Dual Use Technologies 2022
Cybersecurity and Digital Applications in Defence

Hispasec]

Are corporate mobile devices well protected?

]

OUR ORIGINS

Chronology

Una al día

Una Al Día was launched, daily newsletter about computer security

1998

Hispasec]

Hispasec was born. Big demand of services

1999

VIRUSTOTAL

Virustotal development, inspiring new projects. Google purchased it in 2012

2012

MAIA

MAIA. Cyber intelligence applied to Android devices

2018

WHERE WE WORK

BUSINESS AREAS

Hispasec has been offering cyber security services and online anti-fraud during the last 20 years. This experience, accumulated knowledge, reputation and *"knowhow" guarantees us to be able to execute services with a high contrasted quality*.

International banking and financial sector, big retail, health, services, industries, public administrations.

Banking
73 customers

Health
5 customers

Big retail
38 customers

Services
53 customers

Industry
26 customers

Public administration
57 customers

THREAT INTELLIGENCE

MAIA

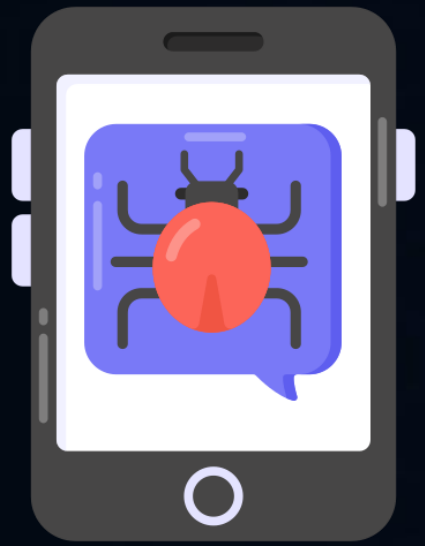
CYBER INTELLIGENCE ON ANDROID DEVICES

MAIA

CYBER INTELLIGENCE ON ANDROID DEVICES

MAIA is a system included in our Threat Intelligence service which monitors the security status of Android devices.

Real time monitoring

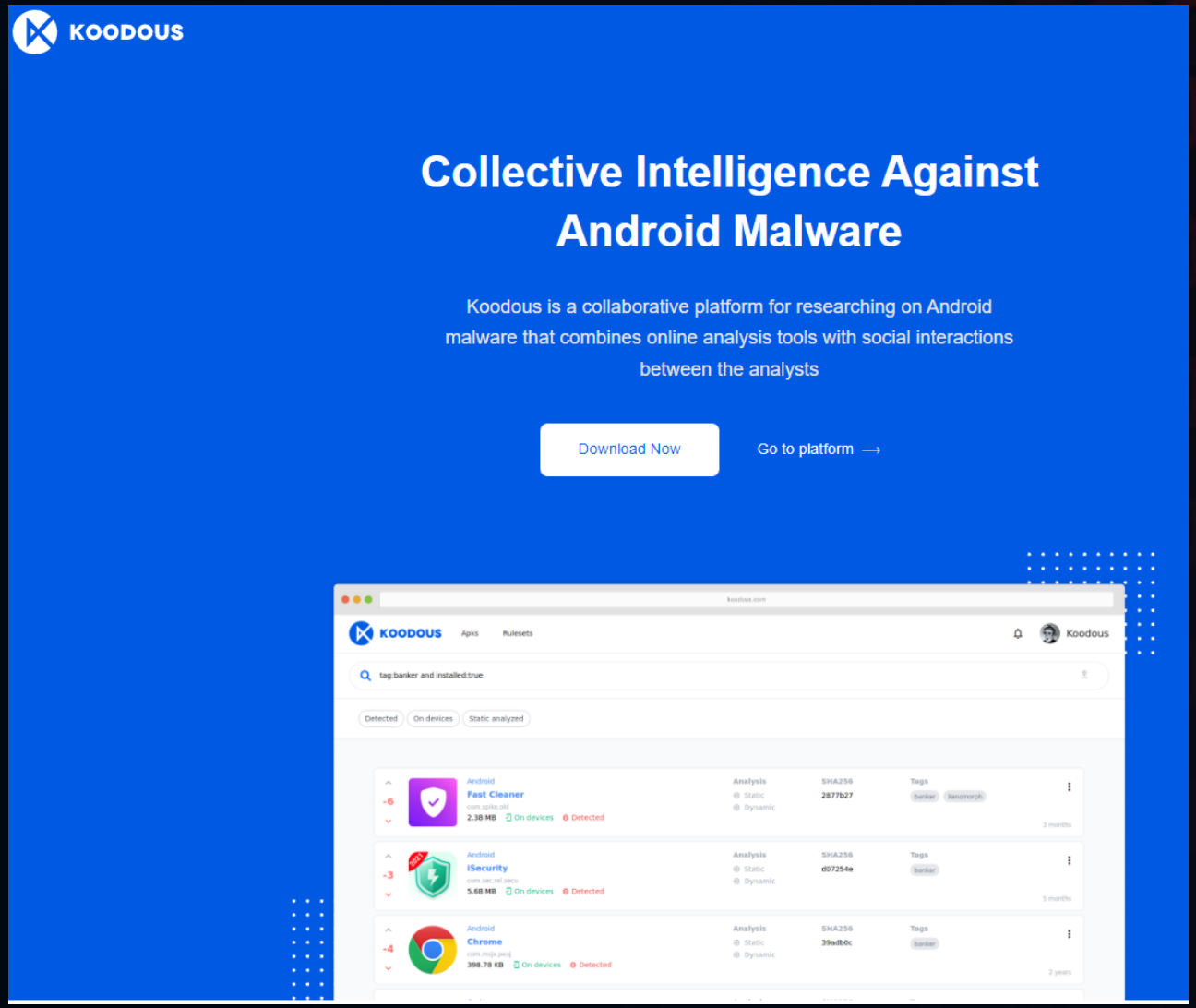


Malware analysis on android device

Allows actions to be taken according to the level of the risk

MAIA POWERED BY KOODOUS

KOODOUS



MAIA

CYBER INTELLIGENCE ON ANDROID DEVICES

- MAIA allows the registration of devices and the analysis of the applications installed on them. This would allow to know if the device is infected by malware in real time.

- By storing the applications installed on the device, it is also possible to find out if the device has had malware in the past that has been discovered later.

MAIA

REAL USE CASE

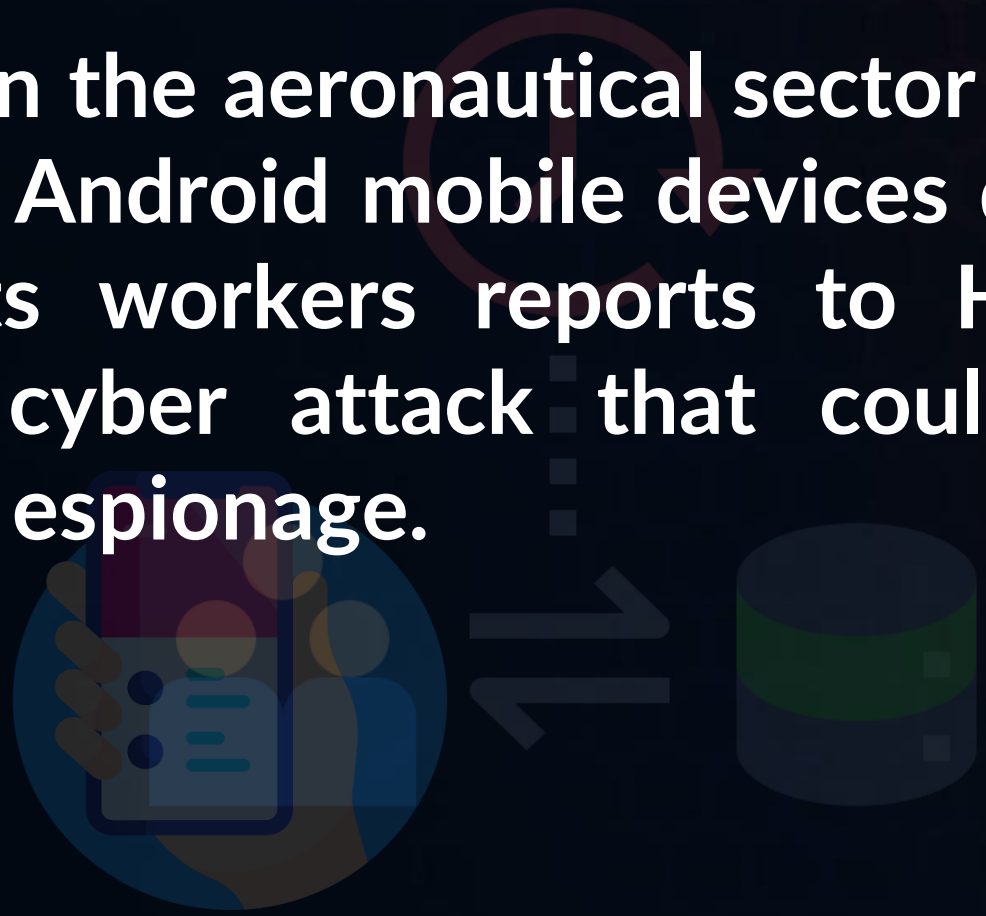
- Through the telemetry offered by this tool we were able to detect an attack by means of a Trojan with keylogger functions on a client in the aeronautical sector.

- In this way, we were able to detect all the corporate devices that were affected, thus protecting all their sensitive corporate information.

MAIA

USE CASE

A Client in the aeronautical sector with more than 200 Android mobile devices distributed among its workers reports to Hispasec a possible cyber attack that could lead to industrial espionage.



MAIA

USE CASE

Hispasec proceeded to implement MAIA API integrated with client's SOAR and immediately found some apps that were carrying out various malicious actions on more than 10% of the workers' devices. ¿What did Hispasec detect?

1. Installation of keyloggers with the ability to detect any action or typing on the devices: 67%

2. Installation of droppers that allow the download of other malicious applications, most of which are Trojans: 12%

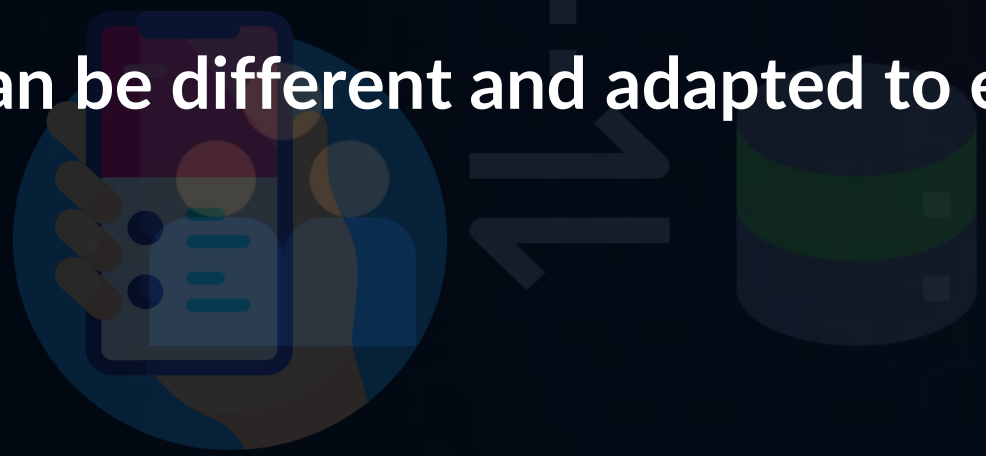
3. Exfiltration of data and professional secrets

MAIA

USE CASE

The company receives the reports of the affected devices via API and integrates the information with its SIEM/SOAR. In this way, protocols are created in the SOAR that automate the response and mitigation processes.

This mitigation can be different and adapted to each device.



MAIA

CONCLUSIONS

1. Industrial and technological espionage is a fact.
2. Companies related to the Defense sector are being a preferential target
3. Mobile devices are one of the most used attack vectors by cybercriminals

THANKS

Miguel Manteca

mmanteca@hispasec.com

Hispasec]