# GLOBAL **MOBILE SECURITY** REPORT

2022

pradeo

# INDEX


# INTRODUCTION

In 2021, the number of reported data leaks increased by 68%, reaching an all-time high that exceeded the previous record by more than 23% according to the U.S.-based Identity Theft Resource Center's annual report.

Among the **thousands of organizations affected** by these data breaches were the social networks Facebook and LinkedIn, the Thai and Brazilian governments and internet giant Comcast, among others.

Although some of these incidents were caused by human error, most of them were the result of **cyberattacks** that led to unauthorized access to private data. In most cases, these cyberattacks were carried out using **information initially stolen from the mobile devices** of organizations' employees and clients, through spyware or phishing campaigns, among others.

Mobile devices are essential for the performance of any organization's workforce, and this central position makes them a **prime target** for cybercriminals and cyberactivists seeking sensitive information to sell and disclose.

To ensure the safety of data stored on their organization's mobile devices, security teams apply guidelines: for each detected threat, a security response is scheduled and deployed, either manually or automatically depending on the needs and tools in place.

In this regard, **the ability to accurately detect and prioritize threats is essential**. Without this accuracy, false positives soar and end-users are unfairly impacted.

When applied to securing mobile applications, this precision translates into the **careful detection** of every data manipulation and behavior programmed and/or executed by an application, as well as its connections, its code vulnerability, the potential viral signatures it embeds and the permissions it requires. By knowing these facts, a **precise security and compliance status** can be assessed, leading to the **most accurate response**.

Today, mobile security is an essential part of **endpoint protection strategies**. Pradeo, expert in the field with more than 10 years of experience in identifying mobile threats, publishes every year its report on the threats that target mobile devices and applications, enabling security professionals to better understand and apprehend them.

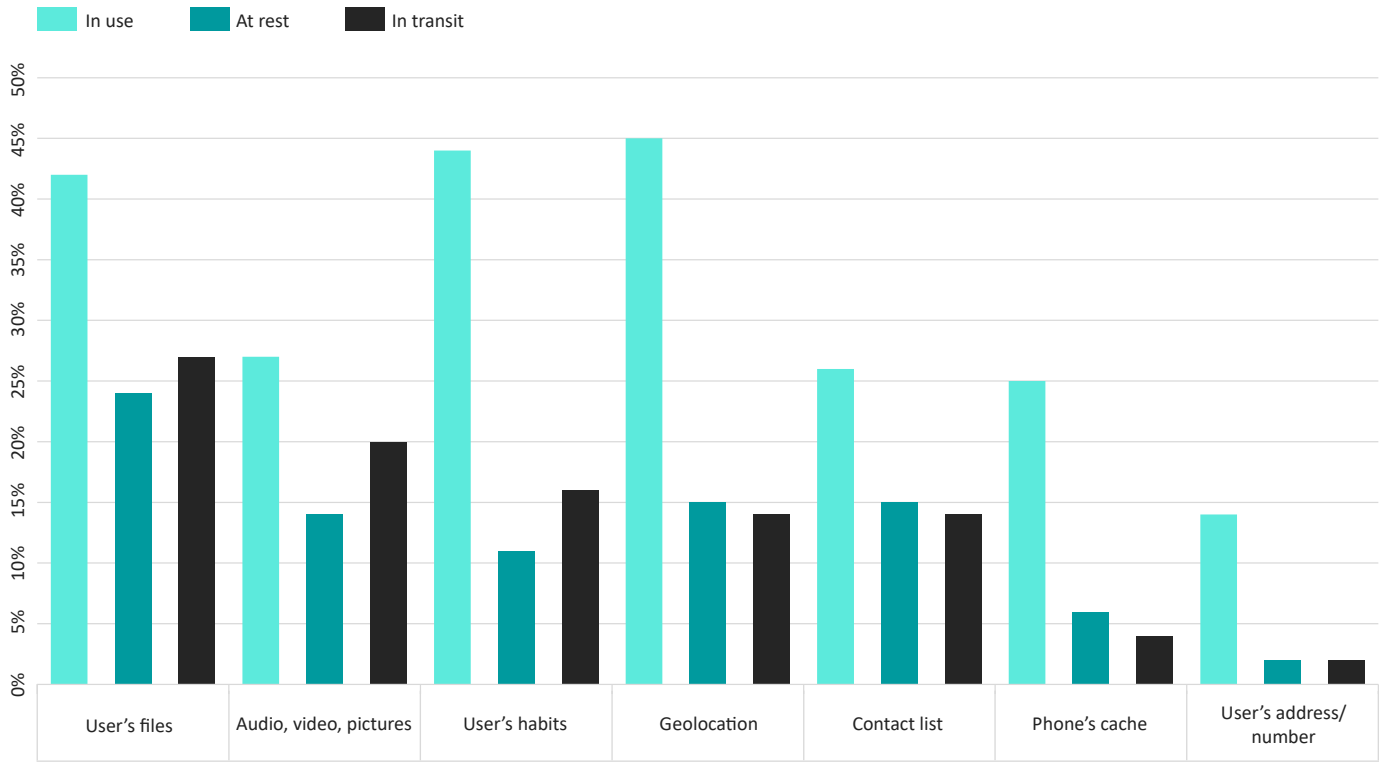
# **MOBILE APPLICATIONS:** HOW DO THEY HANDLE OUR DATA?

When it comes to protecting confidential information, we realize that clients require different approaches or have different protection needs.

Some customers need to protect the files on their employees' mobile device in case they get lost. Others want to ensure that their information is never stored on shared folders. Sometimes, security teams need to prevent their data from being sent over the Internet. This list of examples is not exhaustive.

To best protect the private information handled by mobile applications, it is necessary to be able to control all the processing they undergo:

- **In use:** The information is accessed by the application.
- **At rest:** The information is stored by the application in the file system, in a local database, shared resources, logs, clipboard…
- **In transit:** The information is sent out of the device through the internet or cellular network.




20% of mobile applications send users' pictures, video and files outside the device

# **LIBRARIES** THAT MAKE APPLICATIONS VULNERABLE

During the development of an application, it is common to add libraries within its code to benefit from specific turnkey services, which allow, for example, to develop faster, to increase the performance of an application, to analyze crashes or to generate an income (advertising libraries).

In this last case, when ad libraries are installed in an application, they display advertising and collect as much information as they can about users. The application then become a real advertising space, and all the data that it legitimately collects for its operations are also sent to the servers of advertising companies.

Regardless of their purpose, the most popular libraries are embedded in hundreds of thousands of applications, even though many of them have code vulnerabilities that jeopardize the security of applications hosting them.

On average an Android mobile application embeds 8 libraries, and 1 out of 8 has identified vulnerabilities. An iOS application contains an average of 21 libraries, of which 4 are vulnerable to cyberattacks.

> Within an Android app, 1 in 8 libraries are vulnerable to attack. On iOS, the ratio is 1 to 5

# MALWARE: TROJAN-DROPPER GOT A MAKEOVER

Witnessing more and more attacks targeting smartphones, many mobile users are now being cautious. To fool them, hackers must work on the appearance of their tools.

A trojan-dropper, also called dropper, is a program designed to install malware on its users' device. On mobile, a dropper takes the form of a real application, delivering a functional service. Once installed, this malicious application performs checks on the system it is running on and initiates the installation of the malware when the timing is appropriate.

The use of a dropper is not new, but throughout the years the tool has been perfected to ensure its survival and improve its efficiency. Before, a dropper contained in its code the malware it planned to install (also known as payload) as well as the command lines to install it. Now, the latest versions of droppers connect to C&C (Command & Control) servers and download their payload from the Internet, once installed on a device.

Over the past 12 months, 4.92% of the mobile apps we tested connect to C&C servers and 2.45% install apps downloaded from the network. By doing so, hackers maximize their chances to successfully pass security tests in app stores that do not perform dynamic scans.

**4.92% of mobile apps connect to C&C servers, 2.45% install apps downloaded from the network**

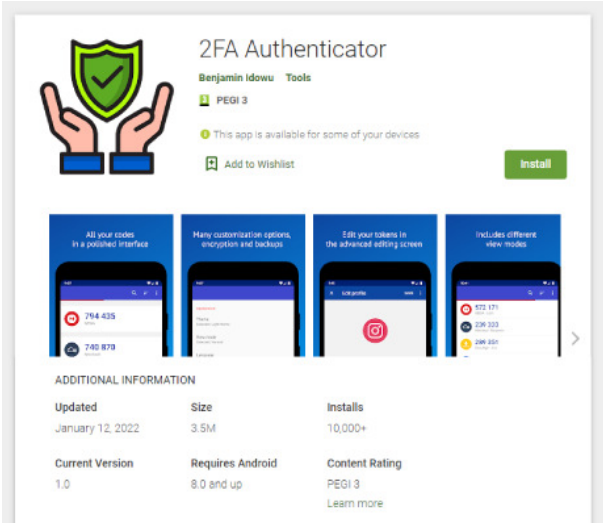
## Real life case study: 2FA Authenticator

Early 2022, our researchers identified a trojan-dropper app distributed on Google Play and installed by over 10.000 people. The app itself, 2FA Authenticator, provides a true two-factor authentication service by using the open-source code of the official Aegis app, to which the hackers injected malicious code.

Our analysis revealed that this dropper carries out its attack in two stages. In the first stage, it collects information about its users to find out which banking applications they use, and it disables some security features of the device. The launch of the second stage is based on the information gathered in the first step.

When some conditions are met, our analysis revealed that the dropper installs Vultur, an advanced kind of malware that mostly targets online banking interface to steal users' credentials and other critical financial information.

More details about this real case in this article.



# SPYWARE: A SPY IN YOUR POCKET?

Always within reach, a smartphone carries almost all the data related to a person: location, contacts, credit card data, passwords, photos, calendar, conversations... When sold on the dark web, this information can be very lucrative for hackers, and they are aware of it. For this reason, an increasing number of cybercriminals target mobile devices with advanced techniques.

According to a survey conducted by Pradeo in February 2022, almost half of mobile users believe that spyware is the main cyber threat on mobile devices. Our analysis confirms this feeling: One in five mobile devices (22%) contains at least one application that exfiltrates its user's data, without it being necessary to run properly.

There are two types of spying on mobile devices. The most common type is carried out daily and on a large scale through mobile applications that excessively collect data from their users and pass it on to global corporations that want to know everything about their advertising targets. The second type, the rarest, consists in harvesting information from a specific target, through a combination of advanced hacking techniques. Pegasus belongs to this second type.

**1 mobile in 5 host a spyware**

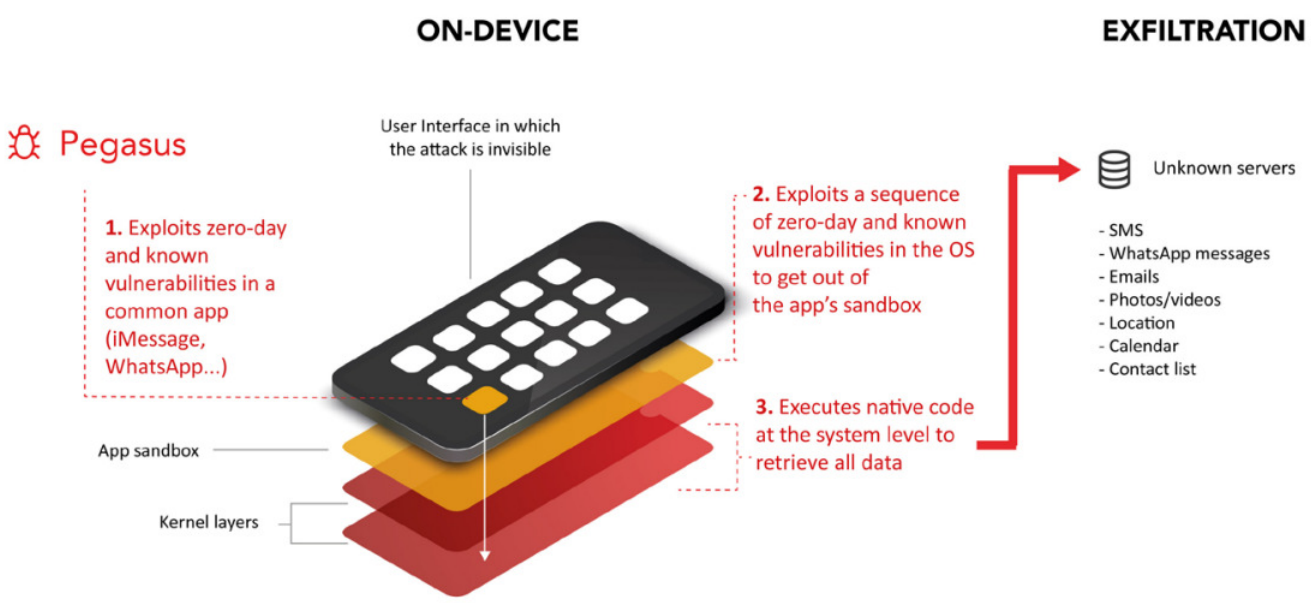
## Real life case study: Pegasus

To compromise high-value targets, the Pegasus spyware exploits vulnerabilities in common apps such as iMessage, FaceTime, Safari, WhatsApp, etc. that have a web module (WebKit, WebView…) to silently reach invisible and unclassified dynamically generated URLs.

The reached pages then execute JavaScript code to exploit vulnerabilities to get out of the applications' sandboxes, hence bypassing all mechanisms in the Android and iOS systems.

Once in the kernel layers, Pegasus exploits a sequence of zero-day and known processor vulnerabilities to execute arbitrary code (Arbitrary Code Execution) without requiring the system to be rooted or jailbroken.

The code is directly loaded into the RAM and not as an application, making it tricky to be detected. After achieving all these steps, Pegasus massively exfiltrates users' data, including encrypted ones (WhatsApp, Signal, Telegram conversations...).



# CLONES AND FAKE APPLICATIONS: A LUCRATIVE BUSINESS

Worldwide, more than 700 websites currently operate as application stores that offer copies of official apps. Third-party app stores are in such high demand that in 2020, three of them were more prolific than Google Play and the App Store in terms of new apps uploaded each year (source: RiskIQ).

Modified applications, also called MOD, are copies of original applications to which changes are made by third-party developers to add features or unlock premium subscription. During the tampering, most of MODs are injected with malicious code to spy on users by accessing their gallery, contact list, digital wallets, etc…, exfiltrate their data and display untimely ads. For the company whose identity is impersonated, the negative image impact is significant and often difficult to counter.

**41% of applications are vulnerable to code injection**

Pradeo has identified numerous copies of official applications that under the guise of offering free-of-charge use of Netflix, Spotify, ExpressVPN, Avira Antivirus, The Guardian, etc., infect mobile devices with malware, spyware and adware unbeknownst to their users.

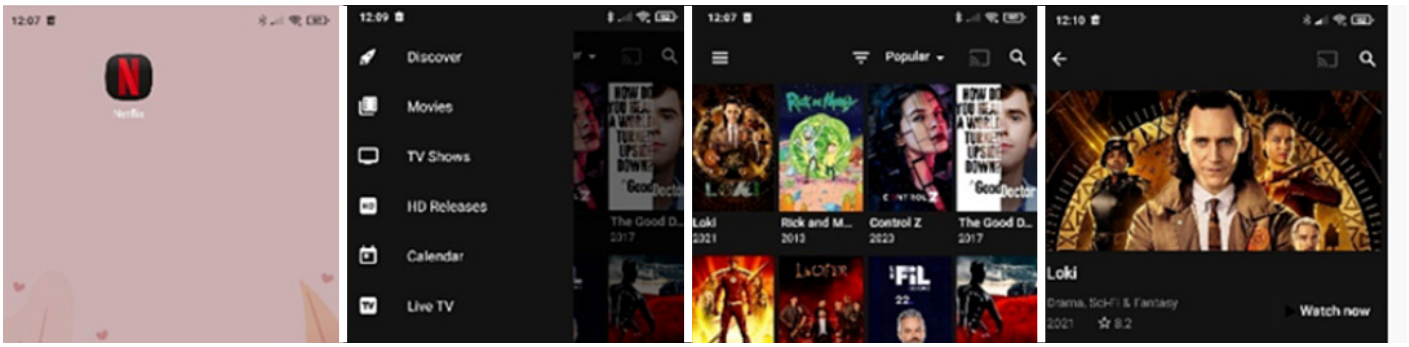
Code vulnerabilities and a lack of good security practices make it easy for hackers to copy and inject code into mobile applications. By impersonating well-known applications, counterfeit apps trick users into stealing their personal information and committing various frauds.

## Real life case study: Netflix

Our team has identified online hundreds of modified versions of the original Netflix application. More than simply impersonating the company's name and/or logo, the interface of the fake Netflix apps we found look nearly the same as older versions of the original Netflix app.

When performing a security analysis of these fake apps with the Pradeo Security engine, it appears that they have been injected with malware, spyware and/or adware. Besides, the featured malicious programs (Remote-Access-Tool, smishing trojan, rootkit…) do not require a device with root access to breach it, hence maximizing its reach.

Comparing the official app's code to modified ones highlights that despite most folders and files being similar, some new content has been added. Looking deeper, we found new ad libraries, JavaScript code to reach external servers and commands to download new APKs onto the device (dropper).



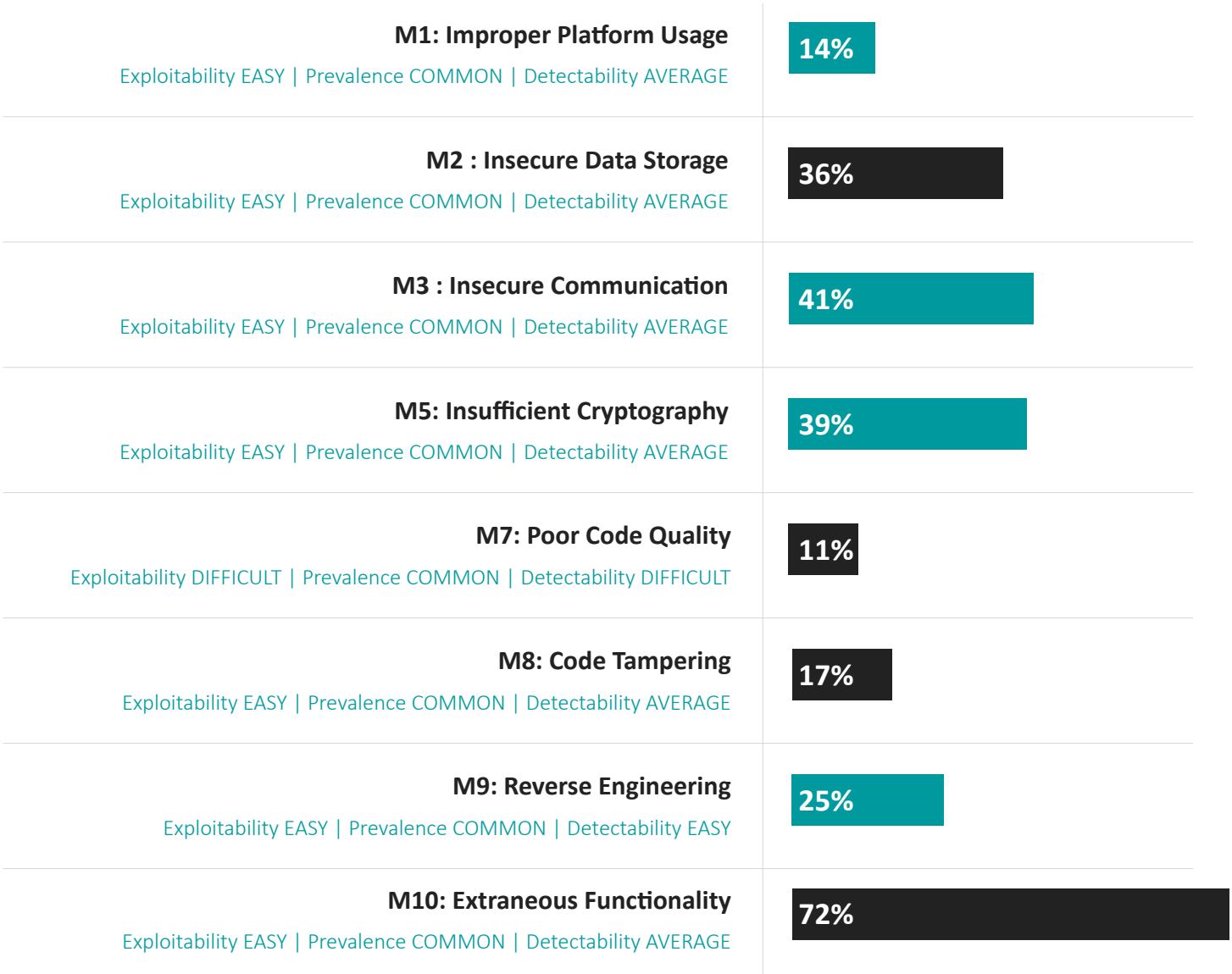
# TOP 10 OWASP MOBILE RISKS

The OWASP Foundation works to improve software security through projects, discussions and conferences led by a community of thousands of members around the world. To strengthen mobile app security, the collective released the Top 10 Mobile Risks in 2016, a public framework that developers and organizations can use to assess the reliability of their mobile apps before releasing them.

Our analysis engine, Pradeo Security, detects code vulnerabilities in mobile applications that expose them to the risks classified by OWASP. Today, even though this framework is widely known and shared, 74% of mobile applications distributed on Google Play are exposed to at least one of the OWASP Top 10 risks.

## 3/4 of mobile applications have a vulnerability identified in the OWASP Top 10

Top 10 OWASP mobile risks



# PHISHING FOR INFORMATION IS GROWING

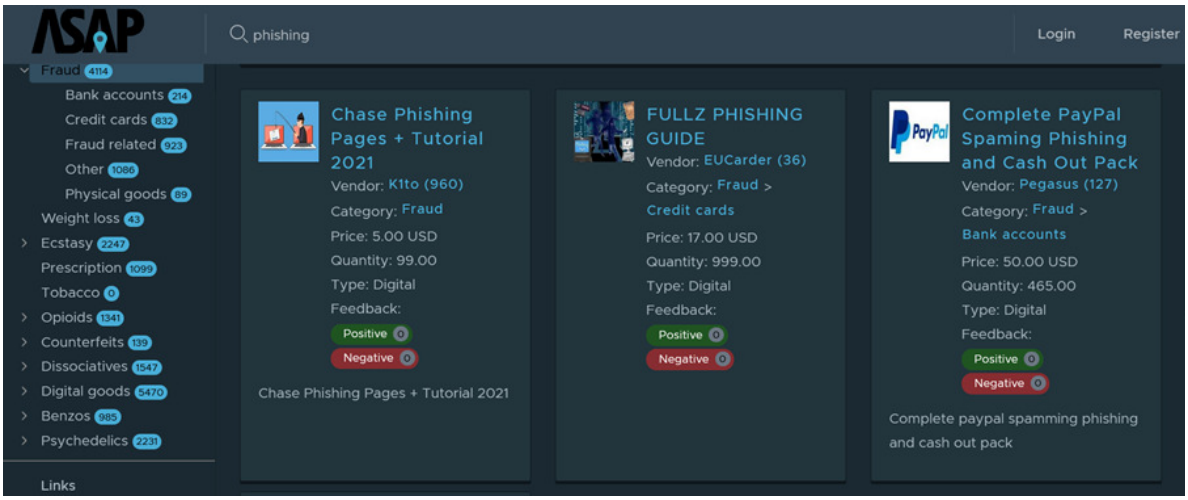
Phishing is a scam technique that coaxes users, usually by impersonating a trusted person or website, into providing personal information.

According to a February 2022 general survey conducted by Pradeo, 27% of respondents consider phishing as the threat they are most exposed to on their mobile. A few years ago, not many of these respondents were aware of this attack, but today its prevalence on mobile makes it difficult to avoid.

In 2021, the average employee received 13 emails or text messages containing a link to a phishing site on their mobile device used for work. This technique is used in large-scale attack campaigns, but also in targeted attacks called spear phishing.

On the dark web, ready-to-use phishing kits are for sale for negligible amounts and enable hackers to mainly target customers of financial institutions such as Chase or Paypal (see screenshot below). Offers to create malicious websites are also available.

An employee is targeted by **13 phishing attempts** per year on their work mobile




# MITRE ATT&CK®: SPECIFIC RISKS ON MOBILE DEVICES

The Mitre corporation references in its MITRE ATT&CK for Mobile matrices the tactics and techniques used by hackers to corrupt mobile activities. The information they provide can be used to test defenses, identify potential gaps and strengthen a mobile security strategy.

Ideally, an organization with a mobile fleet should have implemented solutions that can detect, prevent and respond to the elements identified in the MITRE ATT&CK for Mobile matrices.

Contact us for a complete list of the MITRE ATT&CK for Mobile matrix techniques detected by Pradeo.

| | | |
|---|---|---|
| **Persistance** | **39%** | Foreground persistence |
| | **2.27%** | Modify trusted execution environment |
| **Defense Evasion** | **0.85%** | Delete device data |
| | **0.63%** | Device lockout |
| | **27%** | Supress application icon |
| | **1.68%** | Uninstall malicious application |
| **Credential access** | **51%** | Access stored application data |
| | **2%** | Capture SMS messages |
| **Discovery** | **45%** | Location tracking |
| **Collection** | **2%** | Access call log |
| | **26%** | Access contact list |
| | **51%** | Access stored application data |
| | **27%** | Capture audio/camera |
| | **2%** | Capture SMS messages |
| | **45%** | Location tracking |
| **Exfiltration** | **4.20%** | Data encrypted |
| **Impact** | **0.85%** | Delete device data |
| | **0.32%** | Device lockout |
| | **0.62%** | SMS control |
| **Network-Based effects** | **4%** | Eavesdrop on insecure network communication |
| | **0.54%** | Manipulate device communication |
| | **0.03%** | Rogue cellular base station |
| | **6%** | Rogue Wi-Fi access points |

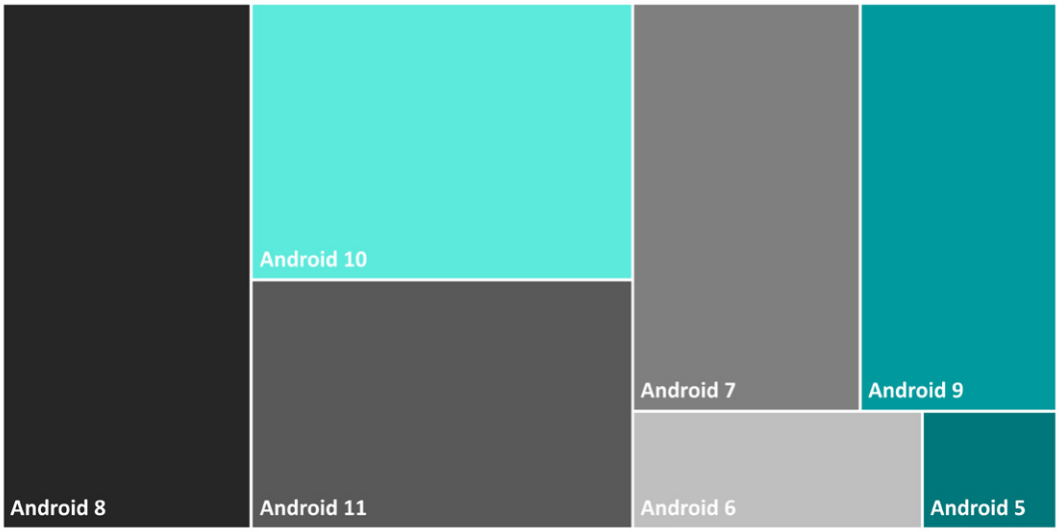
# OUTDATED OPERATING SYSTEM: AVOIDABLE LOOPHOLES

On a regular basis, security holes are discovered in the code of operating systems. Once detected, OS publishers develop patches that they push to users through updates and simultaneously disclose the vulnerabilities (CVEs) existing in the former version. Once made public, cybercriminals can exploit outdated devices' vulnerabilities to gain extended rights and illegally access data or communications.

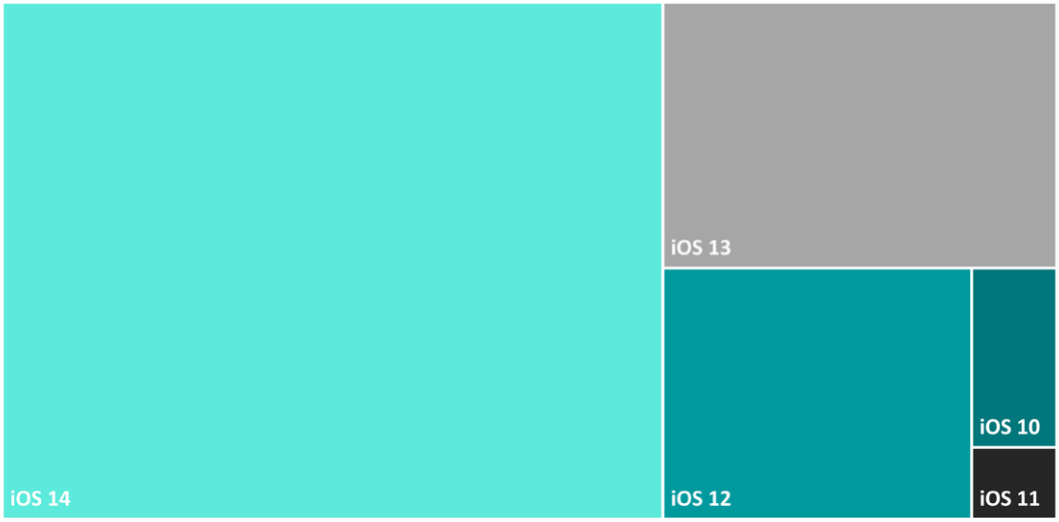
**81%** of iOS devices and **82%** of Android devices use outdated OS versions

Among organizations' mobile fleets, 81% of iOS devices and 82% of Android devices are running outdated OS versions, for various reasons. Most often, users are unaware of the risks involved in delaying system updates and do not activate them to save time. Sometimes, mobile devices are not of the newest generation and their models do not support the new versions. And finally, there are cases in which administrators may hold back updates for organizational reasons, such as with Android 10, which was often delayed because it came with the obligation to move to Android Enterprise.

Repartition of Android versions




Repartition of iOS versions



# UNIFIED MOBILE SECURITY WITH PRADEO

## Pradeo, global leader of mobile security.

The company ensures the protection of all mobile usages, by offering services dedicated to securing smartphones, tablets and mobile applications.

Pradeo's cutting-edge AI-based technology, Pradeo Security, is **recognized** as one of the most advanced mobile security technologies **by Gartner, IDC, Frost & Sullivan and Forrester**. It provides a reliable protection from mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

Pradeo counts Governments, public administrations and Fortune 500 companies from various industries among its clients. Along the years, Pradeo has developed strong relationships with enterprise mobility leaders (Microsoft, BlackBerry, IBM, Samsung, VMware...) through advanced integrations and joint solutions.


## Pradeo Security answers the following use cases:

- **Protect collaborators' mobile devices:** A Mobile Threat Defense solution that ensures a multilayer and real-time protection of mobile devices (COPE, BYOD, Android, iOS…).
- **Provide secure mobile services to collaborators using non-managed devices:** A Secure Private Store offer to safely distribute mobile services to BYOD devices, without requiring managing them.
- **Ensure mobile applications' security level:** A Mobile Application Security Testing tool providing visibility on applications' behaviors and vulnerabilities, in one click. Comes as a ready to use web platform or an API to integrate within developers' interface.
- **Protect mobile applications' data and transactions:** A security module (SDK) to integrate within mobile applications to protect them from threats operating on users' device.

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