**Patrocinen**

andornet

**Deloitte.**

OptimumTIC

auren

ÍTACA
advanced analytics

ISACA
Barcelona Chapter

*Ciberseguretat:*
**De les tendències de 2023 als desafiaments de 2025**

Ponent

**Santi Romeu**

*Cap d'Unitat de Ciència i Analítica de Dades Àrea del CIC4Ciber de l'Agència de Ciberseguretat de Catalunya*

Barcelona, 12 de febrer de 2024

**Suport Institucional**

informàTICa

COL·LEGI OFICIAL ENGINYERIA INFORMÀTICA

iapp

ISMS forum spain

UAB Universitat Autònoma de Barcelona

telecos.cat

economistas

NCN

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

AQPE

Project Management Institute Barcelona, Spain

ISACA
Barcelona Chapter

ISACA Barcelona

@ISACABCN

Més informació sobre aquest canal >

Subscrit

Inici Vídeos Llistes de reproducció Comunitat

Més recents Populars Més antics


XII Congrés ISACA Barcelona (2023). [Vídeo 1/8] Benvinguda i Presentació Institucional

37 visualitzacions • fa 3 setmanes


XII Congrés ISACA Barcelona (2023). [Vídeo 2/8] Bruno Pérez - Ciberseguretat en l'entor...

47 visualitzacions • fa 3 setmanes


XII Congrés ISACA Barcelona (2023). [Vídeo 3/8] Tom de Beer - 'OT Governance, NIS...

23 visualitzacions • fa 3 setmanes


XII Congrés ISACA Barcelona (2023) - [Vídeo 4/8] Taula Rodona: 'El triangle del bulling'

31 visualitzacions • fa 3 setmanes


XII Congrés ISACA Barcelona (2023). [Vídeo


XII Congrés ISACA Barcelona (2023). [Vídeo


XII Congrés ISACA Barcelona (2023). [Vídeo


XII Congrés ISACA Barcelona (2023). [Vídeo

www.isacabcn.org

YouTube @ISACABCN

ISACA
Barcelona Chapter

BARCELONA CYBERSECURITY CONGRESS

MAY 21 - 23, 2024
BARCELONA - GRAN VIA VENUE

Fira Barcelona

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA



# SECURE TODAY, SAFEGUARD TOMORROW

Secure your space for 2024! Book your slot now and be part of the most importantCybersecurity Gathering in Europe!

ISACA Barcelona Chapter

# De les tendències del 2023... als desafiaments pel 2024

**Santi Romeu Sala**
Cap de la Unitat de Ciència i Analítica de Dades

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA
Generalitat de Catalunya

# Tendències del 2023

# Un món en conflicte, també al ciberespai

En un món on la rivalitat geopolítica creix, augmenta el ciberespionatge en forma d'intrusions, robatoris d'informació i distribució de *info-stealers*

L'any després de l'inici del conflicte entre Ucraïna i Rússia: *wipers* i atacs de DDoS, distribució d'*info-stealers* i campanyes de desinformació

Grups *hacktivistes* i cibercriminals s'han alineat amb els actors en conflicte

El 7 d'octubre de 2023, va arrencar un conflicte bèl·lic al Pròxim Orient que també ha sobrepassat el món físic i ha transcendit a Internet amb un comportament similar

**Els països més atacats són els relacionts amb conflictes internacionals Ucraïna, Israel, Corea...** [Microsoft Threat Intelligence]

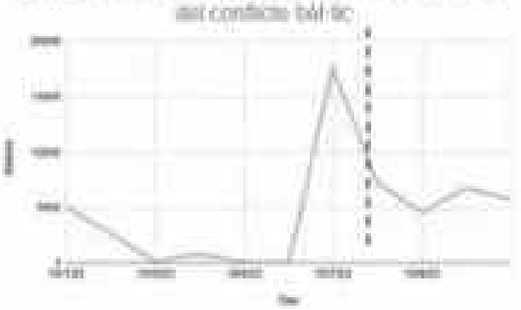
Taula dels països més atacats per regió (juliol 2022-juny 2023)

| Europe | Middle East & North Africa | Asia Pacific |
|---|---|---|
| 1. Ukraine (23%) | 1. Israel (36%) | 1. Korea (17%) |
| 2. United Kingdom (11%) | 2. United Arab Emirates (12%) | 2. Taiwan (15%) |
| 3. France (5%) | 3. Saudi Arabia (9%) | 3. India (13%) |
| 4. Poland (5%) | 4. Jordan (8%) | 4. Malaysia (9%) |
| 5. Italy (4%) | 5. Iraq (5%) | 5. Japan (5%) |
| 6. Germany (3%) | 6. Bahrain (4%) | 6. Australia (5%) |

**El nombre d'atacs de DDoS contra Israel es multiplica x10** [Imperva]

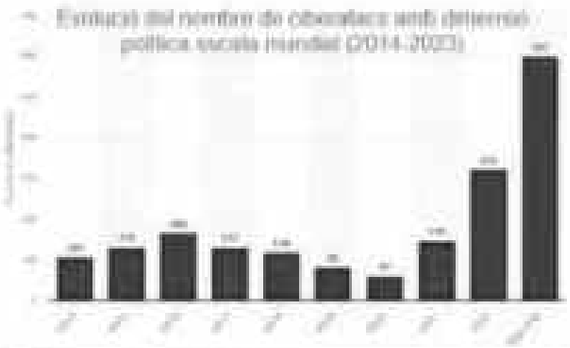
Sobretot dirigits a web governamentals i bancs.

Nombre d'atacs de l'DDoS vs Israel els primers dies del conflicte bèl·lic



**El 2023, l'any de més ciberatacs amb motivació política** [Statista]

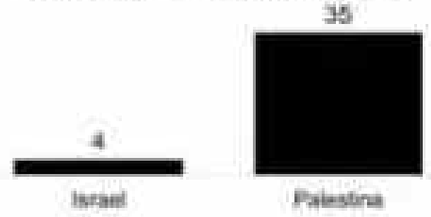
Evolució del nombre de ciberatacs amb diferents política sucosa mundial (2014-2023)



**Posicionament del *hacktivisme*** [The CyberExpress]

En els dos dies posteriors a l'inici de l'ofensiva d'Israel, van irrompre posicionant-se diferents grups *hacktivistes*.

Nombre de grups hacktivistes que s'han posicionat en el conflicte a favor d'Israel o Palestina



# Un món en conflicte, també al ciberespai

**Es descobreix una campanya de ciberespionatge dirigit a les ambaixades estrangeres a Bielorússia**

La campanya està enfocada a ambaixades europees, asiàtiques i africanes. Podria estar activa des de 2017 i MoustacheBouncer, un grup alineat als interessos de Bielorússia, en seria el responsable.
Els atacs s'han produït mitjançant la tècnica AiTM (*Adversary in The Middle*), és a dir, instal·lant un servidor *proxy* entre un usuari objectiu i el web que l'usuari/usuària vol visitar, tot fent que aquest servidor sigui un lloc de *phishing* sota el control dels atacants. Així, aquests poden obtenir les credencials d'accés dels usuaris/usuàries.

**Es detecta una campanya de *wiper* perpetrada per un grup pro-Hamàs**

S'ha detectat que l'actor d'amenaces conegut com Arid Viper ha utilitzat un *malware* conegut com BiBi-Linux Wiper dirigit a destruir els sistemes operatius d'entitats israelianes, tot i que no s'ha revelat cap víctima fins al moment.
Arid Viper és conegut per tenir dos subgrups d'operacions de ciberespionatge dirigits cap a Israel i opositors palestins. Destaca per l'ús de l'enginyeria social i el *phishing* com a vectors d'atac inicials per infectar les víctimes amb *malwares* com Micropsia (*infostealer*) i variants com Arid Gopher.

**Palo Alto Networks descobreix una campanya de ciberespionatge de l'APT29 a Ucraïna**

La Unit 42 de Palo Alto Networks (EUA) ha detectat una campanya de ciberespionatge dirigida a diplomàtics en missió a Ucraïna. Per enganyar els diplomàtics, els enviaven informació sobre venda de vehicles, un bé molt preuat en aquesta professió. Si s'obria el document adjunt, s'acabaven instal·lant diferents *malware* que deixaven l'equip compromès.
La campanya, vinculada a l'APT 29 i presumptament patrocinada per Rússia, es va dirigir a 22 missions estrangeres, d'entre les més de 80 que hi ha Kiiv.

**La lluita pel relat del conflicte ha provocat un augment de la desinformació i notícies falses**

Enmig de la creixent violència del conflicte, cada bàndol s'esforça per guanyar-se l'opinió pública internacional. Això s'ha demostrat en l'intercanvi d'acusacions arran de l'atac a l'hospital Al-Ahli de la ciutat de Gaza. A més a més, alguns analistes ja han començat a alertar sobre l'augment de desinformació i *fake news* que corren per la xarxa, amb el conseqüent risc d'una escalada del conflicte, que podria arribar més enllà d'Israel i Palestina.

**Atacs de DDoS van acompanyar l'atac de Hamàs**

Dotze minuts després de l'inici de les hostilitats de Hamàs, l'empresa de ciberseguretat Cloudflare (EUA) va detectar un seguit d'atacs de DDoS contra els webs israelians que ofereixen informació i alertes als civils sobre atacs amb coets. Altres objectius d'aquest tipus d'atacs han estat els mitjans de comunicació i les empreses de desenvolupament de *software*. D'altra banda, també van identificar atacs de DDoS dirigits a organitzacions palestines, especialment del sector bancari o proveïdors de serveis d'Internet.

**El conflicte entre Hamàs i Israel és una nova oportunitat per a l'estafa virtual**

Els ciberdelinqüents aprofiten les situacions del moment per treure'n benefici, i el conflicte entre Hamàs i Israel, igual que el de Rússia i Ucraïna, els ha suposat una oportunitat per engegar campanyes de frau.
Enmig de la intensa cobertura sobre el conflicte, ja han aparegut pàgines que demanen ajudes econòmiques per als afectats. En realitat, els diners aniran a parar als propis ciberdelinqüents.

# Ciberatacs contra els operadors de subministraments bàsics

L'objectiu dels ciberatacs amb motivació geopolítica és desestabilitzar l'adversari i perjudicar la confiança amb les estructures

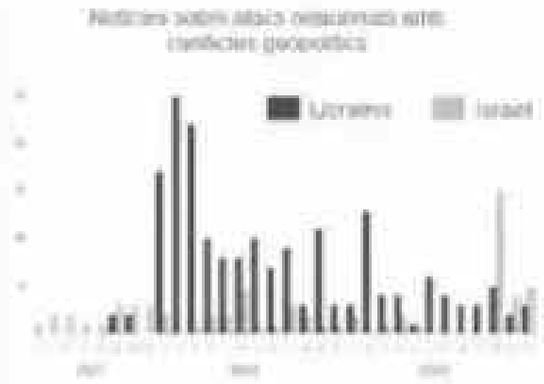
Proliferen els ciberatacs contra objectiu industrials vinculats a sectors com l'alimentari i els subministraments d'aigua o energia

Grups APT (*Advanced Persistent Threat*), PSOA (*Private-Sector Offensive Actor*) i grups cibercriminals han entrat en joc en el conflicte

Aquests grups aprofiten el conflicte per actuar amb la impunitat que els ofereix la confusió internacional

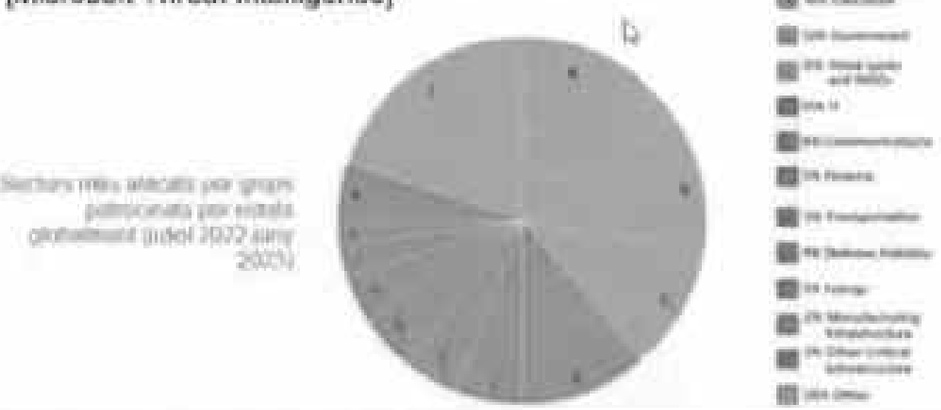
Els ciberatacs escalen ràpidament a la resta del món i involucren nous països: Iran, els EUA, Irlanda...

**Arrenca l'activitat cibernètica relacionada amb el conflicte del Pròxim Orient mentre que el d'Ucraïna-Rússia segueix viu** [Agència]




**Els ciberatacs amb motivació geopolítica afecten a tercers** [Agència]


**El 41% de les notificacions d'amenaça de MS dirigides a infraestructures crítiques** [Microsoft Threat Intelligence]



# Ciberatacs contra els operadors de subministraments bàsics

L'objectiu dels ciberatacs amb motivació geopolítica és desestabilitzar l'adversari i perjudicar la confiança amb les estructures

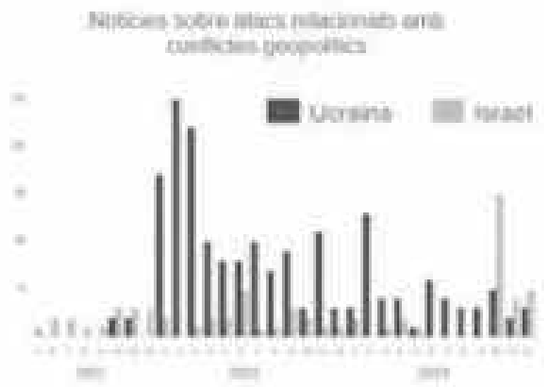
Proliferen els ciberatacs contra objectiu industrials vinculats a sectors com l'alimentari i els subministraments d'aigua o energia

Grups APT (*Advanced Persistent Threat*), PSOA (*Private-Sector Offensive Actor*) i grups cibercriminals han entrat en joc en el conflicte

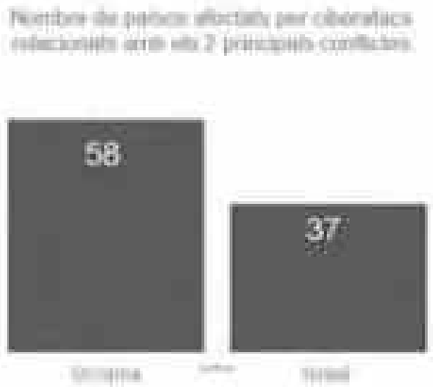
Aquests grups aprofiten el conflicte per actuar amb la impunitat que els ofereix la confusió internacional

Els ciberatacs escalen ràpidament a la resta del món i involucren nous països: Iran, els EUA, Irlanda...

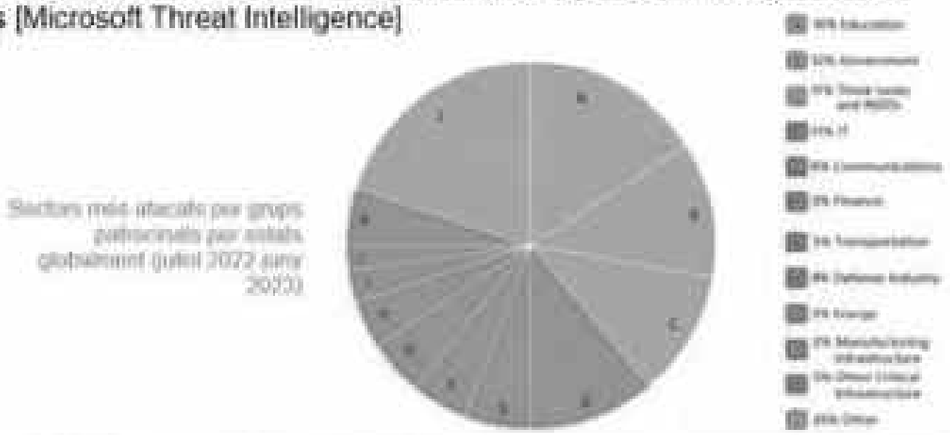
**Arrenca l'activitat cibernètica relacionada amb el conflicte del Pròxim Orient mentre que el d'Ucraïna-Rússia segueix viu** [Agència]




**Els ciberatacs amb motivació geopolítica afecten a tercers** [Agència]




**El 41% de les notificacions d'amenaça de MS dirigides a infraestructures crítiques** [Microsoft Threat Intelligence]



# Ciberatacs contra els operadors de subministraments bàsics

**Alguns grups *hacktivistes* van al darrere de sistemes ICS o SCADA palestins o israelians**

Després de que el grup cibercriminal ThreatSec publiqués a les seves xarxes atacs efectuats cap a ambdós bàndols, analistes de CyberNews han detectat intents d'atac per part de *hacktivistes* pro-israelians i pro-palestins contra sistemes ICS i SCADA per afectar infraestructures crítiques de les dues regions. Analitzant l'entorn industrial dels dos bàndols, els analistes han detectat organitzacions israelianes que tenen xarxes Modbus (protocol de comunicació SCADA) exposades, igual que el sector palestí que també té sistemes d'automatització Siemens, entre d'altres.

**Un grup de cibercriminals propalestí ataca una important fàbrica de farina israeliana**

El grup de cibercriminals propalestí "Soldats de Salomó" assegura haver accedit a la infraestructura d'una de les majors fàbriques de farina israelianes, causant danys greus. S'apunta que fan ús d'un *ransomware* dissenyat *adhoc*.
S'han difós captures de pantalla dels sistemes de control de la planta i afirmen haver-ne afectat el cicle de producció. Aquest atac podria tenir un impacte significatiu en la cadena d'aprovisionament alimentari. El grup ha dirigit altres atacs recents, incloent-hi un ciberatac a la planta solar israeliana d'Ashalim.

**La Corporació Elèctrica Israeliana pateix talls de subministrament importants**

Israel ha patit extenses pèrdues d'energia i talls d'internet després del col·lapse de dues unitats de producció de la companyia Israel Electric Corporation. Se sospita d'un ciberatac l'autoria iraniana, tot i que la companyia ha negat que es tracti d'un ciberatac.
Malgrat que unes 150.000 persones van veure's afectades inicialment, només 34.000 van romandre sense energia. Les autoritats israelianes estan investigant i, si es confirma que es tracta d'un ciberatac fet des d'Iran, seria una nova mostra de l'escalada en el conflicte.

**Un ciberatac d'un grup vinculat a Israel afecta un 70% de les gasolineres a l'Iran**

El 70% de les gasolineres a tot Iran han patit una interrupció dels serveis a causa d'un ciberatac reivindicat pel grup israelià anomenat Gonjeshke Darande.
El grup va afirmar que aquest atac era una represàlia als moviments agressius de l'Iran, assegurant que no tenen com a objectiu la població civil.
En qualsevol cas, l'Iran afirma haver iniciat una investigació sobre l'incident.

**La Creu Roja emet normes per als *hacktivistes* en temps de guerra**

El Comitè Internacional de la Creu Roja (CICR) ha publicat un nou conjunt de normes que insten els *hacktivistes* a complir el dret internacional humanitari en temps de conflicte. Adverteix que els ciberatacs realitzats per civils en temps de guerra estan causant cada cop més interrupcions a objectius no militars. A més, aquests atacs també podrien significar que els *hacktivistes* es posen en perill, ja que indiquen a les forces oposades que són un objectiu militar legítim.

# Ciberatacs contra els operadors de subministraments bàsics

**Ciberatacs amb vincles iranians dirigits a instal·lacions d'aigua dels EUA**

El govern dels EUA investiga diversos ciberatacs a instal·lacions d'aigua del país, presumptament realitzats per un grup cibercriminal iranià. Un d'aquests atacs, reivindicat pel grup Cyber Av3ngers, va afectar la infraestructura OT de la Pennsylvania Water Authority, fins al punt que els automatismes van haver de passar a ser gestionats manualment. Aquest ciberatac ha tingut afectació global, fins i tot ha impactat entitats de Catalunya.
El ciberatac evidencia com les tecnologies d'origen israelià (en aquest cas les màquines del sistema Unitronics) són objectiu dels ciberatacs.

**Cyber Av3ngers talla el subministrament d'aigua a dues localitats irlandeses en suport a Palestina**

El grup iranià Cyber Av3ngers, va afirmar que havia aconseguit tallar el subministrament d'aigua a dues localitats irlandeses durant dos dies, atacant la infraestructura d'un sistema de bombeig d'aigua d'un fabricant israelià. Precisament,
Els responsables de la companyia han mencionat que no comptaven amb un *firewall* prou segur i aquest havia sigut el vector d'entrada.

**L'APT Sandworm ataca Ucraïna i provoca talls en el subministrament elèctric**

El grup APT Sandworm, vinculat a Rússia, hauria perpetrat un ciberatac dirigit a la xarxa elèctrica d'Ucraïna per forçar apagades durant un bombardeig rus.
Els ciberatacants van executar un programari maliciós específic per a tecnologies d'operació (OT) d'entorns industrials, el qual va activar els protectors de sobrecàrrega i va provocar caigudes elèctriques. Posteriorment, van desplegar una variant del *wiper* CADDYWIPPER per esborrar-ne el rastre. Tot i que encara es desconeix com van accedir a la xarxa, se'n tenen evidències des del juny de 2022.

**Un ciberatac rus talla l'accés a Internet per a milions d'ucraïnesos després de l'atac a Kyivstar**

El major proveïdor de serveis de telecomunicacions d'Ucraïna, Kyivstar, ha experimentat una interrupció massiva dels serveis de telefonia i d'Internet, atribuïda a un ciberatac d'origen rus.
L'atac tenia com a objectiu destruir la infraestructura virtual de l'empresa. Tot i que Kyivstar va prendre mesures per limitar els danys, la restauració dels serveis no té un termini clar.
Aquest és un episodi més en la tensió digital contínua entre Ucraïna i Rússia enmig del conflicte militar.

**Blackjack ataca la infraestructura digital de Rosvodokanal, empresa d'aigua russa**

El grup ucraïnès Blackjack ha reivindicat un atac cibernètic contra l'empresa russa d'aigua Rosvodokanal, en el qual ha eliminat més de 50 terabytes de dades.
L'atac podria haver comptat amb l'ajuda dels serveis de seguretat ucraïnesos.
S'especula la possibilitat que es tracti d'una represàlia per l'atac cibernètic rus a Kyivstar. Tot i així, no s'ha emès cap comunicat oficial, i la investigació continua.

# L'estabilitat social i econòmica en risc

També, els periodes electorals que fonamenten les democràcies s'han convertit en un moment crític en què s'intensifiquen els ciberatacs, especialment de DDoS

Amb la incorporació creixent de TIC en aquests processos democràtics neixen noves oportunitats per ciberatacar

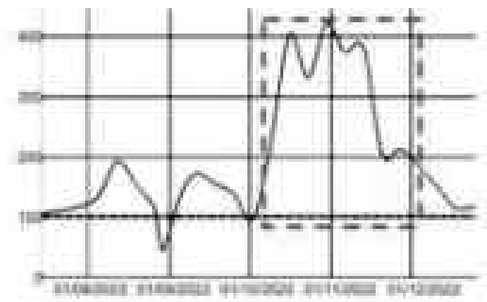
Els grups cibercriminals aprofiten l'avinentesa per a la difusió de campanyes de *phishing* per cometre fraus

Al mateix temps, la ciberseguretat esdevé un element bàsic per preservar l'estabilitat social i econòmica

**Augmenten els ciberatacs en periodes electorals** [Google]

Google disposa d'una eina gratuïta de protecció contra atacs de DDoS dirigits a webs d'organitzacions de protecció de drets humans, candidats a càrrecs públics i portals de monitorització d'eleccions. L'anàlisi de la seva activitat mostra un augment d'atacs durant les *midterms* (eleccions per a la renovació del Congrés i un terç del Senat dels EUA) a la tardor del 2022.

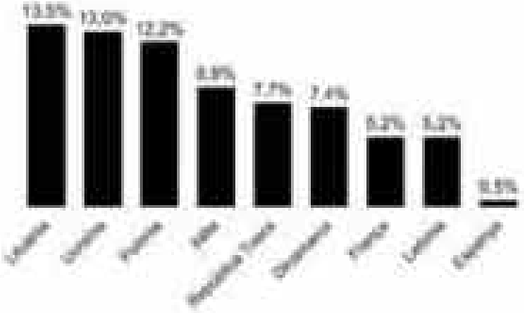
Atacs DDoS per setmana detectats per Google durant el 2022, en vermell el període de midterms



**Poca activitat de NoName057 a Espanya abans de les eleccions** [Sekoia]

Abans de la campanya d'atacs de NoName057 dirigits a les eleccions estatals del 23J, l'activitat del grup cibercriminal al país representava només un 0,5%.

% d'atacs del grup NoName057 per país de maig a juny del 2023



# L'estabilitat social i econòmica en risc

**Diferents webs de l'administració espanyola experimenten atacs de DDoS durant el 23J**

Els atacs els va perpetrar el grup cibercriminal NoName057, vinculat al Kremlin i especialitzat en atacs a objectius polítics.
L'ofensiva era en resposta a la implicació d'Espanya a favor d'Ucraïna en el conflicte bèl·lic. El grup va dur a terme una sèrie d'atacs de DDoS contra webs governamentals, les quals van quedar fora de servei, en alguns casos, durant hores. Alguns dels webs afectats van ser el del Ministeri d'Interior, l'INE, la Junta Electoral i el govern d'Espanya. Segons Interior, es tractava de la major ciberofensiva a Espanya des de l'inici del conflicte.

**Durant el 23J, NoName057 també va atacar mitjans de comunicació i empreses**

L'ofensiva de NoName057 no només es va limitar a atacs de DDoS contra institucions governamentals de l'estat espanyol, sinó que també va dirigir els seus atacs contra mitjans de comunicació i empreses.
Alguns dels mitjans afectats van ser El Mundo, ABC, El Español i el diari econòmic Expansión. Pel que fa a les empreses, destaquen RENFE, TMB, els metros de Madrid i València, i els Transports de les Illes Balears.

**Un ciberatac altera el cartell d'una farmàcia i mostra un missatge electoral**

Una farmàcia de Ceuta va patir un ciberatac que va provocar la modificació del seu cartell lluminós. A la creu verda que indica la presència d'una farmàcia s'hi podia llegir el missatge "Que te vote Txapote".
El propietari de l'establiment, desconeixedor del fet, va començar a rebre missatges de diferents motivacions, al telèfon i a les xarxes socials. Posteriorment, va presentar denúncia a la Policia Nacional i va declarar que no sabia com algú podia haver entrar al seu ordinador des d'on gestiona, via *bluetooth*, el cartell lluminós.

**Campanya de *phishing* amb el pretext de la mesa electoral per robar dades personals**

Un cop ja s'havia efectuat el sorteig dels integrants de les meses electorals del 23J, des del Ministeri d'Interior es va detectar una campanya de *phishing* des d'una adreça de correu que suplantava aquest ministeri i un enllaç a un lloc web fraudulent des del qual es podien verificar les dades censals i si s'havia estat cridat a una mesa electoral.
El Ministeri d'Interior va informar a les xarxes socials que es tractava d'una campanya fraudulenta enfocada al robatori de dades personals i bancàries, i que els avisos d'aquest tipus no venen mai per correu electrònic sinó per correu certificat.

**Diversos ciberatacs van dificultar el vot electrònic en les eleccions d'Equador el 20A**

Segons la presidenta del Consell Electoral Nacional, diversos ciberatacs, dels quals no en va donar detalls, van inutilitzar la plataforma virtual que el govern de l'Equador havia elaborat per tal que els equatorians i equatorianes que visquessin a l'estranger poguessin votar electrònicament.
A la plataforma s'hi van registrar uns 120.000 ciutadans, però no tots van poder exercir el seu dret a vot, ja que la plataforma estava fora de servei o no funcionava correctament.
Les investigacions van concloure que els atacs provenien de països com l'Índia, el Pakistan, Rússia, Ucraïna o la Xina.

**Autoritats del Brasil haurien demanat a un especialista manipular una urna electrònica**

Segons Walter Delgatti Neto, un especialista en sistemes informàtics, Jair Bolsonaro, quan era president del Brasil, hauria demanat a un especialista que manipulés una urna electrònica per tal de demostrar que el sistema electoral era vulnerable al frau. La idea era agafar una urna electrònica, instal·lar-hi el seu *software* i que, al prémer un botó per votar, s'obtingués un altre resultat.
L'especialista apunta que, presumptament, la manipulació de les urnes electròniques s'hauria d'haver fet un mes abans de la primera volta de les eleccions, però finalment no s'hauria realitzat.

# La IA irromp en la ciberseguretat

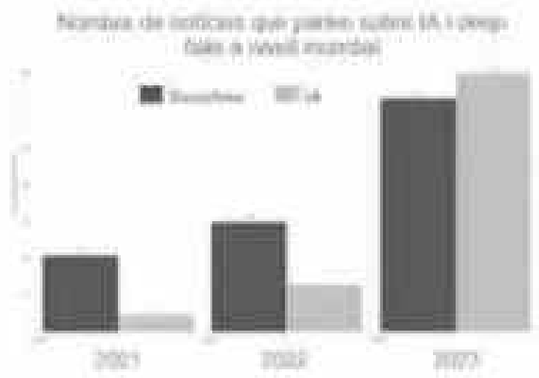
La irrupció d'eines d'IA generativa permet generar *deep fakes* per desenvolupar continguts il·lícits, difondre desinformació o crear campanyes de frau

La IA Generativa facilita que els ciberdelinqüents obtinguin capacitats per crear o evolucionar *malware*, identificar vulnerabilitats a explotar i elaborar campanyes de *phishing*

Però també permet fer-ne ús per a la ciberseguretat: escriure programari, comprendre codi, identificar problemes de seguretat a les aplicacions, consells...

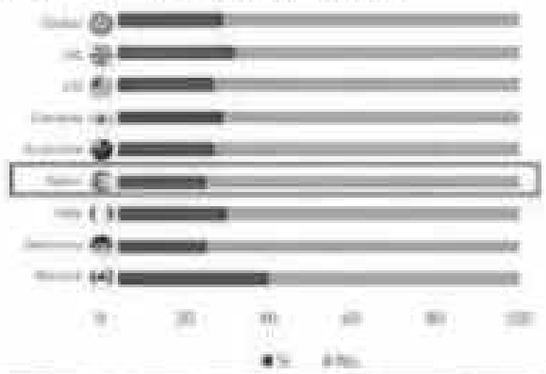
la IA es fa imprescindible, de manera que ja es pot afirmar sense por a equivocar-se que la pròxima generació de tecnologies de ciberdefensa es basarà en aquesta

**Augment de l'ús de la IA i els *deep fakes* en els ciberatacs** [Agència]




**L'estat espanyol a la cua del coneixement del què és un *deep fake*** [iproov]

Una enquesta global a més de 16.000 persones destaca que un 71% dels enquestats no coneixen què és.



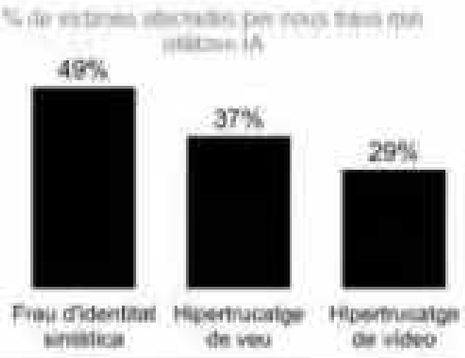
**Millora de les tècniques d'enginyeria social amb IA** [DarkTrace]

Un informe destaca que, des de l'aparició del ChatGPT, hi ha hagut un augment del 135% d'atacs d'enginyeria social que utilitzen tècniques lingüístiques més sofisticades com ara:

- Augment del volum de text.
- Millora de la puntuació.
- Més longitud de les frases sense enllaços ni fitxers adjunts.

**Noves tècniques de frau**

Una enquesta global a 1.069 professionals de diferents sectors destaca les afectacions per nous fraus :



# L'estabilitat social i econòmica en risc

**Diferents webs de l'administració espanyola experimenten atacs de DDoS durant el 23J**

Els atacs els va perpetrar el grup cibercriminal NoName057, vinculat al Kremlin i especialitzat en atacs a objectius polítics.
L'ofensiva era en resposta a la implicació d'Espanya a favor d'Ucraïna en el conflicte bèl·lic. El grup va dur a terme una sèrie d'atacs de DDoS contra webs governamentals, les quals van quedar fora de servei, en alguns casos, durant hores. Alguns dels webs afectats van ser el del Ministeri d'Interior, l'INE, la Junta Electoral i el govern d'Espanya. Segons Interior, es tractava de la major ciberofensiva a Espanya des de l'inici del conflicte.

**Durant el 23J, NoName057 també va atacar mitjans de comunicació i empreses**

L'ofensiva de NoName057 no només es va limitar a atacs de DDoS contra institucions governamentals de l'estat espanyol, sinó que també va dirigir els seus atacs contra mitjans de comunicació i empreses.
Alguns dels mitjans afectats van ser El Mundo, ABC, El Español i el diari econòmic Expansión. Pel que fa a les empreses, destaquen RENFE, TMB, els metros de Madrid i València, i els Transports de les Illes Balears.

**Un ciberatac altera el cartell d'una farmàcia i mostra un missatge electoral**

Una farmàcia de Ceuta va patir un ciberatac que va provocar la modificació del seu cartell lluminós. A la creu verda que indica la presència d'una farmàcia s'hi podia llegir el missatge "Que te vote Txapote".
El propietari de l'establiment, desconeixedor del fet, va començar a rebre missatges de diferents motivacions, al telèfon i a les xarxes socials. Posteriorment, va presentar denúncia a la Policia Nacional i va declarar que no sabia com algú podia haver entrar al seu ordinador des d'on gestiona, via *bluetooth*, el cartell lluminós.

**Campanya de *phishing* amb el pretext de la mesa electoral per robar dades personals**

Un cop ja s'havia efectuat el sorteig dels integrants de les meses electorals del 23J, des del Ministeri d'Interior es va detectar una campanya de *phishing* des d'una adreça de correu que suplantava aquest ministeri i un enllaç a un lloc web fraudulent des del qual es podien verificar les dades censals i si s'havia estat cridat a una mesa electoral.
El Ministeri d'Interior va informar a les xarxes socials que es tractava d'una campanya fraudulenta enfocada al robatori de dades personals i bancàries, i que els avisos d'aquest tipus no venen mai per correu electrònic sinó per correu certificat.

**Diversos ciberatacs van dificultar el vot electrònic en les eleccions d'Equador el 20A**

Segons la presidenta del Consell Electoral Nacional, diversos ciberatacs, dels quals no en va donar detalls, van inutilitzar la plataforma virtual que el govern de l'Equador havia elaborat per tal que els equatorians i equatorianes que visquessin a l'estranger poguessin votar electrònicament.
A la plataforma s'hi van registrar uns 120.000 ciutadans, però no tots van poder exercir el seu dret a vot, ja que la plataforma estava fora de servei o no funcionava correctament.
Les investigacions van concloure que els atacs provenien de països com l'Índia, el Pakistan, Rússia, Ucraïna o la Xina.

**Autoritats del Brasil haurien demanat a un especialista manipular una urna electrònica**

Segons Walter Delgatti Neto, un especialista en sistemes informàtics, Jair Bolsonaro, quan era president del Brasil, hauria demanat a un especialista que manipulés una urna electrònica per tal de demostrar que el sistema electoral era vulnerable al frau. La idea era agafar una urna electrònica, instal·lar-hi el seu *software* i que, al prémer un botó per votar, s'obtingués un altre resultat.
L'especialista apunta que, presumptament, la manipulació de les urnes electròniques s'hauria d'haver fet un mes abans de la primera volta de les eleccions, però finalment no s'hauria realitzat.

# L'estabilitat social i econòmica en risc

També, els periodes electorals que fonamenten les democràcies s'han convertit en un moment crític en què s'intensifiquen els ciberatacs, especialment de DDoS

Amb la incorporació creixent de TIC en aquests processos democràtics neixen noves oportunitats per ciberatacar

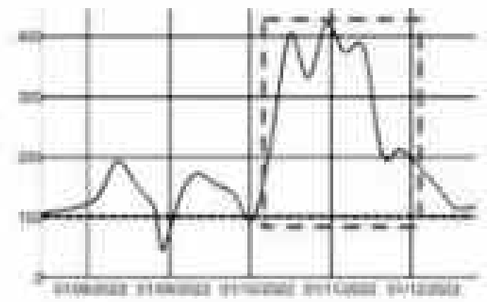
Els grups cibercriminals aprofiten l'avinentesa per a la difusió de campanyes de *phishing* per cometre fraus

Al mateix temps, la ciberseguretat esdevé un element bàsic per preservar l'estabilitat social i econòmica

**Augmenten els ciberatacs en periodes electorals** [Google]

Google disposa d'una eina gratuïta de protecció contra atacs de DDoS dirigits a webs d'organitzacions de protecció de drets humans, candidats a càrrecs públics i portals de monitorització d'eleccions. L'anàlisi de la seva activitat mostra un augment d'atacs durant les *midterms* (eleccions per a la renovació del Congrés i un terç del Senat dels EUA) a la tardor del 2022.

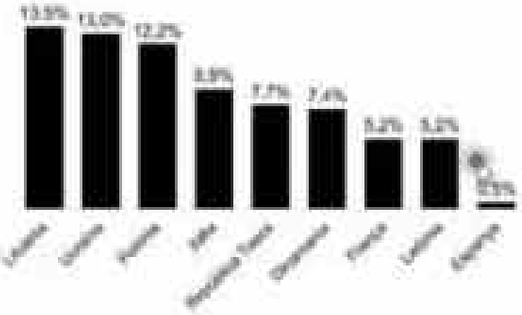
Atacs DDoS per setmana detectats per Google durant el 2022, en vermell el periode de midterms



**Poca activitat de NoName057 a Espanya abans de les eleccions** [Sekoia]

Abans de la campanya d'atacs de NoName057 dirigits a les eleccions estatals del 23J, l'activitat del grup cibercriminal al país representava només un 0,5%.

% d'atacs del grup NoName057 per país de inici a país del 2023



# La IA irromp en la ciberseguretat

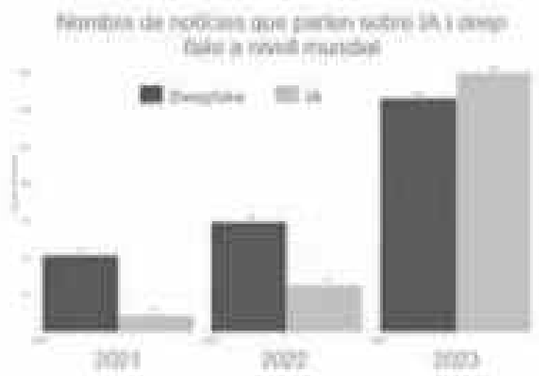
La irrupció d'eines d'IA generativa permet generar *deep fakes* per desenvolupar continguts il·lícits, difondre desinformació o crear campanyes de frau

La IA Generativa facilita que els ciberdelinqüents obtinguin capacitats per crear o evolucionar *malware*, identificar vulnerabilitats a explotar i elaborar campanyes de *phishing*

Però també permet fer-ne ús per a la ciberseguretat: escriure programari, comprendre codi, identificar problemes de seguretat a les aplicacions, consells...

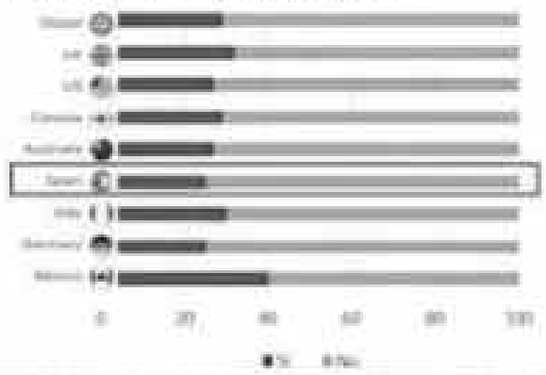
la IA es fa imprescindible, de manera que ja es pot afirmar sense por a equivocar-se que la pròxima generació de tecnologies de ciberdefensa es basarà en aquesta

**Augment de l'ús de la IA i els *deep fakes* en els ciberatacs** [Agència]




**L'estat espanyol a la cua del coneixement del què és un *deep fake*** [iproov]

Una enquesta global a més de 16.000 persones destaca que un 71% dels enquestats no coneixen què és.



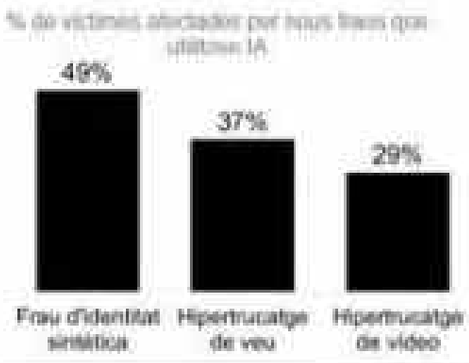
**Millora de les tècniques d'enginyeria social amb IA** [DarkTrace]

Un informe destaca que, des de l'aparició del ChatGPT, hi ha hagut un augment del 135% d'atacs d'enginyeria social que utilitzen tècniques lingüístiques més sofisticades com ara:

- Augment del volum de text.
- Millora de la puntuació.
- Més longitud de les frases sense enllaços ni fitxers adjunts.

**Noves tècniques de frau**

Una enquesta global a 1.069 professionals de diferents sectors destaca les afectacions per nous fraus :



# La IA irromp en la ciberseguretat

**Cloudflare alerta sobre amenaça de *deepfakes* i desinformació en un any electoral crucial als EUA**

Els EUA s'encaminen cap a un any electoral crucial, on les perspectives per les properes eleccions són incertes. L'empresa Cloudflare ha identificat diferents ciberamenaces i tendències de ciberatacs que podrien posar en perill unes eleccions segures i fiables.
Les ciberamenaces inclouen desinformació disseminada amb l'ajuda de la intel·ligència artificial. Els *deep fakes* podrien jugar un paper crucial on es podria veure un augment de les amenaces cibernètiques, amb *deep fakes* i desinformació.

**L'FBI adverteix sobre l'ús d'imatges generades amb IA per dur a terme *sextorsions***

L'FBI ha observat la tendència d'alguns cibercriminals a dur a terme sextorsions a partir d'imatges alterades amb IA. Segons els investigadors, els cibercriminals agafen imatges que les víctimes pengen a les xarxes socials i les modifiquen amb IA per tal de convertir-les en pornogràfiques. Aleshores, els malfactors, sota l'amenaça d'enviar les imatges a familiars o publicar-les a les xarxes socials, exigeixen diners o fotos reals de la víctima despullada.

**Ratan Tata denuncia l'ús fraudulent de la seva identitat en una estafa d'inversió amb *deep fake***

L'empresari industrial Ratan Tata ha estat víctima d'una sofisticada falsificació de la seva identitat en un vídeo *deep fake* associat a esquemes d'inversió fraudulents.
El vídeo manipulat provenia del compte de l'usuari Sona Agrawal, en el qual es mostrava l'empresari fent-se passar pel gerent del Grup Tata recomanant diferents inversions que reforçaven la narrativa ficticia. Ratan Tata ha alertat públicament d'aquest *deep fake*, titllant-lo de "fals" i negant qualsevol implicació en els mencionats projectes d'inversió.

**Estafa telefònica amb simulació d'IA**

Després de diverses denúncies, l'augment de les estafes telefòniques que simulen les veus de familiars demanant diners fan saltar les alarmes a Espanya.
Aquesta pràctica està experimentant un augment entre estafadors, els quals utilitzen serveis com el d'Eleven Labs, una empresa especialitzada en la síntesi de veu amb intel·ligència artificial.
L'increment d'aquest tipus de frau es deu a la facilitat de les eines per suplantar veus, així com a la baixa despesa associada al servei, amb tarifes que oscil·len entre 4,65 i 279 €/mes.

**La simulació d'un segrest per IA arriba fins a un comitè del Senat dels EUA**

A l'abril, uns criminals van obtenir unes mostres de veu d'una noia de 15 anys a partir d'entrevistes que havia fet a l'escola. Utilitzant la IA, van aconseguir reproduir la veu de la noia i van trucar a la seva mare simulant un segrest. Van exigir un rescat d'1 M€. Afortunadament, la mare va aconseguir posar-se en contacte amb la seva filla per un altre canal i va comprovar que estava bé.
Aquest mes, el cas ha arribat al Comitè Judicial del Senat dels EUA, fruit dels nombrosos casos de fraus i intents de frau que ja hi ha hagut amb suplantació de la veu generada per IA.

**ChatGPT permet escriure programari maliciós i neixen alternatives sense limitacions**

Investigadors de l'empresa israeliana de seguretat Check Point Research han reportat que alguns ciberdelinqüents, amb poca o cap experiència en programació, han utilitzat ChatGPT per escriure programari i correus electrònics que podien utilitzar-se per al espionatge, *ransomware*, *spam* i altres tasques malicioses. Check Point revela que alguns usuaris/usuàries de fòrums clandestins ja comparteixen consells i fragments de codi per crear ransomware i altres programaris maliciosos gràcies a la tecnologia ChatGPT.
Neixen, també, noves versions de chatGPT sense limitacions: wormGPT, freedomGPT, PoisonGPT, ChaosGPT,...

# La IA irromp en la ciberseguretat

**El Parlament Europeu aprova el projecte llei per regular la Intel·ligència Artificial**

Europa està més prop de convertir-se en la primera regió del món a tenir un marc regulador vigent al voltant de la IA. La iniciativa de llei europea al voltant de la IA proposa la creació d'un sistema de categorització en el qual les solucions d'IA es classifiquen en funció del "risc potencial" que suposen per al benestar social. Els requisits, responsabilitats i prohibicions que s'han de complir per part de les empreses tecnològiques que treballen en projectes d'IA es determinaran en funció d'aquesta classificació. També exigeix mesures de ciberseguretat adequades per evitar l'explotació de vulnerabilitats i el *data polsoning*.

**L'institut Nacional d'Estàndards i Tecnologia dels EUA (NIST) publica un Marc de Gestió de Riscos de la IA**

Es tracta d'un document, no vinculant, que serveix per orientar a les organitzacions que dissenyen, desenvolupen, despleguen o utilitzen sistemes d'IA per a ajudar a gestionar els nombrosos riscos d'aquesta tecnologia. Tot i que és evident que les autoritats i els governs estan començant a fer els primers passos per a la regulació de la IA, els actors tecnològics continuen desenvolupant noves eines i serveis que plantegen nous escenaris i riscos.

**La Xina va aprovar una llei sobre elements generats amb IA**

A principi d'any, la Xina va aprovar la *Provisions on the Administration of Deep Synthesis of Internet Information Services*. Es tracta d'una llei dirigida a protegir les persones de la suplantació digital de la seva veu o imatge sense el seu consentiment, i a la prevenció de la difusió de notícies falses.
Per exemple, en els serveis d'hipertrucatge (*deep fake*), els usuaris/usuàries hauran d'autenticar-se amb la seva identitat real i elaborar algun tipus d'etiqueta o avís que notifiqui que el producte ha estat produït o alterat mitjançant una eina d'IA.

**Telefónica desenvolupa una eina per detectar *deep fakes* en temps real**

Telefónica desenvolupa una eina de detecció de *deepfakes*, anomenada Deep Fake Detector (DFD), inspirada en el test de Voight-Kampff de Blade Runner. Es realitza l'anàlisi dels trets facials, els ulls, la simetria facial... Cercant anomalies a través d'una xarxa neuronal entrenada.
Encara no té plans comercials i, per ara, l'eina busca ser la millor possible. De fet, Fran Ramírez, del projecte "Ideas Locas" de Telefónica, destaca la "cursa" per treure al mercat eines de detecció d'imatges trucades.

**Automatització en múltiples fases de les feines d'un SOC**

La necessitat d'automatització s'està convertint en una aposta de la indústria de la ciberseguretat, especialment en els *Security Operation Centers*. De totes les organitzacions amb resiliència cibernética, IBM estima que el 62% de les empreses ha implementat eines i processos d'automatització, IA i aprenentatge automàtic.

**El govern dels EUA està construint una *sandbox* d'IA per abordar el ciberdelicte**

Un esforç conjunt entre diferents entitats governamentals dels EUA, on hi ha la Direcció de Ciència i Tecnologia (S&T), el Departament de Seguretat Nacional (DHS) i l'Agència Ciberseguretat de Seguretat d'Infraestructures (CISA), permetrà desplegar una *sandbox* que utilitzarà la IA perquè els investigadors col·laborin i provin enfocaments analítics i tècniques per combatre les amenaces cibernètiques. La plataforma d'anàlisi anomenada CAP-M (*CISA Advanced Analytics Platform for Machine Learning*) es farà servir tant en entorns *on-premise* com del núvol.

# L'activitat dels grups de *ransomware* de rècord

Baixa el percentatge de víctimes que paguen

Les organitzacions grans o essencials, que no poden aturar la seva activitat i poden fer fronts a pagaments importants, es converteixen en objectiu

Puja l'explotació de vulnerabilitats *zero-day*

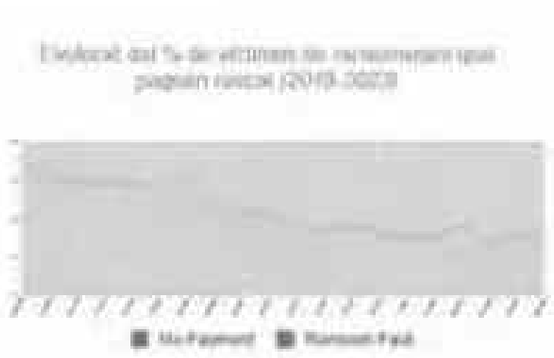
Els atacs s'industrialitzen amb eines d'automatització

Creix la capacitat d'extracció de grans volums de dades amb l'objectiu d'extorsionar

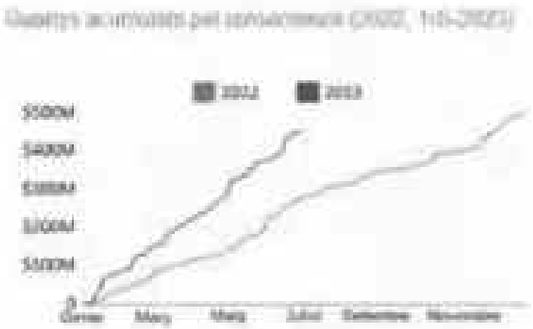
Les ramificacions de les cadenes de subministrament impulsen els ciberatacs amb afectacions globals

La venda intensiva d'accessos i l'ús de múltiples programaris de xifratge impulsen els atacs de doble *ransomware*

**Cada vegada menys víctimes paguen rescat** [Coveware]

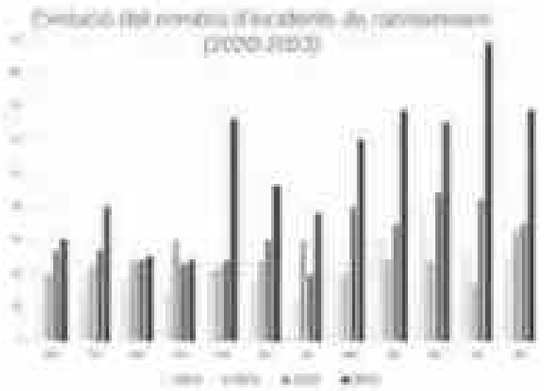


**Els ingressos pel ransomware es disparen** *[Chainalysis]*



**El principal vector d'atac és desconegut, *zero-days?*** [Coveware]

**Rrècord en els incidents de *ransomware*** [BlackFog]



# L'activitat dels grups de *ransomware* de rècord

Baixa el percentatge de víctimes que paguen

Les organitzacions grans o essencials, que no poden aturar la seva activitat i poden fer fronts a pagaments importants, es converteixen en objectiu

Puja l'explotació de vulnerabilitats *zero-day*

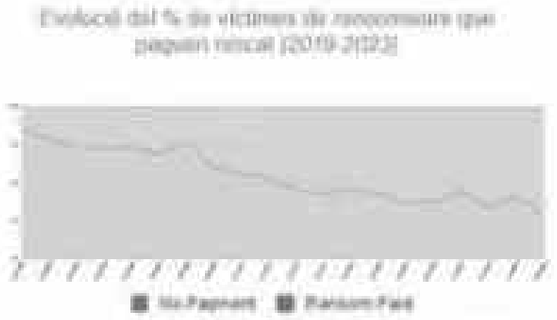
Els atacs s'industrialitzen amb eines d'automatització

Creix la capacitat d'extracció de grans volums de dades amb l'objectiu d'extorsionar

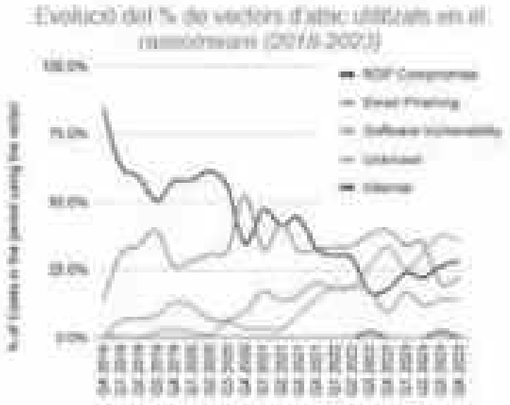
Les ramificacions de les cadenes de subministrament impulsen els ciberatacs amb afectacions globals

La venda intensiva d'accessos i l'ús de múltiples programaris de xifratge impulsen els atacs de doble *ransomware*

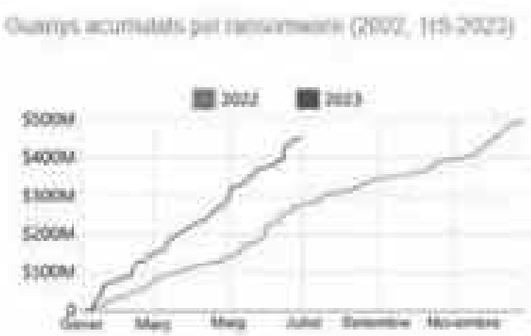
**Cada vegada menys víctimes paguen rescat** [Coveware]



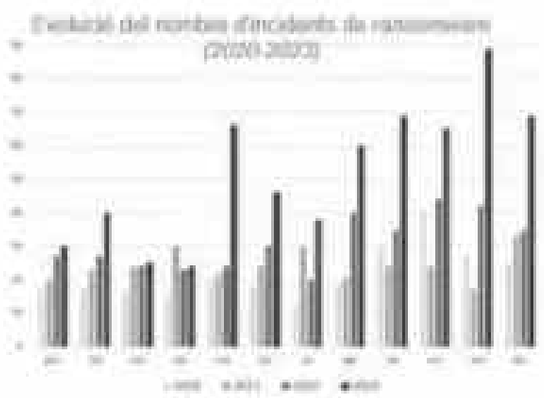

**El principal vector d'atac és desconegut, *zero-days?*** [Coveware]




**Els ingressos pel ransomware es disparen** *[Chainalysis]*




**Rrecord en els incidents de *ransomware*** [BlackFog]



# L'activitat dels grups de *ransomware* de rècord

**Creuers del Port de Barcelona viu un atac de *ransomware* de LockBit**

L'empresa, que gestiona cinc terminals del Port de Barcelona, va viure un atac de *ransomware* de LockBit. No s'han fet públics els detalls tècnics de com es va produir ni de l'afectació en les operacions de l'empresa.
Sí que se sap que LockBit va exercir la doble extorsió: va posar el 25 d'abril com a data límit per pagar el rescat a canvi de no publicar la informació que havien robat. En la publicació de l'ultimàtum, LockBit oferia la possibilitat de pagar 1.000 € per ampliar el termini 24 hores, o pagar 299.999 € per la destrucció o la descàrrega de la informació.

**Mediapro pateix un atac de *ransomware* de conseqüències desconegudes**

La multinacional catalana ha patit un atac de *ransomware* que ha afectat part dels seus sistemes. L'incident ha tingut diverses afectacions, tot i que no s'han fet públiques, però no ha afectat les emissions audiovisuals de la companyia.
Tampoc s'ha fet pública l'autoria de l'atac, si hi ha hagut nota de rescat o no, o si hi ha hagut dades de caràcter personal afectades.

**Ciberatac contra l'Agència Catalana de Notícies**

L'ACN va ser objectiu d'un ciberatac, tot i que no va tenir conseqüències sobre els seus sistemes ni afectacions al servei. Els sistemes de detecció de l'Agència de Ciberseguretat de Catalunya van identificar una intrusió a la xarxa de l'ACN que va activar la intervenció dels equips de resposta a ciberincidents. Els tècnics de l'ACN i l'Agència de Ciberseguretat van treballar conjuntament en aquest incident.
En el moment de la detecció, es va desplegar un pla destinat a la disrupció i erradicació de l'activitat intrusiva, al mateix temps que es van desplegar mecanismes per assegurar l'activitat operativa.

**El Royal Mail (Regne Unit) viu un atac de *ransomware* que interromp els enviaments internacionals**

Inicialment, no es va donar gaire informació sobre l'atac i es va catalogar com un ciberincident, però ben aviat es confirmà que es tractava d'un atac de *ransomware* perpetrat per l'operador LockBit. L'atac no va afectar el correu postal domèstic, però sí que va crear endarreriments en la missatgeria internacional, tant la que entrava com la que sortia, en una clara intenció de perjudicar un servei essencial. Es desconeix si es va demanar un rescat i quina quantitat.

**La noruega DNV, víctima d'un atac de *ransomware* que afecta més de 1000 vaixells**

L'empresa, que proveeix un *software* per a la gestió de flotes de vaixells, va patir un atac de *ransomware*. Aquest fet va provocar que hagués de desconnectar els servidors i l'operació amb 1.000 vaixells durant uns quants dies, tot i que podien mantenir les seves funcions bàsiques fora de línia. No hi ha detalls dels autors de l'atac o del l'exigència d'un rescat, tot i que el fet que l'empresa ha estat cooperant estretament amb les autoritats policials fa pensar que no s'ha fet cap pagament.

**L'incident a IFX, probablement de la mà de RansomHouse, afecta 17 països i més de 700 empreses**

L'atac a IFX Networks, operador de telecomunicacions colombià, ha afectat 762 empreses de 17 països, en els quals oferia els seus serveis de *cloud*. Més enllà de Colòmbia, destaquen les afectacions a països com Xile, Argentina o Panamà.
L'empresa va rebre una nota de rescat en què s'exigia un rescat en criptomonedes que no ha transcendit. Tot i que l'atac no ha estat reivindicat, per la similitud de la nota amb d'altres, s'apunta a RansomHouse, el mateix operador que el març de 2023 va atacar l'Hospital Clínic de Barcelona.

# L'activitat dels grups de *ransomware* de rècord

**Es detecten 500 casos d'infeccions d'ESXiArg en un sol dia**

ESXi és un producte de VMWare que permet allotjar màquines virtuals que utilitzen diferents sistemes operatius en un mateix servidor físic. El CERT francès fou el primer en descobrir i avisar que un operador de *ransomware* desconegut estava explotant una vulnerabilitat antiga en aquest tipus de servidors desactualitzats per instal·lar-hi el *malware* de xifratge batejat amb el nom ESXiArg.
Dues setmanes després de la detecció de la campanya a França, el buscador Censys va detectar en un sol dia més de 500 casos d'infecció a països europeus com França, Alemanya, Holanda, el Regne Unit i Ucraïna. A la fi, els servidors afectats es compten per milers.

**Una vulnerabilitat ha disparat els atacs de *ransomware* durant el mes de març**

La vulnerabilitat CVE-2023-0669 es troba en el programari GoAnywhere MFT (*Managed File Transfer*), de l'empresa Fortra (EUA), que s'utilitza per a la transferència segura d'arxius. La vulnerabilitat es troba en el pas de preautenticació, ja que un dels paràmetres permet injectar codi. Ara bé, per fer-ho, cal tenir visibilitat d'un port de gestió intern o ser usuari/usuària amb accés.
L'operador de *ransomware* Cl0p la va explotar en forma de *zero-day*, fet que li va permetre atacar, i robar informació, més de 130 empreses en 10 dies. Aquest fet, sumat a l'activitat habitual de grups com LockBit, Play o BlackCat, ha convertit el mes de març com un dels més prolífics pel *ransomware*.

**S'ha explotat la vulnerabilitat de MOVEit per dur a terme un atac a la cadena de subministrament**

MOVEit és un sistema d'intercanvi de fitxers, internament i entre organitzacions, desenvolupat per Progress Software Corporation (EUA). A final de maig, l'empresa va començar a detectar una activitat inusual i, poc després, fruit de les investigacions, es feia pública una nova vulnerabilitat a principi de juny. Aquesta permetia escalar privilegis i aconseguir un accés no autoritzat a l'entorn de MOVEit. Tot i la publicació d'un pegat, el grup de *ransowmare* Cl0p ja havia engegat una campanya d'atacs que s'allargaria durant setmanes i que els hauria permès robar les dades de la cadena de subministrament d'usuaris i usuàries de MOVEit.

**Vice Society automatitza el robatori de dades a través d'un *script* de PowerShell**

L'operador de *ransomware* Vice Society, conegut per utilitzar el codi d'altres operadors disponible als mercats negres de la *dark web*, ha desenvolupat un *script* de PowerShell, força complex, que automatitza el robatori de dades.
L'*script* conté diferents funcions com Work(), Show(), CrateJobLocal() i fill(), que serveixen per identificar potencials directoris a robar, facilitar el robatori i filtrar les dades dins de peticions HTTP POST fins als servidors de Vice Society. A més, abans del xifratge, un altre *script* desactiva les alertes que podrien emetre els programaris de seguretat dels sistemes vulnerats.

**Operadors de *ransomware* busquen noves maneres d'extorsionar les víctimes**

Els operadors de *ransomware* busquen noves maneres d'extorsionar les víctimes a fi i efecte d'assegurar-se el pagament del rescat.
En aquets cas, BlackCat, en el seu atac contra Western-Digital, va ser capaç d'aconseguir accedir a les *webcam* dels dispositius dels treballadors, guardar les imatges i, posteriorment, amenaçar la víctima en difondre-la en cas de no pagar el rescat.

**L'FBI avisa sobre l'auge dels atacs de doble *ransomware***

L'FBI ha emès una alerta (*Private Industry Notification*) en què alerta de l'auge dels atacs de doble *ransomware* i del fet que poden arribar a succeir en només 48 hores de diferència.
Aquest fet pot tenir una doble explicació. Primer: els grups cibercriminals disposen de diferents variants de *ransomware* i, un cop a dins els sistemes de la víctima, primer n'executen un i després un altre. Segon: els *Initial Access Brokers* venen el mateix accés a la xarxa de la víctima a diferents operadors de *ransomware* i, d'aquesta manera, cada un d'ells infecta la mateixa víctima per separat.

# El negoci de les fuites de dades personals

Alguns grups de *ransomware* passen directament a l'extorsió mitjançant el robatori d'informació confidencial

Augment alarmant de fuites de dades personals amb impacte als ciutadans de Catalunya

El robatori de dades alimenta un negoci lucratiu al mercat negre de la *dark web*

Les operacions policials contra els mercats il·lícits a la *dark web* fan que els cibercriminals pensin en Telegram com a alternativa, confidencial i molt més accessible

Les dades personals robades permeten realitzar campanyes de frau dirigides, com l'*smishing* perpetrat per grups cibercriminals locals

L'activitat s'accentua els periodes especials, com les vacances o les festivitats nadalenques, propicis per defraudar els usuaris o atacar empreses

**Europa té les taxes més altes d'afectats per fuites de dades** [Surfshark]

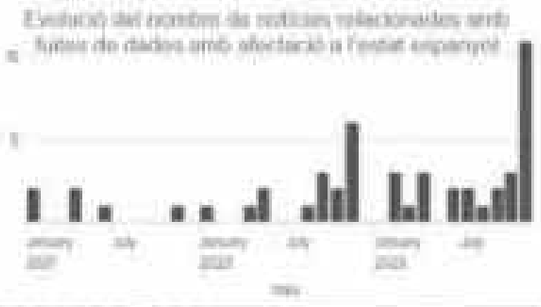
1 de cada 5 usuaris d'Internet europeus s'han vist impactats per una fuita de dades

Aquesta xifra és més de 4 vegades superior a la mitjana mundial.

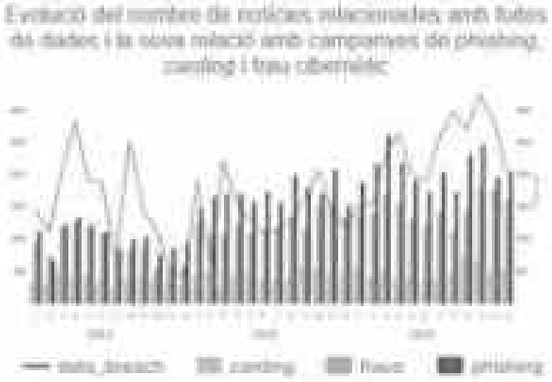
Oceania ocupa el segon lloc amb 1 de cada 8 usuaris impactats per una fuita.

**Novembre, un mes rècord de fuites de dades a l'estat** [Agència]

El nombre de notícies relacionades amb aquest tema ha quasi duplicat l'anterior rècord del mateix mes de 2022. Els sectors més afectats han estat el **financer, telecomunicacions i educació**.




**Tendència a l'alça en fuites de dades, així com campanyes de *phishing*, *carding* i fraus cibernètics** [Agència]




**Proliferació de bots maliciosos** [Imperva]

Es dispara l'activitat de *botnets* que cerquen vulnerabilitats a les API de plataformes de comerç electrònic per extreure dades de clients o redirigir les transaccions.

# El negoci de les fuites de dades personals

**S'estima que Cl0p podria guanyar entre 75 i 100M€ gràcies a la campanya de MOVEit**

La campanya Cl0p contra els usuaris i les usuàries del sistema FTP MOVEit ha afectat centenars d'empreses a tot el món, i s'espera que segueixi afectant-ne encara més.
Cl0p, també darrere dels atacs a GoAnywhere MFT, ha canviat d'estratègia i s'ha dedicat directament al robatori d'informació, sense xifratge, tot exigint un rescat a canvi d'esborrar i no publicar-la. Els experts estimen que els guanys en aquesta campanya podrien ascendir a entre 75 i 100 M€.
Si l'estimació fos certa, amb aquesta campanya Cl0p superaria les pèrdues causades per la baixada en nombre de víctimes que paguen rescat.

**Inversis Banco pateix un ciberatac en què es comprometen les dades personals de clients**

El banc espanyol Inversis va experimentar un ciberatac el passat 1 de novembre, en el qual a través d'un accés no autoritzat es van comprometre les dades personals de clients. La plataforma, vinculada a la Banca March, ha activat les mesures de seguretat pertinents i col·labora en una investigació amb les autoritats. Tot i que encara no es coneix l'abast real del ciberatac, l'entitat assegura que les dades exposades no representen un risc econòmic ni permeten realitzar transaccions.

**Potencial fuita de dades confidencials imminent d'Endesa de més de 1.800 clients**

E-distribució, empresa associada a Endesa, hauria patit una presumpta filtració de dades arran d'un atac *ransomware* que podria haver suposat la filtració de dades confidencials. Es podrien haver vist afectades les dades personals de 1.800 clients a tota Espanya, incloent-hi informació com noms, documents d'identitat i adreces.
Endesa desmenteix que ningú hagi accedit als seus sistemes i afirma que està investigant el possible atac. Tot i això, a BreachForums s'ha publicat una mostra de la filtració.

**Dades dels clients de Sprinter han estat compromeses**

La cadena de botigues d'esports alacantina Sprinter ha patit una filtració de dades que compromet informació de clients, incloent-hi noms, DNI i adreces. Sprinter assegura que no s'han compromès les dades bancàries ni tampoc les contrasenyes, ja que aquestes compten amb mecanismes de xifratge i no estan emmagatzemades als servidors.
Encara no es coneixen els detalls de l'incident i la investigació continua oberta.

**Possible filtració de dades bancàries i personals a Vodafone**

Vodafone alerta d'un accés no autoritzat als sistemes d'un dels seus col·laboradors, donant lloc a una filtració de dades bancàries i personals de clients espanyols amb comptes d'empresa, persones autoritzades, autònoms i particulars. S'haurien obtingut dades de caràcter personal i bancàries.
Vodafone ha informat els afectats mitjançant SMS o correu electrònic, assegurant que les entitats implicades han resolt el problema i reforçat la seguretat.

**LockBit amenaça en publicar dades de clients d'un dels bufets d'advocats més grans de l'IBEX 35**

La filial espanyola de la firma legal internacional CMS ha estat víctima d'un ciberatac que ha derivat en el robatori de 500 GB de dades confidencials dels seus servidors de dades.
El grup de *ransomware* LockBit, que ja havia afectat altres firmes legals com Allen & Overy (Regne Unit), ha estat identificat com l'autor de l'atac. CMS ha assegurat que altres filials no han estat afectades i està col·laborant amb experts forenses per abordar l'incident.

# El negoci de les fuites de dades personals

**Un esdeveniment a la *dark web* desencadena un intercanvi massiu de dades personals**

Mentre el món celebrava l'esperit nadalenc, els cibercriminals van deixar la seva empremta amb una versió *dark* del Nadal. Diferents grups cibercriminals van compartir massivament filtracions de dades de països de tot el món, entre les quals destaca un paquet de dades de Movistar Perú amb 22 M de registres exposats.
La conseqüència d'aquest acte global, etiquetat com a "Free Leaksmas", és que les dades intercanviades poden ser emprades en futurs fraus o usurpacions d'identitat.

**Desarticulada Genesis Market, la plataforma més gran de venda de credencials a la *dark web***

Una operació policial ha desarticulat la que es considera, fins al moment, la plataforma més gran de venda de credencials, dedicada especialment a la suplantació d'identitats. L'operació ha estat liderada per l'FBI, amb la col·laboració de l'Europol i 17 països més, entre els quals hi ha Espanya. També s'han detingut 119 persones que utilitzaven la informació facilitada per Genesis Market per suplantar les víctimes en els serveis en línia.

**El *phishing* com a servei, tendència de ciberdelinqüència a Telegram**

Telegram s'està convertint en un dels mitjans preferits dels ciberdelinqüents per oferir els serveis de *Phishing-as-a-Service*. Segons les ofertes, a canvi d'una subscripció de pagament, els usuaris i usuàries tenen accés a un seguit d'eines i serveis relacionats amb el *phishing*. Alguns dels serveis són kits de *phishing*, webs falsos, plantilles de correus o un *bot* telefònic que demana als usuaris/usuàries l'OTP (*One-Time Password*) amb l'objectiu d'utilitzar-lo per saltar-se el 2FA. Segons Kaspersky, en els últims sis mesos, s'han detectat fins a 2,5 M de pàgines generades amb kits de *phishing*.

**Els Mossos d'Esquadra detenen un home per cometre 30 estafes de *smishing***

Les estafes van començar el 12 de desembre de 2022 i, fins que el van detenir, es creu que l'autor, un home de 20 anys, podria haver acumulat fins a 15.000 €. Aquesta persona, que tenia coneixements informàtics, enviava SMS amb un enllaç a una pàgina clonada que suplantava un banc. Si la víctima queia en el parany, li robava les dades bancàries que s'aprofitaven per extreure diners de caixers automàtics.

**Estafes personalitzades per telèfon a clients de banca per robar milers d'euros**

Un client de ING direct de l'estat espanyol va ser víctima d'una estafa en la qual un ciberdelinqüent va contactar-lo per telèfon fent-se passar per membre del servei de seguretat del banc ING. Per donar-hi més credibilitat, va utilitzar una eina per suplantar el número de telèfon real d'una sucursal bancària i va proporcionar detalls específics sobre els comptes bancaris de la víctima. L'estafador, va induir la víctima a transferir més d'11.000 €. La víctima sospita d'una possible filtració de dades, ja que els atacants tenien coneixement detallat dels seus comptes bancaris.

**Onada de correus de *phishing* que simulen reserves hoteleres**

A l'inici de l'època de vacances ja es van començar a detectar campanyes de *phishing* enfocades al robatori de credencials i a la disseminació de *malware*. En aquest cas, el correu informava la víctima d'algun problema en la reserva que havia fet a través del portal Booking i adjuntava un document per solucionar la situació. El document adjunt dirigia a una pàgina web que sol·licitava el *password* del correu de la víctima. A banda de robar les credencials d'usuari, també tenia l'objectiu de descarregar un *malware* a l'equip de la víctima.

**Falsa enquesta de Renfe ofereix bitllets gratuïts en el *Black Friday***

Ciberdelinqüents aprofiten el *Black Friday* per difondre una estafa que aparentment ofereix bitllets gratuïts de Renfe a canvi de completar una enquesta. Difosa a través de correus de *phishing*, la falsa promoció busca obtenir dades personals per accedir als comptes de les víctimes i suplantar-ne la identitat.
La urgència de l'oferta i el límit fictici en el nombre de targetes regal reforcen l'estratègia enganyosa. Renfe ha alertat sobre el frau i destaca que no ofereix aquesta promoció.

# Alerta als sectors sanitari, AAPP i centres educatius

Arran de les dificultats del *ransomware* per cobrar rescats, els sectors essencials dirigits a la ciutadania es converteixen en objectius prioritaris

El sector sanitari és objectiu d'atacs de motivació cibercriminal (*ransomware* i robatoris de dades) i geopolítica (DDoS)

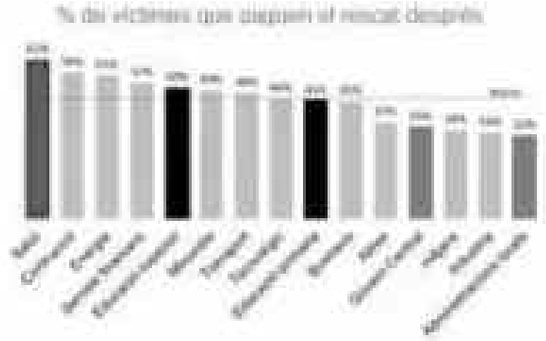
Les administracions locals són víctimes de ransomware (que aturen els tràmits administratius) i robatoris de dades (disposen de gran quantitat de dades personals i confidencials)

Els cibercriminals concentren els ciberatacs de *ransomware* contra les universitats i centres educatius en el període crític de final i inici del curs, i perpetren robatoris de dades personals

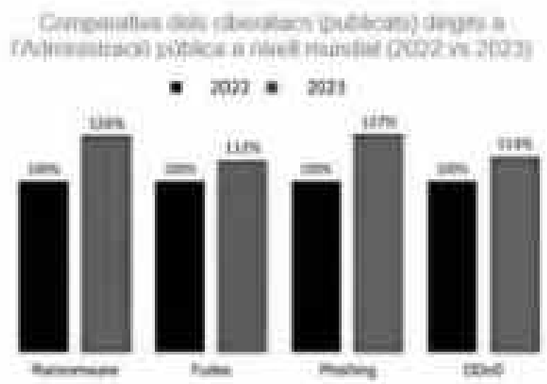
La ciberseguretat s'evidencia com un element clau per minimitzar l'afectació a la ciutadania

**El sector sanitari és el més propens a pagar rescats de *ransomware*** [Sophos]

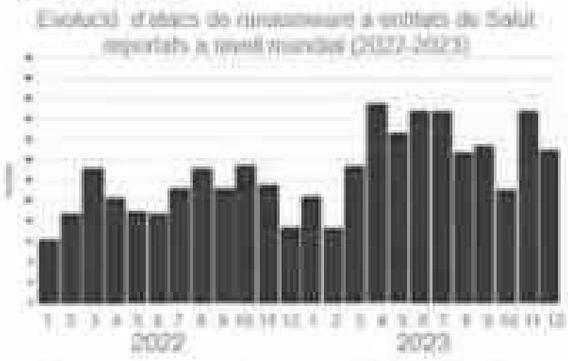
La mitjana se situa pels volts del 46%.




**Augmenten els ciberatacs a l'Administració pública** [Agència]




**Augment global d'atacs a proveïdors de salut respecte del mes de desembre de l'any anterior** [The Record]




**El *ransomware* és el principal atac contra universitats** [Agència]

En una anàlisi de 456 publicacions sobre incidents contra universitats (2021-2023):

- **42%** dels incidents detectats a les publicacions són de *ransomware*.
- **38%** dels incidents detectats a les publicacions són de fuites de dades, que en alguns casos deriven d'atacs de *ransomware*.
- **43%** més d'incidents publicats durant el 2023 comparat amb el 2022.

# Alerta als sectors sanitari, AAPP i centres educatius

**L'Hospital Clínic pateix un atac de *ransomware* que en paralitza l'activitat**

L'Hospital Clínic va ser víctima d'un atac de *ransomware* per part del grup RansomHouse que, a més, va afectar els CAP Borrell, Casanova i Les Corts. L'atac va provocar la cancel·lació de 150 intervencions i més de 2.000 visites externes. L'activitat del centre va passar realitzar-se de forma manual i el transport sanitari urgent es va derivar a altres hospitals. Va ser un atac dirigit a entorns virtualitzats en el qual es va xifrar la informació i es van robar 4,5 TB de dades, per la qual cosa els cibercriminals van exigir un rescat de 4,5 M€. Les tasques de recuperació van fer que l'endemà s'hagués pogut aixecar un 15% dels sistemes de l'hospital.

**Diversos hospitals, entre ells el de la Seu d'Urgell, afectats per un ciberatac a la cadena de subministrament**

L'atac ha estat dirigit concretament contra Denario, una empresa proveïdora que gestiona el *software* de recursos humans d'instal·lacions sanitàries. Entre els centres sanitaris afectats es troben la Fundació Sant Hospital de la Seu d'Urgell i l'Hospital Sant Bernabé de Berga.
Per la seva part, l'Hospital de la Seu d'Urgell ha informat que l'atac ha estat controlat i s'han aïllat els dispositius que podien estar afectats. També ha fet saber que les dades i nòmines dels treballadors no s'han vist compromeses gràcies a les còpies de seguretat existents.

**Catalunya registra 4 ciberatacs a hospitals en els últims tres mesos**

L'Hospital Trueta de Girona i els hospitals barcelonins de Sant Pau i la Vall d'Hebron van patir ciberatacs perpetrats per Killnet, un grup especialitzat en atacs de DDoS. Es van constar notificacions d'amenaça d'atac per part de Killnet els dies 28 i 31 de gener. Les mesures de seguretat van poder bloquejar els ciberatacs, i només en el cas del Trueta el web de l'hospital va quedar inactiu durant unes hores.

**Alerten sobre un fals correu electrònic de Sanitat sobre una dosi addicional de la vacuna de la covid**

INCIBE ha alertat sobre una campanya de *phishing* que busca suplantar el Ministeri de Sanitat. El correu informa sobre una nova dosi de la vacuna de la covid i dona l'oportunitat a l'usuari/a perquè esculli la marca que vol inocular-se. Això es fa descarregant un document, que en realitat és un .zip que conté un arxiu maliciós.
INCIBE aclareix que, en cas d'haver-ne estat víctima, cal posar-se en contacte amb l'equip d'incidents de INCIBE-CERT.

**Metges gironins alerten d'estafes per obtenir les seves dades**

El Col·legi de Metges de Girona ha emès un comunicat en què adverteix que s'ha detectat una campanya telefònica de frau dirigida a obtenir el DNI i el carnet col·legial dels facultatius.
La campanya consisteix en trucar als i a les professionals fent-se passar pel propi Col·legi, amb l'excusa que s'apropa la caducitat del certificat digital. Per renovar-lo, han d'enviar una fotografia del DNI i del carnet col·legial a un correu fals.

**Un grup de *ransomware* publica fotos de pacients de càncer nus**

La xarxa d'assistència sanitària Lehigh Valley Health Network (EUA) va patir un atac de *ransomware* durant el mes de febrer. El centre es va negar a pagar el rescat, la quantitat del qual es desconeix. Per tal d'exercir més pressió, el responsable de l'atac, l'operador de *ransomware* BlackCat, ha començat a publicar informació robada, entre la qual destaquen les fotos de malalts oncològics nus que rebien tractament de radioteràpia.

**En el sector hospitalari, el temps de recuperació a la normalitat després d'un ciberatac és molt variable**

A mitjan març, un hospital belga va patir un ciberatac, del qual no es van difondre detalls, però es va informar que es va recuperar en unes 24 hores. Contrasta amb el fet que un altre hospital belga va viure un ciberatac el novembre i quatre mesos després encara segueix amb sistemes desconnectats. I és que diversos factors poden influir en el temps de recuperació: el tipus d'atac, els sistemes afectats, la mida de l'hospital, els serveis que ofereix, el nivell de protecció en ciberseguretat...

# Alerta als sectors sanitari, AAPP i centres educatius

**La protecció del Catalonia SOC arriba a 118 ajuntaments i 26 consells comarcals**

Des de 2022, l'Agència de Ciberseguretat de Catalunya ofereix el Model de Ciberseguretat a les administracions locals, per brindar un servei públic i gratuït amb solucions de ciberseguretat i cobertura davant de les amenaces digitals, formació i sensibilització per al personal responsable. A més a més, també ofereix resposta als incidents a través del servei CATALONIA-CERT®. El 2022, l'Agència ha gestionat 287 ciberatacs dirigits a administracions del món local català: *ransomware*, suplantació d'identitat, filtració de credencials, infeccions per troians, intrusions a webs o aplicatius.

**La Universitat Pompeu Fabra bloqueja el seu sistema informàtic per un ciberatac**

La UPF va haver de bloquejar temporalment la connectivitat als seus servidors informàtics després de detectar un ciberatac. Els tècnics de la universitat, juntament amb l'Agència de Ciberseguretat de Catalunya, van activar un pla de mesures preventives per evitar un incident informàtic. Tot i que s'ha pogut continuar amb l'activitat docent, l'activitat informàtica s'ha hagut de suspendre temporalment. La pròpia universitat ha comunicat que s'hauran de "prendre mesures per evitar possibles afectacions futures de més envergadura".

**L'Ajuntament de Cubelles, víctima d'un atac de *ransomware***

L'atac, del qual no n'ha transcendit l'autoria, va afectar el sistemes informàtics interns però no el web ni la seu electrònica del consistori. Tot i que el Registre General es va tancar i l'atenció presencial va veure's afectada, els ciutadans encara podien fer tràmits i gestions a través de canals alternatius. La màxima preocupació és conèixer si s'han robat les dades confidencials de treballadors, ciutadans i proveïdors. En aquest sentit, s'ha fet una crida a tota la ciutadania per extremar la precaució contra possibles estafes.

**La Universitat de Saragossa desconecta l'accés remot durant un cap de setmana**

Al maig, l'oficina de coordinació de ciberseguretat del Ministeri d'Interior va alertar la Universitat de Saragossa d'un intent d'accés als servidors de la institució a través de dos comptes d'usuaris remots. Des del mateix Ministeri espanyol es va advertir que es podia tractar d'un *ransomware*. No es va detectar cap afectació considerable a cap servei, però es va aconsellar deixar els ordinadors desconnectats durant el cap de setmana. Arran d'aquest incident, i per recomanació del CCN-CERT, el campus va decidir tancar l'accés remot; els usuaris/usuàries que l'haguessin d'utilitzar havien de passar un procés de revisió.

**L'Ajuntament de Sils rep un atac de *ransomware* que no en paralitza l'activitat**

A finals de mes, l'Ajuntament de Sils rebia un atac de *ransomware*, d'autor desconegut. L'incident es va detectar quan els funcionaris del consistori van descobrir que no podien accedir als seus documents. Els atacants també van enviar una nota de rescat de la qual no ha transcendit la xifra exigida per desxifrar les dades. Seguint indicacions dels Mossos d'Esquadra, el consistori no l'ha contestada.
Tot i així, l'atac no ha afectat el funcionament de l'ajuntament, atès que disposava d'un gestor d'expedients en línia que treballa des del núvol.

**La Casa Blanca convoca la primera cimera per abordar la problemàtica del *ransomware* a les escoles**

A principi d'agost, la Casa Blanca convocava una cimera per respondre a la "plaga" d'atacs de *ransowmare* que les escoles del país han estat patint des de fa anys, i que s'ha vist incrementada durant el 2023, especialment a partir de maig.
Entre les mesures acordades, la CISA (Cybersecurity and Infrastructure Security Agency) farà avaluacions de ciberseguretat als centres de primària. També hi haurà una assignació de 190 M€ en tres anys per millorar les ciberdefenses de les escoles, i el compromís d'empreses com Google, Amazon o Cloudflare d'oferir suport.

# Desafiaments pel 2024

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

## Les crisis econòmiques, geopolítiques i climàtiques del món impulsen les ciberamenaces

La **crisi econòmica** impulsarà el creixement d'una **cibercriminalitat de proximitat** experta en atacs d'**enginyeria social**

Les tensions i crisis geopolítiques accentuaran l'amenaça cibernètica als **sectors essencials** amb el risc d'afectar l'**equilibri social i econòmic**

Les **crisis energètica i climàtica** atrauran els ciberatacs sobre els **subministraments bàsics**: energia, aigua...

S'accentua la divisió del món cibercriminal: unes bandes **capaces d'amenaçar** l'estabilitat dels **estats** i d'altres de **perfil baix** fora del focus internacional

## Les previsions de frenada de l'economia global condicionaran les politiques empresarials i la transformació digital en matèria de ciberseguretat.

**Ciberseguretat a dues velocitats** en teixit empresarials: les **grans corporacions invertiran**, mentre que les **pimes prioritzaran l'austeritat** malgrat els riscos que comporta

Els **fons NextGen** arribaran per impulsar la **digitalització** i millorar la **ciberseguretat** de les empreses

La **falta de professionals de la ciberseguretat** i el seu esgotament accentuarà les **dificultats per a la transformació digital** de les empreses

## Els grups *hacktivistes* i cibercriminals es posicionaran i participaran activament en els conflictes geopolítics

Els grups ***hacktivistes* i els cibercriminals** prendran posicions en els conflictes geopolítics

Els grups *hacktivistes* i cibercriminals mantindran **conflictes paral·lels en el món virtual** i hauran de ser selectius a l'hora d'acceptar nous membres

Els ciberatacs amb motivació geopolítica buscaran **perjudicar la confiança de la ciutadania** i l'estabilitat de l'adversari a través de la **desinformació** i ciberatacs als **serveis essencials**

## El cibercrim s'adaptarà a les noves realitats per maximitzar l'efectivitat i l'impacte dels ciberatacs

El cibercrim buscarà grans impactes atacant les **cadenes de subministrament**

Els ciberatacs seguiran explotant els mecanismes per **esquivar la barrera del doble factor d'autenticació**

**Noves generacions de *botnets*** per aprofitar el potencial dels nous dispositius per elevar els atacs de DDoS a un altre nivell

La digitalització seguirà **augmentant** la generació de **dades personals** i la necessitat de desplegar **mesures de protecció** davant dels robatoris

Gir cap a una **ciberseguretat proactiva** que haurà de fer focus en la **gestió de vulnerabilitats**

## La IA esdevindrà un element clau en una nova generació d'atacs cibernètics, però també per protegir-se

Les IA generatives suposen un **impuls a l'activitat cibercriminal**

La IA com a **amplificador del talent** dels **professionals** de la ciberseguretat i també dels **atacants**

L'**automatització intel·ligent** guanyarà terreny, tant per fer el bé com el mal

**Reglament d'IA** esdevindrà una **referència global** per regular els riscos de la IA

La necessitat d'incloure la IA per donar suport a les funcions de ciberseguretat exigirà **personal especialitzat competent en els dos àmbits**

## Tecnologies de zero trust i innovació per fer front als nous reptes en ciberseguretat

Arran de la consolidació del **treball híbrid,** les organitzacions emprendran el camí cap a un model de **zero-trust**

Seguirà augmentant el nombre d'empreses que adopten solucions **SASE** (Secure Access Service Edge) per securitzar les operacions al **núvol**

Els serveis de ***rating*** per avaluar el nivell de ciberseguretat contribuiran a establir **vincles de confiança** entre proveïdors i clients

La **ciberseguretat** esdevindrà essencial per a la proliferació exitosa de ***data spaces*** i podrà aprofitar-se'n com a mecanisme de **col·laboració**

L'ús de *digital twins* permetrà afrontar millor la ciberseguretat d'**entorns complexos** amb sistemes ciberfísics

Les **primeres solucions criptogràfiques** resistents a la computació quàntica veuran la llum

## La IA esdevindrà un element clau en una nova generació d'atacs cibernètics, però també per protegir-se

Les IA generatives suposen un **impuls a l'activitat cibercriminal**

La IA com a **amplificador del talent** dels **professionals** de la ciberseguretat i també dels **atacants**

L'**automatització intel·ligent** guanyarà terreny, tant per fer el bé com el mal

**Reglament d'IA** esdevindrà una **referència global** per regular els riscos de la IA

La necessitat d'incloure la IA per donar suport a les funcions de ciberseguretat exigirà **personal especialitzat competent en els dos àmbits**

## Tecnologies de zero trust i innovació per fer front als nous reptes en ciberseguretat

Arran de la consolidació del **treball híbrid,** les organitzacions emprendran el camí cap a un model de **zero-trust**

Seguirà augmentant el nombre d'empreses que adopten solucions **SASE** (Secure Access Service Edge) per securitzar les operacions al **núvol**

Els serveis de ***rating*** per avaluar el nivell de ciberseguretat contribuiran a establir **vincles de confiança** entre proveïdors i clients

La **ciberseguretat** esdevindrà essencial per a la proliferació exitosa de ***data spaces*** i podrà aprofitar-se'n com a mecanisme de **col·laboració**

L'ús de *digital twins* permetrà afrontar millor la ciberseguretat d'**entorns complexos** amb sistemes ciberfísics

Les **primeres solucions criptogràfiques** resistents a la computació quàntica veuran la llum

## Les noves legislacions de la UE activen els sectors públic i privat per garantir un procés digitalitzador segur amb marca propia

Els **estats** membre hauran de **transposar** la **Directiva NIS 2** i la **Directiva de resiliència** per entitats crítiques

El **sector financer** haurà de **preparar-se** pel **Reglament DORA**

Els **serveis de criptoactius** hauran de començar a **complir el Reglament MiCA**

El **sector públic** i les **entitats** del sector privat que li prestin solucions hauran de **començar a complir l'ENS**

...

...

La UE aprovarà el **Reglament de ciberresiliència** per regular la ciberseguretat dels productes dissenyats amb algun component digital

La UE aprovarà el **Reglament de cibersolidaritat** per regular les capacitats per detectar, preparar-se i respondre a amenaces cibernètiques

La **proliferació i diversitat de normes** crearà la necessitats de **professionals** especialitzats i **eines d'auditoria automatitzades**

## Pronòstic d'amenaces

**#1 *Ransomware***

**#2 Compromís de credencials associats a *infostealers***

**#3 Intrusions a partir de la infecció amb troians**

**#4 Atacs de grups *hacktivistes***

**#5 Compromís de comptes de correu professional per al *phishing***

# Per acabar...

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

# L'**Agència de Ciberseguretat** de Catalunya

## Objectiu

Garantir la ciberseguretat
a tot el territori de **Catalunya**

## Els nostres pilars

### Desplegar

un servei públic
de ciberseguretat
executant polítiques
públiques.

### Impulsar

una cultura de
ciberseguretat que
permeti assolir una
ciutadania digital
plena en matèria de
ciberseguretat.

### Garantir

la ciberseguretat de
l'Administració de la
Generalitat de
Catalunya, del seu
sector públic i de la
resta d'entitats i
institucions
públiques.

### Potenciar

el sector econòmic
de la ciberseguretat
com a sector
estratègic.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

# Activitat de l'**Agència de Ciberseguretat**

## Volumetria

A la Generalitat de Catalunya **gestionem un incident de seguretat cada**

**4,03h**

**Generalitat de Catalunya**

**24** Departaments i organismes rellevants

**+2.200** Sistemes d'informació

**+220m** Usuaris

**Àmbits**

**Salut** | **Universitats** | **Administració local**

**Centres de recerca** | **Infraestructures crítiques**

**>4.400M** Atacs detectats durant el 2022

**=2.175** incidents de seguretat anuals gestionats

**+24** Programes de seguretat / any

**OAT** Entitat certificadora de l'ENS

**Internet Segura** Conscienciació i sensibilització de la societat

**+70** Més de 70 normes i estàndards

Dades memòria Agència Ciberseguretat de Catalunya 2022

# Activitat de l'**Agència de Ciberseguretat**

**ciberseguretat.gencat.cat**

**@ciberseguracat**

**linkedin.com/company/ciberseguracat**



# Gràcies!!

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya