2020 REPORT

ENTERPRISE MOBILE THREAT LANDSCAPE

pradeo

INTRODUCTION

Along the massive usage of mobile devices and applications in our day-to-day life, mobile security has become a major focus for organizations. Today, employees leverage mobile services to enhance their performance and cybercriminals are well aware of it. To reach companies' data, hackers have shifted to a data centric approach that extensively targets the mobile workforce.

This year, we have adapted the focus of our annual mobile security report to present current mobile threats from the perspective of a mobile fleet that includes company owned and BYOD devices. To build this report, researchers from the Pradeo Lab went through the mobile threat intelligence generated by the Pradeo Security engine, based on billions of mobile security events collected in 2019 and early 2020.

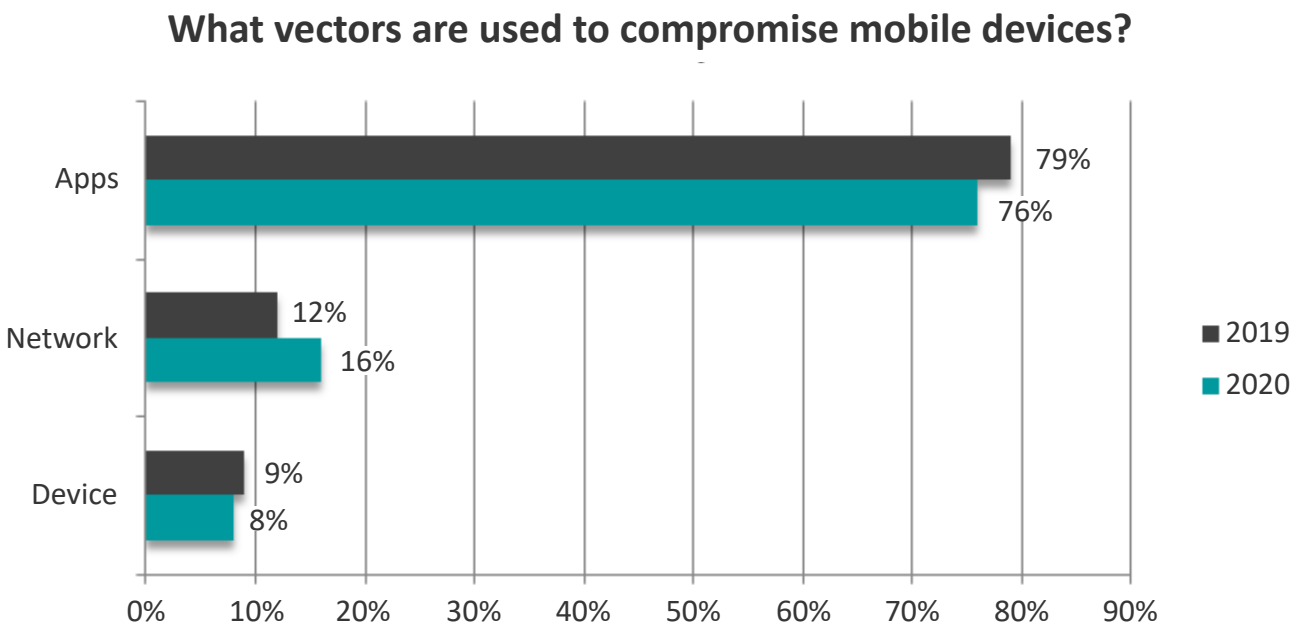
If you are wondering what threats currently threaten mobile fleets across the world along their frequency, dive in!

INDEX

To compromise mobile devices, mobile apps still are cybercriminals' favored vector

Since our first mobile security report almost a decade ago, mobile apps are in pole position when it comes to exfiltrating data from mobile devices, and it is no coincidence. Mobile devices used in the workplace host an average of 103 applications and a recent report from Frost & Sullivan indicates that mobile users spend an average of 2.8 hours every day on them. With such a position at the center of operations coupled with the multitude of techniques available to exploit them, apps represent a juicy target.

On the other hand, network attacks have increased by 4% in the last year, driven by the continuous growth of Man-In-The-Middle in North America and Asia specifically. Finally, attacks exploiting the operational system of mobile devices slightly declines and now accounts for 8% of all attacks.

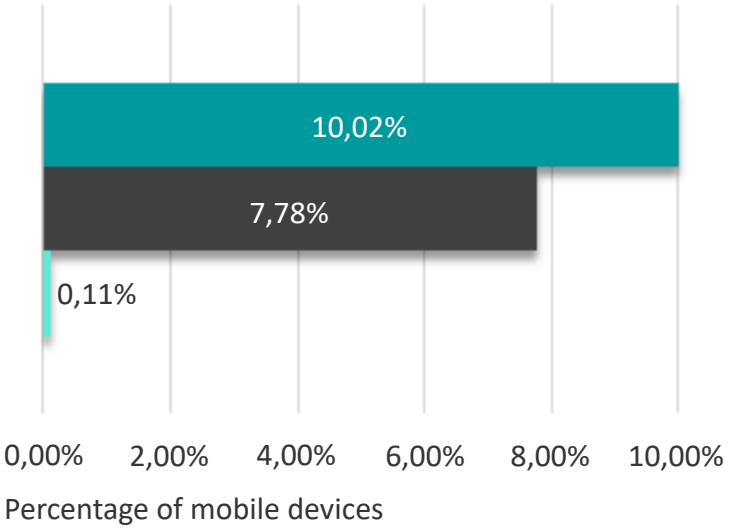


APPLICATION THREATS

Malware

A malware is specifically designed to disrupt, damage, or gain authorized access to a legitimate device or data while the victim often remains **unaware of the attack**. The number of devices infected by malware, such as keylogger, screenlogger, overlay, etc. is low but continues to grow year after year. We differentiate known malwares (on Android) that have a viral signature, and 0-day malwares (on Android and iOS) that are not referenced by antivirus databases and can only be identified with behavioral analysis.

How many mobile devices host a malware?



- Android 0-day malware
- Android known malware
- iOS 0-day malware

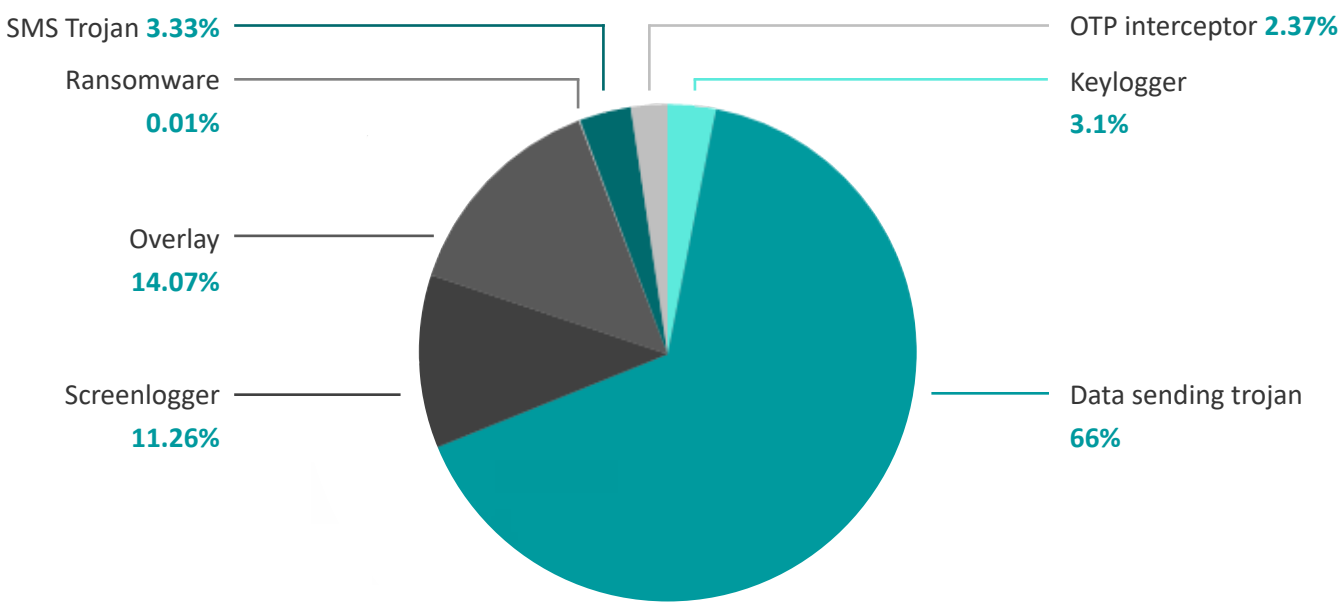
In a company mobile fleet of 50.000 Android devices:

- 5.100 devices host a 0-day malware
- 3.890 devices host a known malware

In a company mobile fleet of 50.000 iOS devices:

- 55 devices host a 0-day malware

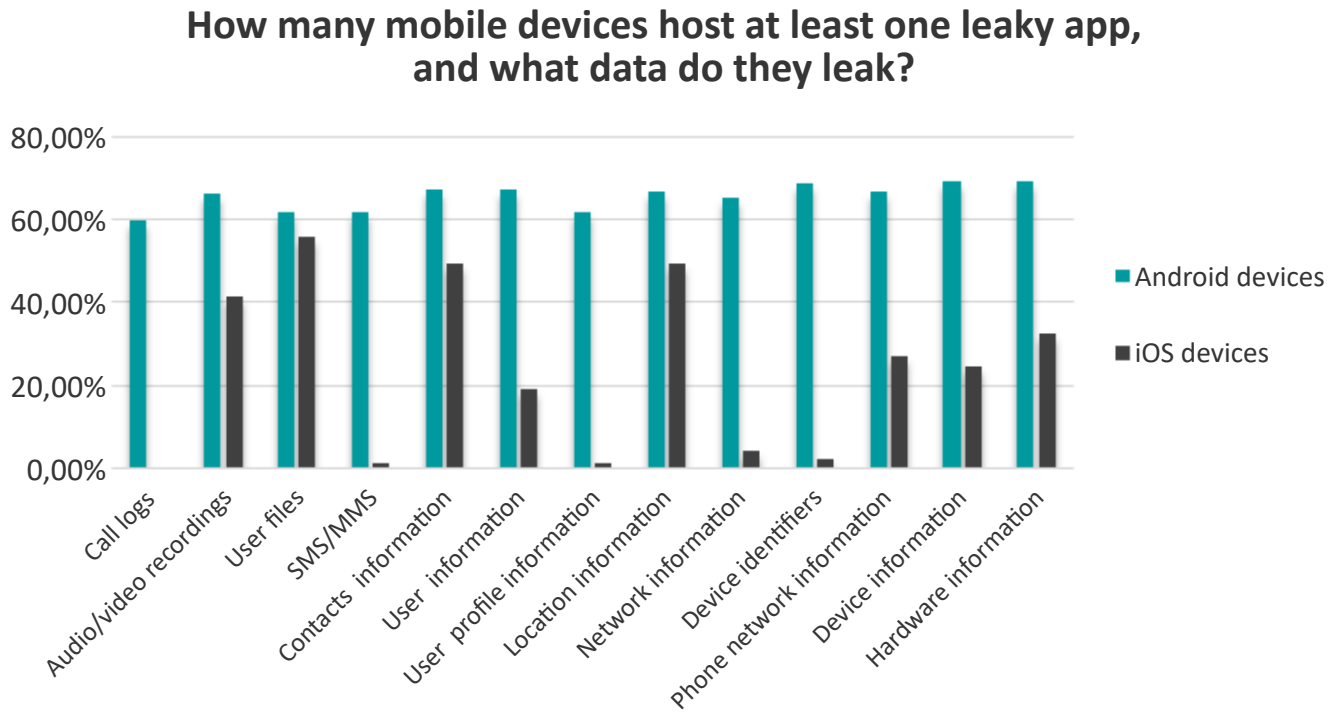
What are the most encountered 0-day malwares?



APPLICATION THREATS

Leaky and intrusive applications

A mobile application can perform unwanted actions because of the external libraries it hosts (79% of mobile applications embed third-party libraries) or as a result of a development negligence between testing and production. Both can lead to **silent data leakage** and potentially **unwanted and unknown data processing**. Android devices tend to exfiltrate more data than iOS ones, but still, both overly process the data they are granted access to.



In a company mobile fleet of 50.000 Android devices:

- 33.560 devices send contact information over the network
- 29.865 devices send call logs over the network

In a company mobile fleet of 50.000 iOS devices:

- 24.670 devices send contact information over the network
- 200 devices send call logs over the network

Phishing (through applications)

The phishing technique traps mobile users into clicking on malicious links, opening infected files or downloading malwares from emails, SMS, or messaging, social and gaming apps. **85% of phishing is now carried out through mobile applications**, hence its addition to the application-borne threats category.

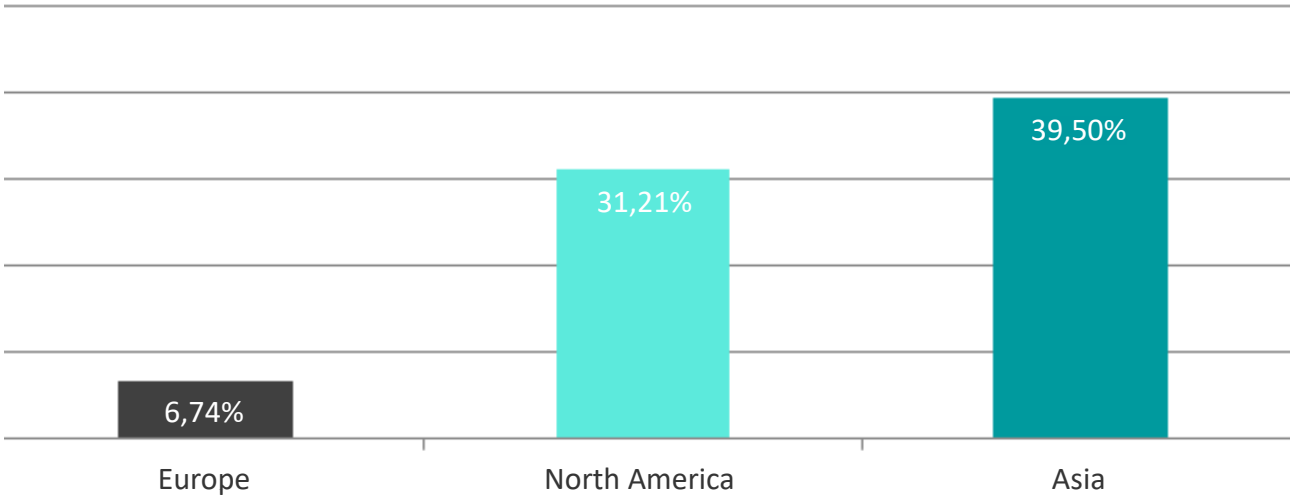
NETWORK THREATS

63% of companies allow employees to work remotely, according to an Upwork study. As a result, more employees are getting connected outside the office to unsafe networks, exposing corporate data in the process. The results below are based on a **6-month time-lapse and are representative of both Android and iOS.**

Unsafe WiFi connections

As mobile phone plans in North America and Asia are more expensive than in Europe, the practice in these regions of the world is to get connected to a public WiFi when out of home or the office. The number of mobile devices getting connected to unsafe WiFi hotspots by region reflects this practice.

How many mobile devices get connected to unsafe WiFi?



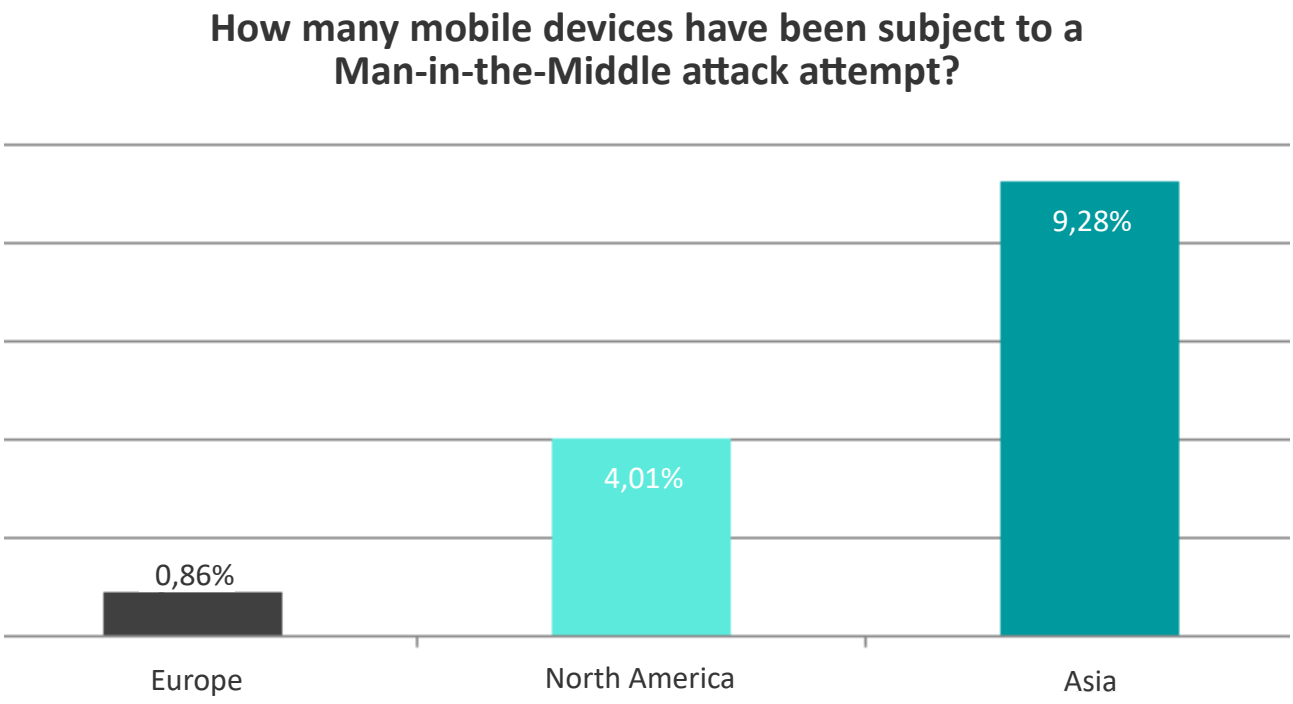
On a company's mobile fleet of 50.000 devices:

- In Europe, 3.370 devices connected to unsafe WiFi hotspots
- In North America, 15.605 devices connected to unsafe WiFi hotspots
- In Asia, 19.750 devices connected to unsafe WiFi hotspots

NETWORK THREATS

Man-In-The-Middle attacks

Unsecure connections are exploited by cybercriminals mostly to perform Man-In-The-Middle attacks, which consist in **intercepting** or **altering a communication between two parties**. It can lead to data theft or fraud, if a transaction is performed by the mobile user while the attack happens. Here, we are talking about “attack attempts” as the targeted mobile endpoints in question were protected by Pradeo Security and the attacks were successfully stopped before they could do any harm.



Among a company's mobile fleet of 50.000 devices, in the last 6 months:

- In Europe, 430 devices were subject to a Man-in-the-Middle attack
- In North America, 2.050 devices were subject to a Man-in-the-Middle attack
- In Asia, 4.640 devices were subject to a Man-in-the-Middle attack

OS THREATS

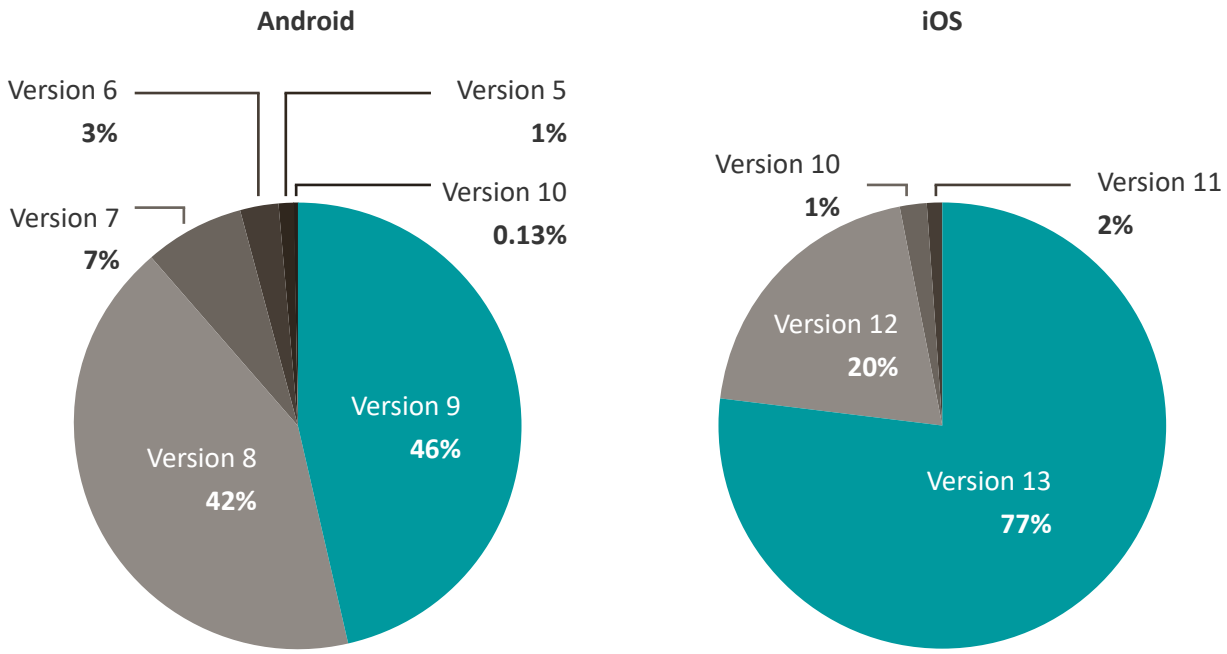
On a regular basis, security holes are discovered in the code of operating systems. Once detected, companies quickly develop patches that they push to users through updates and simultaneously publish documents disclosing the vulnerabilities (CVEs) that existed in the former version.

Once made public, cybercriminals can exploit outdated devices' vulnerabilities for their own illicit gain. When exploited, a vulnerability can provide hackers with extended rights, such as consulting and exfiltrating data or communications.

Outdated OS

54% of Android devices run an outdated OS version compared to 23% of iOS devices. *To be noted that Android 10 was only released to a few devices at the time of the report, so we considered Android 9 as current.*

How many mobile devices run a vulnerable outdated OS?



Currently, among a company's Android mobile fleet of 50.000 devices:

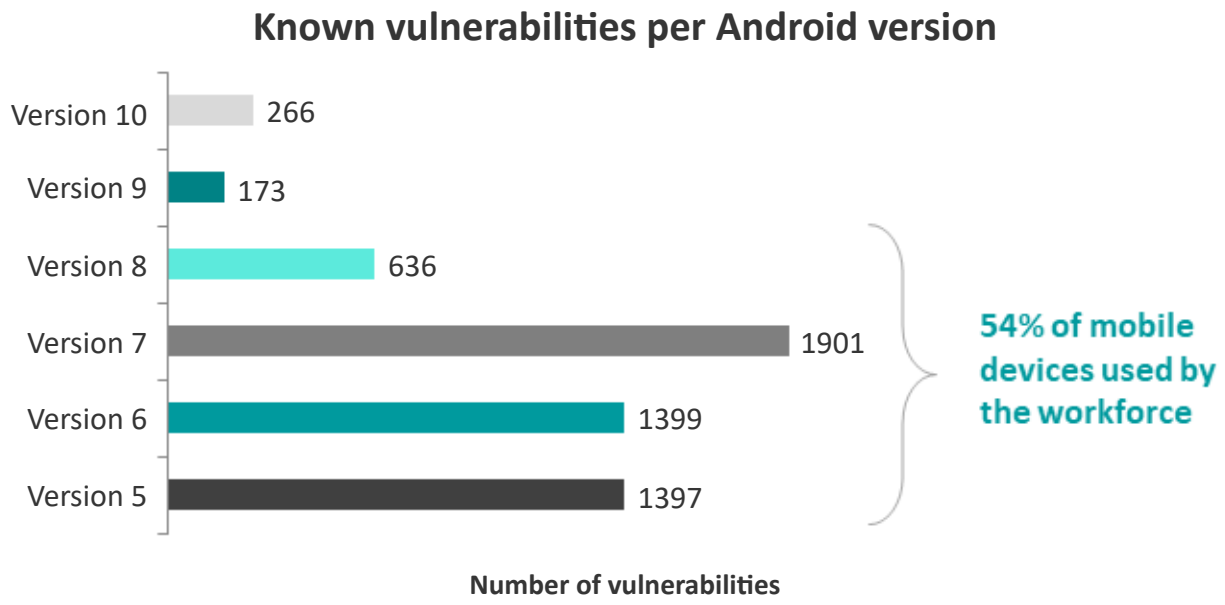
» 27.000 devices are outdated

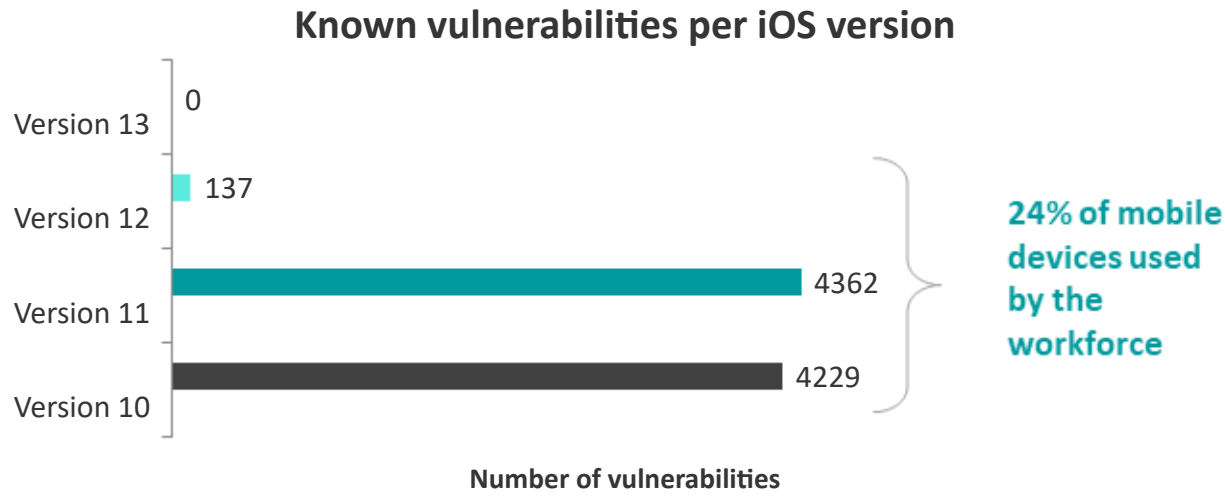
Currently, among a company's iOS mobile fleet of 50.000 devices:

» 11.500 devices are outdated

OS THREATS

Known vulnerabilities in outdated OS (CVEs)





ABOUT PRADEO

Pradeo is a global leader of mobile security. It provides mobile threat intelligence services as well as solutions to protect the data handled through smartphones, tablets and mobile applications.

Pradeo developed Pradeo Security, a patented mobile security technology that uses Artificial Intelligence and machine learning to automatically detect and ward off known, unknown and advanced mobile threats including zero-days. Pradeo Security has been recognized as one of the most advanced mobile security technology by Gartner, IDC, Frost & Sullivan and 37 other research firms in 2018. It provides a reliable detection of mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

Pradeo Security offers a complete and automatic protection of the data manipulated by mobile devices and applications, aligned with organizations' security policy, while preserving business agility.

"Pradeo continues to raise the bar in mobile security. By delivering high quality products that are easy to deploy, automated, highly accurate, user-friendly and compliant with data protection laws, the company has emerged as a clear market leader. With its strong overall performance, Pradeo has earned the 2019 Frost & Sullivan Global Product Line Strategy Leadership Award." **Vikrant Gandhi, Industry Director, Frost & Sullivan.**

For more details, visit www.pradeo.com or write to contact@pradeo.com.