digital.ai™

2024 APPLICATION SECURITY THREAT REPORT

Security threats to apps operating outside the firewall

Quantifying the risks, examining new trends in cybersecurity threats for applications running “in the wild”

Contents

Introduction and key findings	3
Terminology	4
How at risk is your app in 2024?	5
Risks to apps by industry	7
Risks to apps by device type	8
The relationship between risk and popularity	10
Risks across app instances	11
Protecting your apps in the wild	14
Contact us	15
Appendix: methodology	16

digital.ai

Introduction and key findings

There is no question that we're living in an app-happy world. The Apple Store now offers 1.96 million apps; the Google Play store has 2.87 million apps;[1] and a whopping 148.2 billion mobile, desktop, and web apps were downloaded in 2023.[2] More than 52,000 new apps were released on Google Play in February 2024 alone.[3]

The problem is that these apps, which typically run outside corporate firewalls ("in the wild"), are prime targets for cybercriminals. And the security risks are rising even faster than app usage. There are now more than a billion malware programs out there, and 560,000 new pieces of malware are detected daily.[4]

However, since most research focuses only on threats and attacks *inside* corporate firewalls, app users have only a vague notion of the risks that could impact them, and security researchers have little guidance on how to protect apps and their users.

This study continues the work Digital.ai initiated in 2023 by illuminating and quantifying threats to apps in 2024. It also offers insights about the rising use of AI (by app developers and cybercriminals), along with advice on specific actions security teams can take to stay a step ahead of hackers.

Key findings

01 **Overall risk is up:** The likelihood of an app being attacked over a 4-week period rose from 57% in 2023 to 65% in 2024.

02 **Gaming and FinServ vulnerabilities remain high:** Gaming and financial services (FinServ) apps face the highest risk of attack (76% and 67%, respectively), and the risk in both sectors is up since 2023.

03 **Android and iPhone attacks surging:** Android apps remain more likely to be run in unsafe environments than iPhone apps (70% vs. 94%, respectively), but the likelihood of both has spiked in 2024.

04 **Popularity does not increase risk:** Less popular apps are often attacked more frequently than popular apps.

[1] 42matters, April 2024.

[2] Statista, February 2024.

[3] Statista, March 2024.

[4] AV-Test Institute, 2024.

Terminology

Application or app: One discrete executable that runs on a mobile operating system, in a browser, or on a desktop/server operating system.

Consumer: The end-user of applications created by Digital.ai customers.

Instance: One discrete executable on a single consumer's device.

Attack: Any action taken on a mobile/web/desktop app that violates the EULA (End User License Agreement) of the organization creating the app and/or the App Store/Play Store.

Guard: A protection added to an application to frustrate reverse engineering or tampering attempts.

FinServ app: Any consumer-facing application created by a bank, insurance company, credit card issuer, or payments platform.

Gaming app: Any web, mobile, or desktop app used to play games, exclusive of apps used to place bets or to gamble.

All other verticals: An application made by an organization in any industry other than the gaming or FinServ industry — for instance, medical devices, manufacturing, online retail, industrial controls, etc.

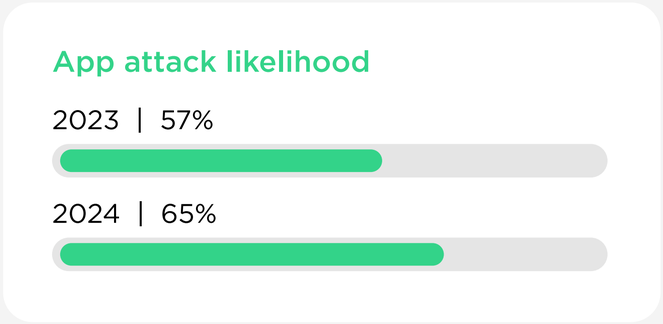
digital.ai™

How at risk is your app in 2024?

The data in this report is anonymized and aggregated global customer data collected over a four-week period from February 1 to February 28, 2024. “Risk,” in this case, is measured from the enterprise creating the application’s perspective. In other words, if 100 enterprises create 100 apps and 58 of those apps experience an attack on one or more instances of that app, the report will state that 58% of apps were under attack.

Overall threat level

In 2023, the inaugural year of this study, the likelihood of an app being attacked in a four-week period was **57%**, which was higher than the experienced Digital.ai research team had predicted. In 2024, that figure rose to **65%**. This uptick, however, was not unexpected. The convergence and/or evolution of several trends contributed to the increase:



- **Tool democratization** among threat actors continues. For example, reverse-engineering tools such as Ghidra and dynamic instrumentation toolkits such as Frida are becoming increasingly sophisticated and popular, simplifying application inspection and malware creation.
- **Cryptocurrencies are on the rebound** after a wild ride in 2023. Cryptocurrencies make it easier for threat actors to “cash out” of schemes, particularly if ransomware is involved.
- **The nationalization of attacks** continues to open up enormous state-sponsored resources for threat actors.
- **An increase in “jailbreaking”** has taken root within the community of hackers, threat actors, and pranksters dedicated to frustrating Apple’s efforts to lock down their OS.
- **Surging use of AI/ML** dramatically increases the productivity of both app developers and malware developers, resulting in more apps to attack and more attack vectors in use.

How at risk is your app in 2024? *(cont.)*

Let's take a closer look at the impact of AI. A recent McKinsey study[5] found that, overall, generative AI can increase development speed by 10-30 percent, depending on the complexity of the task. Creating, testing, and deploying new malware is a relatively complex task; however, even a small increase in the productivity of hackers is likely to translate to a significant increase in the overall threat to apps in the wild for several reasons:

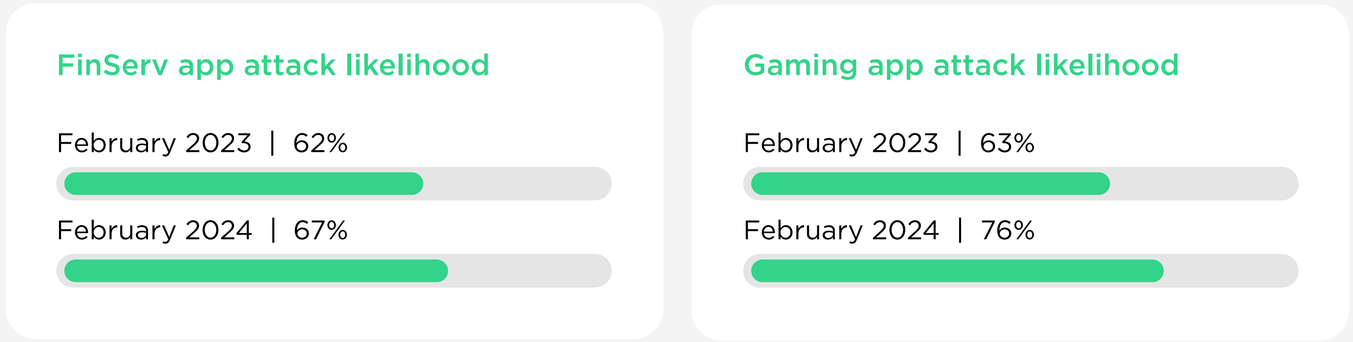
- Threat actors are handling the development of their software with increasing alacrity, acting more and more like complex organizations. For instance, many have help desks, QA departments, etc.
- Sophisticated threat actors can use AI to assess vulnerabilities in apps as well as accelerate malware coding, leading to faster and more effective attacks.
- Threat actor groups are evolving to exploit each of the factors listed above. For example, the nationalization of attacks increases the resources threat actors have for launching attacks, including large numbers of people to help with social engineering, staff help desks, and more.

Consider a specific example of how AI increases threats to apps in the wild. The release of ChatGPT4 gave cybercriminals access to AI coding tools that help them evaluate the apps they are attacking and write malware code 10-30 percent faster than before. They can also push the attacks out faster using ChatGPT4's automation capabilities. Net result: more attacks to more apps in less time.

[5] McKinsey & Co., "Unleashing Developer Productivity with Generative AI," June 27, 2023.

Risk to apps by industry

The study analyzed results from multiple industry sectors and found that gaming apps and FinServ apps continue to be the most likely to be attacked.



It may seem counterintuitive that gaming apps would have a higher threat level than FinServ apps since many gaming apps are free and FinServ apps are directly tied to money. The 2023 study covered the primary reasons for this; below is a quick recap.

- **There is money to be made** from selling game cheats. In addition, with real credit cards being used to buy "extras" such as emotes, harvesting tools, gliders, and outfits, there is plenty of incentive to attack games to steal credit card info or PII while the complicated in-game economies are ripe for criminal organizations to use to launder money.
- **Notoriety from hacking games.** Some of the most active Reddit communities and forums revolve around "cracking" or reverse engineering games. While most users are just consumers of cracks and cheats, those who can crack the most protected games are regularly hailed in comments and enjoy a kind of celebrity within the community.

Interestingly, the threat gap between gaming and FinServ apps actually widened between 2023 and 2024. Why is this? One reason might be that the gaming industry is growing fast. The mobile gaming market alone is estimated at $100.54 billion in 2024 and is expected to reach $164.81 billion by 2029, growing at a CAGR of **10.39%** during that period (2024-2029).[6] With more people playing more games, there are more opportunities for bad actors to be…bad.

Apps outside of FinServ and gaming still have a **66%** chance of being attacked. The reasons are broad, diverse, and industry-specific. To cite just a few examples:

- **Implantable medical devices** interface with patients' phone apps as well as clinicians' phones and tablets. The incentives to hack those applications range from a curious patient wanting to experiment with a drug delivery system to a truly malicious actor looking to inflict bodily harm on another human.
- **Bluetooth-connected phone apps** that start our cars are becoming increasingly available, making them somewhat obvious targets for threat actors looking to steal cars or the goods stored inside them.
- **Dozens of other threat vectors** emerge in almost any industry—from apps used by oil prospectors, to apps used for computer-aided design, to apps used by your favorite retailer.

[6] Global Information, 2024.

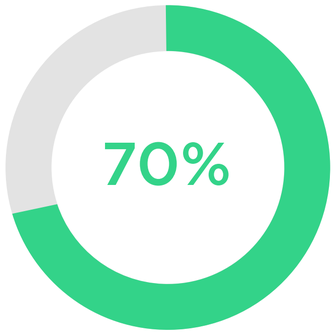
Risks to apps by device type: iOS vs. Android

The 2023 edition of this study dispelled the notion that iOS apps are orders of magnitude safer than Android apps.

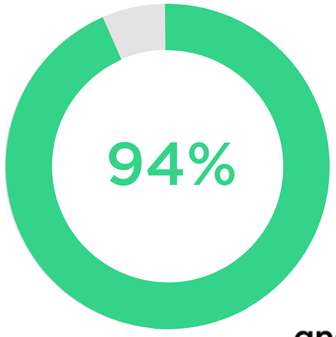
Yes, iOS apps are less of a security risk since Apple controls the production of all iPhones while Google licenses the Android OS to many different device makers, making Android more accessible to threat actors. However, both platforms are, in fact, open to some degree, and the study's data confirms that apps on both platforms are susceptible to multiple threats. Equally important, apps on both platforms experienced a sharp increase in attacks in 2024.

Android apps remain more likely to be targeted with environmental attacks than iPhone apps (70% vs. 94%, respectively), but attacks on both have spiked in 2024.

IOS app likelihood of unsafe environment



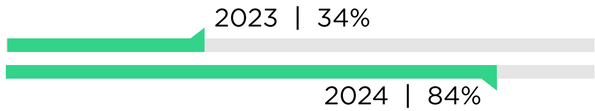
Android app likelihood of unsafe environment



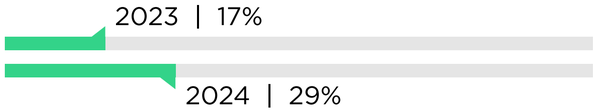
The rise in iOS vulnerabilities can be partially explained by the ongoing phenomenon of iOS **jailbreaking**, which declined temporarily in the first half of 2023 but accelerated again in the second half of the year. Jailbreaking an iPhone gives the end-user full execute and write access, allowing them to break free from the restrictions and limitations imposed by Apple's iOS so that they can customize them to their liking. Often, this means compromising the built-in security structures such as Apple Mobile File Integrity, Sandbox, Read-Only Root File system, and disabling or tampering with trusted apps.

Jailbreaking or rooting a phone, of course, is not in and of itself a particularly malicious or severe attack. It is, however, a necessary precursor to just about every other type of attack. Integrity attacks—attacks that modify an application's code or signature—can cause much more damage. And integrity attacks also saw a sharp rise, as follows:

Android app attack likelihood



iOS app attack likelihood



Risks to apps by device type: iOS vs. Android *(cont.)*

In 2024, there was an even sharper uptick in specialized *attacks*—attacks that violate an application's integrity through, for example, a malicious change in application code. Attributing this uptick to any one factor is difficult, but we hypothesize that more attacks are reported as customers update and fortify their application protection blueprints (aka GuardSpecs). This is a phenomenon akin to becoming more aware of theft as more and more security cameras are installed to track thieves.

iOS app likelihood of being run with modified code

2023 | 6%

2024 | 20%

Android app likelihood of being run with modified code

2023 | 28%

2024 | 63%

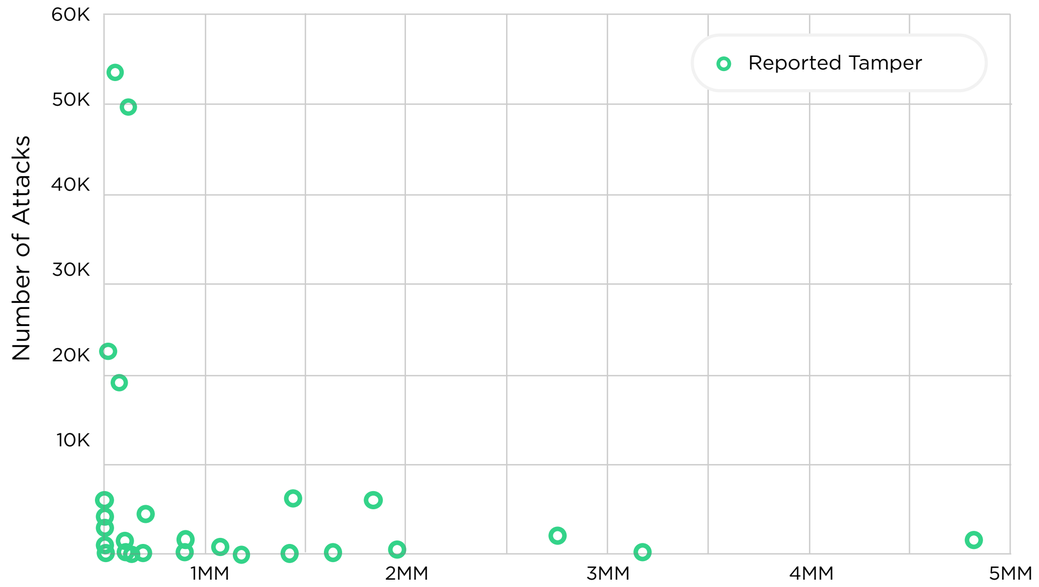
While Apple has consistently invested time, money, effort, and ingenuity into preventing jailbreaks, the threat jailbreaking poses continues to grow and evolve and will remain a threat in 2024.

The relationship between risk and popularity

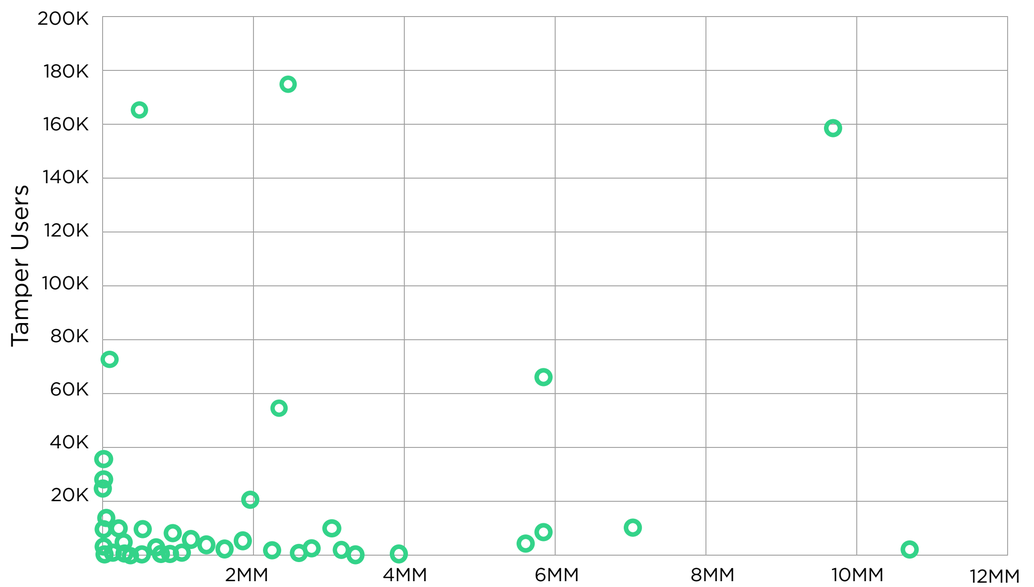
Similarly to the findings of our 2023 study, the 2024 edition found no correlation between the likelihood of being attacked and the app's popularity. The scatterplots below show that many popular apps are attacked less frequently than unpopular apps.

While the lack of correlation between an app's popularity and the likelihood of it being attacked might seem illogical to a casual observer, we know from experience that the reasons and motivations for attacking any particular app are varied. As a result, app makers tend to decide how to protect apps based on the value of the data they protect as opposed to the app's relative popularity.

Popularity vs. attack frequency 2023:



Popularity vs. attack frequency 2024:



Risks across app instances

The preceding sections of this report explored the landscape of application threats from a macro perspective, evaluating the susceptibility of apps as discrete entities operating across various platforms. This approach shows the breadth of vulnerabilities at the enterprise level, highlighting that a significant proportion of apps, counted as unique executables, face the specter of cyber attacks.

However, to grasp the full scope of cybersecurity challenges, it is imperative to delve deeper into the granularity of **app instances**, a singular execution of an application on a customer's device. This provides a more precise lens through which to gauge risk across an entire customer base so that companies can understand the risks to each of their individual customers.

Consider the scenario where two banks, each with 100 customers, have deployed their banking apps across their customer base. At the instance level, if 45 app instances from Bank #1's customers are compromised, alongside five from Bank #2's, we uncover a more detailed threat rate: 25% of app instances have been attacked. This instance-level analysis reveals not just the prevalence of threats across apps but also the likelihood of attacks that individual consumers face. It underscores that while the **proportion** of targeted apps might suggest a certain level of risk, the **instance-level attack rate directly measures the threats that actual users encounter.**

The chart below illustrates the risk of suffering from a certain type of attack, using attack types as defined by **OWASP** (the Open Worldwide Application Security Project, a non-profit online community that produces an array of resources in the fields of IoT, system software, and web app security). Each guard category is part of the **OWASP MASVS** (Mobile Application Security Verification Standard) "Resilience" group, which Digital.ai products protect against and are monitored and reported on in this Threat Report.[7] For readability, the types of attacks (Threat Vectors) are listed across the top of the table. The specific protections that are triggered by those types of attacks are listed in the "Guards" column.

[7] For details visit **OWASP MASVS - OWASP Mobile Application Security**

Risks across app instances *(cont.)*

Attack risk by OWASP MASVS guard category

		Threat vector									
Guard category	Guards	Ip theft	Protocol analysis	Security bypass	Malware	Certificate bypass	Instrumen-tation	OS API spoofing	Data theft	Code injection	Cloning
Unsafe Environment Guards (OWASP MASVS-RESILIENCE-1)	Root Detection				✓	✓	✓	✓			
	Jailbreak Detection				✓	✓	✓	✓			
	Emulator Detection				✓	✓	✓	✓			
	Virtualization Detection				✓	✓	✓	✓			
Application Integrity Guards (OWASP MASVS-RESILIENCE-2)	Checksum			✓						✓	✓
	Resource Verification			✓						✓	✓
	Signature Check			✓						✓	✓
	Code Lifting Detection	✓		✓						✓	✓
	Repair Guard			✓						✓	✓
Obfuscation Guards (OWASP MASVS-RESILIENCE-3)	String Encryption	✓	✓	✓							
	Code Obfuscation	✓	✓	✓							
	Control Flow Obfuscation	✓	✓	✓							
	Resource Encryption	✓	✓	✓							
	Class Encryption	✓	✓	✓							
	Numeric Literal Hiding	✓	✓	✓							
	Renaming	✓	✓	✓							
	Damage Repair	✓	✓	✓							
Instrumentation Detection Guards (OWASP MASVS-RESILIENCE-4)	Debugger Detection		✓			✓	✓		✓		
	Dynamic Instrument		✓			✓	✓		✓		
	Hook Detection		✓			✓	✓		✓		
	Swizzle Detection		✓			✓	✓		✓		

Risks across app instances *(cont.)*

Guard categories[8] and threat assessment

Unsafe environment guards require an application to validate the integrity of the platform, including checking if a device is rooted or jailbroken, if the app is running on an emulator, whether the application is running in a virtualizer, or when the app is checking if any malicious applications are installed on the device.

The odds of an individual instance of an app suffering an attack on its environment, across the apps we protect, were .96%

Application integrity guards require an application to implement anti-tampering mechanisms, which include checking the application package signature, validating the application's DEX and native code integrity, and validating application resource integrity.

The odds of an individual instance of an app suffering an integrity attack were .19%

Obfuscation guards are of paramount importance. While there are nearly limitless ways to obfuscate code and thus frustrate attempts to reverse engineer code, it is not possible to *detect* or *prevent* static code analysis (other than by using Resilience groups 1, 2, and 4).

Instrumentation detection guards require an application to implement anti-dynamic analysis techniques, which include debugging detection, dynamic instrumentation framework detection (such as **Frida**), method hooking, and swizzling detection.

The odds of an individual instance of an app suffering an instrumentation attack were .02%

[8] For detailed information about the Guard Categories visit **https://mas.owasp.org/MASVS/**

Protecting your apps in the wild

Application owners know all too well the pressures of creating more applications faster, and AI is helping global enterprises create more apps faster than ever. However, AI has also helped threat actors create malware more quickly—and attack the growing number of apps in the wild with increasing precision. At the same time, faster development has also led to G2000 enterprises short-shrifting security—either not including it in the DevOps process, seeing it as an impediment, or simply not knowing where to start.

Digital.ai has hundreds of application security customers worldwide who protect over 1 billion instances of applications. Many of those customers contributed anonymized data that led to the findings of this study. If you are an existing Digital.ai Application Security customer and would like to contribute data to future studies, contact us at **https://digital.ai/why-digital-ai/contact/**

For all of our existing and new customers, we offer application security solutions that build in security in multiple ways:

Embedding security into the application development process

- Obfuscate code to prevent reverse-engineering
- Prevent tampering by detecting unsafe environments and code changes
- Configure customized or automated protections on-premises or in the cloud

Providing visibility into at-risk apps

- Produce stand-alone reports or integrate with existing Security Operations Center tools
- Create searchable logs
- See which guards and protections are activated

Automatically responding to threats

- Force step-up authentication
- Alter app features
- Shut down applications that are under attack

Get more information about our Digital.ai Application Security solution and its capabilities by accessing the resource below. Then, contact us to get started on your journey. Once you're underway, please contribute to our next study by giving Digital.ai permission to include your company's aggregated and anonymized data.

Read more about our Application Security solution.

CONTACT US

Appendix: methodology

This study was conducted using anonymized and aggregated data gathered from Digital.ai App Aware customers around the globe. The data in this report was collected over a four week period from February 1 to February 28, 2024.

App Aware is Digital.ai's threat monitoring system. Customers who use App Aware have data on the number and locations of app instances they have in production, as well as information on when and where each of those apps is either modified or placed in an unsafe environment.

About Digital.ai

Digital.ai is an industry-leading technology company dedicated to helping Global 5000 enterprises automate software delivery workflows across complex technology environments. The company's AI-powered DevSecOps platform automates software releases, improves mobile application testing and security, and provides insights across the software lifecycle. Digital.ai empowers large enterprises to embrace AI responsibly, reduce software-related risk, and amplify developer productivity to deliver innovations that drive business outcomes.

Additional information about Digital.ai can be found at **digital.ai/** and on **Twitter**, **LinkedIn**, and **Youtube**.