ZIMPERIUM®

2022 Global Mobile Threat Report

Executive Brief

With our mobile devices processing and accessing critical information like passwords, multi-factor authentication apps, and corporate files and communications, it's no surprise that the threats have increased over the last few years—and that malicious actors continue to invest more in targeting these devices and applications with increasing levels of sophistication.

With our mobile devices processing and accessing critical information like passwords, multi-factor authentication apps, and corporate files and communications, it's no surprise that the threats have increased over the last few years—and those malicious actors continue to invest more in targeting these devices and applications with increasing levels of sophistication.

In our analysis of the mobile threat landscape, 2021 was the year of both big revelations and reboots of previously discovered malware. Pegasus, the spyware program sold to governments around the world, reappeared in the news after revelations of a campaign targeting 50,000 journalists, human rights activists, political leaders, and more. Initially unveiled by Amnesty International, the spyware campaign featured zero-day exploits targeting iOS devices. Shockwaves of this discovery have continued for months as additional information about the attacks and victims is revealed.

It is essential for enterprises not to lose sight of the strategic importance of comprehensive mobile security surrounding the devices and applications connected to their critical systems. The mobile world grows in complexity, with new apps, features, and capabilities introduced yearly. Still, it is essential to realize that security, like these devices, is a constantly moving target. It is about understanding the risks involved and their potential impact and making a calculated decision with the right tools and resources in place.

Here are some of the most impactful data points from this year's report:

Pandemic Preparedness

- **Before the COVID-19 pandemic arose, 60% of organizations had no BYOD policies in place.**
- **...and the BYOD landscape it left in its wake:**

66%

of smartphones within the enterprise were employee-owned

55%

of tablets within the enterprise were employee-owned

The Growing Global Threat

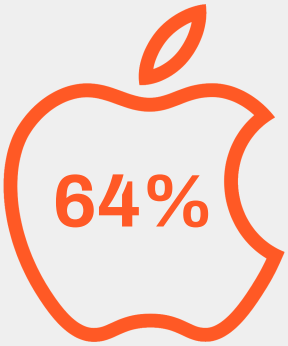
- **In 2021, the Zimperium zLabs team discovered numerous threats impacting over 10M devices in at least 214 globally.**
- **Zimperium detected 2,034,217 new malware samples in the wild in 2021.**

Mobile as a Threat Vector

- According to our research, 42% of organizations report mobile devices and web applications have led to a security incident.
- Based on our analysis of more than 1.3 million Android and iOS apps, 131,000 used public cloud services in their backend, and 14% of those apps had misconfigurations exposing users' personal information.
- 23% of endpoints encountered one form or another of malicious applications in 2021.
- 30% of known, zero-day vulnerabilities discovered in 2021 targeted mobile devices.

- In 2021, there was a 466% increase in exploited, zero-day vulnerabilities used in active attacks against mobile endpoints.
- 75% of the phishing sites analyzed specifically targeted mobile devices and delivered content appropriate for the mobile format.
- On average, 77% of Android and 46% of iOS apps use, or potentially use, at least one vulnerable encryption algorithm.
- Approximately 81% of financial applications potentially leaked sensitive information.

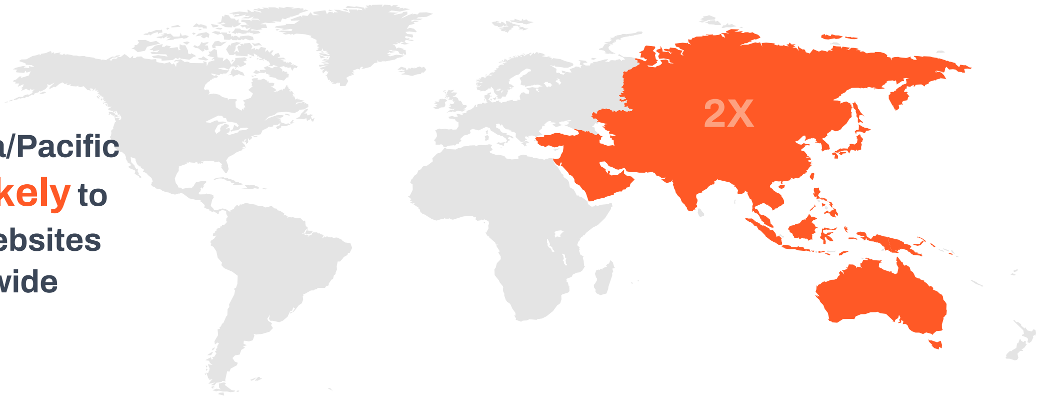
Challenging Assumptions About the Security of Mobile Operating Systems



- In 2021, iOS vulnerabilities accounted for 64% of mobile-specific exploited zero-day attacks.

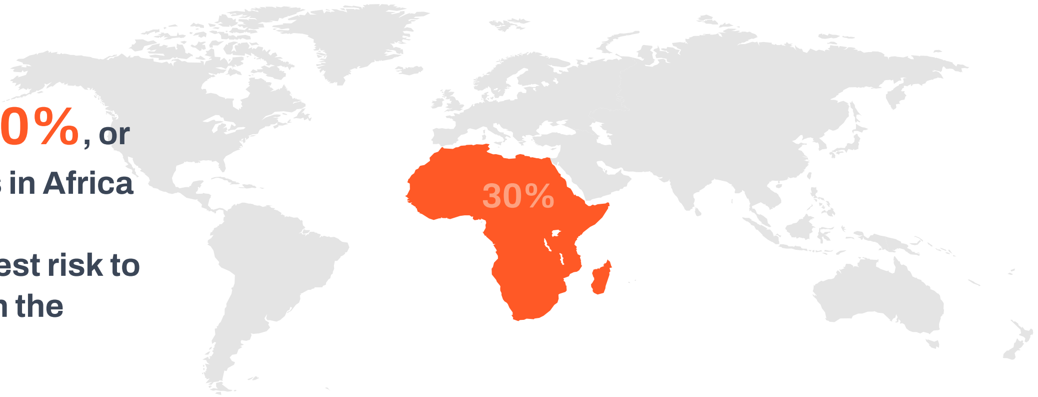
Regional Trends in Highly Developed Mobile Technology Geographies

- Mobile users in the Asia/Pacific region are **twice as likely** to encounter malicious websites compared to the worldwide average.



Compared with Trends in Developing Mobile Markets

- In 2021, a staggering **30%**, or 1 in 3, mobile endpoints in Africa encountered malware, accounting for the biggest risk to enterprises and users in the region.



From device exploits to application misconfigurations, malware, and leaky databases, the mobile device has become a ripe target for malicious actors globally. The data points above demonstrate there was no shortage of threats targeting mobile ecosystems. 2022 should be the year people start approaching mobile devices and apps with the same advanced security mindset as traditional endpoints.

As mobile threats continue to evolve and expand, Zimperium remains dedicated to providing the advanced mobile threat defense and mobile application security tools necessary for organizations to stay ahead of the threats. We hope the 2022 Global Mobile Threat Report and the data therein serves to inform how your organization tackles the current challenges, as well as the new challenges that will undoubtedly arise as we all explore the infinite new use cases for these complex computing devices we refer to as our “phones."

To learn more and download the full report, visit
www.zimperium.com/global-mobile-threat-report

ZIMPERIUM®