Tendències de ciberseguretat per a l'empresa: on som i on anem?

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

FEGP FEDERACIÓ EMPRESARIAL DEL GRAN PENEDÈS

Santi Romeu
Ciència i Analítica de Dades
23/03/2023

ciberseguretat.gencat.cat
@ciberseguracat
linkedin.com/company/ciberseguracat

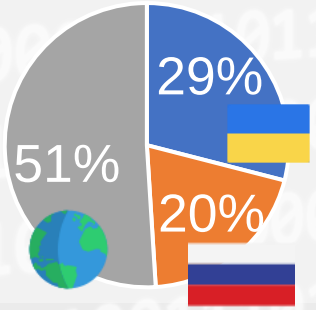
On som?

1. El conflicte bèl·lic entre Rússia i Ucraïna afecta la ciberseguretat d'arreu del món
2. El *ransomware*, obligat a evolucionar per guanyar eficiència
3. Cibercrim a l'alça i amb un catàleg d'activitats ampli i accessible
4. Accions governamentals, regulacions i cooperació policial internacional per a la lluita contra l'activitat cibercriminal

1 El conflicte bèl·lic entre Rússia i Ucraïna afecta la ciberseguretat d'arreu del món

"Cas exemplar d'una guerra híbrida que impacta tot el món"

- L'objectiu: generar desconfiança, desinformar o sabotejar serveis essencials
- *Wipers* i atacs de DDoS per destruir, desinformació per apoderar-se del relat i *phishing* oportunista
- No només entre els dos països, sinó que també ha afectat als seus aliats

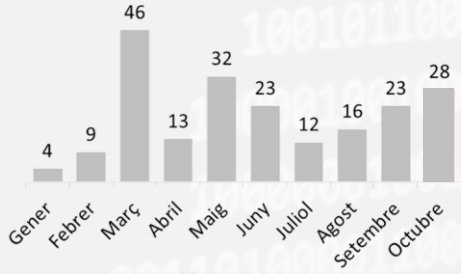


Un 51% dels ciberatacs vinculats al conflicte entre Rússia i Ucraïna han afectat altres països [CyberPeace Institute]

"*Hacktivistes* i grups cibercriminals prenen part en la ciberguerra "

- Diferents actors, tant cibercriminals com *hacktivistes* (com Anonymous, la IT Army, Killnet o Conti) s'han posicionat en un dels dos bàndols
- Els ciberatacs amb motivació *hacktivista* han estat vinculats a altres conflictes a l'Índia, Iran, Brasil o als conflictes territorials de la Xina

Evolució del nombre de ciberatacs amb motivació *hacktivista* durant el 2022



"Els atacs de DDoS augmenten en nombre i prestacions"

- Els atacs DDoS creixen en magnitud i sofisticació que els fa més difícils de bloquejar i, per tant, més destructius
- Diferents tipus de paquets enviats, peticions de capa 7 OSI, canvi d'adreces IP, ràfegues,...
- Afecten el funcionament de serveis web essencials o operadors telco

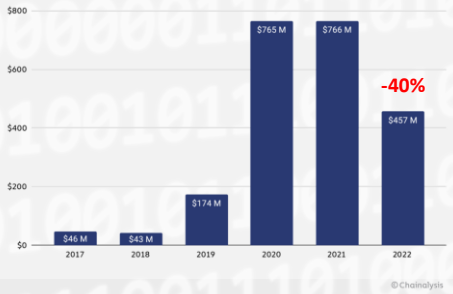
3,47 Tbps
(bloquejats per Microsoft)

46 Mrps HTTPS
(bloquejats per Google)

2 El *ransomware*, obligat a evolucionar per guanyar eficiència

"Indicis de frenada en l'afectació del *ransomware*"

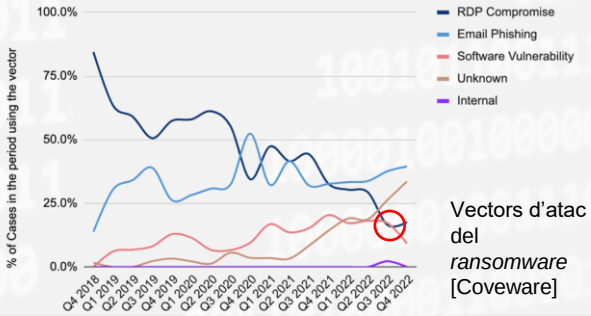
- El nombre d'incidents es manté en registres alts... Però cau el nombre de víctimes que paguen rescats
- Millores de seguretat: securització d'accessos remots, *backups*, ciberassegurances,...
- L'aparició constant de nous operadors de *ransomware* augmenta la competència i els obliga a reinventar-se



Evolució del valor dels pagaments rebuts pels operadors de *ransomware* [Chainalysis]

"La gestió de vulnerabilitats, clau per protegir-se dels atacs de *ransomware*"

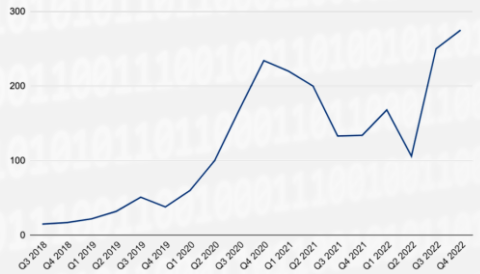
- Per primera vegada, s'han fet més atacs per explotació de vulnerabilitats que pel compromís de ports RDP
- S'han detectat més explotacions de vulnerabilitats de dia zero que mai.
- Els ciberatacants estan més capacitats tècnicament i disposen de capacitat econòmica per comprar exploits.



Vectors d'atac del *ransomware* [Coveware]

"L'objectiu se centra en els sectors crítics i empreses grans"

- En un context de crisi energètica a la UE, el sector energètic europeu ha estat objectiu de diversos ciberatacs que han posat en risc la seva operativa
- Enguany, les publicacions de ciberatacs amb afectació al sector públic català han augmentat un 150% respecte del 2021



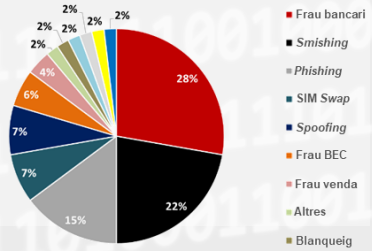
Núm d'empleats de les empreses impactades per *ransomware* [Coveware]

3 Cibercrim a l'alça i amb un catàleg d'activitats ampli i accessible

"Més dades personals robades avui pels ciberatacs de demà"

- Les dades personals permeten realitzar atacs d'enginyeria social personalitzats a cada víctima, incrementant la probabilitat d'èxit
- *Phishing* omnipresent: *emails*, apps de missatgeria, xarxes socials, motors de cerca, sol·licituds d'aplicacions de serveis al cloud, etc.
- El cost mitjà d'una fuita de dades ha augmentat un 42% des del 2020 i, per 12è any consecutiu, el sector sanitari és on és més elevat

Activitat dels grups cibercriminals detinguts a Catalunya el 2022 publicats als mitjans [Agència]



"Atacs de BEC i criptomonedes atrauen l'activitat cibercriminal"

- L'elevada cotització dels criptovalors va atraure fraus en criptomonedes i NFT a principis d'any
- Rècord de 3.000 M€ en robatoris de criptomonedes explotant vulnerabilitats a plataformes de criptomonedes
- Augmenten els casos d'estafa de correu professional (BEC). A Espanya, han augmentat més d'un 400% respecte del 2021

Evolució del nombre d'atacs de BEC publicats als mitjans amb afectació a l'estat espanyol [Agència]

"*Crime as a Service* econòmic i accessible"

- Els preus dels serveis maliciosos oferts a la *dark web* han baixat, en part, gràcies a l'augment de l'oferta: el 90% d'*exploits* a la venda estan per sota dels 10 €
- Arran de les detencions d'alguns responsables de mercats negres del web fosc, els cibercriminals recorren a Telegram per ofertar la seva activitat anònimament.

Preus de productes i serveis cibercriminals al *dark web* [Privacy Affairs]

Servei	Preu mínim	Preu màxim
Malware	41 €	5.060 €
Documentació física	138 €	3.496 €
Serveis de processament de pagaments	9 €	920 €
DDoS	9 €	782 €
Comptes Criptomonedes	83 €	368 €
Documentació	9 €	152 €
Dades de targetes de crèdit	9 €	110 €
Xarxes socials	1 €	60 €
Serveis hackejats	3 €	37 €
Bases de dades de comptes de correu	92 €	110 €

4 Accions governamentals, regulacions i cooperació policial internacional per a la lluita contra l'activitat cibercriminal

"Noves regulacions europees per reforçar un nivell de ciberseguretat comú"

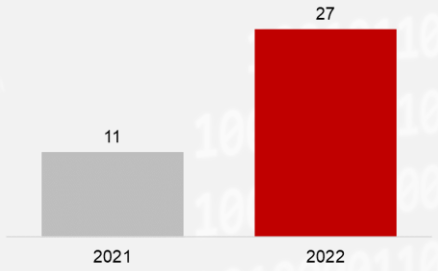
- Reial Decret 311/2022, del 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
- *El Reglament europeu Digital Operational Resilience Act (DORA) per al sector financer*
- La Directiva NIS 2 per als sectors essencials i indústries importants

44% de totes les sancions a la UE d'aquest 2022 s'han efectuat a l'estat espanyol, tot i que només representen el **4%** de l'import econòmic total

"Gran activitat de les forces de l'ordre contra el cibercrim"

- Cada vegada són més habituals les operacions policials coordinades internacionalment per detenir grups cibercriminals organitzats.
- Algunes trames criminals involucren centenars de detinguts i grans quantitats de diners.

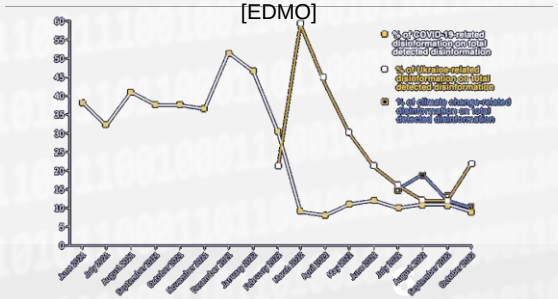
Evolució del nombre d'accions policials contra grups cibercriminals de Catalunya publicades [Agència]



"Accions per al conflicte cibernètic"

- Davant del conflicte cibernètic, la comunitat internacional va oferir suport a Ucraïna i es va autoprotegir per possibles represàlies
- El conflicte ha creat una batalla pel relat de la guerra que ha derivat en un allau de *fake news*.
- Rússia va restringir Facebook, YouTube,... La UE va vetar emissions de Russia Today (RT) i Sputnik

Evolució de les noticies falses a la UE [EDMO]



On anem?

1. Les crisis globals esperonaran els ciberdelictes
2. La crisi econòmica condicionarà les polítiques de ciberseguretat empresarials
3. El cibercrim mutarà per continuar optimitzant l'èxit
4. Tecnologies i innovació en ciberseguretat en espera de la gran disrupció

1 Les crisis globals esperonaran els ciberdelictes...

"Més cibercrim, atacs de menor complexitat i monetització ràpida"

- La criminalitat cibernètica esdevindrà una sortida a les dificultats econòmiques
- Nova delinqüència de proximitat i tècnicament menys capacitada
- Proliferació de campanyes de *phishing*, *smishing*, *vishing*
- Fraus i atacs de BEC molt dirigits

"Un cibercrim de primera i un altre de segona"

- Bandes cibercriminals que desafien l'equilibri social i econòmic des de la impunitat d'algunes geografies i l'opacitat de les xarxes
- Operacions policials internacionals focalitzades en el cibercrim més capacitat
- D'altra banda, proliferació del cibercrim de perfil baix, fora del radar principal de les autoritats

"Ciberatacs de gran impacte contra sectors estratègics, valuosos o poc madurs"

- En plena crisi energètica i aigua, els ciberatacs als serveis de subministrament bàsics permeten maximitzar l'impacte
- Com és habitual, el valor dels sectors de les finances i sanitari atrau els ciberatacs
- El sector agroalimentari, en plena digitalització però amb poca maduresa en matèria de ciberseguretat, és un objectiu apetitós

2 La crisi econòmica condicionarà les polítiques de ciberseguretat empresarials

"IA per millorar l'eficiència en la vigilància, detecció d'amenaces, diagnosi d'incidents..."

- Augment del nombre de ciberatacs que complica la resposta a temps real
- Complexitat de les xarxes i les ciberamenaces, inassolible per a un humà
- Manca de talent i excés de treball que alimenten l'estrès i el fenomen de *burnout*
- Necessitat de nous perfils professionals que combinin ciberseguretat i IA

"La ciberseguretat, clau en el desenvolupament dels projectes NextGen"

- El reclam de l'augment del valor dels actius digitals
- Desenvolupament de tecnologies innovadores amb nous riscos cibernètics
- Les pròpies iniciatives del pla, font potencial de fraus o de projectes mal dissenyats en matèria de ciberseguretat

"La inversió en ciberseguretat en risc"

- Aposta ferma de les empreses grans organitzacions per la digitalització cibersegura
- Les pimes veuen les seves inversions condicionades a les conseqüències de la crisi econòmica

3 El cibercrim mutarà per continuar optimitzant l'èxit

"Ciberatacs a la cadena de subministrament amb afectacions massives"

- Empreses de serveis i productes TI són una passarel·la per arribar als clients
- Desenvolupadors de programari, plataformes de compartició i MSP, objectius per a la difusió de *malware*, robatori de dades i atacs de *ransomware*
- Els espais amb molta interrelació i dependència entre organitzacions són objectiu prioritari de *ransomware* i DDoS

"Atac al 2FA"

- El cibercrim disposa de capacitats per esquivar les solucions de 2FA
- *SIM-Swapping*, finestres d'autenticació falses, esgotament per enviament de peticions falses, enginyeria social, troians per a la injecció de codi (*On-Device Fraud*) o *infostealers* per al robatori d'OTP,…

"Nova generació de *botnets* per elevar el cibercrim al següent nivell"

- Xarxes de *bots* més versàtils per a l'activitat cibercriminal des de l'anonimat: *spam*, difusió de *malware*, control de xarxes socials,…
- *Bots* al *cloud* per utilitzar la capacitat de computació pel *criptojacking* i realitzar DDoS complexos
- Ciberatacs a entorns industrials (IIoT) que permeten amenaçar el món físic i l'exigència de rescats

4 Tecnologies i innovació en ciberseguretat en espera de la gran disrupció

"Adopció d'IA per gestionar la complexitat de la ciberseguretat"

- IA per a l'anàlisi de riscos, models de *Threat Intelligence,* defensa predictiva i reactiva
- IA com a assistència al compliment normatiu de lleis, marcs de control, certificacions,…
- Eines de *rating* per a l'auditoria i presa de decisions: inversions, compres, *partnering*,…
- ... I alerta a la *weaponization* de la IA.

"Desapareix el perímetre i els models *zero trust* ja són una realitat"

- Teletreball, entorns *cloud* i xarxes corporatives, una realitat consolidada
- Insuficiència dels controls de perímetre (FW, VPN) per controlar els accessos
- Les VPN com a mecanisme d'atac utilitzat en nombrosos ciberatacs
- És l'hora de les arquitectures SASE i SD-WAN, i models de *Zero-Trust*

"Albirem la quàntica"

- El BSC tindrà un ordinador quàntic el 2023.
- Necessitat de nous xifrats quàntics.
- Posicionament estratègic per a un *game changer* que s'acosta a poc a poc…

Agents de l'ecosistema de ciberseguretat a Catalunya

Centres tecnològics i de recerca

Estudis de màster i postgrau

Estudis d'FP

CSIRT/ CERT

Institucions i administració pública

Associacions i esdeveniments

Principals conclusions del mapatge de l'ecosistema de ciberseguretat a Catalunya

495 empreses

9.414 treballadors vinculats a la ciberseguretat

Facturació de 1.071 M € directament vinculats a la ciberseguretat

CLASSIFICACIÓ DE LES EMPRESES

PIME	85%
Menys de 10 anys de vida	29,1%
Startups	9,5%
Exportadores	28,7%
Dones al Consell d'Administració	13,8%
Facturació	21,7% >10 M€ / 53,6% >1 M€

DISTRIBUCIÓ DE LES CAPACITATS

Protegir	89,7%
Identificar	58,7%
Detectar	37,0%
Respondre	33,6%
Recuperar	20,6%

TOP 5
CATEGORIES DE SOLUCIÓ

1. **Backup/Storage Security** (PROTEGIR)
2. **IT Service Management** (IDENTIFICAR)
3. **Anti Virus / Worm / Malware** (PROTEGIR)
4. **IoT Security** (PROTEGIR)
5. **Risk management strategy development & consulting** (IDENTIFICAR)

ECS

L'**ECSO** (European Cybersecurity Organization) defineix el **Market RADAR**, una eina visual per representar els proveïdors de productes, consultoria i serveis de ciberseguretat ubicats a Europa, segons 5 àmbits de capacitat principals: identificar, protegir, detectar, respondre i recuperar.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

L'**Agència de Ciberseguretat de Catalunya** vetlla per una societat digital segura per al conjunt de la societat catalana i la seva Administració Pública. L'Agència és l'encarregada d'executar les polítiques públiques en matèria de Ciberseguretat i desenvolupar l'estratègia de Ciberseguretat de la Generalitat de Catalunya.

OBJECTIUS ESTRATÈGICS I LÍNIES D'ACCIÓ

Estratègia per als anys 2019-2023 en matèria de ciberseguretat de la Generalitat de Catalunya

- País cibersegur
- Servei públic de ciberseguretat
- Administració cibersegura
- Cultura de la ciberseguretat
- Innovació, talent i activitat econòmica de la ciberseguretat

Moltes gràcies!

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

ciberseguretat.gencat.cat

@ciberseguracat

linkedin.com/company/ciberseguracat