AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Generalitat de Catalunya

Alerta! Seguretat en comerços i vehicles- Ciberseguretat

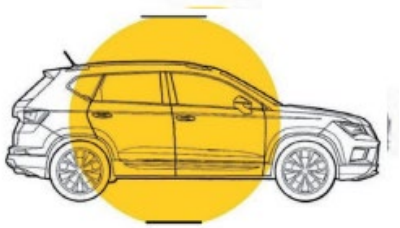
20/09/2022

DIGITALITZACIÓ

PASSAT

- Connectivitat bàsica
- Unitat principal, aire condicionat, clau amb comandament a distància, alçavidres,...
- 20-30 ECU / <10M LoC

AVUI



- Connectat a la xarxa mòbil
- Unitat principal avançada, quadre digital, wifi, Bluetooth, GPS, TPMS (*Tire-pressure monitoring System*),...
- 50-80 ECU/TCU / <100M LoC

FUTUR

- Sempre connectat (5G)
- Gran quantitat de sensors (vehicle completament autònom),...
- >100 ECUTCU / 100-200M LoC

Els vehicles digitals estan superant els *smartphones* com a "dispositius mòbils" més complexes

775 M de vehicles connectats circularan per la carretera el 2023

1 M de vehicles autònoms en previsió de vendes fins el 2025

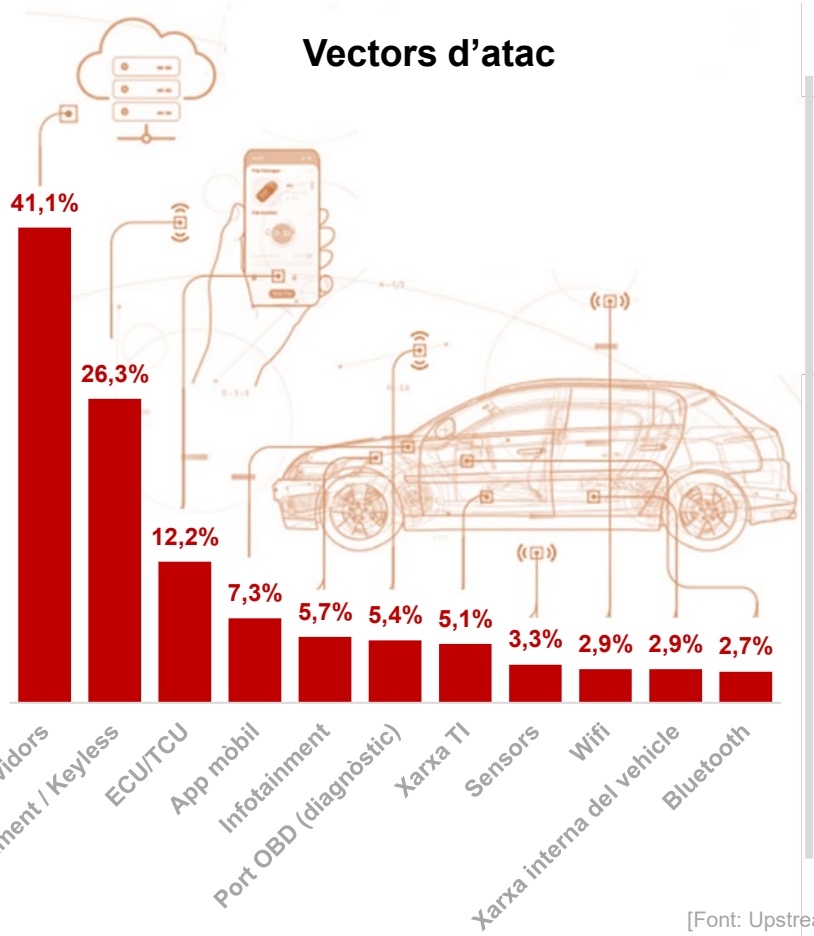
[Font: EUROCYBCAR, Juniper Research, HIS Markit]

** ECU: Electronic Control Unit*
TCU: Telematics Control Unit
LoC: Lines of Code

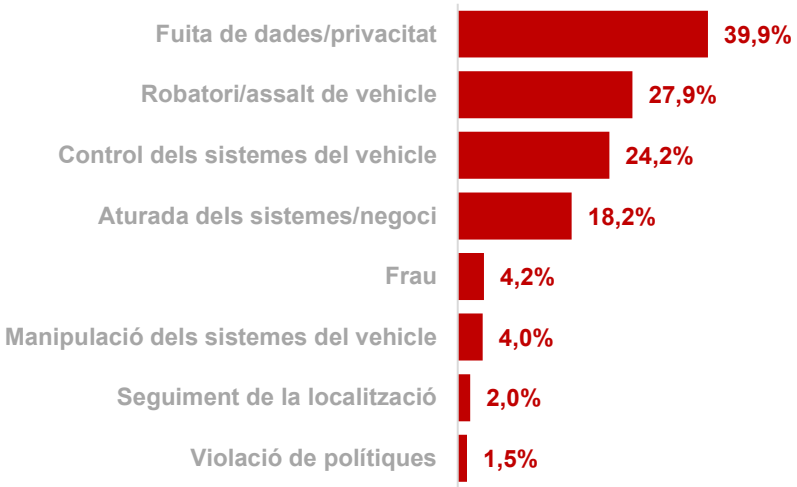
CIBERATACS

Els darrers 3 anys, la indústria de l'automoció ha experimentat un creixement del 225% dels ciberatacs amb origen i afectació en tota la cadena de subministrament

Vectors d'atac



Impactes



[Font: Upstream Security]

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

** Percentatges sobre un recull de més de 900 incidents cibernètics publicats entre 2010 i 2020*

CIBERATACS DESTACATS

Top incidents in 2021:

JANUARY
A hacker exploited a vulnerability in a major European Tier-1 infotainment system that was deployed in an Asian OEM's vehicle. This was achieved by plugging in a USB device, then executing the exploitation to gain root shell access to the system.[36]

FEBRUARY
An Asian OEM's American business arm experienced a ransomware attack by the DoppelPaymer gang, who demanded $20 million in exchange for a decryptor and not leaking stolen data.[37]

APRIL
A North American insurance agency with some 17 million vehicle policyholders, experienced a data breach that compromised drivers license ID numbers in early 2021.[38]

APRIL
The doors of a North American EV manufacturer's vehicle were hacked using a drone carrying a Wi-Fi dongle, exposing the vulnerabilities these vehicles have to wireless adjacent attacks.[39]

MAY
Numerous vulnerabilities discovered in a European manufacturer's infotainment system, which could be exploited to take control of multiple in-cabin functions.[40]

JUNE
Hackers exploited a feature in modern vehicles' ECUs, and managed for the first time to misuse it and remotely attack other ECUs. The hackers managed to attack and shutdown the powertrain ECU and power steering ECU in to vehicles.[42]

A data breach hit two European OEMs, impacting more than 3.3 million customers and prospective buyers in North America.[41]

JULY
Hacking the CAN bus of a European OEM's vehicle, a hacker was able to wirelessly transmit vehicle data to a third party device.[43]

AUGUST
An Asian EV OEM was investigated by the Chinese law enforcement due to claims that car data was tampered with following a fatal collision.[44]

Hackers exposed multiple vulnerabilities in the operating system used by major agriculture OEMs, allowing black-hat actors to remotely manipulate machinery, even taking them out of service.[45]

DECEMBER
Researchers found vulnerabilities affecting devices or properties embedded in or used for connected cars, chargers, in-vehicle infotainment (IVI) systems, and digital remotes with car chargers were at risk, including vehicle-to-grid (V2G) systems in Europe.[46]

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Generalitat de Catalunya

Oriol Torruella

Director General
Agència de Ciberseguretat de Catalunya