2024

# GLOBAL MOBILE THREAT REPORT

The Rise of a Mobile-First Attack Strategy

ZIMPERIUM®

# Table of Contents

**Executive Summary** **2**
**The Enterprise Mobile Footprint** **4**
**Global Threat Landscape** **8**
Key Stats 8
Top Threats By Platform 8
Top Threats in Public Sector 9
Top Threats in the Private Sector By Vertical 9
Top 3 Drivers 10
**Threats Enterprises Must Prioritize** **11**
From Phishing to Mishing! 11
Industries Targeted by Phishing 15
**Mobile Malware: Advanced Attacks** **15**
Malware Families by Region 17
Unsecured Networks 18
**The Sideloading Saga** **20**
Why Sideload Apps 20
Sideloaded Malware Family Distribution 21
Sideloaded App Attack Chain on Android 21
Sideloading on iOS 21
**Application Vetting** **23**
Third-Party Work Apps 23
Where is my enterprise data going? 23
Is the app asking for dangerous permissions? 24
Does the app have secure communication? 25
In-House Developed Apps 26
Are the apps easy to reverse-engineer? 26
Is the Third-party code safe? 27
Personal Apps From Public Stores 28
Apps Removed From Stores 28
Personal VPN Apps 31
Platform & OS Vulnerabilities 32
**Conclusion** **34**
**Sources** **35**
**About Zimperium** **36**

# Executive Summary

**The exponential growth of mobile devices including mobile phones and tablets that have access to critical business applications and data has empowered and enabled workers and enterprises across the world. However, evidence shows that security controls and policies have not kept pace with the evolving threat that this may pose. More than half of organizations(54%)in a recent study experienced a data breach[1] due to employees' inappropriate access to sensitive and confidential information on their mobile devices. It seems that cybercriminals and other bad actors have recognized the opportunity that lies within this new mobile-focused environment.**

**82%**

of organizations allow BYOD

Organizations continue to strike a balance between Bring Your Own Device (BYOD) and Corporate-Owned, Personally Enabled (COPE). According to Samsung about 15% of businesses issue mobile devices to all employees, while 39% of companies rely fully on a Bring Your Own Device (BYOD) approach.[2] The remaining 46% of businesses take a hybrid approach, providing devices to some employees while allowing others to use their own. This dual use, however, presents a high risk of data exposure and enterprise infiltration due to the sophistication of mobile threats today which are beyond the capabilities of traditional MDM and MAM solutions. Employees increasingly expect the flexibility to use mobile devices for work, while businesses seek to maintain control over corporate data.

The ubiquitous nature of mobile applications on enterprise devices exacerbates this complexity. This enterprise app footprint comprises apps developed in-house or from a third-party and personal apps installed from the public store. Enterprise apps can be for employees, partners, or customers. Having both enterprise and personal apps on the same device create unique security risks. Enterprise apps often handle sensitive corporate and customer data and may have vulnerabilities, particularly third-party apps. Personal apps downloaded from public app stores can introduce malware or exploit platform vulnerabilities, potentially compromising enterprise apps and in-app data.

Over 40,000 applications from these groups were reviewed, and the top violations were Insecure Communication (76%) and Insecure SSL/TSL (27%) on iOS. On Android, Leaky Storage (53%), Insecure Communication (59%), and Dynamic Data Leakage (31%) are major security issues.

*All statistics in this report, unless otherwise noted in a footnote, are from Zimperium Labs research.

Contrary to perception, app stores are not responsible for preventing every malicious app from getting in or protecting apps from abuse. With more than 300 public app stores, 1,300 device manufacturers, and constant OS updates, enterprise mobile device risk postures become very dynamic. Because so few enterprises prioritize the security of mobile apps and devices, this becomes the attack surface of choice.

Recognizing these vulnerabilities, attackers have adopted a **"mobile first" attack strategy** as mobile presents a large, unsecured, and unmanaged attack surface for entry to the network and to corporate data.

**Mishing (Mobile-Targeted Phishing Attacks)** - **83%** of phishing sites specifically targeted mobile devices

**Application Vulnerabilities** saw a surge in privacy vulnerabilities around data storage, privacy controls and app supply chain security[3]

**Mobile Malware** - unique malware samples increased by **13%** over the previous year

**Sideloaded Apps** - threats from sideloaded apps are dominated by riskware and trojans (which total **80%** of observed malware)

OS

**Platform Risks** - **14%** of Android devices and 1% of iOS devices monitored in today's enterprises cannot be upgraded, leaving them susceptible to exploitation

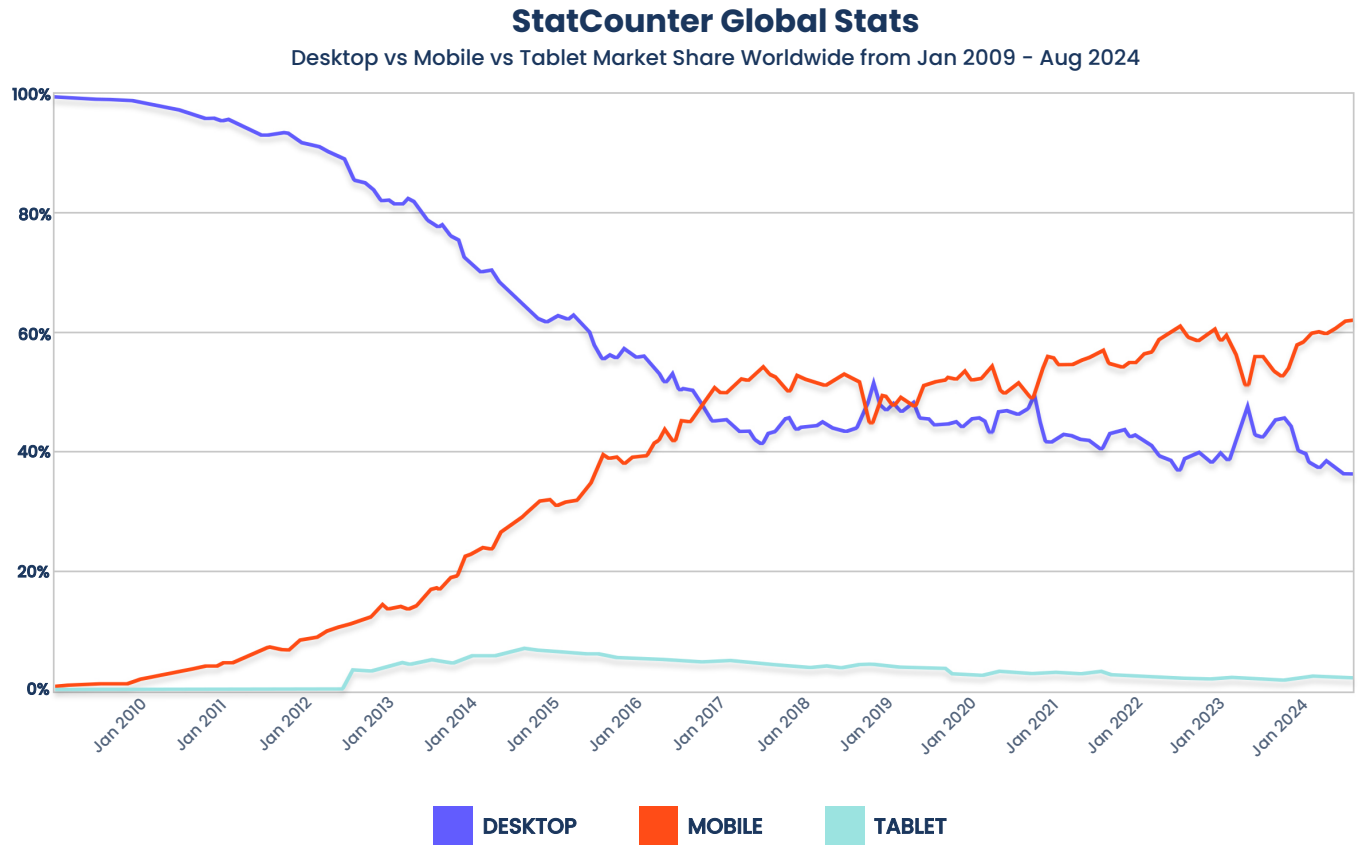
Concentrating on these key areas allows enterprises to take decisive steps to neutralize the most significant risks and protect their mobile environments from risks, threats, and attacks.

# The Enterprise Mobile Footprint

## Enterprises are more mobile than ever

As of 2024, there are approximately **6.8 billion smartphone users** worldwide. If we include all mobile devices—such as tablets, feature phones, and wearables—the number exceeds **16 billion connected mobile devices globally**.[4] This figure reflects a world where many people own multiple mobile devices and where the internet of things (IoT) is increasingly integrated into daily life. According to IDC,[5] nearly 60% of the U.S. workforce today are mobile, frontline workers -- employees who don't require a desk or an office to do their work. This estimate includes both corporate-issued devices and personal devices used for work purposes, as the majority of organizations believe that mobile is critical to enhancing worker productivity and fostering business growth. As a result, mobile workforces, remote work, and enterprise mobility initiatives have grown exponentially, allowing mobile devices to access more data and interact with more enterprise systems every year.

In addition to smartphone's very large global use footprint the devices possess more processing power than most of today's PCs and are more powerful than mainframe computer NASA used to send astronauts to the moon.[6]



## The number of apps has exploded.

Today, the work app footprint in enterprises is comprised of in-house developed apps, third-party applications, and personal apps on work devices.

There are now around 1,889,653 Apple iOS applications, and 3,466,806 Android apps within their respective app stores. Add in the other 300 or more non-official stores and these numbers get even larger. A typical smartphone user has at least **80** mobile applications installed,[7] with anywhere between 5 to 11 of these being work apps pushed to their device by their employer.

These statistics provide a better understanding of how much our personal devices are used for work.

- **71%** of employees leverage smartphones for work tasks.
- Over **60%** of employees use their smartphones for work-related communication.
- **48%** of employees use their smartphones for accessing work-related information.

Adopting mobile apps has tangible benefits, but enterprises should ask if they are really built to protect their employees, sensitive data, and infrastructure. We analyzed over 40,000 of the most famous work and non-work categories and apps to help get insights into this question. Let's look at the data.

### Table 1 - iOS - Avg. Number of Violations per Application

| App Category | MASVS | GDPR | NIAP | PC | HIPAA |
|---|---|---|---|---|---|
| business | 18 | 17 | 8 | 5 | 9 |
| medical | 19 | 17 | 8 | 5 | 9 |
| financial | 20 | 18 | 9 | 6 | 9 |
| productivity | 16 | 14 | 7 | 5 | 8 |
| travel | 19 | 20 | 8 | 6 | 9 |
| Developer tools | 14 | 10 | 5 | 4 | 6 |
| Social networking | 20 | 19 | 8 | 6 | 10 |
| dating | 19 | 19 | 8 | 6 | 9 |
| entertainment | 17 | 16 | 7 | 5 | 9 |
| shopping | 21 | 19 | 9 | 6 | 9 |
| utilities | 17 | 15 | 7 | 5 | 9 |
| gaming | 23 | 20 | 9 | 8 | 13 |

## Table 2- Android - Avg. Number of Violations per Application

| App Category | MASVS | OWASP | NIAP | PCI | GDPR | HIPAA |
|---|---|---|---|---|---|---|
| communication | 24 | 21 | 9 | 5 | 11 | 5 |
| shopping | 27 | 24 | 11 | 5 | 13 | 6 |
| financial | 26 | 22 | 12 | 5 | 12 | 5 |
| business | 24 | 21 | 10 | 5 | 11 | 6 |
| medical | 25 | 22 | 10 | 5 | 11 | 5 |
| dating | 26 | 22 | 12 | 5 | 14 | 5 |
| gaming | 25 | 23 | 9 | 5 | 12 | 5 |
| Developer tools | 20 | 18 | 6 | 4 | 8 | 5 |
| travel | 26 | 22 | 10 | 5 | 12 | 5 |
| utilities | 23 | 19 | 8 | 4 | 9 | 5 |
| social networking | 25 | 22 | 10 | 5 | 12 | 5 |
| productivity | 24 | 20 | 9 | 4 | 10 | 5 |
| entertainment | 24 | 21 | 9 | 4 | 10 | 5 |

These frameworks and regulations—**MASVS, OWASP, NIAP, PCI, GDPR,** and **HIPAA**—serve as important security and privacy standards across different industries and regions. Running apps that violate security frameworks like MASVS, OWASP, PCI, GDPR, or HIPAA on enterprise devices exposes businesses to severe risks. These include cyberattack vulnerabilities, significant non-compliance fines, data breaches, and privacy violations. Financial penalties, reputational damage, and operational disruptions can follow, particularly when sensitive customer or financial data is compromised.

With the continued rise of no-code/low-code development approaches, developers will look to build cloud-native apps up to 10 times faster than traditional coding while using up to 70 percent fewer resources. However, focusing on speed often means that best security practices are overlooked or improperly implemented. This could lead to more exploitable apps being deployed into production without the proper app protections and security testing, increasing the likelihood of data breaches and compromised systems.

## How Prepared Are You for Mobile Risk

Mobile devices and their app footprint make them an easy target for attacks and require an effort to secure them. Use of the same device for work and personal use is not new. This has been the case for desktop and laptop computers for decades but mobile is different.

### HERE IS WHY:

1. The devices are **controlled by the end-user,** not the enterprise IT team. You can't really lock them down or force the user to update software on their device.
2. There are an unlimited combination of mobile device hardware and operating systems out there. So each mobile device has a different risk posture.
3. 85% of the apps on the device are personal apps and they all impact the risk exposure to the enterprise.

Unlike traditional endpoints like desktops or laptops, mobile devices operate in a **constantly shifting environment**, they are constantly exposed to unsafe networks—public Wi-Fi, harmful apps, and phishing links, malware etc —exposing the enterprise to a variety of potential threats.

The question becomes:

***Can your current security framework handle this diversity and unpredictability?***

# Global Threat Landscape

All statistics in this report, unless otherwise noted in a footnote, are from Zimperium Labs research.

## Key Stats

### Network

- The number of unsecured networks detected increased by **36%**.
- The number of devices connecting to unsecured networks increased by **45%**.
- The number of devices connecting to a rogue access point has increased by **100%**.

### Phishing

- **82%** of phishing sites are adapted to mobile.
- **76%** of phishing sites are using HTTPS.
- **40%** of phishing sites detected in 2023 used the .dev domain.

### Malware

- **1 in 4** protected devices worldwide encountered malware.
- We detected over 87K malware a month. **13%** increase Y-o-Y.
- **80%** more spyware samples detected on enterprise devices. Most not known by the industry.

### Platform

- **80%** of iOS versions in 2023 were actively exploited at some point.
- **15%** of devices running a vulnerable or non-upgradeable Android version.

## Top Threats by Platform

### Android

- **28%** Sideloaded Apps
- **18%** Vulnerable Non-upgradable Android Version
- **15%** Passcode Not Enabled
- **12%** Malware
- **6%** Malicious Websites

### iOS

- **27%** Passcode Not Enabled
- **24%** Sideloaded App
- **19%** Vulnerable Non-upgradeable
- **11%** Unsecured Wi-Fi
- **9%** Captive Portal

## Top Threats in U.S. Public Sector

**Federal, State & Local Governments**

1. Unsafe Networks - **57%**
2. Phishing - **10%**
3. Passcode Not Enabled - **3.5%**

## Top Threats in the Private Sector By Vertical

**Automotive**

1. Mishing - **13%**
2. Passcode Not Enabled - **9%**
3. Vulnerable Non-upgradable Android - **8%**
4. Sideloaded Apps - **7%**

**Communications**

1. Unsafe Networks - **24%**
2. Vulnerable and Non-upgradeable Android - **6%**
3. Sideloaded Apps - **1%**

**Consulting**

1. Sideloaded Apps - **28%**
2. Vulnerable and Non-upgradeable - **7%**
3. Risky Device Setting - **7%**

**Consumer Goods**

1. Unsafe Networks - **51%**
2. Sideloaded Apps - **5%**
3. Passcode Not Enabled - **2%**
4. Vulnerable and Non-upgradeable - **4%**

**Energy & Utilities**

1. Unsafe Networks - **45%**
2. Unsecured Wi-Fi - **36%**
3. Mishing - **26%**

**Financial Services**

1. Sideloaded Apps - **68%**
2. Unsecured Wi-Fi - **11%**
3. Passcode Not Enabled - **2%**
4. Mishing - **2%**

**Healthcare**

1. Unsafe Networks - **50%**
2. Mishing - **39%**
3. Sideloaded Apps - **1%**

**Higher Education**

1. Unsafe Networks - **81%**
2. Mishing - **5%**

**Information Technology**

1. Unsafe Networks - **68%**
2. Sideloaded Apps - **15%**
3. Vulnerable and Non-upgradeable - **4%**
4. Mishing - **4%**

**Manufacturing**

1. Unsafe Networks - **86%**
2. Mishing - **2%**

**Retail**

1. Mishing - **48%**
2. Unsafe Networks - **4%**

## Top 3 Drivers

1

**BYOD - Personal Devices For Work**

Nearly 67% of employees use personal devices for work,[8] regardless of whether their company has a formal bring-your-own-device (BYOD) policy. Alarmingly, 70% of businesses fail to adequately secure personal devices used for work purposes.[9] This lack of security likely increases the actual risk, reinforcing the belief held by 55% of professionals that smartphones are the most exposed endpoints in their organization.[10]

2

**Cyber Hygiene is Poor on Mobile Devices**

User behavior often blurs the lines between work and personal activities, increasing the chances of breaches when checking personal messages or emails on a work device or using unsecured Wi-Fi networks. Notably, 71% of employees admit to engaging in actions they knew were risky.[11] As noted above, Zimperium research found **15% or more of employees do not have a passcode enabled on their mobile devices**.

3

**AI-Powered Bad Actors**

Bad actors increasingly leverage artificial intelligence (AI) to discover new attack surfaces and vulnerabilities, rapidly adapting their techniques to enhance attacks on mobile devices that access enterprise networks.

Some of the most common uses of AI-driven attacks include:

- Automatic tailoring of phishing vectors (QR code, websites, URLs etc)
- Automation of malware sample creation
- Mutation of malware samples to avoid detection
- Automatic tailoring of phishing emails and messages

# Threats Enterprises Must Prioritize

Despite the large number of mobile threats and risks, there are four that are paramount to tackle and doing so will reduce risk from the rest. The four most important threats are:

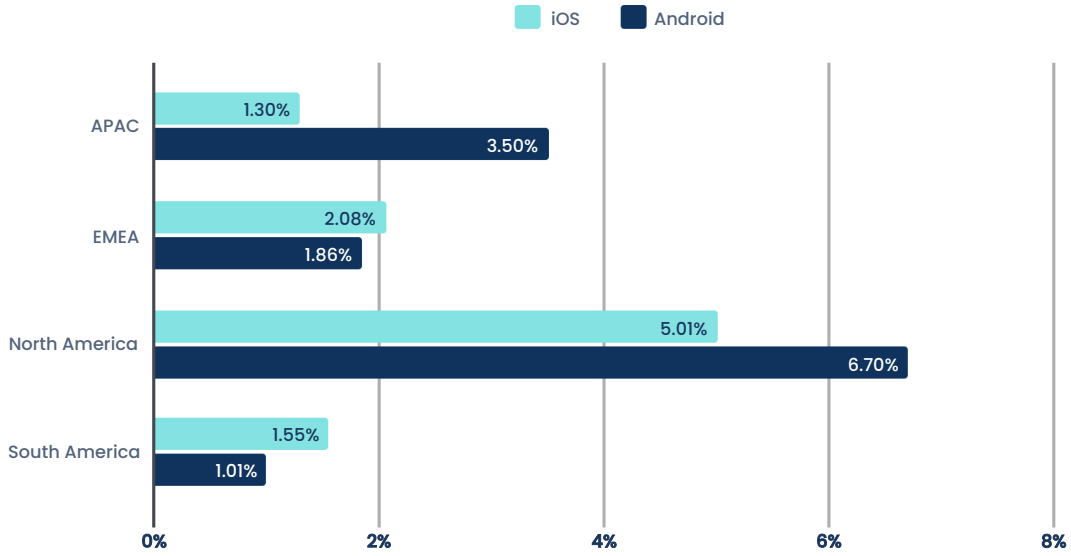
i. Mishing: Mobile-Targeted Phishing Attacks
ii. Mobile Malware
iii. Sideloaded Apps
iv. Application Vetting and Protection for your users mobile apps
v. Platform Vulnerabilities

Here is a detailed look at each threat so we can better understand how it works and how we can defend against it.

## From Phishing to Mishing!

In 2023, the Anti-Phishing Working Group reported nearly five million phishing attacks,[12] marking it the **worst year on record** and surpassing the 4.7 million attacks seen in 2022. Zimperium's zLABS threat data aligns with this trend, underlining the increasing sophistication of phishing sites. **Notably, 82%** of phishing sites examined by Zimperium specifically targeted mobile devices, delivering content formatted for mobile, reflecting a 7% increase over the last three years. **25%** of mobile users tapped on at least one phishing link every quarter in 2019.[13]

Percentage of Devices that Encountered a Phishing Attack



This trend underscores the growing number of phishing attacks targeting mobile users. Compared to desktop systems, mobile devices often have fewer security measures in place. Users may not install security software or be less likely to notice phishing attempts due to smaller screen sizes and less visible security indicators, such as hidden URL bars.

**76%** of phishing sites using HTTPS now employ this protocol. This can give users a false sense of security, leading them to believe the website is legitimate.

**79%** of credentials were harvested through phishing attacks.
Source: Egress

**50%** of phishing sites are detected within 72 hours of creation.
Source: Zimperium

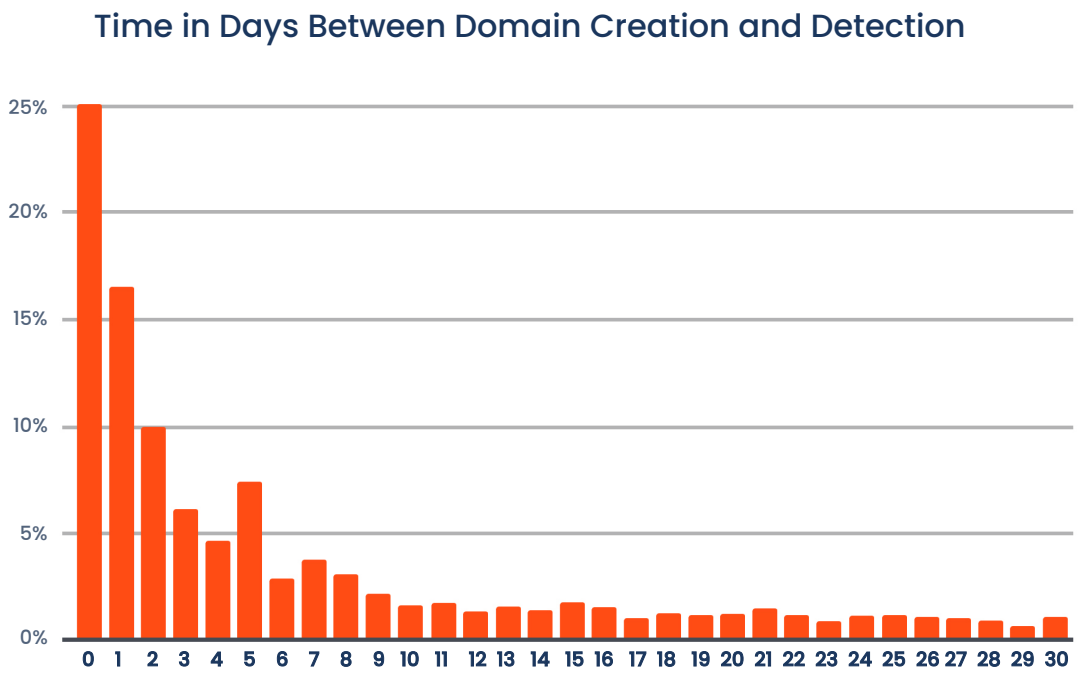
The four standard types of mobile targeted phishing attacks include **Mobile-Targeted Email Phishing, Smishing, Vishing** and **Quishing**. These four phishing attack methods go beyond tailoring emails to be deceptive on the small screens of our mobile devices. Three methods leverage the unique features of a mobile device: text/sms features (Smishing) , voice features (Vishing) and the fact that it is a camera enabled device (Quishing). The fourth, Mobile-Targeted Email Phishing consists of an attack that is launched via a standard email message, but only executes when a link (or attachment) is clicked by the user from a mobile device. If clicked from a standard endpoint device such as a laptop, the attack is aborted.

Hence a new name is needed that covers all four of these phishing methods:

**Mishing!**

## The Struggle to Keep Up with Phishing

Phishing sites exemplify a hit-and-run approach in the digital threat landscape. These deceptive domains are notorious for their rapid setup and equally swift disappearance, creating significant challenges for cybersecurity defenses. Moreover, Zimperium reports that around one-quarter of **phishing sites become operable less than 24 hours after their creation**, launching malicious activities almost immediately. This quick deployment enables cybercriminals to reap substantial rewards in a short time frame before the site vanishes or is taken down by authorities.




Following the trend of previous years, the US continues to lead the top countries hosting phishing sites, accounting for 84% of such sites. This does not imply that most phishing attacks originate from the US but rather that attackers are leveraging its infrastructure, such as hosting services or new types of top-level domains, to carry out these activities.

Understanding this fast-paced lifecycle is key to developing countermeasures and protecting sensitive information from being harvested. Attackers operate incredibly quickly and precisely, hooking their prey and reaping the rewards as stolen credentials quickly lead to account takeovers.

Addressing this problem on mobile demands a reevaluation of current approaches and the exploration of more dynamic and proactive measures.

Potential strategies might include:

- **Enhanced Detection Speed:** Leveraging on-device detection techniques to identify phishing domains before they are clicked on.
- **Real-Time Blocking:** Implementing systems that update URL blocking/filtering in real-time, minimizing the window during which sites can be accessed.
- **Public Awareness and Education:** Increasing efforts to educate employees about the risks of phishing attacks and how to recognize suspicious links, reducing the success rate of such attacks.

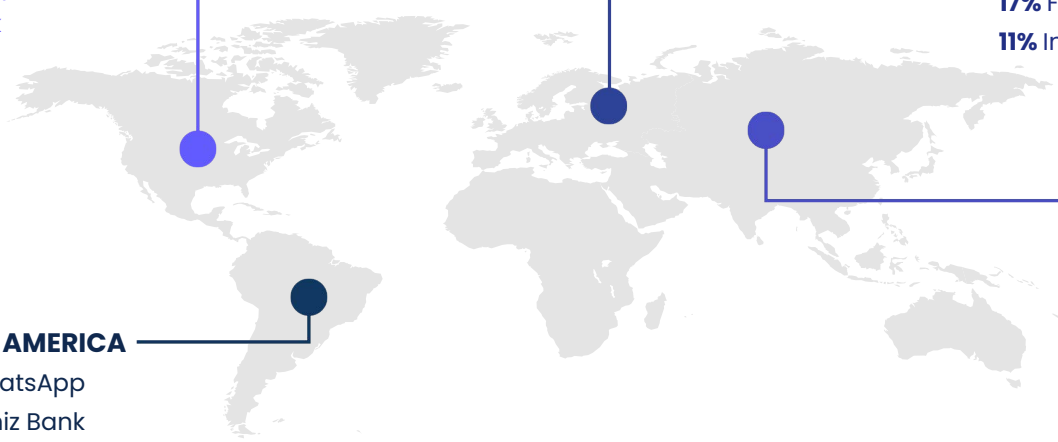
**Phishing ranks as the second most expensive attack, costing organizations an average of $4.76 million USD per incident.** [14]

## THE MOST PHISHED BRANDS GLOBALLY

Most Imitated Brands:

- **23%** Microsoft 365
- **15%** facebook
- **5%** Aviation
- **5%** WhatsApp
- **4%** Apple

## BRANDS PHISHED BY REGION



**NORTH AMERICA**
**57%** Microsoft
**13%** WhatsApp
**6%** Facebook

**EMEA**
**37%** Gazprom
**17%** Facebook
**11%** Instagram

**APAC**
**26%** Bet365
**14%** Facebook
**13%** Garena

**SOUTH AMERICA**
**33%** WhatsApp
**10%** Deniz Bank
**9%** Facebook

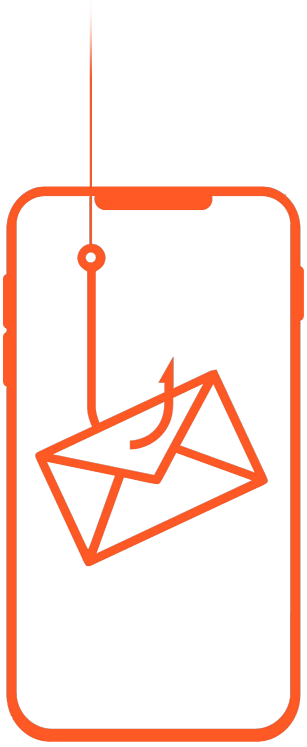
### Industries Targeted by Phishing

No industry is immune to the insidious threat of phishing attacks. Zimperium threat data revealed the healthcare industry experienced the highest number of threats in 2023, with a staggering 39% of its mobile threats attributed to phishing attacks.

**39% HEALTHCARE**

**4.2% HIGHER EDUCATION**

**2% MANUFACTURING**



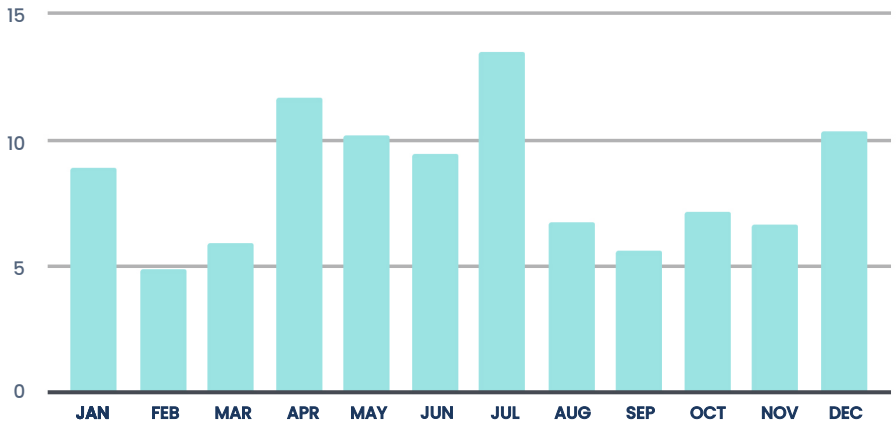
According to the World Economic Forum,[15] the increase in mobile-connected devices and AI-driven cyberattacks are key factors contributing to the growing vulnerability of critical infrastructure. The proliferation of mobile devices and their use in accessing essential services make them prime targets for ransomware,[16] leading to significant disruptions in critical sectors like healthcare, energy, and transportation.

# Mobile Malware: Advanced Attacks

Think you've got mobile malware under control? Think again. With its widespread accessibility and immense scale, malware has become the weapon of choice for nearly every cybercriminal. Mobile malware rapidly spreads and extensively disrupts systems, with millions of unique variants and new malicious apps emerging daily. According to a recent survey, when asked about their primary cybersecurity concerns, **41% of CISOs cited malware**, while 32% expressed concern about ransomware. (Pulse).

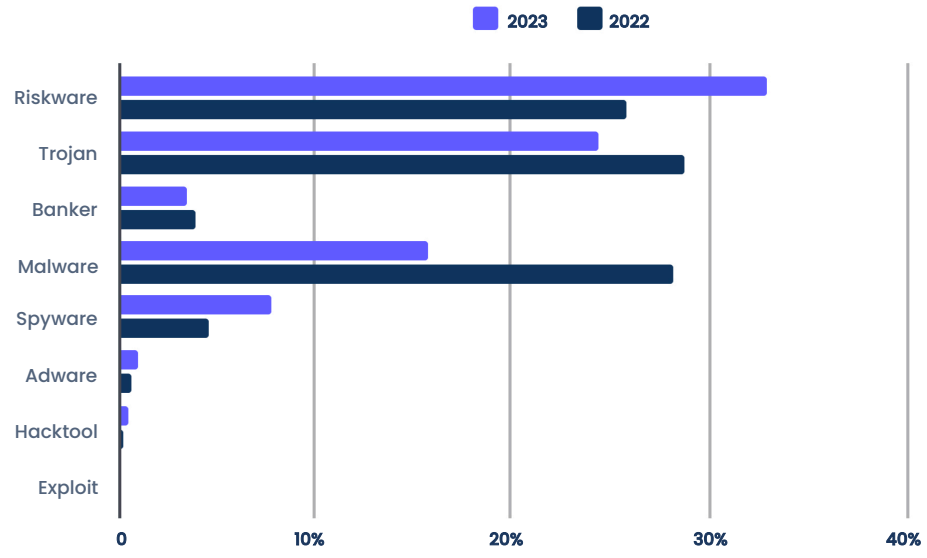
**Zimperium researchers analyzed over 859k malware samples detected in the wild.**
On average, that equates to over 16,500 new malware samples a week. Remarkably, 72% of the malware samples were completely unknown at the time of detection (not known to the free av engines), highlighting Zimperium's advanced capabilities in staying ahead of the curve when it comes to malware identification and protection.

## Malware Detections by Month (2023)




In July 2023, Zimperium recorded the highest number of malware detections for the year, representing nearly 15% of all events for the year.

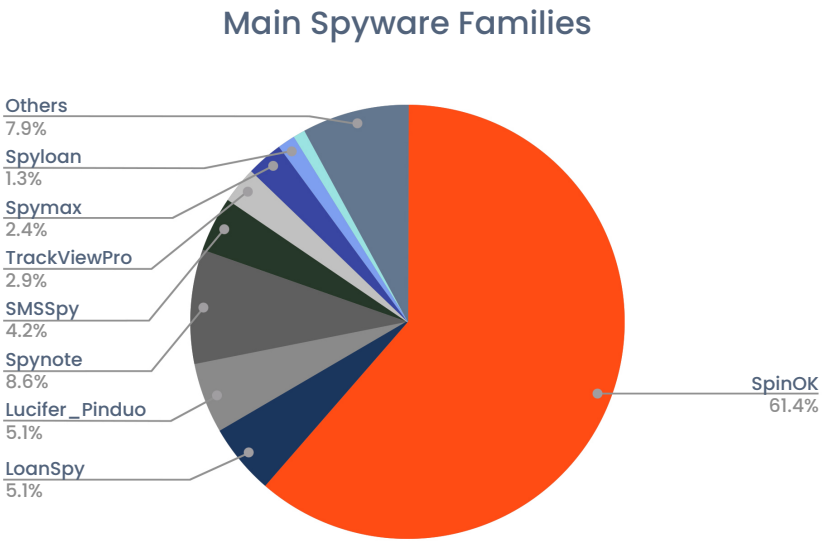
## Malware Family Distribution



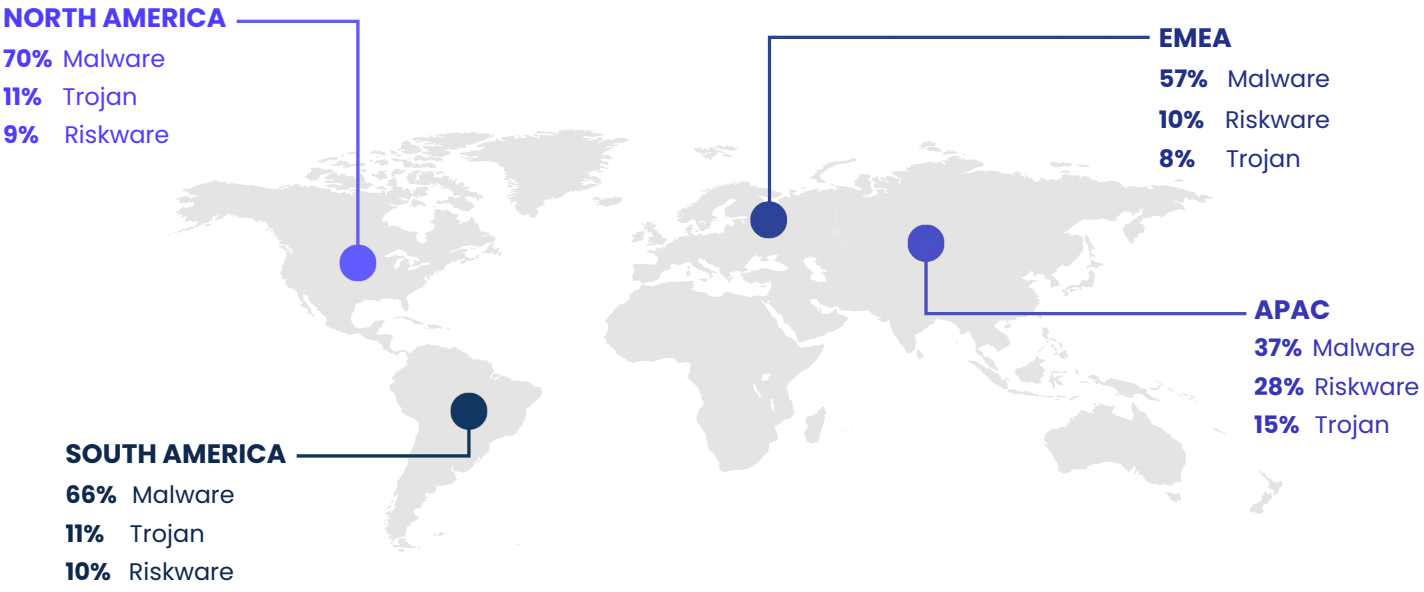

While the number of unique malware samples has risen by 13% since 2022, there has been a notable increase across the various malware families. Specifically, riskware and spyware have seen significant growth compared to other types of malware.

## WHAT IS RISKWARE?

It's a potentially vulnerable app.




## Malware Families by Region




General purpose malware is a global issue, with North America experiencing the highest impact, accounting for 70% of malware events. With one in twenty protected devices encountering malware in a year, extrapolating this means 15.5 million devices are affected by malware yearly.[17]

## Unsecured Networks

An unsecure network is a network that lacks adequate security measures such as encryption, making it vulnerable to unauthorized access and data interceptions. Connecting to these networks is bad for business because it can lead to data exfiltration, resulting in financial losses, legal liabilities, and access to intellectual property.

In 2023, the **number of devices connected to unsecured networks increased by 45%**. Zimperium found that on average, a mobile device connects to a risky network 17 times in the span of a year. Additionally other reports indicate that around 35% of individuals access public WiFi three to four times a month and **four in 10 have had their information compromised while using public WiFi**. This highlights that public WiFi is frequently used as a last resort when a cell connection is unavailable, allowing people to stay connected for leisure and work purposes.

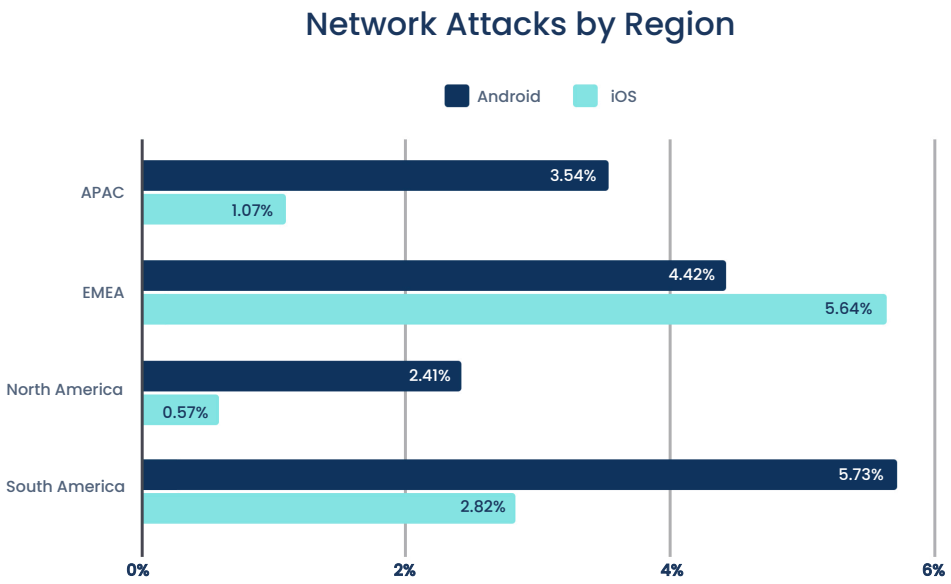
Using public Wi-Fi while traveling poses a higher risk to online security compared to usage at fixed locations. Among respondents who had their online security compromised while using public Wi-Fi, the highest percentage—23%—reported that these incidents occurred at the airport.[18]

**Only 5% of individuals think public WiFi is completely unsafe, suggesting a need for more information and resources to help make informed decisions about using these unsafe networks.**[19]

Attackers can easily intercept traffic through man-in-the-middle (MitM) attacks or lure employees into using rogue Wi-Fi hotspots; it means they exploit vulnerabilities in network security to gain unauthorized access to data being transmitted between devices and networks. **Zimperium identified that 33% of network threats are MiTM**. In a MiTM attack, an attacker secretly intercepts and possibly alters the communication between two parties they believe are directly communicating with each other.

# Network Attacks by Region

With the rise of cloud-based services for mission-critical tasks, mobile devices have become indispensable for business operations. Zimperium threat data shows that Europe, the Middle East, and Africa (EMEA) experience the highest number of network attacks, with nearly 6% of iOS devices and 5% of Android devices encountering such threats.




## An Early Warning Sign for Imminent Threats

Zimperium conducted a study on the security of Wi-Fi networks and rogue access points. The findings indicate that when devices connected to these unsecure or rogue networks, **it took less than ten minutes** for malicious activities, such as interception, unauthorized access, or the installation of malware to be detected on the devices. This highlights the risk associated with connecting to unsecured networks and the speed at which cyber threats can compromise mobile devices in such environments.

**Network detections in EMEA have quadrupled with malware occurring at nearly double the rate.**

(Radar.cloudflare) (WatchGuard)

# The Sideloading Saga

Sideloading is the practice of installing mobile apps on a device that are not from the official app stores. This is typically done on a rooted Android device or a jailbroken iOS device. With the blurring of personal and professional boundaries, sideloaded apps are increasingly showing up on personal devices used for work.

Zimperium's threat data shows that approximately one in four Android devices face this issue. While sideloading is much more prevalent on Android, the recent Digital Markets Act (DMA) is expected to increase its prevalence on iOS.

## Why Sideload Apps

With each sideloaded app, employees unknowingly expose their mobile devices or corporate ecosystems to vulnerabilities by bypassing standard app stores such as Google Play.

Here are some reasons why users choose unofficial store apps:

- To access apps unavailable in their region or banned.
- To unlock features that are otherwise restricted.
- To download free or cheaper games and movies.
- To engage in illegal activities like bypassing Digital Rights Management (DRM).

In the most severe cases, sideloading apps can lead to a **complete mobile device compromise,** granting remote attackers full control. This could enable threat actors to access sensitive user information, such as corporate information, credentials, or personal information, and impersonate the user for unauthorized access to banking accounts or other critical systems, among other potential consequences.

APAC outpaces all regions, with

**43%**

of Android devices sideloading apps.

### TOP 3 CATEGORIES OF SIDELOADED MALWARE

Riskware
**73%**

Trojan
**11%**

General Purpose Malware
**10%**

Researchers at Zimperium found that riskware and trojans are the most common malware families found in sideloaded apps. As riskware often includes potentially unwanted programs (PUPs) and adware, its high occurrence indicates a broader spectrum of threats beyond traditional malware. Additionally, trojans, known for their deceptive nature in disguising themselves as legitimate apps, present a persistent challenge in evading detection and compromising device security.

Our research indicates that globally, users who engage in sideloading are **200% more likely to have malware** running on their devices than those who do not. In fact, sideloading is a great contributor to malware risk; in 8.3% of cases where malware was detected, the source can be traced back to a sideloaded application.

## Top Industries Sideloading Mobile Apps

**73%** Financial Services

**45%** Consulting Services

**23%** Consumer Goods

## Sideloaded App Attack Chain on Android

The following attack examples illustrate real instances where devices were tampered with following being sideloaded. While sideloading an app may mark the first step in the attack chain, the true sequence often begins months earlier when users enable device configurations that make the device vulnerable (such as developer options, USB debugging, and installations from third-party sources.)

### SIDELOADED APP ATTACK CHAINS

**France**
**Pixel 2**
**Android 10**
**Application Sideloaded**
**Trojan detected**
**System compromised**
**Device rooted**

**United States**
**Pixel 6**
**Android 13**
**Application Sideloaded**
**Dropper detected**
**System compromised**

## Sideloading on iOS

Sideloading isn't exclusively for Android; iOS users also engage with the practice, although until recently, it required the use of jailbroken devices to install apps from non-vetted app stores. The main installation sources for iOS are Telegram and AppValley.

The recent Digital Markets Act (DMA) is expected to increase the prevalence of these practices, particularly within the European Union (EU). New EU legislation has led Apple to endorse third-party app marketplaces, provided they obtain Apple's approval. This process is similar to the scrutiny apps undergo in the formal App Store, ensuring a level of security and compliance.

## Exploring the Landscape of Non-Formal App Stores

Non-formal app stores on iOS can be broadly categorized into two types:

- **Unmodified iOS App Libraries:** These are simply repositories of iOS apps, often seen as less risky because they do not modify the app codes. However, the lack of re-signing does not fully mitigate the potential security risks, though their use is generally advised against.
- **Modified iOS Apps Stores:** More concerning are stores like AppValley, which offer modified apps. They often host apps that originate from the formal App Stores but have been modified by either the submitter or the app store owners. These modifications can inject new functionalities into otherwise legitimate apps, significantly increasing security risks to the users due to the minimal review process of these apps.

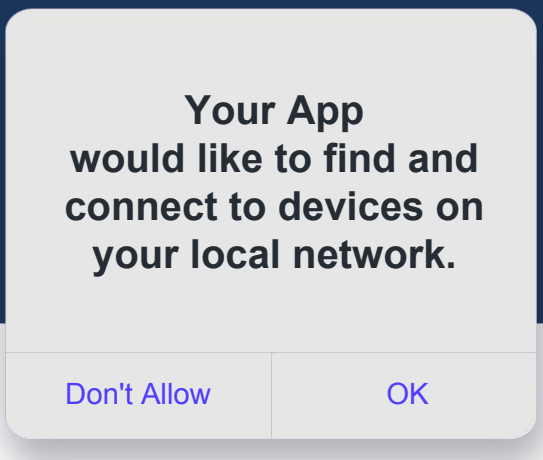
These modifications in these so called "modified apps" are not just minor tweaks but often include major security loopholes in iOS:

- **Sideloaded Patches:** Approximately 20% of these apps included side patches, which are often necessary for specific OS interactions.
- **App Enhancements:** Between 30% and 40% of apps are altered to unlock features, such as converting paid apps to free.
- **Dynamic Libraries:** Nearly 100% of the apps are injected with dynamic libraries by third-party app store owners, introducing potential adware, ad fraud, and malware.

Modified IPA stores frequently need to re-sign apps, often using stolen credentials. Apple combats these practices by revoking these certificates, which prevents further installation of the apps, which require new certificates on a regular basis.

Nearly **4.6M** of non-work apps request permission to access the local network the device is connected to, allowing these apps to communicate with other devices on the same network.

Jailbreaking tools, which make up about 10% of the offerings in these stores, emphasize the demand for more control over devices and lead to significant security vulnerabilities.




**For more in depth information on sideloading, risks and how to mitigate them see our recent blog.**

# Application Vetting

Enterprise-connected devices have work apps developed in-house, third-party work apps, and personal apps. These apps need to be vetted for security, privacy and compliance to protect sensitive enterprise and customer data.  Here are key threats and important questions to consider for each app category.

## Third-Party Work Apps

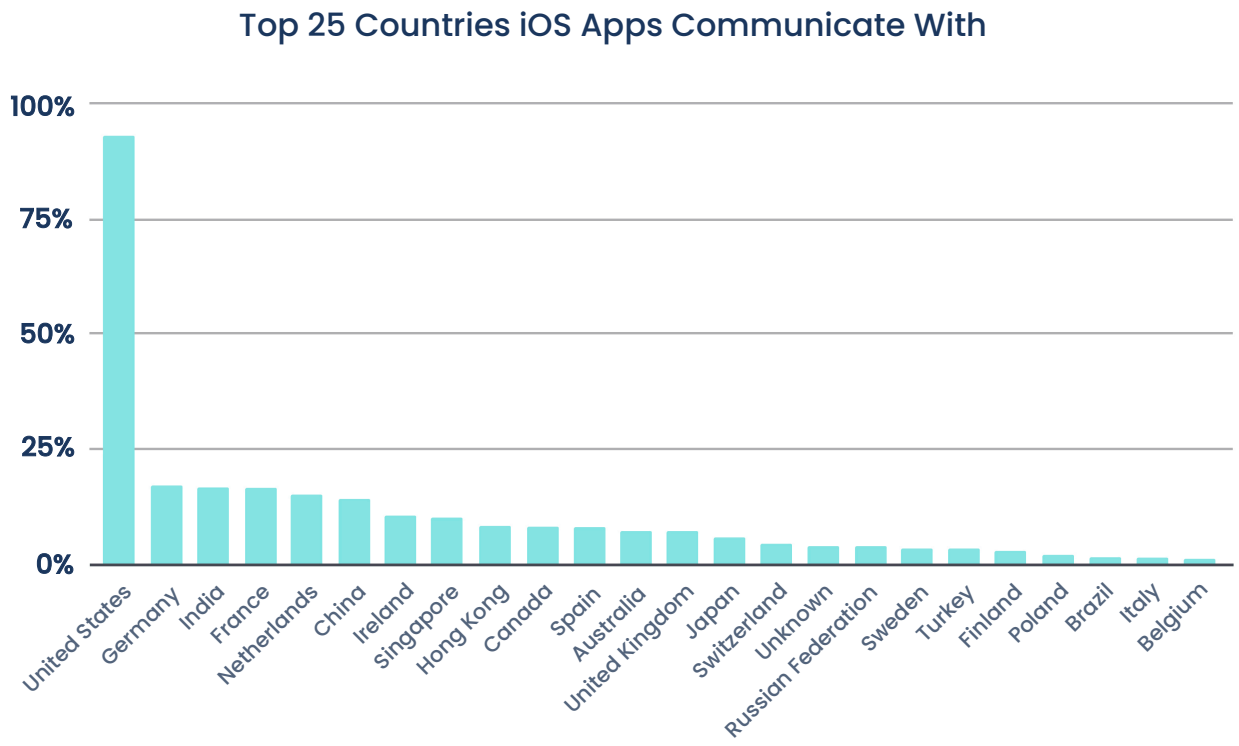
There are three questions to ask about third party work app:

1. Where is my enterprise data going?
2. Is the app asking for dangerous permissions?
3. Does the app have secure communication?

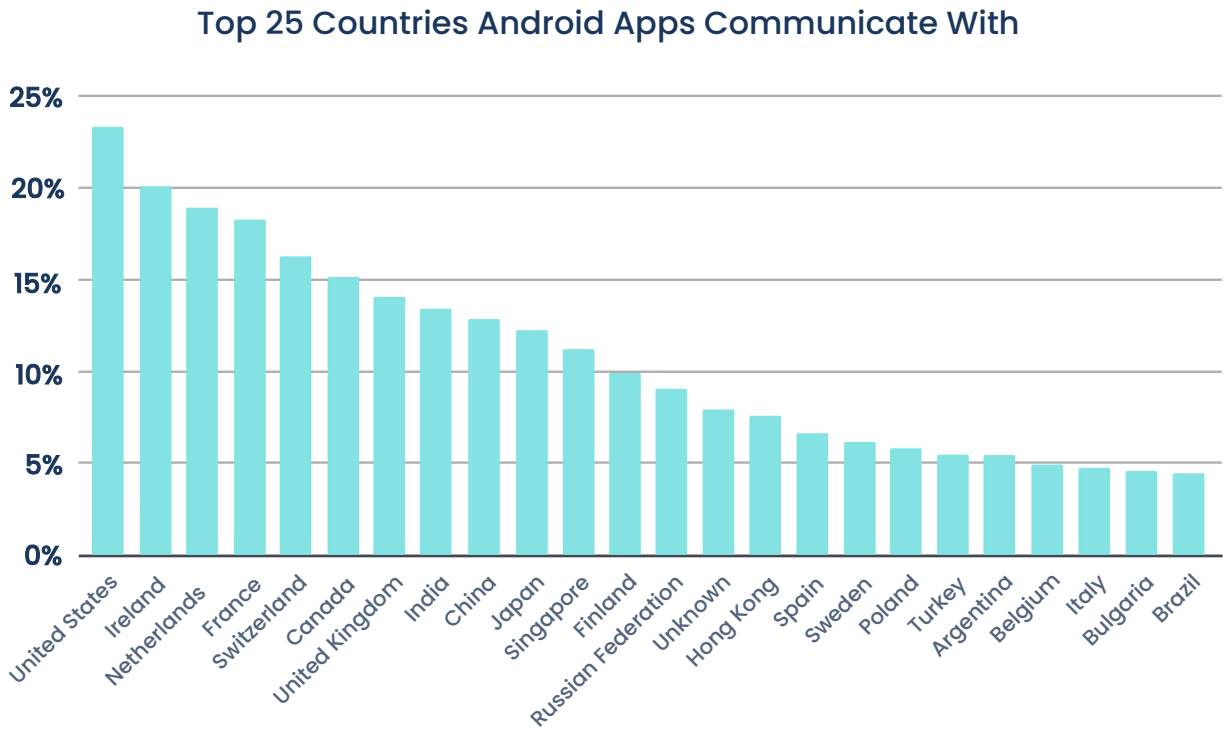
## Where is my enterprise data going?

One of the first questions one should ask when assessing third-party work apps is what data is being **accessed**, where it is being **stored**, and who else the app **communicates** with.

The analysis of work related iOS apps, yielded the following information. The following chart shows that out of the top 25 countries that work related iOS apps communicate with, over **90%** communicate with the US, with all Germany, India, France, Netherlands, China and Ireland are all in double digits. All other countries in the top 25 list are in single digits with Belgium closing the list.



The picture is considerably different for work related Android apps. As the following chart shows, the distribution of the top 25 countries these apps communicate with is more evenly distributed with the US taking the lead at 23% of apps, closely followed by Ireland at 20% with Brazil closing the list with almost 4.5% of apps.




When looking at iOS apps using ChatGPT, the main category of work related apps using it, unsurprisingly are productivity (50%), with utilities (19.7%) and business (10.6%) next.

## Is the app asking for dangerous permissions?

The nature of mobile devices is that in order to perform actions necessary for the app to fulfill its function, the app developer must request the permission of the user (and the operating system) for specific capabilities. But just like most of us never read the EULA, most people pay little attention to the permissions an app is asking for (why would a flashlight app need access to my contacts?).

In addition, each mobile OS defines some permissions as "Dangerous". Meaning, if an app is asking for these kinds of permissions, the user is granting the app the ability to do something that can put the user's data or their entire device in possible danger.

Permission granularity and flexibility differ between the two mobile platforms. In general, Android has more permissions than iOS (due to their different access models). Our analysis looked at apps that would be found on enterprise devices (such as business, financial, and travel apps, for example). For those apps, *we looked at permissions that the OS vendor (Apple, Google) defined as dangerous*, which only appeared in a smaller subset of apps—i.e., our definition of dangerous and "unexpected".

Here are some critical permissions for **work-related** apps that caught our attention.

### iOS

- **Location** - For iOS, the leading dangerous and unexpected permissions were centered around location. Our analysis showed the following:
  - **7.5%** (NSLocationUsage) - Grants apps access to a user's location
  - **7.8%** (NSLocationAlwaysUsage) - Allows continuous tracking, even when the app isn't being actively used.
  - **18.4%** (NSLocationAlwaysAndWhenInUseUsage) - Offers the broadest access, tracking locations in the foreground and background.

- **Bluetooth** - Seemingly innocuous permissions, like Bluetooth access or user behavior tracking, can significantly increase an enterprise's risk exposure. Our analysis showed:
  - **17.5%** (NSBluetoothUsage) - request permissions to track user behavior
  - **14%** - request continuous Bluetooth access (NSBluetoothAlwaysUsage)
  - **15.6%** - request access to Bluetooth peripherals (NSBluetoothPeripheralUsage).

### Android

- For example, roughly 1.8% of apps ask for the permission to mount/unmount the file system. This means that apps that have this permission can fully access the file system. This behavior may be occurring in a small % of apps but this is very risky behavior.
- 5.4% of Android apps ask for permission to get tasks, which was deprecated. This permission allows the app to retrieve information about currently and recently running tasks. This may allow the app to discover information about which applications are used on the device.
- Nearly 10.5% of Android apps (and remember that these are work related apps) have the permission to perform phone calls with 2.6% able to read phone numbers, 1% of the work apps can answer phone calls and read the call log.

## Does the app have secure communication?

### iOS

When looking at iOS apps, we see that almost 36% of work apps use the keychain in a way that might leak data. In addition, roughly the same percentage of iOS apps (36%) do not check the reason for initiated traffic from the app, therefore risking leakage. Roughly 60% of apps write information into the userdefaults store (and almost 75% of apps read data from the userdefault). Information might be exposed by writing possibly sensitive information into the userdefaults store.

### Android

On Android, our analysis of the top 50 apps across the work categories yielded that a little over 50% of them might store information insecurely on the device, but that nearly 40% of them actually do (source). Data stored insecurely means that it can be leaked via the log files that the app generates, or via the network (by using insecure communication) etc.

## In-House Developed Apps

Up until now, we looked at all kinds of different risks that various aspects of the behavior of apps can pose to an enterprise, especially for apps that are used in the context of a work environment.

The various issues with the security of mobile apps prompted the creation of consortiums that banded together to form some sort of basic standard for evaluating the security of apps based on a set of parameters. The two leading standards are the OWASP Mobile Top 10 and MASVS.

These two open standards allow people evaluating the risk of apps, to understand how every app is measured across multiple, different categories such as: insecure communications, insecure data storage etc.

When analyzing apps in the context of these two standards, we can see that

- 16.8% of Android apps and 18.8% of the apps analyzed had issues highlighted by the MASVS testing framework
- 14.5% of Android and 8.7% of iOS apps had issues highlighted by the OWASP mobile top 10.

The advantage of using such testing frameworks is that they provide a standardized set of automated and manual tests that an enterprise can put apps through and understand the risk these apps pose. However, there will always be use cases where such a set of standard tests is not sufficient, and a deeper analysis of the relevant apps is needed.

## Are the apps easy to reverse-engineer?

Another aspect of app security is not only where the app is sending its data (as we discussed previously), but also how secure the app itself is. Consider the following, even if the "bad guy" knows where the app is sending the data, it might be easier to just crack the app itself and get everything from inside the app. Some app developers (but sadly, not all) try to make this more difficult on the "bad guys" by utilizing what's known as code protection and encryption.

When examining code protection, we can identify three types of code protection tools: free, basic, and commercial. When analyzing apps that would be deployed on devices of employees of an enterprise (i.e. apps that are business, financial, travel apps etc) we can identify that roughly **78%** of the apps we've analyzed had some level of code protection. While that number seems high, we need to keep in mind that out of those 78% of apps, 74% are using R8, while it provides some capabilities, it is not really an obstacle for a bad guy looking to reverse an app.

Our analysis also yielded that only **3%** of apps with code protection leverage a commercial code protection tool (with financial apps leading the way). This means that when it comes to protecting one's code, there's much work to be done.

OWASP cites insecure data storage as one of the top 10 mobile application security risks.[20] They also cite application supply chain security as a top 10 threat.[21]

## Is the Third-party code safe?

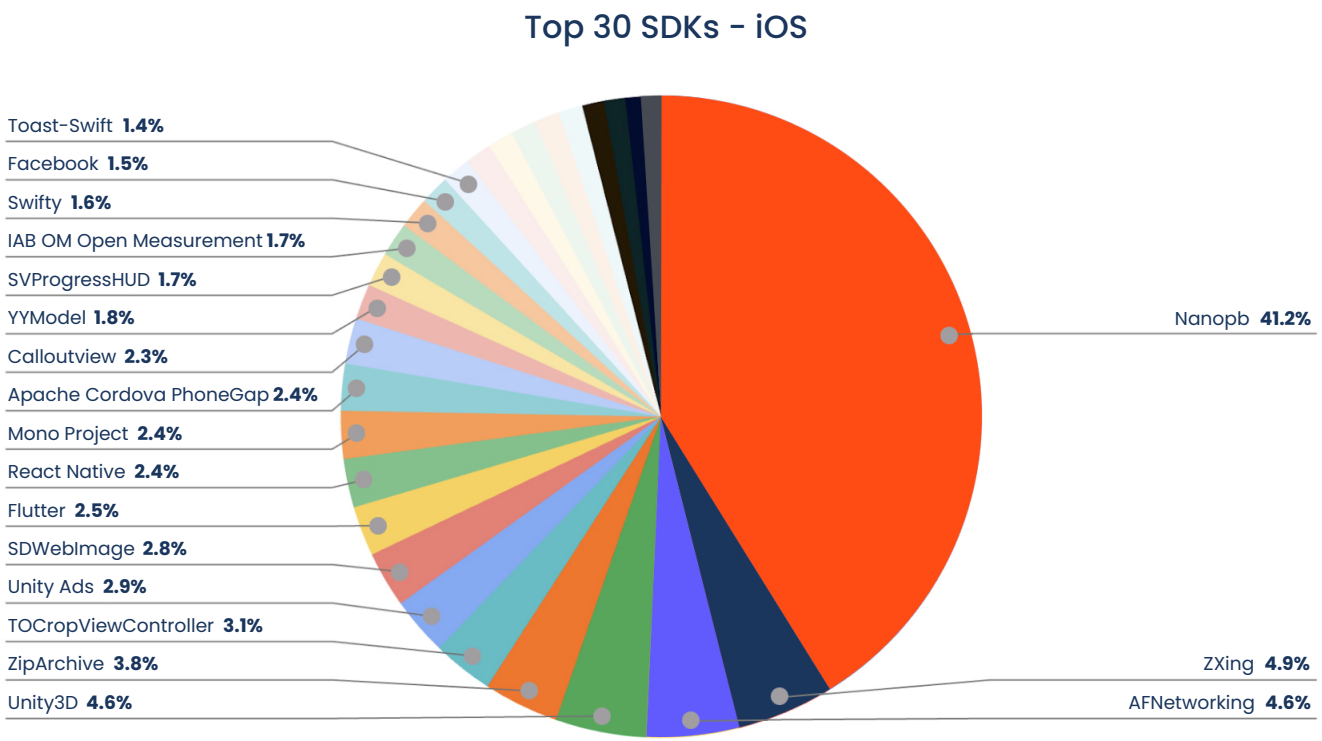
If there's one thing app developers like is that someone else already solved a problem they have before them, and they can reuse that solution. We can roughly divide the idea of third party code into two main parts: OS provided and third party.

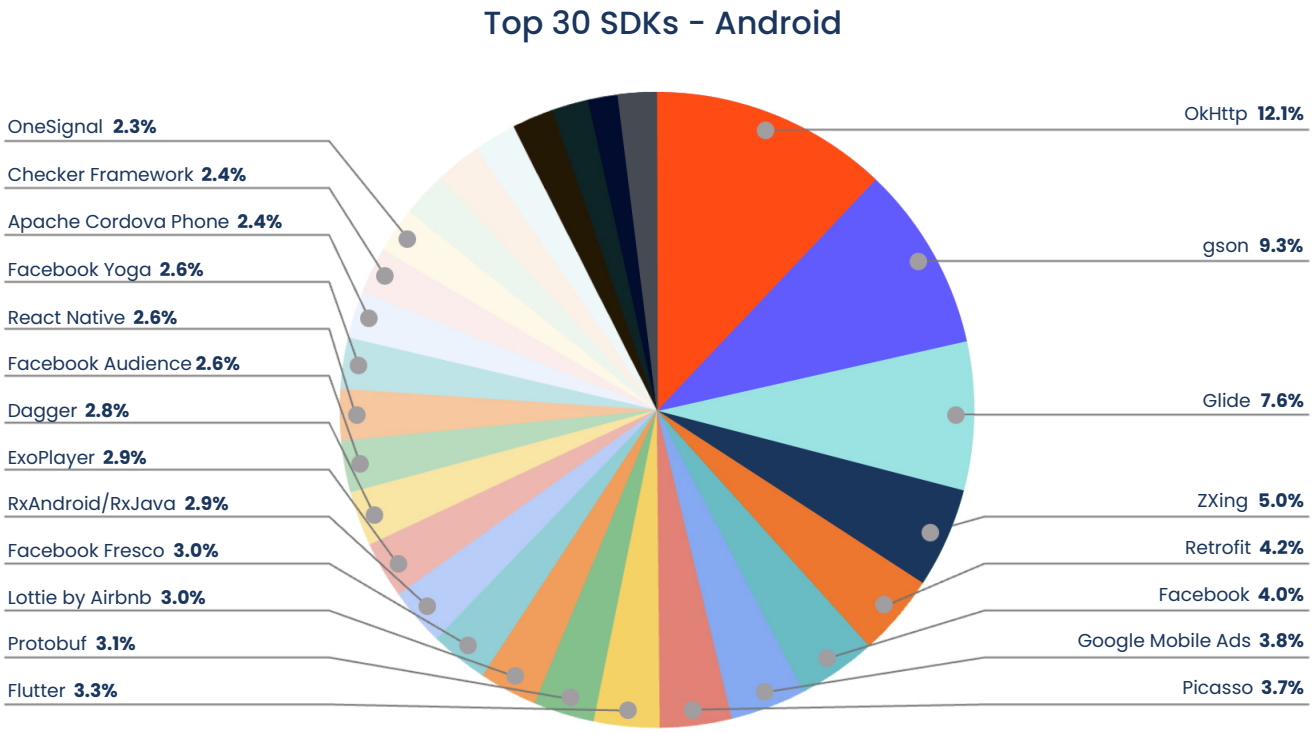
OS provided code comes in the form of system frameworks, system SDKs and various components that are prepackaged with the mobile OS, while third party code is most often open source code found in places such as github in the form of libraries and SDKs. For the purpose of this section, we'll be focusing on third party code.

When analyzing the data for work related Android apps, we can identify that on average we can identify **14 SDKs/Frameworks** packaged with each app, but when focusing only on third party code not provided by the OS vendors, we are left with an average of **9 SDKs/Frameworks** per app.

For iOS, the overall number of SDKs/Frameworks is very close to its Android counterpart at an average of almost **15 SDKs/Frameworks**. However, this number drops down to an average of **6 Frameworks/ SDKs** when taking into account third party code that is not provided by the mobile OS vendors.

The following charts illustrates the distribution across iOS and Android:





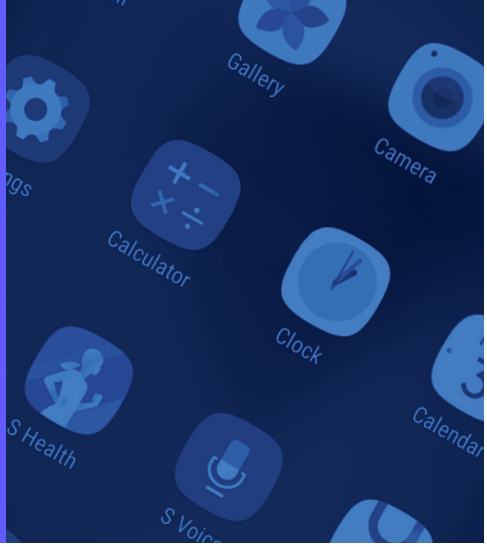

In 2023, Citizen Labs uncovered[22] a significant 0-day vulnerability, dubbed **BLASTPASS**, in the WEBP library used by Flutter, affecting both iOS and Android. The flaw allowed attackers to install malicious payloads via crafted images. Our analysis of thousands of apps revealed that around 1% of Android apps and 10% of iOS apps are built with Flutter, and by the end of 2023, over 90% of Android apps and all iOS apps using Flutter were still vulnerable. This underscores how delays in third-party code fixes and slow responses from developers can leave apps exposed long after vulnerabilities are identified.

A vulnerability in a third-party component could put the enterprise at risk. This is why ensuring that all components are reviewed and analyzed is always important.

# Personal Apps From Public Stores

## Apps Removed From Stores

Apple and Android remove **thousands** of apps from their stores when they discover security vulnerabilities, violations of privacy policies, or malicious behavior. However, once these apps are removed, they often remain on users' devices, leaving them vulnerable to exploits and data breaches.




## Removed Apps Found on Enterprise Devices

**iOS WORK APPS:**
**21.5K**

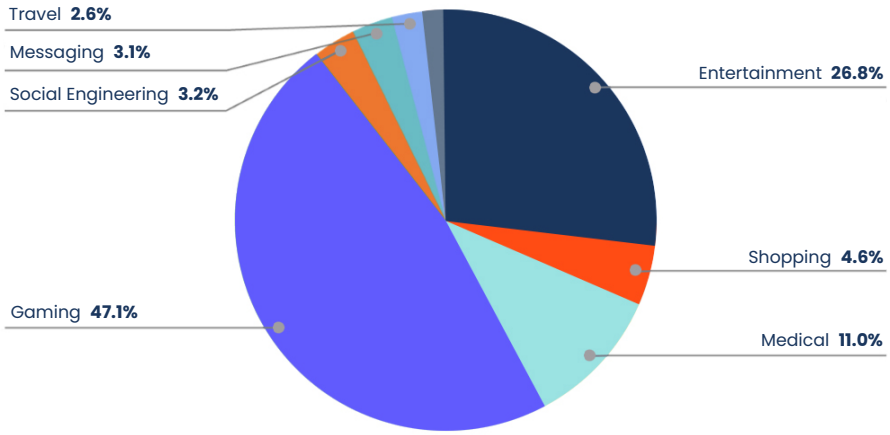
**iOS NON-WORK APPS:**
**36.2K**

**ANDROID WORK APPS:**
**53.1K**

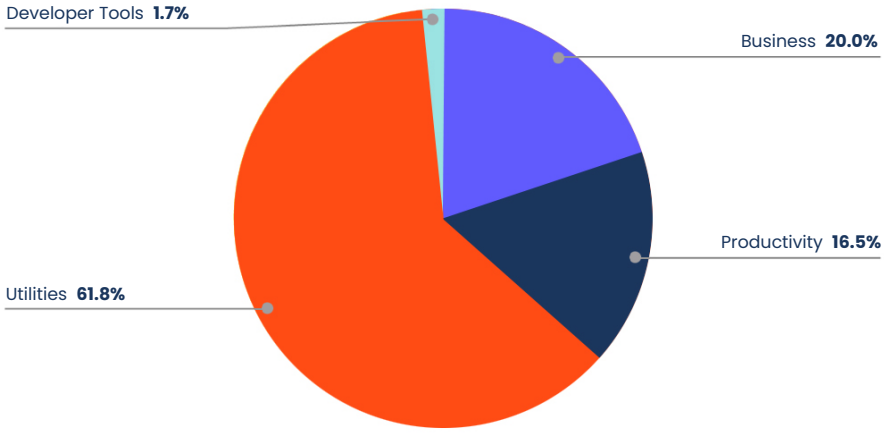
**ANDROID NON-WORK APPS:**
**181.4K**

## Removed Android App Categories

CATEGORIES OF NON-WORK APPS REMOVED FROM STORE SINCE JAN 1, 2023

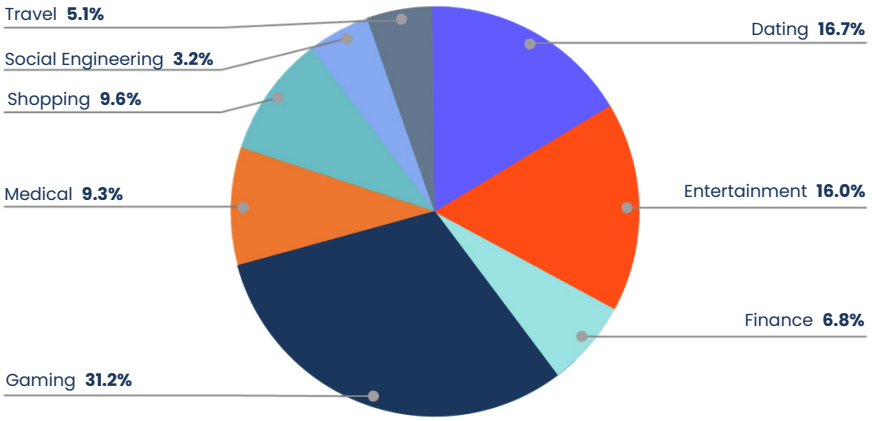



CATEGORIES OF WORK APPS REMOVED FROM STORE SINCE JAN 1, 2023

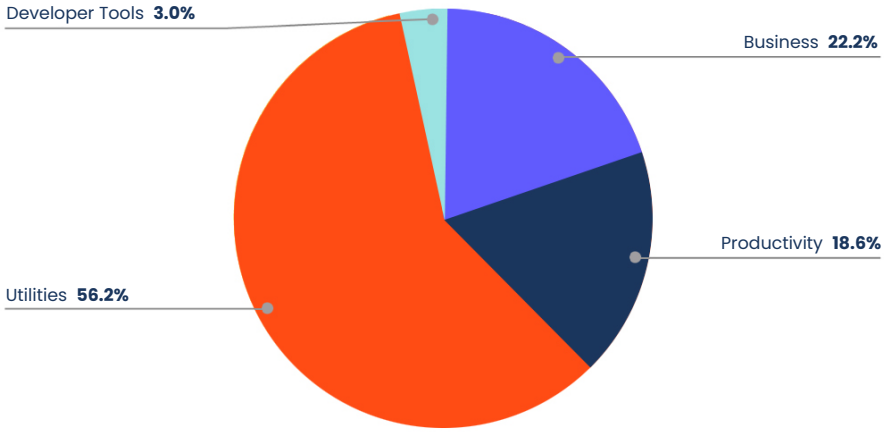


## Removed iOS App Categories

CATEGORIES OF NON-WORK APPS REMOVED FROM STORE SINCE JAN 1, 2023




CATEGORIES OF WORK APPS REMOVED FROM STORE SINCE JAN 1, 2023




Enterprises with BYOD should be concerned because outdated or malicious apps can still access corporate networks and data, posing significant risks to the security of the entire organization. Compliance policies should be in place to identify and ensure that employees remove such apps, which is crucial for reducing exposure to potential threats.

## Personal VPN Apps

VPN apps are popular for both business and personal use. A VPN stands for a "Virtual Private Network," which allows the creation of an encrypted network connection where sensitive data can be sent in a "secure" manner.

We analyzed multiple VPN apps for iOS and Android. **65%** of Android VPN apps contained ads, which suggests they are "free" VPN apps.

Regarding which countries VPN apps communicate with, for Android, the top country communicated with is Ireland (with 25% of Android VPN apps communicating with this country), followed by Singapore and the UK (19.3%). China and the Russian Federation close the top 10 list with almost 13% of Android VPN apps.

For iOS VPN apps, almost 92% communicate with the US, followed by almost 23% to China with the Russian Federation (12.4%), Australia (11.8%) and Singapore (11.1%) closing the top 10 list.

Now that we've examined where these VPN apps communicate, let's examine the types of permissions these apps ask for.

### On Android

- When looking at the Android VPN apps, 21.5% of them are asking for permission to **write to an external storage**. This means that almost 80% of Android VPN apps do just fine without this, which is a red flag.
- 8.6% of Android VPN apps ask for the ability to read the phone's state, and 3.2% ask for camera access and reading media images, another red flag. It seems odd that a VPN app would even care about pictures and image media.

### On iOS

- When looking at iOS VPN apps, and since permissions are handled differently in iOS, 3.7% of VPN apps ask for "Location Always On", "Location While Using" permissions, which, while it makes sense for a VPN app to try to know where the user is, the fact that over 90% of the other VPN apps can perform their function without this permission is a red flag.
- Bluetooth Peripheral Usage permission (3.1%) is one of the permissions that iOS VPN apps request, which allows the app to use Bluetooth peripherals. We will leave it up to the reader's imagination as to what an app whose purpose is to see the device's traffic can do with the permission to communicate with bluetooth peripherals.

When looking at Android VPN apps, almost 29% have OWASP related issues and 22% have MASVS related issues. The situation is similar for iOS VPN apps, where almost 27% have OWASP related issues and 23% have MASVS related issues.

When looking at the categories of issues where our own detections come into play, for Android VPN apps, 16% of the issues that were found during analysis were in the network security category, 3.2% in the data leakage category and 22% in the vulnerability category. For iOS, 15.8% of VPN apps had issues in the vulnerability category and 5% in the network security category.

The meaning of these numbers is simple, a considerable number of these VPN apps, which have access to the network traffic on the device, have issues that might expose sensitive enterprise information.

## Platform & OS Vulnerabilities

Attackers are keenly aware of the opportunities presented by mobile endpoints. According to IBM, up to 70% of successful data breaches and 90% of successful cyberattacks originate from endpoint devices.[23] Samsung reports that only 15% of businesses currently provide smartphones to employees.[24] This reliance on personal devices, which can access sensitive business data but may be so old and outdated that there is no upgrade path to bring the OS into compliance, significantly increases security risks.

In an ideal scenario, all mobile devices would run the latest OS and apps, fully aligned with patch and compliance goals. However, the reality is quite different. Zimperium has identified that 1% of iOS devices monitored in today's enterprises are non-upgradable and open to exploitation. The problem gets worse for **Android, 14% of these devices are unable to be remediated against threats due the same issue**. Without the ability to receive critical security patches and updates, these devices become easy targets for cyber attacks.

Here are some key statistics from our threat data that emphasize the importance of managing platform vulnerabilities for mobile devices.

| | iOS (Current Ver: 17.4.1) | Android (Current Ver: 14) |
|---|---|---|
| **APAC** | 10.3.1 | 5.0 |
| **EMEA** | 10.3.4 | 5.0 |
| **North America** | 10.3.3 | 5.0 |
| **South America** | 12.1.4 | 5.1.1 |

| | 2022 | 2023 |
|---|---|---|
| **Android** | Number of CVEs identified in 2022 for Android: 897<br>Average CVSS Severity Rating for Android: 7.2 or higher<br>Number of (zero-day) CVEs exploited in the wild for Android: 41 | Number of CVEs identified in 2023 for Android: 1421<br>Average CVSS Severity Rating for Android: 6.7<br>Number of (zero-day) CVEs exploited in the wild for Android: 97 |
| **iOS** | Number of CVEs identified in 2022 for iOS: 243<br>Average CVSS Severity Rating for iOS: 7.7<br>Number of (Zero -Day) CVEs exploited in the wild for iOS: 5 | Number of CVES: 269<br>Average CVSS Severity Rating: 7<br>Number of (zero-day) CVEs exploited in the wild: 20 |

**Security Patches Released in 2023 for iOS and Pixel Devices**

| Google | iOS |
|---|---|
| 24 | 35 (Including 2 RSRs) |

The data underscores that **iOS and Android devices are not inherently secure**, with both platforms seeing significant vulnerability increases. Despite frequent updates—24 for Android and 35 for iOS in 2023—enterprises find it difficult to keep up due to the high costs and time constraints involved in managing updates across all devices. Compounding this, **Android fragmentation** poses a major challenge, as various device versions exist across regions, making it nearly impossible to ensure uniform security while driving productivity across the entire workforce. This reality highlights the need for proactive mobile security strategies, as relying solely on platform updates leaves devices exposed.

# Conclusion

## Prioritizing Mobile Security in the Digital Age

As organizations increasingly embrace mobile-first strategies, it is undeniable that mobile devices and apps have become the **most critical digital channel to protect**. These devices serve as a gateway to sensitive data and critical infrastructure, making them prime targets for cyber threats. Bad actors are acutely aware that many mobile devices and apps lack proper security protections, making them easy prey for attacks.

According to the 2024 Verizon Data Breach Investigations Report (DBIR), mobile devices are the fastest-growing attack vector, with mobile malware detections rising by 51% year-over-year. Meanwhile, nearly 82% of mobile devices are targeted by sophisticated phishing attacks, known as "mishing," which are becoming increasingly difficult to detect, as 76% of phishing sites now use HTTPS to appear legitimate. Cybercriminals exploit these vulnerabilities, knowing that organizations have not fully addressed mobile security in the same way they do traditional endpoints.

As enterprises navigate this evolving mobile threat landscape, they must focus on the four key mobile threats that pose the greatest risk:

1. **Mishing (Mobile Phishing)**
2. **Mobile Malware**
3. **Sideloaded Apps**
4. **Application Vetting**
5. **Platform Vulnerability Management**

Taking care of these five critical threats will reduce the overall risk significantly, as they account for most mobile-related attacks. But to effectively protect mobile endpoints, organizations must adopt a **multi-layered security strategy** that includes:

- **Mobile Threat Defense:** Advanced on-device solutions to detect and mitigate mobile malware, phishing, and network threats in real time.
- **Mobile Application Vetting:** Screening both official and sideloaded apps for potential vulnerabilities.
- **Multi-Factor Authentication (MFA):** Ensuring secure access to corporate resources.
- **User Education:** Training employees to recognize phishing attempts, malicious apps, and insecure networks.

Bad actors are already exploiting gaps in mobile security. By focusing on these critical areas, enterprises can close those gaps, strengthen their mobile security posture, and reduce their overall risk exposure. In today's mobile-first world, protecting mobile devices is not optional—it is the cornerstone of a secure digital future.

# Sources

1 https://security.imprivata.com/rs/413-FZZ-310/images/ebook-ponemon-report-2024.pdf

2 https://insights.samsung.com/2023/05/31/mobile-devices-and-your-employees-to-byod-or-not-to-byod/#:~:text=First%20up%2C%20while%20there%27s%20still,it%20comes%20to%20mobile%20devices

3 https://owasp.org/www-project-mobile-top-10/

4 https://explodingtopics.com/blog/smartphone-stats

5 https://www.nasdaq.com/articles/how-mobile-devices-became-a-key-enabler-of-productivity-for-todays-dynamic-workforce-2021

6 https://insights.samsung.com/2021/08/19/your-phone-is-now-more-powerful-than-your-pc-3/

7 https://radixweb.com/blog/mobile-app-usage-statistics#usage

8 https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices/

9 https://wifitalents.com/statistic/remote-work-cybersecurity/#:~:text=Remote%20Work%20Cybersecurity%20Statistics:%20Latest%20Data%20&,devices%20used%20for%20work%20purposes%20adequately%20(DaaS).

10 https://99firms.com/blog/byod-statistics/#gref

11 https://www.proofpoint.com/us/blog/security-awareness-training/2024-state-of-phish-report

12 http://apwg.org/apwg-q4-report-finds-2023-was-record-year-for-phishing/#:~:text=16%20Apr%20APWG%20Q4%20Report%20Finds%202023%20Was%20Record%20Year%20for%20Phishing&text=CAMBRIDGE%2C%20Mass.%2C%20April%2016,year%20for%20phishing%20on%20record.

13 "2024 Mobile Security Index," Verizon Business

14 https://www.ibm.com/reports/data-breach

15 https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/

16 https://ransomware.org/blog/mobile-phone-ransomware-a-primer/

17 https://www.stationx.net/malware-statistics/

18 https://www.forbes.com/advisor/business/public-wifi-risks/

19 https://www.forbes.com/advisor/business/public-wifi-risks/

20 https://owasp.org/www-project-mobile-top-10/2023-risks/m9-insecure-data-storage.html

21 https://owasp.org/www-project-mobile-top-10/2023-risks/m2-inadequate-supply-chain-security.html

22 https://www.zimperium.com/blog/patching-high-impact-vulnerabilities-a-retrospective-on-webp-cve/

23 https://www.ibm.com/reports/data-breach

24 https://www.samsung.com/us/business/short-form/maximizing-mobile-value-2022/thank-you/

# About Zimperium

Zimperium has helped thousands of enterprises and government agencies around the world to successfully employ a mobile-first security strategy—and we're here to help your organization do the same.

Thank you for your interest in this report, and please feel free to **contact us** if we can help your team advance its mobile-first security strategies.

ZIMPERIUM®