels actius crítics i amb el desplegament de mesures de prevenció, protecció i resposta proporcionals.**
- **Les organitzacions han de disposar d'un pla de continuïtat del negoci i un pla de recuperació de desastres, així com de problemes de subministrament dels proveïdors, i han de validar que se n'ha verificat el funcionament a través de simulacres.**
- **Les organitzacions han d'avaluar els riscos dels serveis proporcionats per tercers, desplegar mesures correctives i realitzar auditories o comprovacions.**
- **Les organitzacions han d'aproximar models de confiança zero amb la segregació dels serveis interns de la xarxa empresarial i disposar de protecció perimetral.**

Fets rellevants

- S'han donat nous casos de *smishing* que suplanten empreses de logística a l'Estat espanyol. Els missatges incloïen un enllaç maliciós i arribaven a dirigir-se al destinatari pel seu nom. Si l'usuari clicava l'enllaç accedia a un web fals per robar-li les dades o descarregar una aplicació maliciosa que pretenia ser de Fedex[179].
- Durant el 1r trimestre de 2021 s'ha detectat un nombre elevat de comptes suplantats a Facebook, Instagram, TikTok i OnlyFans. Els ciberdelinqüents generen un nou perfil amb un nom similar a l'original, que només varia en alguna lletra o símbol. L'objectiu es cometre algun frau econòmic amb l'ús de tècniques d'enginyeria social, com ara falsos sortejos i donacions[180].
- L'Àgencia de Ciberseguretat de Singapur (CSA) va alertar que un grup de ciberdelinqüents es feiaa passar per treballadors de la CSA, la policia de delictes cibernètics o el departament de ciberdelinqüència. Amb el pretext d'una investigació, sol·licitaven la víctima que instal·lés un programari que resultava ser maliciós, l'instaven a compartir l'accés als seus comptes o, fins i tot, li demanaven diners per resoldre un suposat problema[181].
- L'empresa de tecnologies de la informació SITA, especialista en comunicacions de transport aeri, ha patit una bretxa de seguretat que ha permès que uns ciberatacants accedissin als servidors. Contenien dades de passatgers de diverses aerolínies del món; una dotzena han hagut d'informar els passatgers que les seves dades havien estat exposades[182].
- Ucraïna acusa Rússia d'estar darrere d'un ciberatac al Sistema d'Interacció Electrònica d'Organismes Executius (SEI EB), utilitzat per compartir arxius entre funcionaris, amb l'objectiu de difondre documents amb macros malicioses per instal·lar *malware*. L'atac es va produir setmanes després d'un atac DDoS contra webs governamentals ucraïneses[183].
- Desenes de despatxos professionals de Lleida i més d'un centenar de Catalunya s'han quedat sense les dades, expedients, informes i tota mena de documentació dels seus clients per un ciberatac que va experimentar el seu proveïdor al núvol; l'atac va xifrar servidors i còpies de seguretat. Els serveis *cloud* havien estat contractats a Esofitec (Lleida), distribuïdora dels servidors *cloud* d'Enuve (Outenuve) del grup Abast[184].
- L'ANSSI, l'agència de ciberseguretat francesa, va rebre l'avís d'una campanya d'intrusió dirigida al *software* de monitorització de l'empresa Centreon, que va impactar diverses entitats franceses. La campanya va començar el 2017 i ha estat activa fins al 2020. L'ANSSI va descobrir diverses *backdoors* en els sistemes afectats [185].
- El grup nord-coreà Thallium, especialitzat en *phishing*, ha dirigit una campanya de distribució de *malware* per instal·lar un RAT en una aplicació de missatgeria utilitzada per una gran quantitat de corredors de borsa[186].
- S'identifica un ciberatac amb l'objectiu de comprometre el mecanisme d'actualització de NoxPlayer, un emulador d'Android per a PC i MAC de l'empresa Nox Limited (Hong Kong); es calcula que té més de 150 milions de jugadors a tot el món. Es van identificar tres famílies de *malware* amb capacitats de monitorització i vigilància que es distribuïen a partir d'actualitzacions personalitzades[187].

[179] *https://blogs.protegerse.com/2021/02/23/siguen-los-casos-de-los-sms-suplantando-a-empresas-de-logistica-como-fedex/*
[180] *https://news.sophos.com/es-es/2021/02/19/oleada-de-casos-de-suplantacion-de-identidad-en-cuentas-de-redes-sociales/*
[181] *https://www.csa.gov.sg/news/news-articles/media-statement-on-technical-support-scam-impersonating-as-csa-officer*
[182] *https://gcfrng.com/2021/03/09/sita-data-breach-affects-millions-of-airline-passengers/*
[183] *https://thehackernews.com/2021/02/russian-hackers-targeted-ukraine.html*
[184] *https://www.segre.com/es/noticias/lleida/2021/02/24/un_ciberataque_secuestra_los_archivos_decenas_despachos_profesionales_lleida_126698_1092.html*
[185] *https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/*
[186] *https://1stcybersecurity.com/index.php/2021/01/06/north-korean-apt37-targets-stock-investors-in-software-supply-chain-attack/*
[187] *https://www.welivesecurity.com/la-es/2021/02/01/ataque-cadena-suministro-apunta-jugadores-videojuegos-online/*

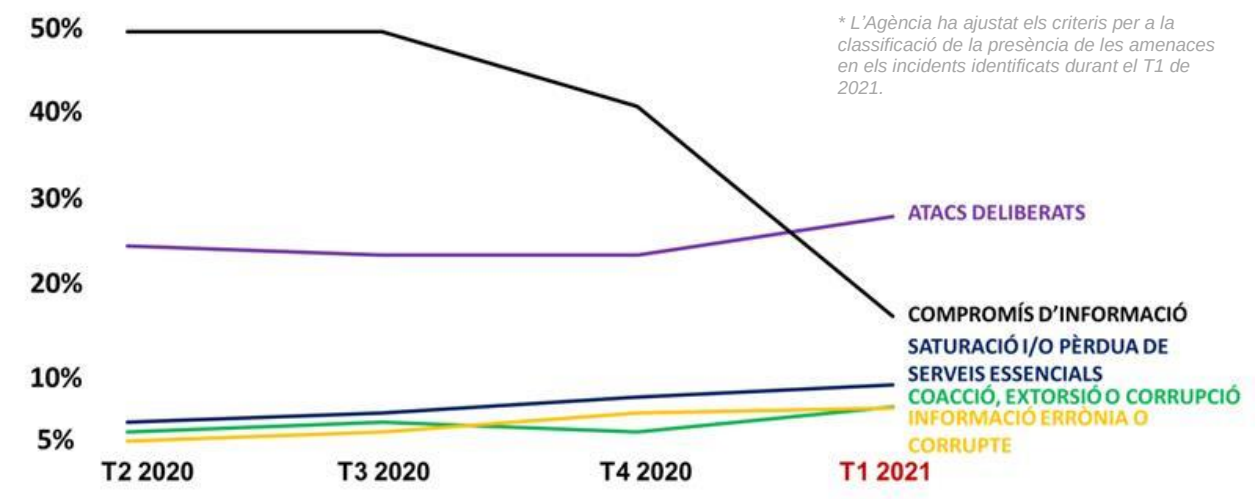
Top 5 de ciberamenaces

Tenint en compte el nombre d'incidents que s'han esdevingut durant el 1r 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.

2S 2020	vs	1S 2020	Ciberamenaces[188]
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	=	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.*
4	=	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.*
5	▲	6	**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.*

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

1. Atacs deliberats

Es detecten diverses campanyes de *phishing* que usurpaven marques conegudes implicades en el subministrament de productes i serveis en línia. L'esquer de les temàtiques relacionades amb la covid-19 encara s'utilitza en campanyes de *phishing* per robar credencials i difondre *malware*. Destaca la campanya d'*smishing* per a la difusió del *malware* Flubot, amb una important incidència a Espanya.

El vishing, o pesca per veu, és una tècnica de pesca en què s'intenta enganyar les víctimes telefònicament, mitjançant la veu per IP.

(font: Termcat)

L'spam, o correu brossa, consisteix en un conjunt de missatges electrònics inoportuns, generalment de caràcter publicitari i sense interès per al receptor, que s'envien indiscriminadament a un gran nombre d'internautes.

(font: Termcat)

Un troià d'accés remot, o RAT, és un programari maliciós que infecta la víctima fent-se passar per un programari lícit i que estableix una connexió amb el ciberdelinqüent, al qual li atorga el control sobre el dispositiu de la víctima.

13/01. Un detingut a València per **robar dades** de més de **4.000 targetes bancàries** per *smishing*. El ciberdelinqüent va crear pàgines fraudulentes com ara www.correo-pagar.com, www.agenciatributaria-es.com i www.agenciatributaria-es.online, amb formularis perquè les víctimes introduïssin les dades de les seves targetes. L'actor maliciós utilitzava les dades per fer **compres en comerços electrònics i retirar diners als caixers**[189].

19/01. L'FBI alerta d'una **campanya de *vishing*** que busca **robar comptes corporatius o credencials a la xarxa i escalar privilegis**. Segons les fonts, la campanya té un abast mundial i ha estat motivada per l'**augment del teletreball**. La campanya es va iniciar al desembre de 2019. El vector d'atac inclou números de **telèfon falsificats** per amagar la identitat i la localització dels actors maliciosos [190].

25/01. Es fan passar pel ***National Health System del Regne Unit* (NHS)** per difondre *phishing* relacionat amb la **vacunació de la covid-19**. En una versió del correu electrònic, es demana als usuaris que confirmin o rebutgin la vacunació contra el coronavirus accedint a l'enllaç corresponent. Independentment de l'opció triada, els enllaços **dirigeixen a una pàgina falsa del NHS** que sol·licita **informació personal** com el nom, data de naixement, número de telèfon i, fins i tot, dades de la targeta de crèdit o d'antecedents familiars[191].

08/03. Es detecten diverses **campanyes malicioses per difondre el troià FluBot** des del gener. La campanya suplantava aplicacions bancàries o de missatgeria (FedEx, DHL, Correos) per **robar informació privada** de l'usuari com ara detalls bancaris o informació dels contactes de la víctima. El troià era distribuït mitjançant missatges de mòbil. La major part de la distribució del troià va ser a Espanya i es van infectar més de **58.000 dispositius**[192].

17/03. Durant el març de 2021 es va detectar una **campanya de *spam*** que utilitzava com a esquer el **pla de rescat dels Estats Units** per infectar els usuaris amb el **troià Dridex**. Els correus electrònics suplantaven el **servei d'impostos interns dels EUA** (IRS) i l'esquer de la campanya **era el pagament** de 1.400 $ en ajuts o l'**accés a la vacunació sense espera**[193].

18/03. Una nova **campanya de *phishing*** dirigida als **contribuents** dels EUA adjuntava **documents** que pretenien estar relacionats amb el pagament **d'impostos**. El missatge demanava als usuaris que **habilitessin les macros** per accedir al document. En última instància, la víctima s'infectava amb els *malwares* **NetWire i Remcos** per a Windows (dos troians *RAT*), que permetien els atacants prendre el **control dels dispositius de les víctimes**[194].

[189] *https://escudodigital.com/ciberseguridad/detenido-valencia-por-robar-datos-mas-de-4-000-tarjetas-bancarias-por-smishing/*
[190] *https://www.seguridadyfirewall.cl/2021/01/el-fbi-advierte-sobre-ataques-vishing.html*
[191] *https://hotforsecurity.bitdefender.com/blog/cybercriminals-impersonate-uks-national-health-service-to-spread-covid-19-vaccination-phishing-emails-25190.html*
[192] *https://www.hackread.com/flubot-android-malware-fedex-chrome-apps-data/*
[193] *https://threatpost.com/covid-19-relief-checks-dridex-malware/164853/*
[194] *https://www.zdnet.com/article/us-taxpayers-targeted-in-netwire-remcos-trojan-attack-wave/*

2. Compromís i/o pèrdua d'informació

Les fuites dades amb milions de registres han estat protagonistes en els primers mesos de 2021. Els errors de configuració i les bases de dades obtingudes a través de tècniques *scrapping* a les xarxes socials tornen a ser protagonistes. També han destacat les filtracions de *hacktivistes*, com ara el grup DDoSecrets. Es consolida la doble extorsió en atacs de *ransomware*, que ha suposat la filtració de grans quantitats d'informació robada.

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

(font: Termcat)

06/01. El grup *hacktivista* **DDoSecrets** ha publicat a la *dark web* **1 TB d'informació confidencial** que inclou més de **750.000 correus electrònics, fotografies i documents de cinc companyies**. El grup també ofereix, en privat, **1,9 TB de dades d'unes altres 12 companyies**. Les empreses afectades pertanyen als sectors farmacèutic, de desenvolupament de *software* i financer [195].

20/01. L'*startup* xinesa **SocialArks** va deixar **obert un servidor ElasticSearch** que contenia **318 milions de registres** de **214 milions d'usuaris** de les xarxes socials **Facebook**, **Linkedin** i **Twitter**. Els registres incloïen noms, telèfons, correus electrònics i fotografies. La companyia va aconseguir les dades mitjançant **tècniques de *scrapping***, tot i que les xarxes socials havien prohibit aquestes pràctiques[196].

01/03. El grup *hacktivista* **DDoSecrets** va filtrar **70 GB d'informació de la plataforma d'ultradreta Gab**. La plataforma és un web que ofereix servei a ideologies d'ultradreta i es presenta com una alternativa de total llibertat d'expressió per als seus usuaris. DDoSecrets ha aconseguit robar i filtrar publicacions privades, perfils d'usuari, missatges directes, contrasenyes d'usuaris en *hash* i contrasenyes de grups[197].

01/03. Un nombre indeterminat de **clients** de **T-Mobile** (EUA) es va veure afectat per atacs de segrest de SIM. Es va descobrir que aquests atacs van tenir l'origen en un ciberatac previ que havia permès a un **actor desconegut accedir a les dades dels comptes dels clients**. Incloïen dades de contacte, números d'identificació personals, números de compte, números de seguretat social, preguntes i respostes de seguretat del compte, dates de naixement, informació del pla i el nombre de línies subscrites als seus comptes. Aquesta informació era utilitzada per demanar **duplicats de les targetes SIM** amb l'objectiu d'esquivar el **doble factor d'autenticació**[198].

11/03. Un grup de ciberatacants va superar la seguretat de Verkada Inc. (EUA) i va obtenir accés a **transmissions en viu** de gairebé 150.000 càmeres de vigilància. Les càmeres de seguretat a les quals van accedir els ciberatacants pertanyien a **presons, hospitals, magatzems i oficines d'empreses com ara Tesla i Cloudflare**[199].

25/03. L'equip de Nightlion Security va identificar diverses bases de dades a un mercat de la *dark web* que incloïen informació de **400 milions d'usuaris de Facebook i Instagram**, així com **300 milions de ciutadans nord-americans** presumptament obtingudes d'**Astoria Company**, una empresa que recopila dades personals per oferir préstecs i productes d'assegurances mèdiques. La base de dades d'Astoria Company s'oferia per **200.000 €**[200].

[195] *https://www.wired.com/story/ddosecrets-ransomware-leaks/*
[196] *https://malwaredevil.com/2021/01/20/chinese-startups-open-database-exposes-214-million-social-media-accounts/*
[197] *https://www.exploitone.com/data-breach/ddosecrets-leaks-sensitive-information-from-right-wing-social-media-users/*
[198] *https://heimdalsecurity.com/blog/t-mobile-confirms-data-breach-and-sim-swapping-attacks/*
[199] *https://www.cpomagazine.com/cyber-security/verkada-data-breach-exposes-feeds-of-150000-security-cameras-targets-include-health-care-facilities-schools-police-stations-and-a-tesla-plant/*
[200] *https://securityaffairs.co/wordpress/115934/breaking-news/astoria-company-data-leak.html*

3. Saturació i/o pèrdua de serveis essencials

Els atacs que han creat una disrupció més important de l'activitat han estat els de *ransomware*, els quals han interromput la producció de grans empreses a tot el món. Els atacs DDoS destaquen per la seva potència i pel fet de ser més elaborats, més que no pas pel nombre d'incidents. En alguns casos, algunes entitats han hagut d'aturar temporalment els sistemes d'informació.

15/02. La plataforma de canvi de criptomonedes **EXMO**, del Regne Unit, va quedar temporalment fora de servei després de ser objecte d'un **atac de DDoS**. L'atac va tenir una magnitud de **30 Gbps** i va afectar tota la infraestructura de la companyia, incloent-hi el web, l'API i el seus sistemes de cartes de valors de canvi. L'atac va ser repel·lit i es van prendre mesures per evitar futures rèpliques[201].

22/02. El gegant de la construcció de vaixells francès **Beneteau** va ser víctima d'un ciberatac que **va afectar la producció**. La companyia té més de 8.000 treballadors a diferents localitzacions arreu del món, tot i que el lloc on l'atac va tenir més impacte va ser a França. S'apunta que es van veure obligats a tancar els sistemes per evitar la propagació d'un *malware* a la xarxa. **Deu dies després, encara treballaven** per recuperar la plena normalitat[202].

14/03. La companyia de begudes **Molson Coors**, que opera als EUA i Europa, va viure un atac, aparentment de ***ransomware***, que va **interrompre la producció**. Segons indica l'empresa, l'atac va causar **retards i disrupció** en alguns negocis de la companyia[203].

15/03. La **Universitat de** Birmingham, amb uns 13.000 estudiants, va **tancar el seu campus** durant **una setmana** a causa d'un **atac de *ransomware*** que va afectar tots els sistemes d'informació. L'atac va obligar el centre a fer les **classes en línia** mentre es realitzava la investigació. A més del xifrat dels sistemes d'informació, l'atac va derivar en el robatori i la filtració de dades[204].

22/03. La pàgina de novel·les gràfiques japoneses **MangaDex** va haver de **tancar temporalment** el web després d'un ciberatac. La pàgina té al voltant de 76 milions de visitants al mes. Segons indiquen els responsables del web, els ciberatacants, van guanyar accés a un compte d'administrador i desenvolupador, i van accedir al codi font gràcies a diverses vulnerabilitats en la web[205].

23/03. La companyia canadenca d'**IoT Sierra Wireless** va comunicar que va ser víctima d'un atac de *ransomware*. L'atac va forçar la companyia a **aturar la producció**, i el web i altres sistemes interns **van experimentar disrupcions**, tot i que indiquen que no va afectar els clients[206].

23/03. Un ciberatac **va impactar les operacions i va inhabilitar la pàgina web de CNA Financial**, companyia líder en **assegurances** dels EUA. L'atac la va obligar a tancar alguns dels serveis, com ara el sistema de subscripcions i reclamacions de la companyia o el correu electrònic[207].

29/03. Un ciberatac va **interrompre l'emissió en directe** a la xarxa d'un canal de la **televisió australiana**. S'investiga si l'atac va ser un sabotatge o un atac d'un grup APT[208].

[201] *https://www.bleepingcomputer.com/news/security/ddos-attack-takes-down-exmo-cryptocurrency-exchange-servers/*
[202] *https://www.ibinews.com/companies/cyber-attack-on-beneteau-production-may-be-disrupted/38357.article*
[203] *https://www.forbes.com/sites/leemathews/2021/03/14/cyberattack-disrupts-operations-at-molson-coors/*
[204] *https://feweek.co.uk/2021/03/15/college-group-closes-all-campuses-for-a-week-following-major-cyber-attack/*
[205] *https://www.bleepingcomputer.com/news/security/mangadex-manga-site-temporarily-shut-down-after-cyberattack/*
[206] *https://www.securityweek.com/sierra-wireless-says-ransomware-disrupted-production-manufacturing-facilities*
[207] *https://www.bleepingcomputer.com/news/security/cna-insurance-firm-hit-by-a-cyberattack-operations-impacted/*
[208] *https://www.bbc.com/news/world-australia-56554641*

4. Coacció, extorsió o corrupció

Els atacs de *ransomware* són la principal causa d'extorsió, tot i que cada cop és més habitual l'ús del robatori de dades i l'amenaça de filtrar-les. En aquest sentit, algunes fuites de dades han derivat en extorsions a empreses per tal d'evitar-ne la venda o publicació a la *dark web*. També s'han identificat algunes campanyes de *sextorsió* que aprofiten l'intens ús d'Internet realitzat durant la pandèmia.

La sextorsió, o extorsió sexual, és el xantatge que es fa a una persona sota l'amenaça de fer públics a la xarxa imatges o vídeos comprometedors, on apareix despullada o fent alguna activitat sexual.

(font: Termcat)

18/01. La policia del Regne Unit alerta de l'**augment d'atacs** de *sextorsió*. Segons s'indica, **les restriccions de mobilitat** han ajudat a incrementar aquest tipus d'atac com a conseqüència de l'augment de les relacions socials en línia. En un cas concret, un jove va ser contactat per xarxes socials per una noia que li va demanar que es despullés. Les **imatges** del noi van ser utilitzades per **extorquir-lo amb 200 £** (una mica més de 230 €) per evitar la publicació entre familiars i amics[209].

08/02. **Dos proveïdors** de serveis sanitaris van ser **extorsionats** després de rebre un atac de *ransomware*. Els atacants **van informar** des del seu web de la publicació de les **dades robades** a la ***dark web***. Les dades incloïen resultats de diagnòstics, assegurances de salut i informació sobre els empleats[210].

09/02. La companyia de serveis de *streaming* il·legal **No Support Linux Hosting** (Regne Unit) **va anunciar el tancament** després que un ciberatac afectés tota la infraestructura: web, administració i base de dades dels clients. No s'ofereixen detalls de l'atac. Tanmateix, cal destacar que altres companyies proveïdores de serveis de *streaming* il·legal, com ara SapphireSecure.net (UK) i KS-Hosting (UK), també van ser víctimes d'atacs sota l'**amenaça** de compartir una **base de dades robada** amb la **policia** si no es pagaven **2 *bitcoins* o tancaven els serveis**[211].

25/02. Un **polític iraquià** va ser víctima d'una **campanya d'intimidació i extorsió en línia**. El polític i la seva família va ser **assetjada** a la seva residència, i posteriorment les **amenaces i l'assetjament** van arribar a les **xarxes socials**. La motivació principal d'aquests atacs era econòmica, i els criminals demanaven gairebé **10 M€ per aturar l'assetjament**[212].

24/02. Es detecten **noves campanyes de *sextorsió*** dirigides a la ciutadania d'Itàlia. Els cibercriminals amenacen de **publicar presumptes dades comprometedores**, com ara vídeos o informació de llocs d'adults, en el cas de no pagar un rescat. Els atacants demanaen uns **800 €**[213].

01/03. La plataforma electrònica de *ticketing* **TicketCounter** (Països Baixos) va **exposar 1,9 milions d'adreces de correu** electrònic en un **servidor desprotegit**. El febrer, un actor maliciós va obrir un fil en un fòrum de la *dark web* per vendre les dades i, poc després, es van posar en contacte amb TicketCounter per demanar **7 *bitcoins* a canvi de no publicar res** i de **no informar els socis de la companyia** de la fuita d'informació[214].

04/03. La companyia californiana de ciberseguretat **Qualys** va ser objecte d'una extorsió per part del grup de *ransomware* Clop. Els atacants van robar **dades confidencials** que **van publicar a la *dark web***, probablement després que Qualys es negués a pagar un rescat. Qualys és una de les companyies que **ha patit extorsió** arran de l'atac al proveïdor Accelion, en la qual es van robar dades d'un gran nombre de companyies[215].

[209] *https://www.zdnet.com/article/uk-police-warn-of-sextortion-attempts-in-intimate-online-dating-chats/*
[210] *https://malware.news/t/extortionists-publish-data-stolen-from-two-healthcare-service-providers/46578*
[211] *https://www.zdnet.com/article/web-hosting-provider-shuts-down-after-cyber-attack/*
[212] *https://www.infosecurity-magazine.com/news/iraqi-mp-suffers-online-extortion/*
[213] *https://www.difesaesicurezza.com/areariservatacat/cybercrime-nuovo-tentativo-di-sextortion-in-italia/*
[214] *https://www.databreaches.net/european-e-ticketing-platform-ticketcounter-extorted-in-data-breach/*
[215] *https://www.hackread.com/it-security-firm-qualys-extorted-clop-gang-data-breach/*

5. Informació errònia o corrupta

Es continuen identificant atacs de tipus *meow*, en què s'eliminen bases de dades desprotegides sense motiu aparent. Els atacs de *ransomware* encara són la principal causa la corrupció de dades que, en la majoria de casos, no són recuperables. Destaca l'incendi al centre de dades OVH que va afectar milers de pàgines a tot el món, i un error de programació al Regne Unit.

El defacement, *o desfiguració, consisteix en la modificació no sol·licitada dels continguts d'un lloc web com a resultat de l'atac a aquest lloc web.*

(font: Termcat)

Un atac de tipus meow és aquell que elimina bases de dades que estan exposades públicament sense cap mena de seguretat, i afecta especialment ElasticSearch i MongoDB. L'atac finalitza un cop s'elimina la base de dades de manera permanent sense cap demanda per part dels atacants. Es desconeixen les motivacions reals dels atacs.

15/01. La policia del Regne Unit va eliminar per error 150.000 registres de detencions que incloïen empremtes, ADN i historials. Les dades van ser etiquetades per eliminar-les a causa d'un **error de codi** i van desaparèixer del sistema policial utilitzat per proveir informació en temps real de vehicles, persones, crims o si algun sospitós té conflictes pendents. Segons fonts de la policia, s'ha identificat el problema i **s'ha corregit** el procés perquè no torni a passar[216].

25/01. Un **ciutadà del Regne Unit** ha estat detingut per ser responsable d'un **atac sofisticat** contra l'**escola Welland Park Academy**, que li va permetre **esborrar el contingut dels discs durs dels dispositius** connectats a la xarxa. L'atac va afectar les **classes remotes i l'accés a material de suport**. En principi no hi ha evidències de la filtració pública de cap dada[217].

04/02. *L'startup* de l'Iran **Raychat** disposava d'un servidor **MongoDB** mal configurat que exposava públicament les **dades** de **267 milions de registres** d'usuaris, amb noms, correus electrònics, contrasenyes, metadades, etc. La informació va ser **eliminada** en un ciberatac automatitzat dut a terme per un *bot*. Els atacants van deixar una **nota de rescat** per valor de **0,019 *bitcoins*** a canvi de retornar les dades[218].

07/02. Un grup de *hacktivistes* desconegut **ha alterat els registres de DNS** de diferents llocs web a Sri Lanka amb l'objectiu de **redirigir** la navegació des d'algunes webs a d'altres que tracten **temes socials que impacten la població local**. La majoria de webs afectats eren de negocis locals i webs de notícies, tot i que també es van veure afectats google.lk i oracle.lk[219].

11/03. Un incendi en el centre de dades del proveïdor d'allotjament i serveis al núvol OVH va impactar la informació de **milions de webs**, especialment de França i Itàlia. També es calcula que el **36% dels 140 servidors afectats** en l'incendi eren utilitzats per diversos **grups de ciberdelinqüència i APT** com els grups Charming Kitten i APT39, vinculats a l'Iran, o Bahamut i l'OceanLotus APT, vinculats al Vietnam[220].

03/03. L'empresa d'analítica de dades del Regne Unit **Polecat va exposar**, des d'un servidor **ElasticSearch mal configurat**, **30 TB de dades amb 12 milions de registres** de dades personals recollides a les xarxes socials. El servidor mal configurat es va detectar el 29 d'octubre i un dia després va experimentar un atac de tipus *meow* que **va eliminar més de la meitat de les dades**. Pocs dies després, es va protegir adequadament[221].

[216] *https://digit.fyi/150000-arrest-records-lost-in-police-data-accident/*
[217] *https://www.theregister.com/2021/01/25/leicestershire_school_computer_misuse/*
[218] *https://www.gizmodo.com.au/2021/02/iranian-chat-app-gets-its-data-wiped-out-in-a-cyberattack/*
[219] *https://www.zdnet.com/article/hacktivists-deface-multiple-sri-lankan-domains-including-google-lk/*
[220] *https://www.xataka.com/pro/millones-paginas-caidas-incendio-ovh-gran-reto-montar-10-000-servidores-dos-semanas*
[221] *https://www.databreaches.net/uk-reputation-risk-intelligence-company-left-30tb-server-exposed/*

Conclusions

Tot i que els **estralls de la pandèmia** encara són ben **presents**, cal planificar com sortir de la **crisi socioeconòmica** causada per la covid-19. En el futur que ens espera, la **transformació digital** ha d'esdevenir un pilar principal, però també ho serà la **ciberseguretat**.

La UE ha posat en marxa els fons **NextGenEU** i, de la seva banda, el juliol de 2020, el Govern de la Generalitat de Catalunya aprovava el **Pla per a la reactivació econòmica i protecció social**[222]. A Catalunya, es va xifrar el cost total de la recuperació en **31.765 M€** distribuïts en projectes com la **transformació digital**, les **tecnologies digitals avançades** i la **innovació**. Així doncs, la societat catalana no serà una excepció i l'exposició davant de les ciberamenaces s'incrementarà. La **ciberseguretat** serà un **aspecte clau** per tal que els **nous projectes** per a la **transformació de la societat de la informació** a Catalunya es despleguin de forma **segura**.

Ara bé, la ciberseguretat, no és únicament un aspecte estratègic de futur. De fet, es constata com la **ciberseguretat** ja és una **prioritat actual**. Els **incidents cibernètics són més nombrosos i propers geogràficament**, però succeeix el mateix amb les mesures per fer-hi front. En quant a la **prevenció** d'incidents cibernètics, a l'Estat espanyol, es constata com els **pressupostos** en matèria de ciberseguretat augmenten, s'amplia la **normativa en ciberseguretat** i les **sancions** per incompliments (com les infringides per l'AEPD en el cas de l'RGPD) són **habituals i severes**. En quant a la **resposta** a incidents cibernètics, cada vegada són més habituals les **operacions policials**, també de Mossos d'Esquadra, que, en coordinació amb altres cossos, actuen contra un cibercrim que no coneix fronteres. Nombroses proves de tot això es pot trobar en aquest informe de tendències i en els dels darrers mesos[223].

I és que la **ciberseguretat** és un aspecte bàsic per reforçar el funcionament de la **societat de la informació** actual, ja que els **ciberatacs** estan explotant en les **relacions digitals essencials** pel funcionalment de l'economia en temps de pandèmia. Avui, un **incident cibernètic** ja no només afecta la víctima; cada vegada són més els casos d'**afectacions massives** que posen en **risc l'economia o l'estabilitat social**. En aquesta línia, la futura **Directiva NIS 2.0**, actualment en fase de discussió entre els estats membres, expandeix en seu abast més enllà dels operadors de serveis essencials i digitals, i inclou **companyies mitjanes i grans** en funció de la seva criticitat per l'economia i la societat. Més que mai, **la ciberseguretat és cosa de tots**.

En aquest context, l'**Agència de Ciberseguretat de Catalunya**, nascuda l'1 de gener de 2020, ha arribat en el **moment oportú**: per fer front a unes **ciberamenaces més actives i persistents**, així com per posar el gra de sorra perquè tots i totes ens en puguem **sortir, més forts i cibersegurs, de la crisi causada per la covid-19**.

[222] *https://web.gencat.cat/web/shared/GENCAT/coronavirus/mesures-coreco/pla-reactivacio-economica-i-proteccio-social/Pla-reactivacio-economica-proteccio-social.pdf*
[223] *https://ciberseguretat.gencat.cat/ca/Informes-de-Tendencies-en-Ciberseguretat/index.html*

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

ciberseguretat.gencat.cat

juliol de 2021