EL MUNDO QUE VIENE EN 2022

La era de la pandemia digital de ataques de 'ransomware'

• Las empresas deben aprender a combatirlos

Shashank Joshi

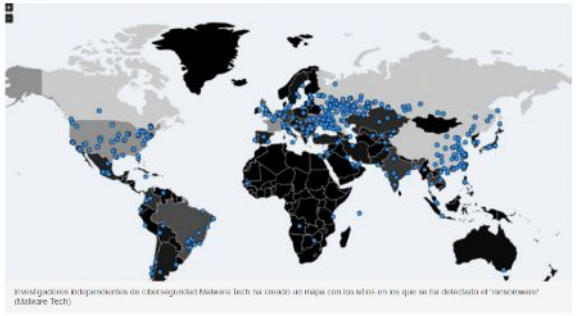
El CSIC está desconectado: radiografía de un 'ransomware', el ciberataque que todos temen

Este tipo de intrusión, que cifra los datos y pide un rescate para liberarlos, causa estragos entre empresas y organismos públicos. Así funciona y se combate la herramienta estrella de los ciberdelincuentes

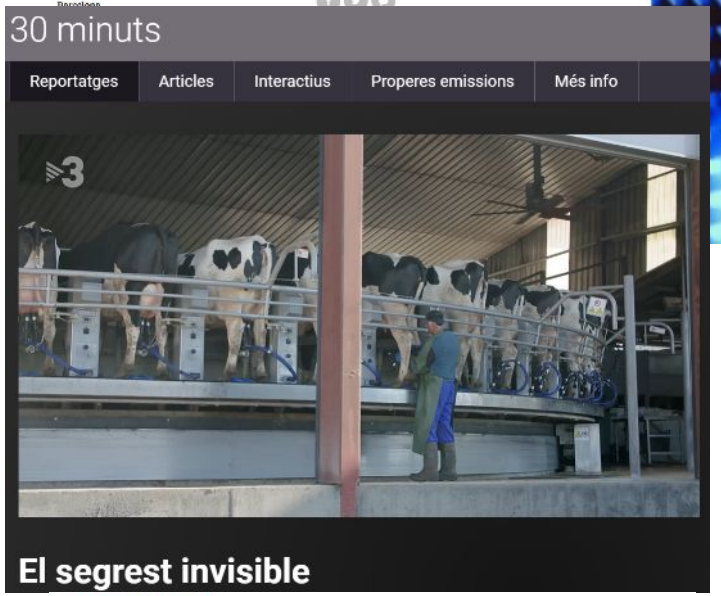
APARECEN NUEVOS AFECTADOS

Europol investiga un ciberataque "sin precedentes" que empieza a remitir

• El virus conocido como ransomware se ha extendido a escala global a más de 125.000 ordenadores en todo el mundo



Redacción



No funciona ningún portal

Un ataque informático con 'ransomware' deja la Universitat Autònoma de Barcelona sin internet

CATALUNYA NIT

Catalunya va registrar dos ciberatacs cada hora durant el 2022

Un 74% dels virus i programaris maliciosos s'instal·len perquè una persona ho autoritza clicant un enllaç

MIQUEL JARQUE

Redactor d'informatius especialitzat

@miqueljarque

02/02/2023 - 17.45 | Actualitzat 02/02

CIBERSEGURIDAD

Un ataque informático paraliza la operativa de Damm

• Fuentes de la compañía no admiten que se trate de un ataque de ransomware y aseguran que se están sirviendo los pedidos con normalidad

• Así actúa el grupo de cibermercenarios que hay detrás de los principales ciberataques

neàpolis

Tecnología Digital Avançada i Ciberseguretat

Jornada tècnica Ciberseguretat

Vilanova, 23 de Març de 2023.

Jordi Guijarro

@jordiguijarro

Cybersecurity Innovation Director

i2cat

Never stop designing the digital future

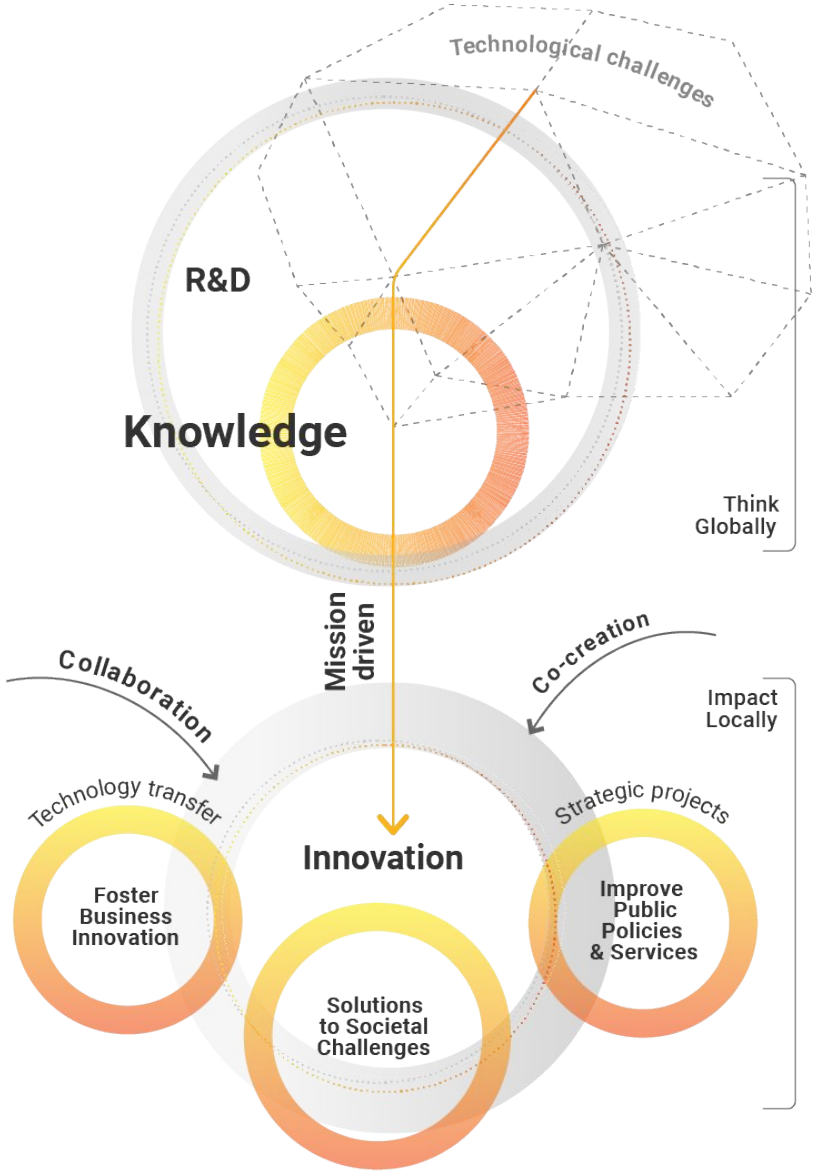
i2CAT.net

CERCA Centres de Recerca de Catalunya

tecnio catalonia | ACCIÓ Generalitat de Catalunya

Vision

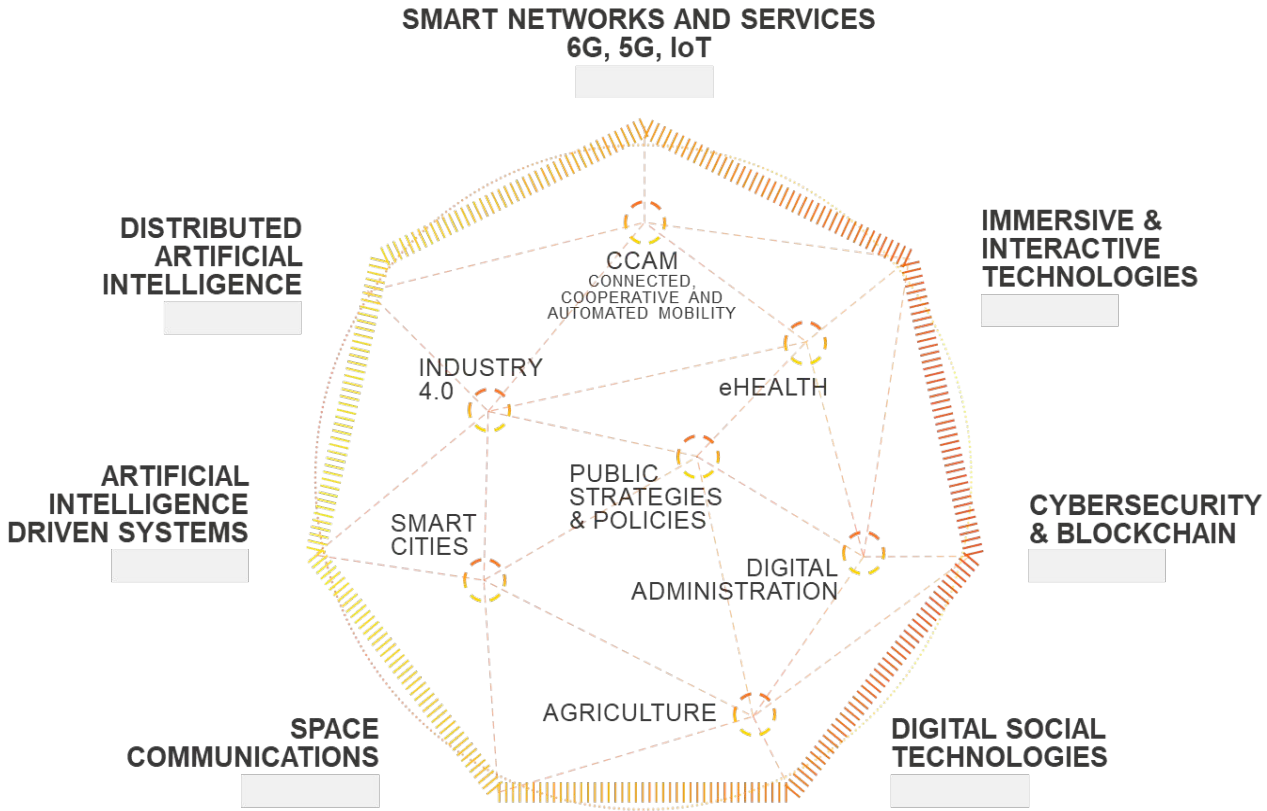
i2CAT wants to lead the challenge of designing the digital society of the future based on research and innovation in advanced digital technologies.



Fundació i2CAT

La **Fundació i2CAT** és un centre CERCA que impulsa activitats de **recerca i innovació** en tecnologies digitals avançades.

El centre col·labora des de 2003 a nivell local i internacional en el desenvolupament de projectes d'R+D+I en àrees com 5G/6G, IoT, Tecnologies Immersives i Interactives, Ciberseguretat, IA, Blockchain, Space Communications i Tecnologies de la Societat Digital



Introducció

En un context on el teixit industrial cada cop es troba més informatitzat i connectat: automatització de processos, monitorització, administració i control econòmic, etc.

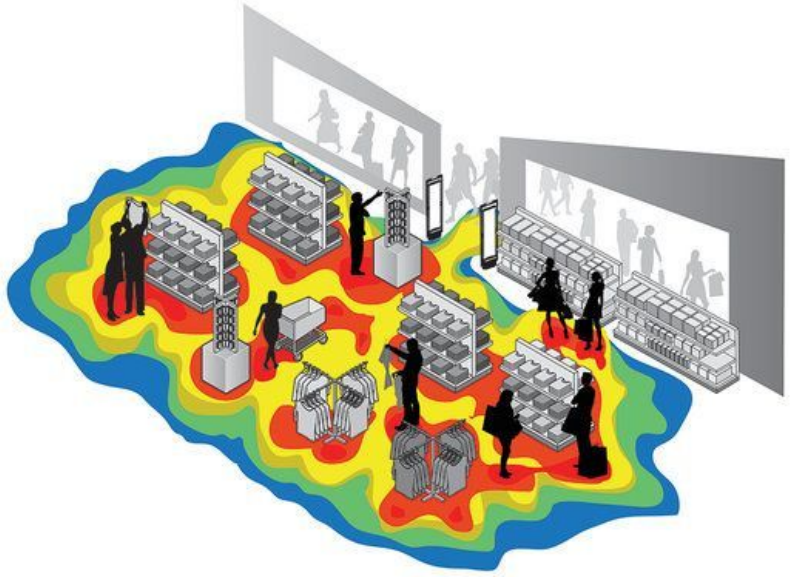
Cada cop més connectats a Internet, la superfície d'atac ha augmentat i són més susceptibles a atacs informàtics.

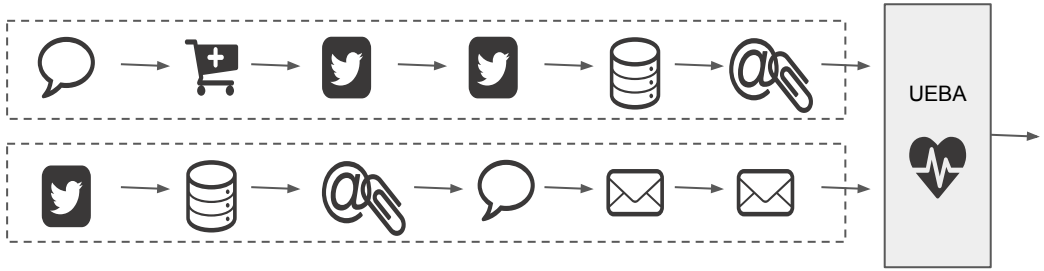
Possibles amenaces:

- Ransomware
- Atacs de sabotatge i manipulació dels controls
- Robatori de dades confidencials: procediments industrials, metodologies, clients i proveïdors.

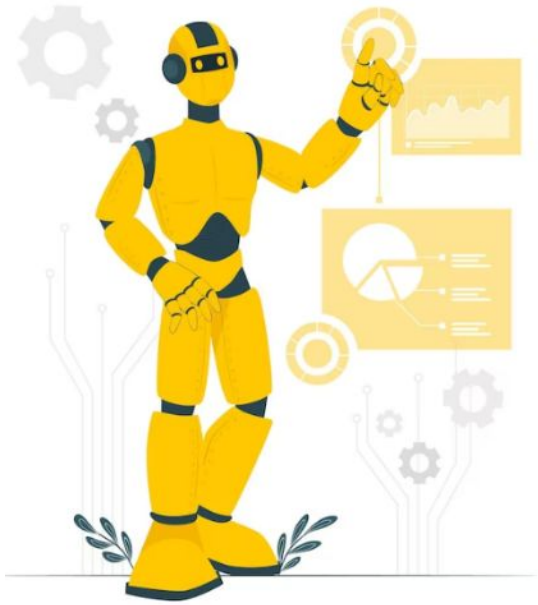
Tècniques defensives

Ús de la IA per combatre els ciberatacs





Ús de la IA per combatre els ciberatacs (II)



Millorar l'anàlisi d'amenaces per reconeixement de patrons de comportament dels usuaris

- Modelatge del comportament normal de l'usuari permet detectar comportaments de risc en temps real **->** Falsos positius i falsos negatius
- IA permet fer aquest anàlisi amb més precisió i reduir els falsos positius, ja que és capaç d'analitzar nous comportaments de l'usuari mitjançant models d'aprenentatge automàtic i veure si s'adapten al seu perfil.
- Exemple de projecte TDACiberseguretat: https://tdacyber.cat

TDACiberseguretat

Ús de la IA per combatre els ciberatacs (III)

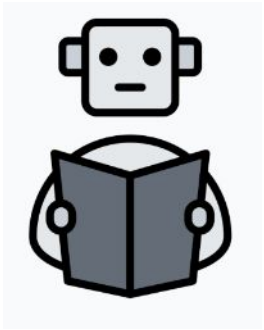
Anàlisi d'amenaces per detecció d'anomalies de xarxa.

- Antivirus i IDS usen detecció de virus amb signatures (patrons coneguts d'activitat maliciosa). Si no hi ha signatura, no es pot detectar -> Zero day
- **IA ajuda a desenvolupar solucions** basades en anomalies per detectar amenaces encara desconegudes, a partir del coneixement previ d'amenaces i activitats històriques.

Ús de la IA per combatre els ciberatacs (IV)

Detecció avançada de programari maliciós

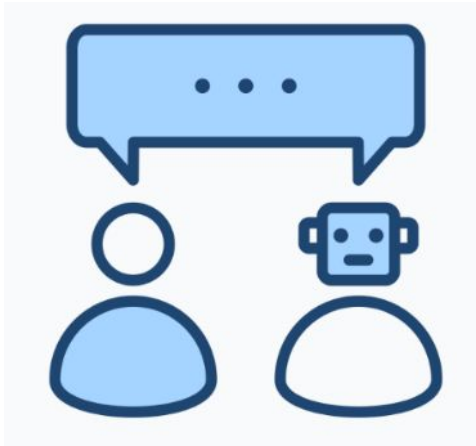
- Millorar les capacitats de l'anàlisi heurística, que analitza el comportament de programes executant-los en una sandbox, i mitjançant unes regles de decisió i mètodes de ponderació decideix si es tracta d'un virus potencial.
- Un altre mètode d'anàlisi és descompilar el programa i analitzar-ne el codi font comparant-lo amb altres malwares coneguts. **La IA permet facilitar i ajustar l'anàlisi de gran quantitat de mostres i comparar-les de manera més ràpida i eficient.**



Ús de la IA per combatre els ciberatacs (V)

Millora de les capacitats de prevenció

- Modela atacs i escenaris d'atac: com arribaria un atacant a un actiu clau? Avaluació de danys potencials, punts febles, automatitzar el procés
- Bloqueig de phishing amb procediments automàtics – **Ús de les capacitats de la IA en processament del llenguatge natural (NLP).**



Tècniques Ofensives

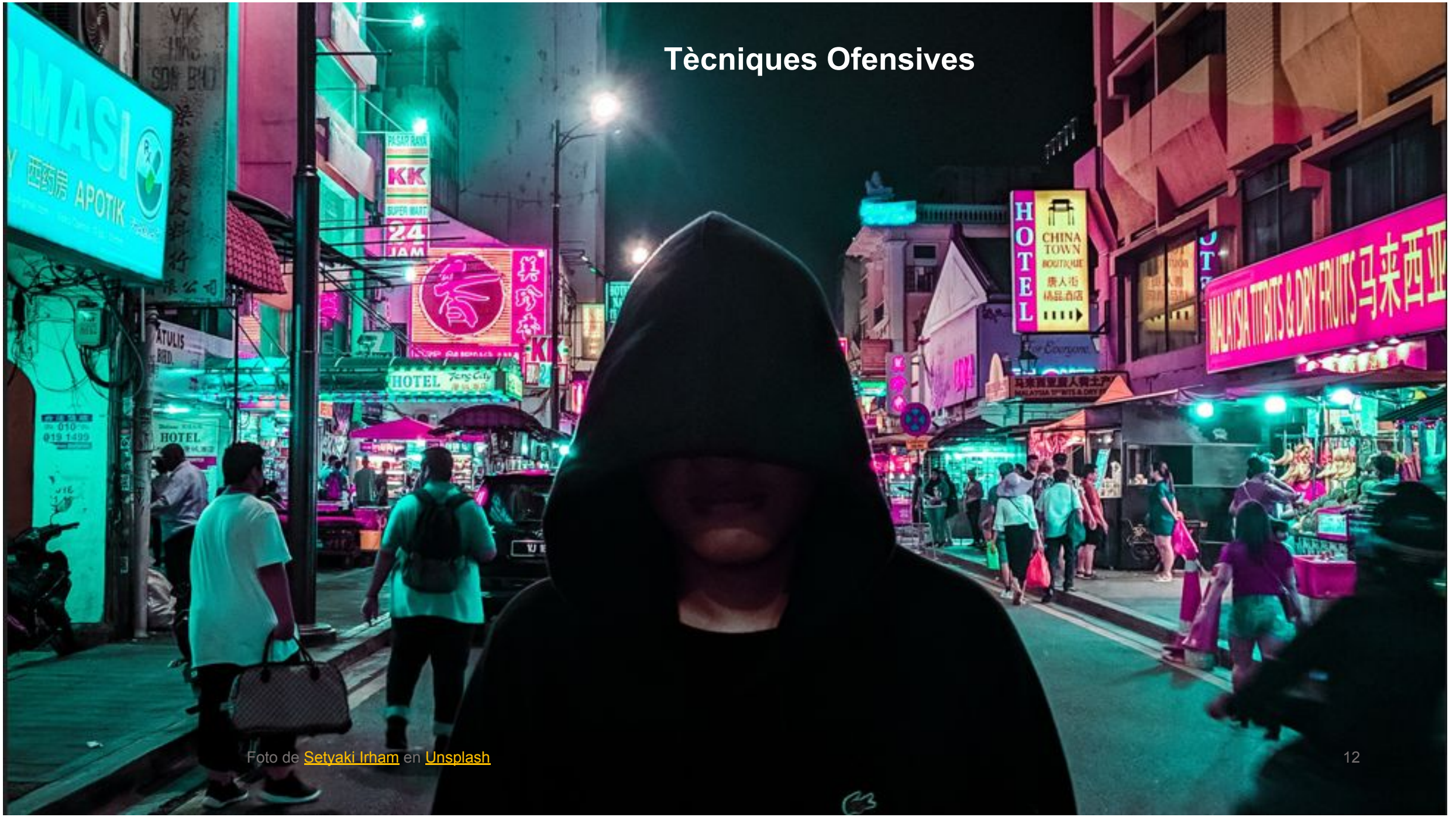
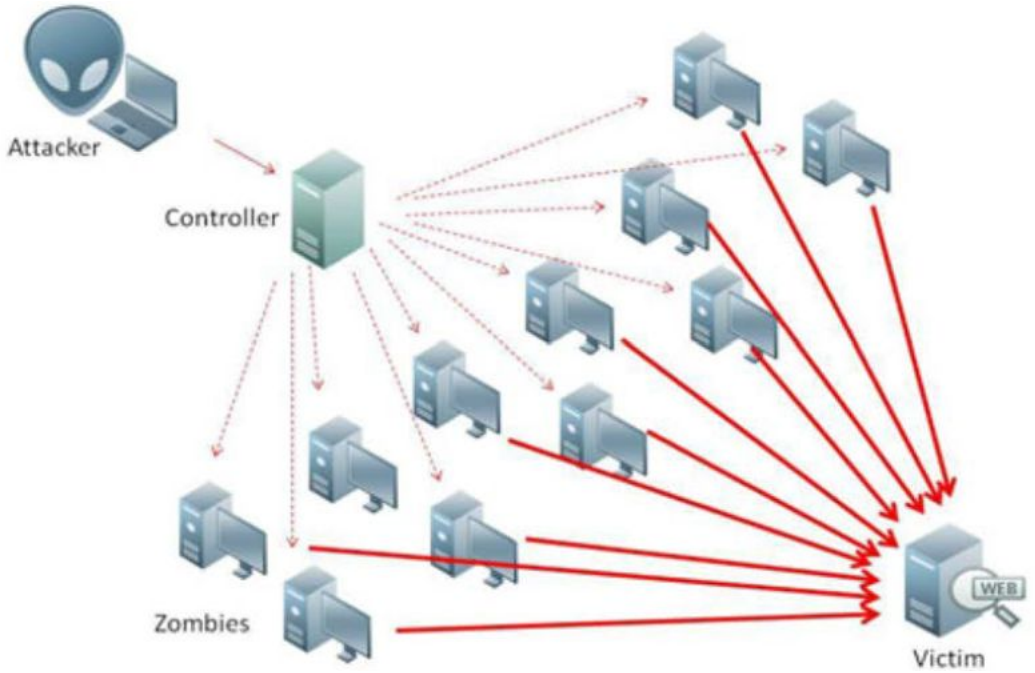


Foto de Setyaki Irham en Unsplash

Noves amenaces potenciades per la IA

Ciberatacs automatitzats

- **Smart DDoS**, que permet variar la tipologia dels paquets, emetre fluxos de dades en rafegues, canviar d'objectius dinàmicament per eludir el blackhole routing.
- **Campanyes de Phishing** - AI permet crear missatges de phishing molt ràpidament, difondre les campanyes ràpidament, interactuar amb els usuaris que responguin, incorporar dades personals dels usuaris per fer atacs més dirigits.



Noves amenaces potenciades per la IA (II)

Programari maliciós polimòrfic

- Generar codi maliciós automàticament (ChatGPT)
- Millorar de les tècniques d'evasió de les defenses de seguretat usant el polimorfisme (canvi de l'estructura del codi cada cop que s'executa) de manera efectiva, segons l'escenari, el sistema que ha infectat i les proteccions d'aquest.
- Llarg camí recorregut des del Morris Worm de 1988

Floppy Diskette containing the source code for the Morris Worm held at the Computer History Museum. CC BY-SA 2.0. Source; Wikipedia

Noves amenaces potenciades per la IA (III)

Imitació automatitzada del comportament humà

- Quan el malware infecta l'equip de la víctima, dedica un temps a aprendre el seu comportament habitual, de manera que després les seves accions seran indetectables.
- Bots Intel·ligents que actuen a les xarxes socials generant desinformació, perfils falsos.

Deepfake i BVCC (Business Videoconference Compromise)

- Hi han exemples de falsificació d'activitats a les xarxes socials usant IA
  - Kyle Vorbach va usar eines basades en IA (Stable difusión) per crear una vida falsa a les xarxes socials com a experiment social. Ho va fer durant un mes.
  - Va llogar un ordinador al cloud amb una GPU potent capaç de realitzar un aprenentatge intens.
  - Va generar disfresses de halloween artificials, va usar IA per generar un viatge inventat a Nova York, amb un acompanyant fictici, i inclús va manipular una imatge per aparèixer al costats de l'actor Ryan Gosling.
- Cada cop els deepfakes podran ser més comuns i dificils de detectar, i serà possible portar els atacs BEC a un altre nivel
- BVCC (Business Videoconference Compromise) en el que es podrà, per exemple, impersonar a una persona amb veu i vídeo o falsificar una videoconferència.

https://www.youtube.com/watch?v=oxXpB9pSETo

https://unaaldia.hispasec.com/2022/12/chico-falsifica-su-vida-en-redes-sociales-con-inteligencia-artificial.html

Altres tecnologies Digitals Avançades

Foto de CHUTTERSNAP en Unsplash

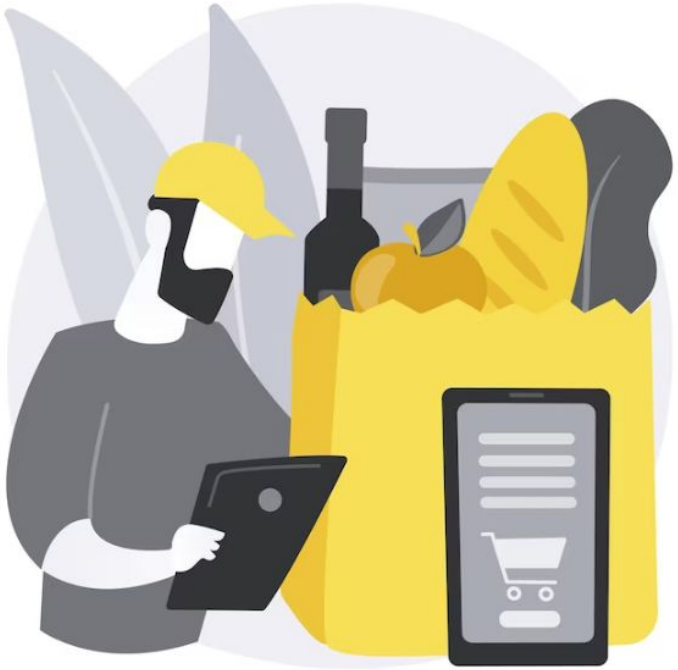
Blockchain per millorar la traçabilitat

Valor afegit

- Descentralització i Immutabilitat
- Seguretat i traçabilitat - entorn digitalitzat amb formularis estandarditzats - abans es feia en paper – deficiencies
- Ús de signatura digital (digital wallet) per identificar l'usuari i interaccionar amb la blockchain

Blockchain ajuda al compliment de normatives

- Seguretat en la cadena de subministrament
- Flux de traçabilitat - conèixer totes les dades i l'evolució de cada una de les etapes de producción - origen, productor, transport, preparació.
- Verificació de que tots els procediments establerts s'estan duent a terme correctament
- Smart contract - mecanisme per verificar la informació (sense una autoritat central)



Gràcies!

Alguna pregunta?

Jordi Guijarro

@jordiguijarro

jordi.guijarro@i2cat.net

i2cat

Never stop designing the digital future

i2CAT.net

Institució CERCA
Centres de Recerca de Catalunya

tecnio catalonia | ACCIÓ Generalitat de Catalunya